ESTRATEGIAS INTEGRADAS DE CIBERSEGURIDAD PARA EL FORTALECIMIENTO DE LA SEGURIDAD NACIONAL

TESIS PARA OPTAR AL GRADO ACADÉMICO DE:
DOCTOR EN DESARROLLO Y SEGURIDAD ESTRATÉGICA

AUTOR:

Mg. Juan Fernando Ormachea Montes

ASESOR:

Doctor Israel Barrutia Barreto

LÍNEA DE INVESTIGACIÓN

Seguridad

LIMA-PERÚ
2019

Jurado evaluador

Los abajo firmantes miembros del jurado evaluador de la sustanciación de la tesis titulada **Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional** dan conformidad de la aprobación de la defensa de la tesis a cargo del Maestro Juan Fernando Ormachea Montes, identificado con documento Nacional de Identidad N° 43337342, sugiriendo continúe con el procedimiento para optar el grado académico de **Doctor en Desarrollo y Seguridad Estratégica.**

_____

Presidente (a)

_____

Secretario (a)

_____

Vocal (a)

Agradecimiento

Me gustaría expresar mi más profundo agradecimiento a las autoridades, catedráticos, asesores temáticos y metodológicos de mi casa de estudios “Centro de Altos Estudios Nacionales, CAEN”; también me gustaría extender mi más profunda gratitud a mi asesor personal, y a todas las personas que contribuyeron en la experiencia para el desarrollo del presente trabajo de investigación y en forma especial a los miembros de mi familia, quienes son y serán siempre el impulso para crecer y ser una mejor persona cada día.

Dedicatoria

A mis queridos padres, por sus ejemplares vidas, sus esfuerzos, sus enseñanzas, sus voluntades, motivación y afecto. Por sostener siempre una visión para que sus hijos seamos profesionales íntegros, con ideal permanente de valores y altos principios, y con compromiso para contribuir a la construcción de una sociedad más libre, justa y digna.

Declaración Jurada de autoría

Mediante el presente documento, Yo, JUAN FERNANDO ORMACHEA MONTES, identificado con Documento Nacional de Identidad N° 43337342, con domicilio real en calle García y García 911 – Residencial La Ensenada de Surco, Edificio 6 A, Dpto. 302, en el distrito de Santiago de Surco, provincia de Lima, departamento de Lima, egresado del ***IV Doctorado en Desarrollo y Seguridad Estratégica*** del Centro de Altos Estudios Nacionales-Escuela de Posgrado (CAEN-EPG), declaro bajo juramento que:

Soy el autor de la investigación titulada ***Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional*** que presento a los 15 días de diciembre del 2019, ante esta Institución con fines de optar al grado académico de ***Doctor en Desarrollo y Seguridad Estratégica***.

Dicha investigación no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por el suscrito, para optar otro grado académico ni título profesional alguno. Declaro que se ha citado debidamente toda idea, texto, figura, fórmulas, tablas u otros que corresponden al suscrito o a otro en respeto irrestricto a los derechos de autor. Declaro conocer y me someto al marco legal y normativo vigente relacionado a dicha responsabilidad.

Declaro bajo juramento que los datos e información presentada pertenecen a la realidad estudiada, que no han sido falseados, adulterados, duplicados ni copiados. Que no he cometido fraude científico, plagio o vicios de autoría; en caso contrario, eximo de toda responsabilidad a la Escuela de Posgrado del Centro de Altos Estudios Nacionales y me declaro como el único responsable.

_ _

JUAN FERNANDO ORMACHEA MONTES

DNI N° 43337342

Autorización de publicación

A través del presente documento autorizo al Centro de Altos Estudios Nacionales-Escuela de Posgrado (CAEN-EPG) la publicación del texto completo o parcial de la tesis de grado titulada **Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional,** presentada para optar al grado de Doctor en Desarrollo y Seguridad Estratégica, en el Repositorio Institucional y en el Repositorio Nacional de Tesis (RENATI) de la SUNEDU, de conformidad al marco legal y normativo vigente. La tesis se mantendrá permanente e indefinidamente en el Repositorio para beneficio de la comunidad académica y de la sociedad. En tal sentido, autorizo gratuitamente y en régimen de no exclusividad los derechos estrictamente necesarios para hacer efectiva la publicación, de tal forma que el acceso a la misma sea libre y gratuito, permitiendo su consulta e impresión, pero no su modificación. La tesis puede ser distribuida, copiada y exhibida con fines académicos siempre que se indique la autoría y no se podrán realizar obras derivadas de la misma.

Fecha, 16 de Julio de 2020

_ _

JUAN FERNANDO ORMACHEA MONTES

DNI N° 43337342

Índice

CAPÍTULO IV

Metodología de la investigación

CAPÍTULO V

Análisis y síntesis

CAPÍTULO VI

Diálogo teórico-empírico

Índice de figuras

Resumen

En las últimas décadas, las nuevas tecnologías, los servicios electrónicos y redes de comunicación se han visto cada vez más integrados en nuestra vida diaria. Las empresas, la sociedad, el gobierno y la defensa nacional dependen del funcionamiento de las tecnologías de la información y comunicación (TIC) y de la operación de las Infraestructuras Criticas de Información (ICI). La multiplicidad de potenciales atacantes incrementa los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por las administraciones públicas, las infraestructuras críticas o las actividades de las empresas y ciudadanos. Además, existen evidencias de que determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la seguridad nacional. En ese orden de ideas, el objetivo de esta investigación es proponer estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad nacional del Perú, 2019. La metodología de investigación fue de diseño no experimental, tipo descriptivo, analítico y propositivo. Concluye que en los indicadores referidos a cooperación regional, bilateral y multilateral, el Perú ha manifestado comportamientos disímiles. El Estado y la sociedad peruana aún transitan por los enfoques de la concientización y del desarrollo de las capacidades cibernéticas militares como indicadores prevalentes en el diseño de las políticas nacionales de ciberseguridad. Aun cuando el liderazgo descanse, en principio, en el Estado, la ciberseguridad constituye un compromiso social que demanda de articulación entre el sector público y el sector privado, lo que en el Perú aún no se concreta. En consecuencia, el diseño de la Estrategia Nacional de Ciberseguridad del Perú constituye una necesidad que demanda ser satisfecha.

Abstract

In recent decades, new technologies, electronic services, and communication networks have become increasingly integrated into our daily lives. Companies, society, government and national defense depend on the operation of information and communication technologies (ICT) and the operation of Critical Information Infrastructure (ICI). The multiplicity of potential attackers increases the risks and threats that can seriously endanger the services provided by public administrations, critical infrastructures or the activities of companies and citizens. Furthermore, there is evidence that certain countries have military and intelligence capabilities to carry out cyber attacks that put national security at risk. In this order of ideas, the objective of this research is to propose integrated cybersecurity strategies necessary to strengthen Peru's national security, 2019. The research methodology was non-experimental, descriptive, analytical and purposeful in design. It concludes that in the indicators referring to regional, bilateral and multilateral cooperation, Peru has shown dissimilar behaviors. The Peruvian state and society still go through approaches to raising awareness and developing military cyber capabilities as prevailing indicators in the design of national cybersecurity policies. Even though the leadership rests, in principle, in the State, cybersecurity constitutes a social commitment that demands articulation between the public and private sectors, which in Peru has not yet materialized. Consequently, the design of the National Cybersecurity Strategy of Peru constitutes a necessity that demands to be satisfied.

Resumo (Português)

Nas últimas décadas, novas tecnologias, serviços eletrônicos e redes de comunicação tornaram-se cada vez mais integrados em nossas vidas diárias. Empresas, sociedade, governo e defesa nacional dependem da operação das tecnologias da informação e comunicação (TIC) e da operação da Infraestrutura Crítica de Informação (ICI). A multiplicidade de atacantes em potencial aumenta os riscos e ameaças que podem comprometer seriamente os serviços prestados pelas administrações públicas, infraestruturas críticas ou as atividades de empresas e cidadãos. Além disso, há evidências de que certos países têm capacidade militar e de inteligência para realizar ataques cibernéticos que colocam em risco a segurança nacional. Nesta ordem de idéias, o objetivo desta pesquisa é propor estratégias integradas de segurança cibernética necessárias para fortalecer a segurança nacional do Peru, 2019. A metodologia da pesquisa foi de caráter não experimental, descritivo, analítico e de propósito. Conclui que, nos indicadores referentes à cooperação regional, bilateral e multilateral, o Peru demonstrou comportamentos diferentes. O estado e a sociedade peruanos ainda passam por abordagens para aumentar a conscientização e desenvolver as capacidades cibernéticas militares como indicadores predominantes no desenho das políticas nacionais de cibersegurança. Embora a liderança esteja, em princípio, no Estado, a cibersegurança constitui um compromisso social que exige articulação entre os setores público e privado, que no Peru ainda não se materializou. Consequentemente, o desenho da Estratégia Nacional de Cibersegurança do Peru constitui uma necessidade que exige ser satisfeita.

Introducción

El exponencial crecimiento de los desarrollos tecnológicos comunicacionales representa un reto para la seguridad y defensa de los Estados. Así como se han desarrollado grandes avances, también se confrontan enormes desafíos, donde los actores políticos en todos los niveles deben asumir la responsabilidad de la seguridad y defensa de los Estados y sus naciones.

Uno de los grandes retos se expresa en la contención de las amenazas que emanan del ciberespacio. La novedosa plataforma donde la vida de las naciones transcurre más allá del plano físico, pero que se ha demostrado capaz de alterar la realidad en dicho plano. Los ciberataques son una realidad que potencialmente puede destruir en cuestión de horas la economía, las instituciones y las estructuras de los Estados vulnerables. De la interconexión global emergen riesgos que se constituyen en peligros inminentes de ser ejecutados por ciberterroristas o incluso por *hackers*, quienes solo experimentan con nuevas herramientas de software sin medir la destrucción que pueden causar.

En ese orden, es indispensable que los Estados asuman la responsabilidad de contener las amenazas potenciales y reales, lo que ha derivado que organismos como la Organización de las Naciones Unidas, la Organización Internacional del Comercio e incluso la Agencia Internacional para la Energía Atómica, adelanten conferencias y convenciones sobre seguridad informática. Constituye un reto de todos y que compete a todos.

En el caso del Perú, la reciente promulgación de la Ley 30999 o Ley de Ciberdefensa constituye un avance en ese sentido, no obstante, es indispensable establecer un diagnóstico eficiente en materia de las Estrategias Nacionales de Ciberseguridad, que posibiliten replicar experiencias internacionales que coadyuven a proteger al Estado peruano y a sus ciudadanos de las crecientes amenazas latentes en el ciberespacio.

Es por ello que este estudio tiene el objetivo de proponer estrategias integradas de ciberseguridad, necesarias para fortalecer la seguridad nacional del Perú, 2019, a partir de experiencias internacionales exitosas.

CAPÍTULO I

Planteamiento del problema

1.1 Descripción de la realidad problemática

En las últimas décadas, las nuevas tecnologías, los servicios electrónicos y redes de comunicación se han visto cada vez más integrados en nuestra vida diaria. Las empresas, la sociedad, el gobierno y la defensa nacional dependen del funcionamiento de las tecnologías de la información y comunicación (TIC) y de la operación de las Infraestructuras Críticas de Información (ICI). El transporte, las comunicaciones, el comercio electrónico, los servicios financieros, los servicios de emergencia y servicios públicos se sustentan en la disponibilidad, integridad y confidencialidad de la información que fluye a través de estas infraestructuras (Pastor, 2009).

Estas nuevas tecnologías de la información y la comunicación dieron origen al ciberespacio (Internet). Este constituye el quinto dominio de interacción humana, y cada día se hace más extenso albergando más información y brindando más y más servicios. Como resultado, este nuevo espacio ha dado lugar a la aparición de nuevas amenazas creadas por individuos, organizaciones o estados que buscan aprovecharse de esta nueva forma virtual de interactuar. Las actividades ilícitas en este medio pueden causar efectos muy importantes a la víctima y reportar sustanciales beneficios al perpetrador, quien además muchas veces no puede ser identificado. Los Estados, como garantes de la seguridad y tranquilidad de sus habitantes, han tenido que adaptar sus estructuras y marcos normativos para prevenir y enfrentar este nuevo escenario donde las fronteras no son claras, y los actores pueden no identificarse claramente (Nagurney y Shukla, 2017).

La multiplicidad de potenciales atacantes incrementa los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por las administraciones públicas, las infraestructuras críticas o las actividades de las empresas y ciudadanos. Además, existen evidencias de que determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la seguridad nacional (Foro Económico Mundial, 2014).

Varios son los factores que contribuyen a la proliferación de acciones delictivas en el ciberespacio, la rentabilidad que ofrece su explotación en términos económicos, políticos o de otro tipo, la facilidad y el bajo costo de las herramientas utilizadas para la consecución de ataques y la facilidad de ocultación del atacante, hacen posible que estas actividades se lleven a cabo de forma anónima, desde cualquier lugar del mundo y con impunidad (Nagurney y Shukla, 2017). Los distintos perfiles de atacantes explotan las vulnerabilidades tecnológicas con el objeto de recabar información de valor para cometer ilícitos, así como también para amenazar los servicios básicos que pueden afectar al normal funcionamiento de un país.

Este nuevo escenario donde se evidencia la dependencia global de los sistemas de información, constituye la gran fortaleza de los mismos, como también su gran debilidad. A pesar de los riesgos que conlleva una sociedad cada vez más interconectada, esta tendencia es imparable, lo que significa que hay que afrontar el futuro y gestionar los riesgos que arribarán (Parada, Florez y Gomes, 2018). El contexto es variado, se puede observar una mayor y más compleja actividad criminal desarrollada por grupos organizados y por delincuentes individuales, una mayor y más compleja actividad de espionaje, ya sea industrial, militar o política, una mayor variedad y cantidad de ataques a las infraestructuras críticas de las naciones, a las libertades públicas y a todo tipo de servicios en los que se basa el funcionamiento de las sociedades. Del mismo modo, se puede apreciar un mayor índice de ataques enmascarados, dirigidos por Estados y encubiertos bajo la apariencia de ataques de bandas criminales, activistas políticos, hackers y otro tipo de atacantes (Amandeep, 2018). Como dato no menor se puede observar una mayor participación de individuos en acciones maliciosas, ya sea por ignorancia, por curiosidad, por diversión, por reto o por lucro. Cabe destacar que la gran cantidad de riesgos surgen a causa de la atracción que el ciberespacio produce, al ofrecer una mayor rentabilidad, facilidad e impunidad para todo tipo de estas actividades.

Como reacción a esta avalancha de amenazas, que en definitiva se consideran amenazas al bienestar y al sistema democrático de los países, surge la necesidad de disponer de herramientas en defensa de sus legítimos intereses, lo

que comprende el desarrollo de capacidades y habilidades en la prevención, defensa, detección, análisis, investigación, recuperación y respuesta a las amenazas, así como también la gestión de los riesgos asociados.

Tradicionalmente, las situaciones de conflicto entre actores políticos nacionales e internacionales disponen de fronteras y límites, que fueron desdibujados en el ciberespacio. Los ataques se reconfiguraron deslocalizando la amenaza y dando paso a la ubicuidad inherente al ciberespacio (Rubio, 2017).

Las infracciones de datos, los ciberataques y las violaciones de privacidad se han convertido en algo común hoy en día. Sin embargo, a pesar de la cantidad de literatura académica e historias de medios sobre estos eventos, no existe una investigación rigurosa que examine una gran muestra de incidentes para evaluar adecuadamente el riesgo y las tendencias de estos eventos (Navarrete, 2014). En cuanto a los delitos cibernéticos que atentan contra la ciberseguridad, se distinguen cuatro tipos de eventos:

- Infracciones de datos (divulgación no autorizada de información personal),
- Incidentes de seguridad (ataques maliciosos dirigidos a una empresa),
- Violaciones de privacidad (supuesta violación de la privacidad del consumidor) e
- Incidentes de phishing/skimming (delitos financieros individuales) (Amandeep, et al., 2018).

De todos los incidentes cibernéticos, las infracciones de datos son de lejos las más comunes. Más allá del nombre y la dirección, los números de tarjetas de crédito y la información médica eran las piezas de información más comúnmente comprometidas. Y los incidentes causados por acciones maliciosas (a diferencia de las actividades accidentales o no intencionales) se han mantenido relativamente constantes en alrededor del 60% de todos los incidentes (Amandeep et al., 2018).

Para comprender mejor los riesgos por industria, existen varias medidas potencialmente relevantes, cada una de las cuales proporciona una visión útil, pero singularmente incompleta. Por ejemplo, si se analiza las siguientes medidas para los incidentes en nuestra base de datos: número total de incidentes, tasa de

incidentes, tasa de litigio, costo total y costo por evento. Mientras que la industria financiera y de seguros sufre la mayor cantidad de eventos cibernéticos, el gobierno y las agencias sufren la mayor tasa de incidentes. Además, las empresas mineras, de petróleo y de gas sufren la mayor tasa de litigios, mientras que las empresas de gestión sufren el mayor costo por evento. En general, cuando se analiza juntas cada una de las medidas, las industrias minoristas, de información, de fabricación y de finanzas y seguros representan el mayor riesgo, mientras que, contrariamente a la creencia común, los servicios de atención médica y educación presentan algunos de los riesgos más bajos.

De tal modo que mientras se estimaban los costos promedio de los eventos cibernéticos en aproximadamente US$ 3.86 millones anuales, el costo típico de una violación de datos es de menos de US$ 200,000 mucho más bajo que los millones de dólares citados a menudo en las encuestas (Carrillo, 2018). Además, se detectó que los incidentes cibernéticos les cuestan a las empresas solo un 0.4% de sus ingresos anuales, mucho más bajo que la contracción minorista (1.3%), fraude en línea (0.9%) y tasas generales de corrupción, errores financieros y fraude de facturación (5%) (Carrillo, 2018).

En el ámbito de la seguridad y defensa, los ataques bélicos normalmente se clasifican en los que se ejecutan en aire, mar y tierra, limitados al territorio físico, pero se excluye los ataques en el terreno cibernético. En la actualidad, los países atacan a otros para obtener beneficios diversos o solo para que el país objetivo se pueda paralizar u obtener información privilegiada de él. El caso emblemático del año 2010 lo protagonizó un “gusano" ─ahora conocido como Stuxnet─, que tomó el control de 1000 máquinas que participaban en la producción de materiales nucleares en Irán y les dio instrucciones de autodestruirse (Marks, 2010).

Fue la primera vez que un ataque cibernético logró dañar la infraestructura del "mundo real". Durante el análisis del gusano, los investigadores descubrieron que el código altamente avanzado del Stuxnet había sido diseñado con objetivos bélicos. El gusano fue creado en laboratorio por Estados Unidos e Israel para sabotear el programa nuclear de Irán, pero las autoridades no han confirmado esa afirmación (Socarrás y Santana, 2019).

El Estado peruano, inscrito dentro de la modernización tecnológica del país, ha implementado TIC para la prestación de servicios. Los servicios básicos esenciales, como el agua y electricidad cuentan cada uno con software especiales para la gestión y el monitoreo. Si estos programas son vulnerados por un malware o un virus informático, afectaría seriamente el funcionamiento y en consecuencia el servicio sería inadecuado, o en el peor de los casos dejarían de funcionar y no existiría la distribución de la energía. Estas empresas estratégicas no cuentan con procedimientos que coordinen con otros subsistemas ni cuentan con el equipamiento para la protección de estos softwares, y esta es una situación común en los profesionales de tecnología de información (TI) por trabajar aisladamente sin una normatividad ni control.

Si en la actualidad los sistemas informáticos de entidades públicas son vulnerados por hackers es porque los estándares de calidad recomendados por la Oficina Nacional de Gobierno Electrónico e Informática no han sido implementados con las normas ISO 17799 y 2700, costando $17,20 millones al año al Estado peruano (Gestión, 2018).

El Perú es uno de los países con escasa conciencia en términos de la protección y riesgos en materia de seguridad informática, además, es uno de los países que poco ha legislado en temas de seguridad de la información y seguridad informática y, sobre todo, en planeamiento de ciberdefensa y ciberseguridad. Cuando se menciona esto no solamente se refiere a proteger una página web, sino contar con estrategias de seguridad nacional.

Conociendo y entendiendo que la ciberseguridad es parte de la seguridad nacional, y por tanto, demanda la toma de medidas de protección contra los ataques cibernéticos en coordinación con los sectores público y privado, las cuales deben ser compatibles con los derechos y libertades individuales consagrados en la Constitución Política del Perú, se propuso el abordaje de la temática desde una perspectiva geoestratégica.

1.2 Preguntas de investigación

1.2.1 Pregunta general

¿Cuáles son las estrategias de ciberseguridad necesarias para fortalecer la seguridad nacional en el Perú, 2019?

1.2.2 Preguntas específicas

- ¿Cuáles son las estrategias integradas de ciberseguridad más eficientes implantadas en tres países seleccionados al 2019?
- ¿Cuál es el marco normativo legal respecto a la ciberseguridad en el Perú, 2019?
- ¿Cuáles son los límites referentes al desarrollo de la ciberseguridad en el Perú, 2019?
- ¿Cuáles son las brechas en materia de desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú, 2019?
- ¿Cómo se pueden abordar las brechas para optimizar el desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú, 2019?

1.3 Objetivos de investigación

1.3.1 Objetivo general

Proponer estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad nacional del Perú, 2019.

1.3.2 Objetivos específicos

- Analizar las estrategias integradas de ciberseguridad más eficientes implantadas en tres países seleccionados al 2019.
- Evaluar el marco normativo legal respecto a la ciberseguridad en el Perú, 2019.
- Identificar las limitaciones referentes al desarrollo de la ciberseguridad en el Perú, 2019.

- Establecer las brechas en materia de desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú, 2019
- Abordar las brechas para optimizar el desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú.

1.4 Justificación y viabilidad

El presente estudio de investigación se justifica porque existe la necesidad e importancia de proteger el valor de la información estratégica y crítica del Estado, y el de las que son publicadas por los peruanos en la red. Aun con el extenso potencial que brinda internet, también conlleva riesgos potenciales, como consecuencia de la permeabilidad de los datos críticos, privados y confidenciales.

Es imperativo que cada sector del Estado sea responsable del uso que hace de la red. Sobre todo de la importancia de evitar los delitos cibernéticos y las posibles amenazas que pueden ser desde las que afectan a la seguridad nacional y a sus industrias, hasta el ciberacoso. En el Perú, el acceso de los adolescentes a las TIC está asociada al nivel educativo del jefe del hogar, así, los porcentajes se distribuyen como sigue: 99,7% donde el jefe del hogar es profesional universitario, 99,2% donde el jefe del hogar posee educación superior no universitaria, 96,6% donde el jefe del hogar posee educación secundaria, y 83,5% en los hogares con educación primaria o inferior (INEI, 2018). La seguridad de este sector vulnerable y de la población en general está asociado a la existencia de una entidad u organización responsable de la normatividad y del planeamiento de estas acciones de manera integral y multisectorial.

Hasta el 2019, cada sector del gobierno normaba a través de directivas y de manera restringida y sectorizada las actividades orientadas a la protección de las redes y la información almacenada en sus *data centers*. La promulgación de la Ley 30999 del 26 de agosto de 2019 reestructura el panorama en materia de Estrategias Integradas de Ciberseguridad, no obstante, los elementos culturales y la aplicabilidad de la norma constituyen retos que demandan atención.

La investigación fue enfocada hacia el estudio de las estrategias integradas de ciberseguridad en el Perú, cuya utilidad tiene la finalidad de analizar los diferentes factores que inhiben el goce del uso de la tecnología con la protección plena de los derechos de privacidad de la información, contribuyendo tanto a identificar los elementos que permiten la afectación de la seguridad en la red como generar estrategias necesarias para fortalecer al Estado en su seguridad y soberanía nacional, así como a los ciudadanos del Perú, 2019.

La viabilidad de la investigación se demostró al disponer de la información suficiente referida a los tres casos internacionales referenciados y de la información nacional del Perú, lo que posibilitó el desarrollo de este estudio.

1.5 Delimitación de la investigación

1.5.1 Espacial: República del Perú.

1.5.2 Temporal: 2019

1.6 Limitaciones de la investigación

Limitado acceso a los expertos internacionales en la materia: la disponibilidad de información pública en materia de ciberseguridad continúa estando limitada por cuanto los Estados mantienen estrictas políticas de confidencialidad en materia de ejecución y de acciones preventivas. En consecuencia, este estudio abordó los elementos normativos, doctrinarios y de enfoque, lo que posibilita subsanar la ausencia de información directa de los expertos en seguridad y defensa internacional.

Las brechas existentes entre las estrategias integradas de ciberseguridad limitan el establecimiento de referenciales provenientes de los países desarrollados que sean aplicables a los países subdesarrollados. En ese orden, el estudio establece dimensiones e indicadores que posibilitan la identificación de categorías estratégicas cuya viabilidad sea demostrable.

CAPÍTULO II

Marco filosófico

El presente estudio se inscribe dentro del paradigma cualitativo-interpretativo, también denominado hermenéutico, de la investigación. Este paradigma se caracteriza por abordar la realidad en la búsqueda de la esencia que explica los procesos desdibujando las apariencias de las formas, para alcanzar los atributos que hacen que esa realidad se exprese como es y no de otra manera (Coello, Blanco y Reyes, 2012).

El paradigma hermenéutico aborda la realidad confrontando las preconcepciones del investigador, retándolo a seguir el método hermenéutico como camino para confrontar los riesgos de la parcialidad en una suerte de roca que rompe el espejo donde el investigador puede encontrar lo que desea encontrar y no la expresión de la realidad tal como es (Ruedas, Ríos y Nieves, 2009).

La hermenéutica como método ha evolucionado desde los escritos platónicos hasta las contribuciones de Dilthey (1949), quien atribuyó a la hermenéutica la facultad de romper con las arbitrariedades interpretativas de los investigadores paracientíficos. Las contribuciones de Hussler (Lambert, 2006), Heidegger (1926) y Gadamer (1993) redimensionaron la visión clásica de la hermenéutica situándola más allá de la interpretación desde el sentido del lector, hacia la interpretación del signo como concepto que expresa univocidad, de lo que es una cosa y la distingue de otra.

En el ámbito de las ciencias sociales, y específicamente desde la perspectiva sociológica, Max Weber (2010) realizó aportes importantes en tanto estableció la necesidad de distinguir los sentidos objetivos y subjetivos del observador, quien al distinguirlos puede interpretar la realidad. La sociología comprensiva de Weber allanó el camino hacia la identificación de categorías y los indicadores que demuestran la presencia de estas dentro del contexto social que se observa.

Dado que la filosofía consiste en la forma cómo se concibe lo que nos rodea, la cual se tornará conforme a la persona u observador que lo estudie, por lo tanto, desde la concepción empírica del investigador el ciberespacio es una realidad, puede que al ser virtual sea intangible para algunos, sin embargo, otros lo

conciben desde una perspectiva malintencionada como una vía para causar daño, lo que puede comprender las ciberamenazas que potencialmente podrían poner en peligro tanto a ciudadanos civiles como al medioambiente e incluso detener la economía de un país y sus actividades gubernamentales, estas situaciones son las que evocan la necesidad de adaptarse a la evolución de las nuevas ciencias tecnológicas y evolucionar paralelamente con el ciberespacio, lo que involucra el crecimiento y creación constante de estrategias de ciberseguridad.

La informática y la cibernética son técnicas que se desplazan en el mismo riel pero que se desarrollan independientemente una de la otra, por lo que la cibernética es plasmada como una disciplina con un método interdisciplinario de interacción con la sociología, la psicología, la economía, la medicina, la biología, la matemática, entre otras, donde inclusive incumbe a la estrategia militar para proveer seguridad nacional a los Estados (Robinet, 2011).

Desde ese enfoque y siendo las categorías o unidades observables en el presente estudio, “las estrategias integradas sobre ciberseguridad desde el ámbito internacional (1ra categoría) y desde el ámbito de la seguridad nacional (2da categoría)”, es posible identificar a la ciberseguridad como una disciplina multidisciplinaria derivada de la cibernética enfocada específicamente en la protección y resguardo de la información de todos los usuarios alrededor del mundo, incluyendo los países y sus gobiernos, o como según estima Leiva (2015); “El conjunto de órganos, organismos y procedimientos que permitan la dirección, control y gestión de la seguridad en el ciberespacio”, que para los efectos de este estudio comprende las dimensiones de protección, enfoque, sector público, sector privado y cooperación, tanto nacional como internacional, según la categoría correspondiente.

Esta protección y resguardo de la información son de vital importancia toda vez que el ser humano amerita transitar en un campo de confiabilidad no solo en las áreas físicas donde nos desenvolvemos, esto y quizás con mayor atención es en el campo informático o digital, esa tranquilidad o confiabilidad involucra otros aspectos como son la integridad y la autenticación, aun cuando el campo en el cual se desenvuelven es virtual, la primera está sustentada en la garantía de una

conducta ética que conlleva intrínsecamente a la segunda (autenticidad); este factor es de amplio espectro ya que abarca tanto la identificación de una persona como los diferentes mecanismos informativos de seguridad (contraseñas) y económicos que el usuario amerita mantener seguros.

En este mundo cibernético que está en constante cambio este estudio aborda la investigación del fenómeno social de la ciberseguridad desde la perspectiva epistemológica del paradigma interpretativo hermenéutico, procurando fomentar el abordaje de la ciberseguridad en forma constante, para disminuir las brechas en materia de seguridad que prevengan desde cualquier parte del mundo el robo de cualquier tipo de datos, indiferentemente de los motivos e intenciones, detrás de esos ataques de espionaje, poder contar con una plataforma confiable y optimizar el desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú.

CAPÍTULO III

Estado del conocimiento

3.1 Antecedentes de la investigación

El tema de establecer estrategias nacionales (integradas) de ciberseguridad en un país necesariamente está relacionado a entender que existen amenazas en el ciberespacio y que el Estado a través de sus políticas públicas y el establecimiento de estrategias debe de evitarlas o enfrentarlas según sea el caso.

Existen trabajos de investigación y estudios, tanto nacionales como internacionales, que tratan de estos temas y que sirven como base y referencia para la ejecución del presente trabajo de investigación después de su estudio y análisis respectivo, a continuación, se describen algunos de ellos que se toman como antecedentes:

3.1.1 Investigaciones internacionales

A nivel internacional existen trabajos de investigación relacionados a la ciberseguridad y las políticas y estrategias que las rigen, particularmente en los países que están avanzados en estos temas, como el caso de España en Europa, Estados Unidos en América del Norte, además de Brasil y Uruguay en América del Sur.

Marcos (2018), en su tesis titulada: “Ciberseguridad aplicada a la e-democracia: análisis criptográfico y desarrollo de una metodología práctica de evaluación para sistemas de voto electrónico remoto y su aplicación a las soluciones más relevantes”, para optar al grado de Doctor en Ingeniería de Producción y Computación, cursado en la Escuela de Ingeniería Industrial, Informática y Aeroespacial de la Universidad de León, España, mediante el desarrollo de una metodología de análisis y la clasificación de sistemas, con el objeto de verificar la existencia de un sistema de tecnología de voto electrónico remoto lista para ser implantada en procesos electorales. Y en caso positivo determinar las condiciones y hasta qué punto en términos de nivel de uso, tecnología y tipología de elecciones sería suficientemente segura su introducción. Para ello, pretende contribuir a la materia desarrollando una metodología práctica de evaluación de sistemas de voto electrónico remoto transversal, para después

aplicarla a los esquemas más relevantes hasta la fecha. Obteniendo, entre otras, como conclusiones que no existe ningún sistema que desde la presente tesis se juzgue como suficientemente seguro para ser utilizado como sustituto del voto tradicional en unas elecciones legislativas de carácter nacional, por lo que en cuanto a las condiciones de seguridad señala que el ataque en el cual se realizara la modificación de los resultados es tan importante que es potencialmente beneficioso para quien maliciosamente pretenda modificarlo encontrando varias debilidades en el sistema VER, por lo que esta es la menos recomendable para esta tipología de comicios.

Machin y Gazapo (2017) desarrollaron un artículo denominado "La ciberseguridad como factor crítico en la seguridad de la Unión Europea". Publicado por la Unidad de Investigación sobre Seguridad y Cooperación Internacional (UNISCI) N° 42, con el objeto de presentar estrategias de ciberseguridad que sean realmente capaces de integrar a las diferentes estrategias nacionales para Europa. Abordan el tema desde la perspectiva de la traslación del conflicto a la plataforma virtual, donde los elementos del ciberespacio (hardware, software, protocolos de red, etc.) y la naturaleza de las interacciones humanas en el ciberespacio cada vez son más dinámicas y complejas, lo que a su vez conlleva a tratar de delimitar los riesgos y amenazas que constituyen un ataque cibernético, en el cual los infractores utilizan las brechas de seguridad presentes en las tecnologías de información para pasar a copiar, borrar o reescribir la información de la víctima. Concluye indicando que el escenario de conflicto (ciberespacio) está en constante evolución, lo que lo hace altamente complejo y que al combinarlo con ciberataques y ataques físicos a estructuras de un país comprueba lo dañinos que son, tal y como se ha demostrado en los enfrentamientos entre Rusia y Estonia por la involucración de los virus Stuxnet, el virus Flame o los ciber. Que ningún país de la Unión Europea está plenamente a salvo de un ciberataque. Solicitan se hagan realidad las propuestas planteadas en los documentos oficiales de la Unión Europea para construir mecanismos de rendición de cuentas que realmente permitan el uso protegido de internet. Desarrollar mejores recursos de carácter digital con colaboración de las empresas públicas y privadas para proteger las infraestructuras críticas. Proteger el

ciberespacio sin que se afecte o dañen los derechos y libertades de los particulares (usuarios) potenciando la colaboración e intercambio de información entre los actores internacionales. La exigencia de diseñar mecanismos de alerta temprana de vulnerabilidad para advertir en el futuro los posibles ciberataques.

Camps (2016) presentó un estudio denominado "Ciberdefensa y ciberseguridad: Nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito", donde señala que la ejecución de actividades que afecten la seguridad de los diferentes países por parte de otras naciones, organizaciones o individuos es posible, y puede causar efectos devastadores. Por esto, los Estados deben adaptar su legislación y crear nuevas estructuras para combatir las nuevas amenazas que surgen del ciberespacio. Uruguay, al igual que los restantes países del orbe, ha modernizado su marco legal y ha incluido a las amenazas provenientes del ciberespacio entre las que pueden afectar el bienestar de su población, pasando estas a ser objeto de la defensa nacional. A pesar de que Uruguay carece de una estrategia de ciberseguridad, ha sido evaluado positivamente en un reciente informe conjunto del Banco Interamericano de Desarrollo y la Organización de Estados Americanos.

Villalba (2015) desarrolló una investigación titulada "La ciberseguridad en España, 2011-2015. Una propuesta de modelo de organización". El objetivo de este estudio fue proponer un modelo de gobernanza en el ámbito de la ciberseguridad en España. El diseño de investigación fue no experimental, de enfoque cualitativo, analítico y propositivo. Tomando en consideración que la ciberseguridad corresponde a un conjunto superior de la seguridad, asociada a los desarrollos comunicacionales. En el campo de la ciencia política, esta investigación, por su carácter prescriptivo, propone soluciones a problemas complejos de organización de modelos de seguridad en el ámbito de la utilización del ciberespacio. Estas propuestas se han incluido en el modelo de gobernanza nacional de la seguridad, estimándose que son factibles y que, de ser implementadas, aumentarían los índices de protección de la sociedad en el ámbito de la ciberseguridad. La investigación propone políticas estructuradas en materia de ciberseguridad y recomienda crear al más alto nivel organizaciones para

enfrentar las nuevas amenazas. En este documento se ha identificado como primordial fomentar el gobierno electrónico y a la vez estructurar a nivel nacional redes que permitan brindar seguridad cibernética y garantizar el libre uso de los recursos reales y virtuales. Estas redes tienen como base la concientización de la población en lo referente a seguridad de la información y su capacitación para utilizar de la mejor forma los servicios.

3.1.2 Investigaciones nacionales

Taipe (2018) desarrolló una investigación titulada "La auditoría de seguridad informática y su relación en la ciberseguridad de la Fuerza Aérea del Perú, año 2017". El objetivo de la investigación fue proponer soluciones en materia de ciberseguridad para el Perú. El diseño de investigación fue no experimental, correlacional y descriptiva. La técnica de recolección de datos fue la encuesta. Los entrevistados expresaron que la Auditoría de Seguridad Informática no tiene repercusiones trascendentes sobre la ciberseguridad de la Fuerza Aérea del Perú, año 2017. En consecuencia, el autor concluye sobre el nivel de conocimiento del personal de las áreas de computación, informática y diseño de políticas de seguridad que posee bajos niveles de conocimiento en materia de ciberseguridad.

Rodríguez (2017) desarrolló una investigación denominada *"*Los mecanismos sociales de la innovación en la era de la información y su relación con los fines y medios en China contemporánea (1978-2017*)*". El objetivo de esta investigación fue establecer los mecanismos implementados por los países para el logro de una serie de objetivos establecidos por una doctrina política (fines). Para lo cual tomó como país de estudio a China, que es el país más activo en los temas de ciberataques que son contrarrestados con eficientes normas y estrategias de ciberseguridad. El autor concluye que la innovación consiste en la relación temporalmente determinada que existe entre medios y fines, ya que los fines de una doctrina política dan lugar a la consecución de medios adecuados para lograr los primeros. La tesis argumenta que un país como China ha venido desarrollando desde 1978 un Sistema Nacional de Innovación (SNI) conformado a su vez por otros subsistemas económicos y de producción tecnológicos, entre otros, con el

propósito de procesar, comprender y recibir información de una red global de información que ha surgido a finales de los años sesenta. Este mismo SNI le permite comprender las nuevas tecnologías, procesarlas y producir nuevos medios de diversa índole, así como asimilar y entender las tecnologías que otros países con su respectivo SNI crean. Existe, por tanto, una relación interdependiente en la creación de conocimiento que implica la obtención de conocimientos y tecnologías de otros países. Por ende, a medida que China ha ido conformando y modernizando su SNI su comportamiento en la región del Mar del Sur de China, zona importante para Beijing en términos políticos, económicos y estratégicos, se ha vuelto más asertivo.

Seclén (2016) desarrolló un estudio denominado "Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001". El objetivo de la investigación fue identificar las causas que restringen la implementación del sistema gestión de seguridad de la información SGSI en las entidades públicas. El diseño de investigación fue no experimental, de enfoque cualitativo, aplicada, transeccional, documental y analítica. El autor realiza siete entrevistas a oficiales de seguridad de la información, encargados de la implementación del SGSI en sus respectivas instituciones públicas, de acuerdo a la NTP-ISO/IEC 27001. Concluye que es necesario encontrar un punto de equilibrio entre el alineamiento del sistema con la estrategia de negocio de la organización y el control de riesgos de seguridad de la información, que faciliten la evaluación del nivel de complejidad de los factores que no permiten el desarrollo de la implementación total de la NTP-ISO/IEC 27001 y cómo estos terminan afectando a la gestión de los procesos de negocio de las organizaciones.

Villanueva (2015) desarrolló una investigación denominada "La incursión digital y la política pública: nuevos actores a partir del conflicto del derecho de autor en el campo digital". El objetivo de la investigación fue caracterizar el conflicto generado por la internet durante los procesos de intercambio de bienes culturales y el derecho de autor. La metodología de investigación fue no experimental, de enfoque cualitativo, documental y analítico. El autor concluye que no existe una articulación efectiva entre las acciones en el campo digital y los

sistemas políticos y que los ciudadanos estamos expuestos a incursiones digitales que permiten que los ciudadanos eludan el control estatal, a pesar de la presión constante sobre países como el Perú por aumentar dicho control. El efecto sobre las políticas públicas es que las deja huérfanas de apoyo orgánico, fomentando la copia sin creatividad, el llamado ventrílocuismo institucional. A partir de la caracterización del derecho de autor como problema político, se establece la manera cómo la internet, un sistema sociotécnico basado en telecomunicaciones y servicios de comunicación de contenidos de interés diverso y alcance global, altera la relación entre los consumidores, los productores y el Estado. Esta alteración va a contrapelo de la realidad de creciente armonización legislativa y, sobre todo de normas, que ha establecido la necesidad de cesión de derechos nacionales en favor de la preeminencia de los derechos de los creadores intelectuales, obligando a los Estados a hacer cumplir leyes de acuerdo con un sistema global latente. Mientras tanto, los consumidores se entregan al consumo irregular pero sin desarrollar una dimensión ciudadana por la falta de articulación efectiva entre las acciones en el campo digital y los sistemas políticos. La Internet aparece entonces a partir de la experiencia del caso del derecho de autor, como una tecnología que crea posibilidades de comunicación para una serie de actores que desarrollan en ella sus propias habilidades e intereses. A partir de Bourdieu, la Internet es vista como un campo digital, con el habitus hacker, es decir, aquel que proviene del grupo humano así denominado, como el factor preponderante en la transmisión de prácticas de uso que refuerzan la autonomía de los individuos; al mismo tiempo que el Estado se debilita por la imposibilidad de solucionar demandas contradictorias de los productores y los consumidores.

3.2 Teorías

3.2.1 Geopolítica

Desde los primeros pasos de la geografía política de Ratzel, contenidos en *Las leyes del crecimiento espacial de los Estados* de 1896 y la obra inmediatamente posterior *Geografía política de 1897*, los elementos geográficos inherentes a la política se posicionaron como herramientas que configurarían la subdisciplina que hoy se denomina Geopolítica (Ferro y Castaño, 2017). La definición inicial de

Ratzel propone: “La geografía política es el estudio del Estado y su dimensión territorial, es decir, para esta disciplina el Estado es una porción de la superficie terrestre donde tienen lugar diferentes actividades humanas de carácter vital, las cuales guardan una relación simbiótica con el suelo (espacio vital) y sus condiciones geográficas (Ratzel, 1987, en Ferro y Castaño, 2017). A finales del siglo XX otros autores realizaron aportes importantes donde las variables poder y conflicto son consideradas como intervinientes en la caracterización de la geopolítica, por cuanto introducen redefinición del concepto de territorio reconociendo la dinámica de estos a consecuencia de la dinámica política y los efectos de los conflictos (Sanguin, 1981; Claval, 2002; Raffestin, 2011). En la actualidad, la geopolítica hace énfasis en el tema del poder y sus implicancias en la relación entre actores, quienes pueden impulsar cambios como consecuencia de las rivalidades por la detentación y ejercicio del poder (Lacoste, 2008).

Ferro y Castaño (2017) definen la geopolítica como la disciplina que estudia todo lo relacionado a las relaciones de poder entre actores de todo tipo, quienes desarrollan acciones orientadas a ejercer el dominio sobre territorios y poblaciones (117). La geopolítica triangula la toma de decisiones, el territorio y el espacio, donde las decisiones políticas son inherentes a actores estatales y no estatales. Lacoste (2008) estableció tres escalas de la geopolítica:

- **Escala global:** La extensión más amplia donde confluyen intereses de diversos actores multinacionales**.**
- **Escala estatal o nacional:** Los actores comprometidos en el ejercicio de acciones y toma de decisiones políticas se circunscriben a las fronteras nacionales de un estado.
- **Escala local/regional:** Corresponde a ámbitos locales donde la interacción entre actores es localizada, pero se distingue de lo nacional por las singularidades que potencialmente pueden inducir cambios en las estructuras nacionales.

Paul Claval (1999) introdujo variables novedosas dentro de la concepción geopolítica, considerando las relaciones sociales y la interacción entre individuos quienes establecen redes físicas y virtuales donde se ejercen actividades que

transversalizan las decisiones políticas, modificándolas y/o generando nuevas. Ballesteros (2015) estableció las aplicaciones de la geopolítica para los Estados, en tanto como disciplina contribuye a la toma de decisiones de los actores que llevan la carga de las mismas. El ámbito de la geopolítica es tan amplio que demanda del concurso de disciplinas conexas que alimentan los análisis referidos a las relaciones entre actores y las rivalidades de poder, fundamentalmente en el establecimiento de distinciones entre actores en base al desarrollo de fuerzas productivas, tipo de régimen y posición dentro del hegemón (Hobsbawm, 1997). La geopolítica ha experimentado cambios en tanto su objeto de estudio se transforma en una dinámica constante (Tabla 1).

Tabla 1
Vinculaciones entre los enfoques clásicos y contemporáneos de la geopolítica y la seguridad

Categorías	Geopolítica clásica	Seguridad clásica	Geopolíticas críticas	Nuevos enfoques de seguridad
Niveles de análisis	La estructura	La estructura	El proceso de toma de decisión	La agencia
Base epistémica	Positivista	Positivista	Posmoderna	Reflectivista
Objeto de estudio	Vinculación entre territorio y la política exterior	El Estado y las amenazas convencionales	Las intenciones dadas a través de un discurso	La percepción de inseguridad en la sociedad
Actores	El Estado	El Estado y el sistema internacional	Múltiples	Múltiples
Finalidad	Conocer y prever dinámicas de poder	Prever amenazas y disuadirlas	Desconstruir realidades socialmente aceptadas	Analizar la naturaleza del proceso conflictivo

Fuente: Cabrera (2017).

3.2.2 Geopolítica de las ciberamenazas

En el mundo de las tecnologías de información y comunicación (TIC), el hegemón se expresa en los ámbitos físicos y virtuales, generando esferas de conflictos y amenazas, que fueron identificadas por el Foro Económico Mundial (2015) donde se identificó los diez principales riesgos por su probabilidad:

- Conflictos entre Estados.
- Deficiencias de la gobernanza nacional.
- Colapso o crisis del Estado-nación.
- Desempleo o subempleo.
- Catástrofes naturales.
- Falta de adaptación al cambio climático.
- Crisis del agua.
- Ataques cibernéticos.

Posteriormente el Foro Económico Mundial (2019) reordenó la jerarquía de las amenazas potenciales:

- Confrontación entre potencias por temas económicos.
- Erosión de los acuerdos multilaterales.
- Confrontaciones políticas entre las mayores potencias.
- Ciberataques: En plataformas comerciales y datos.
- Ciberataques: Interrupción de operaciones e infraestructura.
- Pérdida de confianza en la seguridad colectiva.
- Populismo y agendas étnicas
- Noticias falsas

Según el Foro Económico Mundial las ciberamenazas escalaron posiciones en tan solo 4 años, desplazándose desde el 8º lugar hasta las casillas 3 y 4 del ranking de amenazas globales, incluso por sobre las agendas étnicas.

3.2.3 Ciberseguridad

La seguridad cibernética se refiere a los esfuerzos para prevenir el daño causado por interrupciones, fallas o mal uso de las TIC y para reparar el daño si ha ocurrido. (Rollano, 2012)

Tal daño puede consistir en alguno o todos los siguientes: menor confiabilidad de las TIC, disponibilidad limitada y violación de la confidencialidad y/o integridad de la información almacenada en los sistemas de TIC (Amandeep et al., 2018).

Incrementar la resiliencia digital no es solo responsabilidad de un gobierno, ya que la infraestructura de TIC en sí y el conocimiento sobre esta infraestructura está en gran parte en manos privadas, nacionales e internacionales. Por lo tanto, la seguridad cibernética o ciberseguridad es la suma de los esfuerzos conjuntos de los organismos gubernamentales, la comunidad empresarial, las organizaciones y los ciudadanos, tanto a nivel nacional como internacional (Vargas, Recalde y Reyes, 2017). Al igual que en el mundo físico, nunca se puede lograr el 100% de seguridad en el dominio digital.

Las fronteras entre seguridad exterior e interior se difuminan y las comparticiones de competencias en entidades y ministerios concretos ya no representan una respuesta adecuada a los nuevos retos de seguridad del ciberespacio. Sin embargo, la seguridad sigue siendo una de las principales responsabilidades de cualquier Estado, por lo cual hace falta evolucionar hacia nuevos modelos y nuevas reglas (Fundación Telefónica, 2016).

Se define a la ciberseguridad como la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques (Acosta et al., 2009, citado por Leiva, 2015). La forma de defenderse de estos ataques es compleja, dado que influyen diversos factores. Uno de los elementos críticos es que muchos de los objetivos proclives a ser atacados se encuentran en manos de empresas privadas, por lo que su seguridad depende en gran medida de las acciones que tomen estas para proteger sus sistemas. Ello implica asumir costos que en ocasiones no están dispuestos a asumir, generando riesgos significativos. Otro factor importante es la falta de conciencia en seguridad de algunas partes de la sociedad, lo que dificulta tomar medidas eficaces y poder coordinarlas (Leiva, 2015).

La ciberseguridad se considera, por lo tanto, un ámbito de la seguridad nacional en el que los gobiernos deben definir una estrategia, que necesariamente reclama el concurso de los sectores público y privado, ser compatible con los derechos y libertades individuales y ser coordinada con otras acciones para detectar las distintas amenazas, establecer sistemas de respuesta y recuperación ante eventualidades. Además, se debe fomentar la cooperación internacional como

punto clave para lograr tratados internacionales y colaboración, tal como se evidenció tras el brote Petya. El ataque usando ransomware conocido con ese nombre causó estragos mundiales, infectando computadoras y redes en más de 65 países, incluido Estados Unidos. Al brote de Petya siguió, en tan solo unas semanas, el aún más extendido ataque ransomware WannaCry Adove (Křoustek, 2017). Como lo demuestran estos eventos de alto perfil, la protección de datos confidenciales y el aprovechamiento de los sistemas correctos para detectar, prevenir y remediar infracciones de seguridad continúan siendo un desafío para muchas organizaciones.

Álvarez (2018) refiere la necesidad de implementar Estrategias Nacionales de Ciberseguridad (ENC) a nivel mundial. Con ellas se intentará recoger la visión del gobierno de una nación a la hora de enfrentarse al problema de la gestión de la ciberseguridad en el ámbito global. Los objetivos de estas estrategias no se limitan únicamente en garantizar la seguridad de los ciudadanos y de las infraestructuras críticas del país, sino también incluyen instaurar un ecosistema que fomente la cooperación público-privada y la cooperación internacional.

Es por esta razón que la ciberseguridad es una necesidad social y económica. Dada la influencia de los sistemas de información y telecomunicaciones en la economía y en los servicios públicos, la estabilidad y prosperidad del Perú depende en buena medida de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometidas por causas técnicas, fenómenos naturales o agresiones deliberadas.

Entonces, se puede decir que en la medida que la sociedad se vuelve más dependiente de las TIC, la protección y la disponibilidad de estos activos críticos se convierte cada vez más en un tema de interés nacional (Taipe, 2017). Los incidentes que causan la interrupción de las infraestructuras críticas y los servicios de TIC podrían causar importantes impactos negativos en el funcionamiento de la sociedad y la economía. Como tal, el ciberespacio seguro se ha convertido en uno de los retos más importantes del siglo y, por lo tanto, la seguridad informática se considera cada vez más como una cuestión nacional a nivel estratégico que afecta a todos los niveles de la sociedad.

El grado de conocimiento que necesita un atacante para realizar una agresión a los sistemas de información ha decrecido a través del tiempo, debido al aumento de la calidad, cantidad y disponibilidad de herramientas ofensivas. Actualmente, es relativamente fácil encontrar en internet herramientas de *ethical hacking* basadas en el uso de conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas, sin hacer daño (Leiva, 2015). Existen también herramientas de informática forense y de seguridad informática, entre otras, que son utilizadas con mala intención. Todo ello conforma un escenario de nuevos riesgos para el que es necesario que el gobierno peruano desarrolle planes o estrategias, y se contemple la ciberseguridad como un riesgo al que es preciso hacer frente para mejorar la seguridad nacional.

Una estrategia nacional de ciberseguridad se considera fundamental en la seguridad y defensa de una nación, que redunda en la mejora de la resistencia de las infraestructuras y servicios nacionales de información. Una estrategia nacional se establece en los niveles más altos de la toma de decisiones de los Estados, que establece una serie de objetivos nacionales y prioridades que deben alcanzarse en un plazo determinado. Como tal, proporciona un marco estratégico para los esfuerzos de una nación en el plano de la ciberseguridad (Taipe,2017).

La preocupación es especialmente alta para las agencias gubernamentales. Como guardianes de algunos de nuestros datos más sensibles sobre ciudadanos y empleados públicos, son objetivos atractivos para ataques cibernéticos. Las organizaciones gubernamentales se enfrentan a decenas de ataques focalizados y específicos cada año, uno de cada tres resultan en una violación de seguridad exitosa, según una reciente encuesta de Accenture a ejecutivos de seguridad. El informe de Accenture Security (2016) basado en una encuesta de 150 ejecutivos gubernamentales en los Estados Unidos sugiere que la mayoría de las agencias no cuentan con las tecnologías adecuadas. Casi la mitad de los encuestados del gobierno estatal y local dicen que puede llevar meses identificar infracciones sofisticadas. Para la tecnología necesaria para llenar los vacíos, los encuestados enumeraron con mayor frecuencia seguridad de punto final/red (58 por ciento), encriptación (56 por ciento), inteligencia de amenazas (54 por ciento) y análisis de amenazas cibernéticas (51 por ciento).

Los resultados de la encuesta sobre ciberseguridad de EY (2019) recomienda que las organizaciones de servicios públicos deban integrar las defensas cibernéticas profundamente en sus organizaciones mediante el empleo de un enfoque integral de extremo a extremo para la seguridad digital (Figura 1). Como primer paso, las agencias deben realizar una evaluación exhaustiva de sus capacidades de seguridad cibernética, mientras "prueban a presión" sus defensas para determinar si pueden resistir un ataque dirigido. También necesitan identificar y minimizar su exposición a la red y enfocarse en proteger los activos prioritarios.

Figura 1. Ventajas de las organizaciones con políticas de ciberseguridad
Fuente: EY (2019)

Las siguientes áreas de seguridad cibernética deben considerarse prioritarias para la inversión y una mayor atención del liderazgo:

- Gobernanza: enfóquese en la rendición de cuentas para fomentar una cultura basada en la seguridad cibernética, medir e informar el desempeño de esa seguridad, desarrollar incentivos atractivos de ciberseguridad para los empleados y crear una cadena de mando de ciberseguridad clara. Los líderes necesitan redefinir el éxito de la ciberseguridad como algo más que simplemente lograr los objetivos de cumplimiento. Obtener el nivel correcto de visibilidad y autoridad es fundamental para descubrir y responder a las amenazas de manera oportuna.
- Exposición de la agencia: Evalúe los escenarios de incidentes de ciberseguridad para comprender aquellos que podrían afectar materialmente a la organización. Identificar los factores clave, los puntos de decisión y las barreras para el desarrollo de estrategias de remediación y transformación.
- Contexto estratégico de amenazas: impulse a la organización a explorar amenazas específicas de ciberseguridad, incluido un análisis de riesgos geopolíticos, e identifique las actividades y tecnologías relacionadas con la ciberseguridad que las organizaciones similares están llevando a cabo y desplegando. Estos pasos garantizarán que el programa de seguridad de una agencia se alinee con su estrategia general.
- Resistencia cibernética: evalúe la capacidad de la organización de brindar excelencia operativa frente a adversarios cibernéticos disruptivos, y utilice técnicas de "diseño para la resiliencia" para limitar el impacto de un ataque.
- Preparación para la respuesta cibernética: implemente un plan de respuesta robusto, proporcione vías efectivas de escalamiento de incidentes cibernéticos y asegure la participación sólida de los interesados en todas las funciones de la agencia. Ponga a prueba la capacidad de los miembros del equipo para cooperar durante los incidentes de gestión de crisis.
- Eficiencia de la inversión: Desarrollar la experiencia interna para impulsar inversiones inteligentes en ciberseguridad y la asignación más efectiva de fondos y recursos. Compare las inversiones de la organización con los puntos de referencia, los objetivos organizacionales y las tendencias de ciberseguridad. La administración de activos puede ser difícil para las

organizaciones gubernamentales, pero este es un componente crítico de cualquier campaña de seguridad.

Las agencias gubernamentales deberían enfocarse en la ciberseguridad con una mentalidad organizacional, una capaz de proyectar el desarrollo de estrategias de contención y disuasión de los ciberataques.

3.2.4 Marco normativo legal

En el Perú:

Ley de Protección de Datos Personales Nº 29733: Tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2, numeral 6 de la Constitución Política del Perú́, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

Ley de Delitos Informáticos Nº 30096: Tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información y la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. Cubre de cierta forma el vacío normativo que existía sobre algunos de los ataques más comunes: la vulneración de sistemas informáticos, entre otros. Esta norma luego fue perfeccionada en el 2014.

Ley 30999 o Ley de Ciberdefensa: Que establece la normativa en el ámbito de la protección de los sistemas cibernéticos del Estado peruano. Comprende la regulación de las operaciones militares adelantadas por las dependencias adscritas al Ministerio de Defensa. Define la ciberdefensa como una capacidad militar de contención y respuesta frente a amenazas en el ciberespacio, delegando en las Fuerzas Armadas las tareas de ejecución de la ciberdefensa. Fue promulgada el 9 de agosto de 2019.

En el contexto mundial:

EE.UU.:

Orden ejecutiva 13800: "Fortalecimiento de la Ciberseguridad de Redes Federales e Infraestructura Crítica", en mayo de 2017. La orden abordó las

amenazas actuales a la ciberseguridad nacional, desde el uso de TI obsoleta hasta la falta de adaptación, sistemas operativos actualizados regularmente. La orden ejecutiva exigió que los jefes de los departamentos y agencias ejecutivas realicen auditorías de gestión de riesgos, y entreguen un informe exhaustivo al Departamento de Seguridad Nacional y al Departamento de Comercio en un plazo de 90 días. El informe, titulado "Informe al presidente sobre la mejora de la resiliencia de Internet y el ecosistema de comunicaciones contra las redes robot y otras amenazas automatizadas y distribuidas", clasifica seis oportunidades principales y amenazas:

- Los ataques automatizados y distribuidos son un problema global.
- Existen herramientas efectivas, pero no son ampliamente utilizadas.
- Los productos deben estar seguros durante todas las etapas del ciclo de vida.
- Se necesita educación y conciencia.
- Los incentivos de mercado están desalineados.
- Este es un desafío para todo el ecosistema.

Detalla cinco objetivos complementarios diseñados para mejorar la resiliencia del ecosistema de Internet y comunicaciones:

- Identificar un camino claro hacia un mercado de tecnología adaptable, sostenible y seguro.
- Promover la innovación en la infraestructura para la adaptación dinámica a las amenazas en evolución.
- Promover la innovación en el entorno de las redes para prevenir, detectar y mitigar los deficientes procedimientos y riesgos.
- Construir coaliciones entre las comunidades de seguridad, infraestructura y tecnología operativa a nivel nacional y en todo el mundo.
- Aumentar la conciencia y la educación en todo el ecosistema.

Europa:

Reglamento General de Protección de Datos (GDPR) de la Unión (2018). Pero, aunque la norma fue aprobada para proteger a los ciudadanos europeos de las violaciones de datos, las fronteras difusas de Internet significan que la GDPR afectará a organizaciones de todo el mundo. En resumen, el GDPR establece

reglas de protección de datos para cualquier empresa que recopile datos de un ciudadano de la UE, ya sea que esa empresa tenga su sede en la Unión Europea o no. Esto significa que si una organización en el extranjero recolecta datos incluso de un individuo de la UE, debe cumplir con las regulaciones del GDPR o enfrentar sanciones.

El GDPR cubre una amplia gama de regulaciones, especialmente sobre recolección de datos y transparencia. Cualquier empresa que recopile datos de ciudadanos de la UE necesitará un consentimiento explícito e informado, lo que significa que los términos y condiciones serán más claros y se les pedirá a los usuarios que marquen más casillas para que los sitios web puedan acceder a sus datos. Los consumidores también tendrán derecho a revocar ese consentimiento, así como solicitar a las empresas que les proporcionen una copia de los datos que hayan recopilado. Además, el GDPR establece reglas sobre cómo las compañías pueden compartir los datos que han recopilado, una regla que probablemente complacerá a los consumidores inquietos después del escándalo de Facebook y Cambridge Analytica.

El GDPR también tiene impacto en los informes de incumplimiento. Cuando se infringen los datos, el GDPR les da a las empresas solo 72 horas para notificar a las autoridades y exige que las organizaciones notifiquen a los consumidores sobre las violaciones de datos de alto riesgo "sin demora indebida". Esto significa que empresas como Uber, que esperaron más de un año para notificar a los consumidores una mayor violación de datos, ya no será capaz de mantener los piratas informáticos en secreto.

La estricta regulación exige que las empresas que no cumplan con el GDPR puedan ser penalizadas hasta con € 20 millones o 4% de los ingresos globales anuales, lo que sea mayor. Con penalizaciones altísimas y alcance global, el GDPR está preparado para dar forma al futuro de la ciberdefensa y la legislación en todo el mundo.

América Latina:

Los países latinoamericanos siguen el modelo europeo de tener regímenes de protección de datos integrales, basados en principios y reglas aplicables a todos los datos personales y algunas reglas especiales para tipos específicos de datos,

tienden a estar por debajo de los estándares europeos y de los Estados Unidos. La razón principal de esta deficiencia es que la mayoría de las leyes de protección de datos se diseñaron siguiendo las normas establecidas por la Directiva Europea de Protección de Datos de 1995, que no estaba diseñada para abordar estos problemas relativamente nuevos.

- Brasil: No cuenta con una ley integral de protección de datos que brinde alguna certeza sobre las medidas necesarias que los que manejan datos deben adoptar para proteger los datos personales, y cuáles son sus responsabilidades de comunicación para la notificación de incidentes de seguridad.
- Argentina y Chile tienen leyes obsoletas, abordando la seguridad de los datos solo de manera genérica y sin normas específicas que prescriban la notificación de incidentes de seguridad. Sin embargo, estos países están en proceso de actualizar sus marcos legislativos para abordar estos problemas.
- Colombia, México, Perú y Uruguay cuentan con normativas, pero en algunos casos la única notificación requerida es para los usuarios y no para la autoridad, creando brechas de información que afectan la recolección de información con respecto a la seguridad de incidentes que son cruciales para fines de ciberseguridad.
- Chile, Colombia y Paraguay publicaron estrategias nacionales de ciberseguridad como una herramienta efectiva para resaltar la relación entre la protección de datos y la ciberseguridad.

3.2.5 Estudio de casos

Correspondiente a las estrategias de ciberseguridad hasta el año 2017:

Países Bajos

El dominio digital ha sido parte de la sociedad holandesa por más de dos décadas. Durante este período, la tecnología de la información y la comunicación ha demostrado ser un factor importante en el crecimiento de la productividad y el poder innovador. Los Países Bajos son el líder europeo en la respuesta a las tendencias tecnológicas y el uso eficaz de las herramientas y habilidades TIC.

Los Países Bajos disponen del mercado de Internet más competitivo del mundo y tiene uno de los mayores números de usuarios de Internet. Salvaguardar la seguridad y libertad digital y mantener un dominio digital abierto e innovador son condiciones previas para el funcionamiento adecuado de la sociedad. Por lo tanto, Holanda emitió la primera Estrategia Nacional de Seguridad Cibernética (NCSS1) en 2011. El objetivo del NCSS1 era realizar un dominio digital seguro, confiable y resistente a través de un enfoque de seguridad cibernética integral basado en asociaciones público-privadas, así como aprovechar las oportunidades subsiguientes para la sociedad.

Los desarrollos en el dominio digital, tanto nacional como internacional, se llevan a cabo a un ritmo rápido. En los últimos años, el impacto potencial y real de las amenazas a la seguridad cibernética se ha vuelto más claro debido a una serie de incidentes muy publicitados. Estas amenazas no solo pueden alterar la infraestructura digital, sino también pueden comprometer la integridad, disponibilidad y confidencialidad de la información que documentamos, analizamos e intercambiamos en el dominio digital.

Para continuar respondiendo a estas amenazas, los Países Bajos planean fortalecer aún más y ampliar sus alianzas con los sectores público y privado, tanto nacionales como internacionales. Esto involucra no considerar la seguridad cibernética como un elemento aislado, sino más bien en correlación con los derechos humanos, la libertad de internet, la privacidad, los beneficios socioeconómicos y la innovación.

La Estrategia Nacional de Seguridad Cibernética 2 (NCSS2) explica esta visión más amplia del gobierno sobre la ciberseguridad y las responsabilidades de los estados y los pasos concretos. Alrededor de 130 partes, incluidas las públicas y privadas, instituciones de conocimiento y organizaciones sociales, participaron en la elaboración de esta nueva estrategia de ciberseguridad. Además, se realizaron amplias consultas con la comunidad más amplia de TIC. A petición del gobierno, la Junta de Seguridad Cibernética, que consta de representantes de partes públicas y privadas, así como del mundo académico, dio recomendaciones sobre el curso de la nueva estrategia.

Los Países Bajos disponen de una infraestructura digital sólida y muchos pioneros de Internet e innovadores emprendedores de TIC holandeses se encuentran activos en todo el mundo. Además, los Países Bajos tienen un talento probado en la creación de coaliciones: no solo dentro de sus fronteras, sino también en el área de paz y seguridad internacional. Juntos tienen la capacidad de crear un dominio digital seguro, gratuito y rentable. Para ello es necesario que todos asuman la responsabilidad de su propia capacidad de recuperación digital y de la resistencia digital de la sociedad. El gobierno toma la delantera con esta nueva estrategia y publica informes anuales sobre el progreso realizado.

La nueva estrategia estipulada en el NCSS2 sigue las ideas y recomendaciones que surgen de los siguientes documentos estratégicos de política:

- La Estrategia de Seguridad Nacional (Estrategia NV) tiene como objetivo prevenir el compromiso de intereses nacionales vitales que pueden conducir a la desorganización social. Tanto en 2010 (ciberconflicto) como en 2012 (ciberespionaje), se incluyeron escenarios de ciberseguridad en la Estrategia NV.

- La Estrategia de Seguridad Internacional está dirigida a las acciones tomadas por los Países Bajos en el exterior y en cooperación con otros países para asegurar sus intereses. La seguridad cibernética es un tema importante en esta estrategia, que es mejor actuar en colaboración con los socios europeos e internacionales.

- La *Defense Cyber Strategy* está dirigida al papel de las fuerzas armadas holandesas en el dominio digital. Un elemento importante en esta estrategia es que reconoce que los actores militares y civiles, públicos y privados, nacionales e internacionales, se han vuelto más entrelazados.

- En su agenda digital, el gobierno holandés se centra en que las TIC puedan contribuir al crecimiento económico del país. En dicha agenda, el gobierno formula sus ambiciones de utilizar las TIC para promover el crecimiento y la prosperidad, incluidas las condiciones previas necesarias, para tener una infraestructura abierta, confiable y rápida y para tener suficientes conocimientos de TIC y hacer un uso suficiente de dicha experiencia.

- La estrategia de concientización sobre seguridad de la información contenida en la Carta de Visión sobre el Gobierno Digital 2012-2013 para administradores y gerentes gubernamentales. Con el equipo de trabajo sobre gestión, seguridad de la información y servicios, el gobierno persigue una política de concientización activa para lograr la seguridad de la información del gobierno en el nivel deseado. Esto no es solo una precondición importante para la implementación de los planes estatales sobre el concepto de gobierno digital 2017, pero también en vista de la Agenda de Implementación del Gobierno para los Servicios de Administración Electrónica hasta 2015 (i-NUP), en la cual se realizará una infraestructura básica.

- La carta ePrivacy describe las condiciones previas para una protección de la privacidad de los datos personales, en particular en las relaciones entre los ciudadanos y las empresas.

- La Estrategia de Seguridad Cibernética de la UE (2013) es un paso importante hacia un entorno digital seguro en Europa. El NCSS2 holandés está en línea con los principios fundamentales de esa estrategia de seguridad cibernética, en base a los cuales los Países Bajos están dando nuevos pasos.

- En el otoño de 2013 se presentó a la Cámara de Representantes una visión a mediano plazo del mercado de las telecomunicaciones. El punto de partida de la visión es que dicho mercado no se puede ver como separado de los desarrollos en Internet y que los valores públicos, como la fiabilidad y la apertura, deben ser revisados por el mercado de las telecomunicaciones a la luz del contexto más amplio de la economía de Internet.

Estados Unidos

La actual administración Trump lanzó su Estrategia de Seguridad Nacional. Esta pieza contiene un elemento básico del documento: la ciberseguridad; es un tema candente, pero en comparación con el programa misilístico nuclear de Corea del Norte, las actividades desestabilizadoras de Irán en Oriente Medio, la flexión de China en casi todos los ámbitos del arte de gobernar y el creciente papel de Rusia

como adalid en todo el mundo, el presidente de los EE.UU. se convenció de que el aspecto de la ciberseguridad es esencial y el más importante en estos tiempos.

A la administración se le deben otorgar calificaciones relativamente altas para los componentes de seguridad cibernética del documento, especialmente para reconocer la amplitud de la amenaza y que va a necesitar más que una mesa de ayuda para solucionarla. Es cierto que es una barra bastante baja. Pero los documentos de la estrategia de seguridad nacional no se conocen como documentos donde se produce una gran innovación política. En cambio, lo mejor que está haciendo EE.UU. es articular los amplios contornos de las principales amenazas a la seguridad nacional junto con algunos temas difíciles sobre lo que el gobierno hará para mejorar las cosas. Aquí, la administración no aísla "al cibernético" a los lados; en cambio, al hablar de problemas cibernéticos a través del documento, la administración entiende que el ciberespacio es una parte crítica que prácticamente abarca todos los aspectos de la seguridad nacional.

Comprende un tratamiento más completo de la ciberseguridad como una preocupación central de seguridad nacional que se ha visto en el pasado. Antes, para los demócratas y los republicanos, las prioridades han sido detener el robo de la propiedad intelectual de los EE.UU. Y piratear las empresas de EE.UU. y proteger las redes federales y la infraestructura crítica. ¿Cómo? Conceptos como la "disuasión" a menudo ─tal vez con demasiada frecuencia─ se toman prestados de la Guerra Fría y se insertan en este dominio más complejo. Y está el amor histórico con el intercambio de información. Si bien esta estrategia de seguridad nacional enfatiza objetivos similares, va más allá y dedica poco espacio a la disuasión y al intercambio de información.

No es sorprendente que el documento sea duro para China. De hecho, la administración llama a China por una "guerra económica con capacidad cibernética". El lenguaje es más enérgico que en las pasadas estrategias nacionales de seguridad, pero el tema de golpear a los chinos por el robo de la propiedad intelectual crítica de los EE.UU. no es nuevo.

Más, sorprendentemente, también es difícil para Rusia. La estrategia de seguridad nacional etiqueta las acciones de Rusia en el ciberespacio como

"desestabilizadoras" y afirma que Rusia "utiliza las operaciones de información como parte de sus ciberespacios ofensivos para influir en la opinión pública en todo el mundo".

La mayor decepción, si bien predecible, es que el documento no prioriza las protecciones de las elecciones en los EE.UU. contra las amenazas cibernéticas. Para ser justos, reconoce que los adversarios están atacando las instituciones estadounidenses y que ser parte de una nación resistente "incluye la capacidad de resistir y recuperarse rápidamente (…) de amenazas a (...) al sistema democrático". Y afirma que "actores como Rusia utilizan herramientas de información en un intento de socavar la legitimidad de las democracias". Pero el documento no llega a articular los problemas de ciberseguridad en torno a las elecciones de 2016 y cómo asegurarse de que esos eventos no se repitan. De hecho, el consejero de Seguridad Interior de la Casa Blanca, Tom Bossert, fue muy directo en su afirmación de que Corea del Norte fue el autor del ataque WannaCry en mayo pasado.

La Estrategia de Seguridad Nacional de 2017 de EE.UU. se basa en cuatro pilares. Estos son:

- "Proteger al pueblo estadounidense, la patria y el estilo de vida estadounidense"
- "Promover la prosperidad americana"
- "Preserva la paz a través de la fuerza"
- "Avance de la influencia estadounidense"

La seguridad cibernética se destaca en los tres primeros.

Estados Unidos, China y Rusia son los pioneros en el diseño de estrategias y estructuras nacionales de ciberseguridad, en las que se inspiran la mayor parte del resto de las estrategias nacionales de seguridad y sus modelos organizativos. Del mismo modo, están las diversas organizaciones internacionales que poseen un componente de ciberseguridad: Unión Europea, NN.UU., OTAN y OSCE.

En Estados Unidos, Rusia y China se puede destacar que sus estrategias nacionales de seguridad se han convertido en un modelo del que se desprende la planificación de la seguridad nacional; que la integración de los intereses

nacionales es total, destacando la capacidad económica como referente transversal de la seguridad; que se ha establecido un modelo organizativo similar basado en un consejo de seguridad nacional; y que las estrategias nacionales de seguridad se desarrollan mediante estrategias sectoriales, como es el caso de las estrategias nacionales de ciberseguridad.

España

España se encuentra obligada por el corpus normativo de la Unión Europea. Diversos países de la UE comparten con España características comunes en mayor medida que otros de regiones geopolíticas diferentes. Entre los Estados miembros de la Unión Europea se encuentran el Reino Unido, Alemania y Francia, que presentan entornos que podrían inspirar de modo más adecuado la mejora del modelo nacional de ciberseguridad en España.

En el ámbito de la ciberseguridad de la Unión Europea, los países que la integran dan una importancia capital a la ciberseguridad para favorecer el espacio económico y de desarrollo, habiendo desarrollado su propia estrategia de ciberseguridad, que constituye la piedra angular en la que se sustenta la numerosa reglamentación comunitaria.

En la ONU se debe destacar el proceso de alto nivel en materia de ciberseguridad, basado en las recomendaciones de un grupo de expertos, orientadas al marco de la legalidad y seguridad internacional en el ciberespacio. En la OTAN, la ciberdefensa forma parte del Concepto Estratégico de la Alianza desde la Cumbre de Lisboa en 2010 y cuenta con una Política de Ciberdefensa. En el ámbito de la OSCE se ha impulsado un paquete de medidas de confianza en el ámbito de la ciberseguridad.

Perú

En base a la problemática mencionada anteriormente y debido a que el Perú, al igual que la mayoría de países de Sudamérica, no tiene desarrolladas sus estrategias de ciberseguridad, el presente trabajo tiene como objetivo principal proponer un estudio comparativo de las estrategias nacionales de ciberseguridad de algunas naciones seleccionadas, basado en el análisis de ventajas y desventajas,

recomendaciones y mejores prácticas sobre cómo desarrollar, implementar y mantener una estrategia de ciberseguridad.

Las amenazas cibernéticas y la necesidad de que el Estado peruano cuente con un sistema de reacción inmediata ante un ciberataque inminente hacen necesaria la implementación de una estrategia que vincule a todos los sistemas y redes y que además se cuente con un Equipo Preparado en Emergencias Informáticas (CERT).

Las amenazas cibernéticas nos muestran la importancia estratégica de disponer de un ciberespacio seguro, y conlleva a la creación de un sistema de ciberseguridad nacional basado en una estrategia nacional de ciberseguridad (ENCS), es decir, un conjunto de órganos, organismos y procedimientos que permitan al Estado peruano la dirección, control y gestión de la seguridad en el ciberespacio.

Al respecto, el Decreto Supremo N° 012-2017-DE, en su apartado 4.2.12, señala lo relacionado con las políticas de seguridad y defensa nacional, donde consideran que las tecnologías de la información están cada vez más incorporadas a estructuras físicas, lo que le da un carácter de crítica vulnerabilidad que incrementa el peligro del daño e interrupción de su funcionamiento. Ello afectaría tanto la economía del país como la cotidianidad de los ciudadanos, riesgo este que lo convierte en tema de seguridad nacional. Sin embargo, persisten las debilidades pese a la actividad realizada por la Secretaría de Gobierno Digital y el Sistema de Coordinación de Emergencias Teleinformáticas de la Presidencia del Consejo de Ministros. La falta de aceptación de la debilidad y el amplio nivel de vulnerabilidad aunado tanto a la dificultad de proteger el ciberespacio y los aislados esfuerzos por protegerlo terminan por debilitar la estructura de la defensa, de la cual se pueden servir actores malintencionados desde cualquier parte del mundo, ameritando la creación de un ente rector dotado de tecnologías de alto nivel.

Resalta el grave peligro de gobernabilidad que existe en el Perú, debido a que se considera como el quinto país con una alta tasa de infección de malware o software malicioso dirigido a vulnerar sistemas de las instituciones públicas donde

reposa gran cantidad de información reservada. Otra cifra alarmante es el índice de 0.32 sobre un máximo de 1, obtenido en el sistema Índice Global de Ciberseguridad, que mide el nivel de compromiso de los Estados en relación con la ciberseguridad, escala esta que colocó al Perú por sobre Paraguay, Bolivia y Venezuela.

En consideración de que el desarrollo nacional es una prioridad y cónsono con el desarrollo económico y social del país, con la participación efectiva de las Fuerzas Armadas para proteger y promover el impulso a la consecución de los intereses nacionales, se propone la creación de un denominado Sistema Nacional de Ciberseguridad, que involucre al sector público y privado fomentando la formación de especialistas para la defensa del ciberespacio. Con ello se estima el fortalecimiento de las misiones constitucionales de las Fuerzas Armadas y la Policía Nacional con la finalidad de garantizar la paz internacional y el orden interno; gracias a la especialización de sus capacidades militares/policiales y sus recursos humanos e integración de sistemas relacionados con la seguridad.

Todo esto resalta la necesidad de una ENCS, se puede observar que como el Perú existen naciones que no poseen una estrategia de ciberseguridad y otras que están en el proceso de su elaboración. Advirtiendo la importancia de la situación, este trabajo tiene el propósito de realizar un estudio comparativo de algunas estrategias nacionales de ciberseguridad seleccionadas y además brindar una visión general de la situación actual del Perú. Internacionalmente, la ciberseguridad forma parte de las agendas de las organizaciones (ya sean públicas o privadas) al máximo nivel; sin embargo, en el Perú no existe un organismo que cuente con una composición adecuada y misión de planeamiento político estratégico, y que cuente además con una capacidad ejecutiva para realizar el seguimiento de la implementación del Plan Nacional de Ciberseguridad y de sus planes derivados.

Tampoco existe una organización de nivel operacional de carácter nacional que pueda continuar el proceso de planeamiento a ese nivel de modo integral, así como realizar la implementación de estos planes y su control en los organismos subordinados, que cumpla funciones de coordinación nacional en el ámbito de la

prevención y respuesta a ciberataques, para los tres niveles de las administraciones públicas y para empresas de carácter estratégico, y que se constituya además en centro de referencia para el sector privado.

3.3 Marco conceptual

Ciber: Prefijo que alude la internet y se aplica a las diversas aplicaciones: cibernauta, ciberestudio, ciberespacio, etc. (Piedra, 2011).

Ciberdefensa: Aplicación de medidas de protección efectivas para obtener un nivel apropiado de seguridad cibernética con el fin de garantizar el funcionamiento y las funcionalidades del sistema informático. Esto se logra mediante la aplicación de medidas de protección adecuadas para reducir el riesgo de seguridad a un nivel aceptable. Las principales funciones de la ciberdefensa consisten en proteger, detectar, responder y recuperarse (Vargas, Recalde y Reyes, 2017).

Ciberdefensa activa: Medida proactiva para detectar u obtener información de una intrusión cibernética, ataque cibernético o una operación cibernética inminente, o para determinar el origen de una operación que implica el lanzamiento de una operación preventiva, o un contraataque cibernético contra la fuente (Camps, 2016).

Ciberataque: Intrusión por medio de una red de computadoras con fines delictivos. El atacante busca acceder sin autorización a información, o alterar o impedir el funcionamiento de los servicios (Camps, 2016).

Ciberseguridad: Conjunto de protocolos orientados a resguardar información y procesos que reposan en la red y que pueden ser accesados para su destrucción, robo o fines ilícitos (Camps, 2016).

Botnets: Computadores zombies de uso remoto que intervienen en computadores sin autorización para robar, modificar o dañar información (Pandasecurity, 2019).

Cibernética: Disciplina que atiende los sistemas informáticos computacionales, redes y comunicaciones (Piedra, 2011).

Ciberespacio: Ámbito de las comunicaciones cibernéticas entre equipos de diversos niveles (Piedra, 2011).

Ciberguerra: Refiere la utilización de las plataformas virtuales por algunos actores políticos con el objetivo de adelantar acciones bélicas, ya fuere obstaculizando el flujo de información, derribando los firewalls, causando caos en los servicios o la destrucción de fuerzas productivas (Camps, 2016).

Ciberterrorismo: Acciones adelantadas por actores políticos que atentan contra objetivos específicos y no necesariamente institucionales dentro de las plataformas virtuales (Amandeep, 2018).

Estrategias internacionales sobre ciberseguridad: "Conjunto de órganos, organismos y procedimientos que permitan la dirección, control y gestión de la seguridad en el ciberespacio" (Leiva, 2015).

Malware o badware: Software maliciosos provenientes de la red y que se instalan en los computadores sin autorización del usuario, cuando se realizan descargas de sitios no seguros (Pandasecurity, 2019).

Ransomware: Software maliciosos corridos de manera remota con el objetivo de boicotear el uso del equipo y cobrar por el desbloqueo (Křoustek, 2017).

Spyware: Software espías que sustraen información de los computadores de manera remota o vigilan el uso del mismo (Pandasecurity, 2017).

Backdoor o puerta trasera (o en inglés backdoor): Código de hackeo que elude el software de seguridad y permite el espionaje y/o las descargas no autorizadas de información (Pandasecurity, 2019).

Bot: Programa informático que emula el comportamiento humano (Amandeep, 2018).

Capcha: Programa de verificación de usuario que posibilita distinguir entre robots y humanos, mediante preguntas aleatorias asociadas a la identificación de imágenes (Pandasecurity, 2019).

Cookies: Software que almacena información de uso reiterado por el usuario y anclada a la triangulación computador-navegador-usuario, las cookies potencialmente son riesgosas, por cuanto son de fácil filtración y despliegan información privada a quien acceda al equipo del usuario regular (Amaro, y Rodríguez, 2017).

Cortafuegos: Hardware o software de un sistema diseñado como protector de la información obstaculizando los accesos no autorizados (Pandasecurity, 2019).

Cracker: Pirata informático (del inglés crack, romper), se utiliza para referirse a las personas que rompen algún sistema de seguridad. Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío (Pandasecurity, 2019).

DDoS: Corresponde al Distributed Denegation of Service, bloquea el uso del servicio por el usuario legítimo, consume el ancho de banda y satura los puertos seriales (Pandasecurity, 2019).

Daemon: Se denomina demonio a los malware que se ejecutan en segundo plano, con la singularidad que se reinicia reiteradamente aun cuando el proceso sea interrumpido (Pandasecurity, 2019).

Flame: Es un software espía altamente sofisticado con capacidad de sustracción de información, grabación de audio y bloqueo (Pandasecurity, 2019).

Hacker: Persona responsable de entradas remotas no autorizadas por medio de redes de comunicación como Internet. También incluye a aquellos que depuran y arreglan errores en los sistemas (Pandasecurity, 2019).

Gusano o worms: Corresponde a modalidades de malware con capacidad de autoreplicación que no se adscriben a los archivos, se difunden sin la intervención humana y se propagan remitiendo información de forma continua (Pandasecurity, 2019).

Keyloggers: Modalidad de daemon que replica la actividad del teclado y la difunde a través de la red, es usada frecuentemente para el robo de contraseñas (Pandasecurity, 2019).

Koobface: Gusano diseñado para afectar a los usuarios de redes sociales Facebook, MySpace, Twitter, etc. Consiste en la difusión de atractivos mensajes que instan al usuario a abrirlos y redireccionar las búsquedas hacia sitios no seguros (Pandasecurity, 2019).

Pop-ups: Ventanas de despliegue automático asociadas a la difusión de publicidad (Pandasecurity, 2019).

Rootkits: Software ocultos que permiten el acceso a la información que se encuentra en el computador de forma remota. La singularidad del rootkits es que su remoción es casi imposible y generalmente deriva en el formateo del equipo (Pandasecurity, 2019).

Troyano: Es un virus clásico y altamente dañino que posibilita el manejo remoto de información. El troyano se instala al abrir aplicaciones en sitios donde se encuentre el virus (Pandasecurity, 2019).

Spambot/Pambot: Programas diseñados para la difusión de correos electrónicos de manera masiva (Pandasecurity, 2019).

Spoofing: Tácticas de suplantación de identidad mediante software especializados (Pandasecurity, 2019).

Virus: Se propaga una vez que el usuario hace uso de programas o archivos infectados (Pandasecurity, 2019).

Scada: Supervisory Control And Data Acquisition (Supervisión, Control y Adquisición de Datos); interviene sobre procesos industriales copiando procesos e incluso obstaculizando procesos productivos (Pandasecurity, 2019).

Stuxnet: Virus altamente eficiente capaz de replicar, obstaculizar y boicotear procesos industriales. El ataque más famoso fue el lanzado sobre el programa nuclear iraní (Marks, 2010).

CAPÍTULO IV
Metodología de la investigación

4.1 Enfoque de investigación

El enfoque epistemológico, según Hernández, Fernández y Baptista (2018), fue cualitativo, por cuanto comprende prácticas interpretativas que posibilitan visibilizar una realidad para comprenderla y/o incidir en el objetivo.

4.2 Tipo de investigación

La investigación se efectuó con base al diseño no experimental de tipo descriptivo, analítico y propositivo. Este tipo de investigación persigue inquirir sobre la incidencia de una singularidad sobre una población (Hernández, Fernández y Baptista, 2014, 155). La presente investigación se orientó hacia el establecimiento de las estrategias de ciberseguridad necesarias para fortalecer la seguridad nacional en el Perú, 2020.

4.3 Método de investigación

La metodología que se utilizó en el desarrollo del estudio tiene su fundamento en la hermenéutica, por lo que se agotaron las siguientes etapas:

4.3.1 Etapa exploratoria: Fase inicial de la investigación donde se identificaron las Estrategias Nacionales de Ciberseguridad de los Países Bajos, EE.UU., España y Perú.

4.3.2 Etapa descriptiva: Se desarrolló en dos fases o momentos metodológicos: 1. Descripción de la situación actual de los Países Bajos, EE.UU., España y Perú en lo relacionado a las políticas y estrategias de ciberseguridad y 2. Recopilación de las diversas experiencias en el tema de ciberseguridad.

4.3.3 Etapa estructural: Comprendió el estudio, análisis e interpretación del contenido de documentos y fuentes de información, tanto nacionales como internacionales que fueron utilizados en el estudio (Anexo 3).

4.4 Escenario de estudio

El estudio se desarrolló en el Centro de Altos Estudios Nacionales del Perú. Comprende las estrategias integradas de ciberseguridad de los Países Bajos, EE.UU., España y Perú.

4.5 Objeto de estudio

Estrategias integrales de ciberseguridad necesarias para fortalecer la seguridad nacional en el Perú.

4.6 Observables(s) de estudio

Categoría N° 1. Estrategias integradas internacionales sobre ciberseguridad: "Conjunto de órganos, organismos y procedimientos que permitan la dirección, control y gestión de la seguridad en el ciberespacio…, según las dimensiones: Protección, enfoque, sector público, sector privado y cooperación internacional" (Leiva, 2015).

Subcategorías

Organismos y procedimientos de ciberseguridad internacional:

- Protección: Resguardo de infraestructuras críticas, la economía, la seguridad nacional y el bienestar social.
- Enfoque: Concientización, educación y capacidades militares.
- Sector público: Ejercicio de liderazgo y la coordinación.
- Sector privado: Participación en la estrategia.
- Cooperación internacional: Cooperación con otros países (Leiva, 2015).

Categoría N° 2. Estrategias integradas sobre ciberseguridad en el ámbito de seguridad nacional del Perú: "Conjunto de órganos, organismos y procedimientos (nacionales) que permitan la dirección, control y gestión de la seguridad en el ciberespacio…, según las dimensiones: Protección, enfoque, sector público, sector privado y cooperación internacional" (Leiva, 2015).

Subcategorías

Organismos y procedimientos de ciberseguridad nacional:

- Protección: Resguardo de infraestructuras críticas, la economía, la seguridad nacional y el bienestar social.
- Enfoque: Concientización, educación y capacidades militares.
- Sector público: Ejercicio de liderazgo y la coordinación.
- Sector privado: Participación en la estrategia.
- Cooperación internacional: Cooperación con otros países (Leiva, 2015).

4.7 Fuentes de información

- Legislación, doctrina, convenios, estructuras organizativas, informes de gestión
- Constitución Política del Perú (1993).
- Convenio contra la Ciberdelincuencia o Convenio de Budapest. Febrero 2019
- Decreto Supremo N° 050-2018-PCM. Estableció la definición de seguridad digital
- Decreto Supremo N° 012-2017-DE, Políticas de seguridad y defensa nacional
- Decreto Supremo N° 063-2007-PCM, Reglamento de Organización y Funciones de la PCM.
- Decreto Supremo N° 067-2003-PCM, Reglamento de Organización y Funciones de la PCM, en el cual se crea la ONGEI.
- Decreto Supremo N° 066-2003-PCM, mediante el cual se fusiona la Subjefatura de Informática del INEI con la PCM.
- Ley Nº 29733, Ley de Protección de Datos Personales (2011) y sus modificaciones.
- Ley N° 30090, Ley de Delitos Informáticos (2013).
- Ley N° 30999, Ley de Ciberdefensa (2019).
- Libro Blanco de la Defensa Nacional del Perú, Ministerio de Defensa (2005).
- Plan Nacional de Ciberseguridad (2018).

4.8 Técnicas e instrumentos de acopio de información

4.8.1 Técnicas de acopio de información

Ajustado al canon de Hernández Sampieri y otros, 2018, donde enuncia que el observador cualitativo debe insertarse y mantener una actitud activa en las situaciones sociales, por lo que esta observación va más allá de la simple contemplación del fenómeno.

4.8.2 Instrumentos de acopio de información

Ficha de registro: La ficha de registro constituye una herramienta para estructurar la información que posteriormente será analizada. Constituye el respaldo de los descubrimientos realizados por el investigador y posibilita el ejercicio de triangulación teórica, la contrastación categorial y el descubrimiento de brechas que no son evidentes en *prima facie* (Galeano, 2001).

Ficha de análisis: El análisis de contenido comprende un conjunto de técnicas de investigación, destinadas a estudiar los contenidos de las legislaciones, doctrinas, convenios, estructuras organizativas e informes de gestión en materia de ciberseguridad de los Países Bajos, EE.UU., España y Perú (Galeano, 2001).

4.9 Método de análisis de información

4.9.1 Análisis documental: Se aplicaron las técnicas de la hermenéutica:

- Registro documental: Legislaciones, doctrinas, convenios, estructuras organizativas e informes de gestión en materia de ciberseguridad de los Países Bajos, EE.UU., España y Perú.
- Compendiar toda la información de los observables del estudio.
- Clasificar por categorías los documentos.

4.9.2 Elaboración de la descripción protocolar

Comprende el establecimiento de unidades de significado:

- Revisión del contenido.
- Identificación de documentos contentivos de preconcepciones del investigador y/o autores escogidos.

- Verificación de la observación contextualizada del fenómeno.
- Descripción del documento en la sección de observaciones de la ficha de registro (Anexo 2).

4.9.3 Lectura general de los documentos analizados

Comprende el estudio a profundidad de las legislaciones, doctrinas, convenios, estructuras organizativas e informes de gestión en materia de ciberseguridad de los Países Bajos, EE.UU., España y Perú**.**

4.9.4 Delimitación de las unidades de significado en torno a la unidad temática

Siguiendo las subcategorías e indicadores establecidos se procede a categorizar su manifestación específica.

4.9.5 Expresión del tema central en lenguaje científico

Comprende la fase de discusión y contrastación entre las realidades de los países estudiados.

CAPÍTULO V

Análisis y síntesis

Estrategias de ciberseguridad comparadas

EE.UU.

Los principios clave o ejes sobre los que EEUU establece en su Estrategia cibernética nacional son cuatro:

1. **Protección:** tomar medidas específicas para proteger las redes y la información federales, asegurar la infraestructura crítica, combatir la ciberdelincuencia y mejorar los informes de incidentes.
2. **Promoción:** respaldar una economía digital vibrante y resistente, fomentar y protejer el ingenio estadounidense, y desarrollar una fuerza laboral de ciberseguridad superior.
3. **Interrupción:** identificar, contrarrestar, alterar, degradar y disuadir el comportamiento en el ciberespacio que es desestabilizador y contrario a los intereses nacionales. Mejorar la estabilidad cibernética a través de normas de comportamiento estatal responsable, detectar y responsabilizar por comportamiento inaceptable en el ciberespacio y la imposición de costos a los actores cibernéticos maliciosos.
4. **Preservación:** preservar la apertura a largo plazo, la interoperabilidad, la seguridad y la confiabilidad de Internet, al tiempo que se debe respaldar el crecimiento del mercado para infraestructura y tecnologías emergentes y crear capacidad cibernética a nivel internacional.

Para el cumplimiento del primer principio de Protección, se estableció la Estrategia Nacional de Ciberseguridad, la cual se fundamenta en cinco ejes expresados en la figura 2.

Figura 2. ENSC de EE.UU. 2019
Fuente: ENSC EE.UU. (2019)

En materia de ciberseguridad, el Departamento de Defensa de los EE.UU. estructuró cinco ejes articulados que derivan en el diseño de cinco estrategias:

1. Dominio operacional: El ciberespacio funge de dominio operacional del que se sirve el Departamento de Defensa en el desempeño de sus tareas de planificación, adiestramiento y suministro orientado a explotar al máximo las potencialidades de la red. La irrupción de nuevos dominios: cibernético, espacial y espectro electromagnético se sumó a los tradicionales dominios dominantes hasta el siglo XX como fueron el dominio marítimo, aéreo y terrestre. Desde 1990, la denominada *Revolution* in *Military Affairs* RMA, cambió la perspectiva de las instituciones militares, induciendo cambios como consecuencia de la irrupción de las TIC (Brose, 2019). La RMA constituye un sistema estructurado por subsistemas que posibilitan la observación de los objetivos, comunicación entre mandos y la toma de decisiones, instrumentando al usuario con una herramienta que posibilita una perspectiva extendida del campo de batalla, más en el escenario de los conflictos activos en la actualidad (Fig. 3). La disrupción introducida por las TIC comprende el vasto espacio de los territorios y las arenas de la

confrontación militar y, por ende, alcanza ámbitos diversos e interrelacionados: Inteligencia, comunicaciones, mando, armamento y otras áreas que emergen en la dinámica contemporánea.

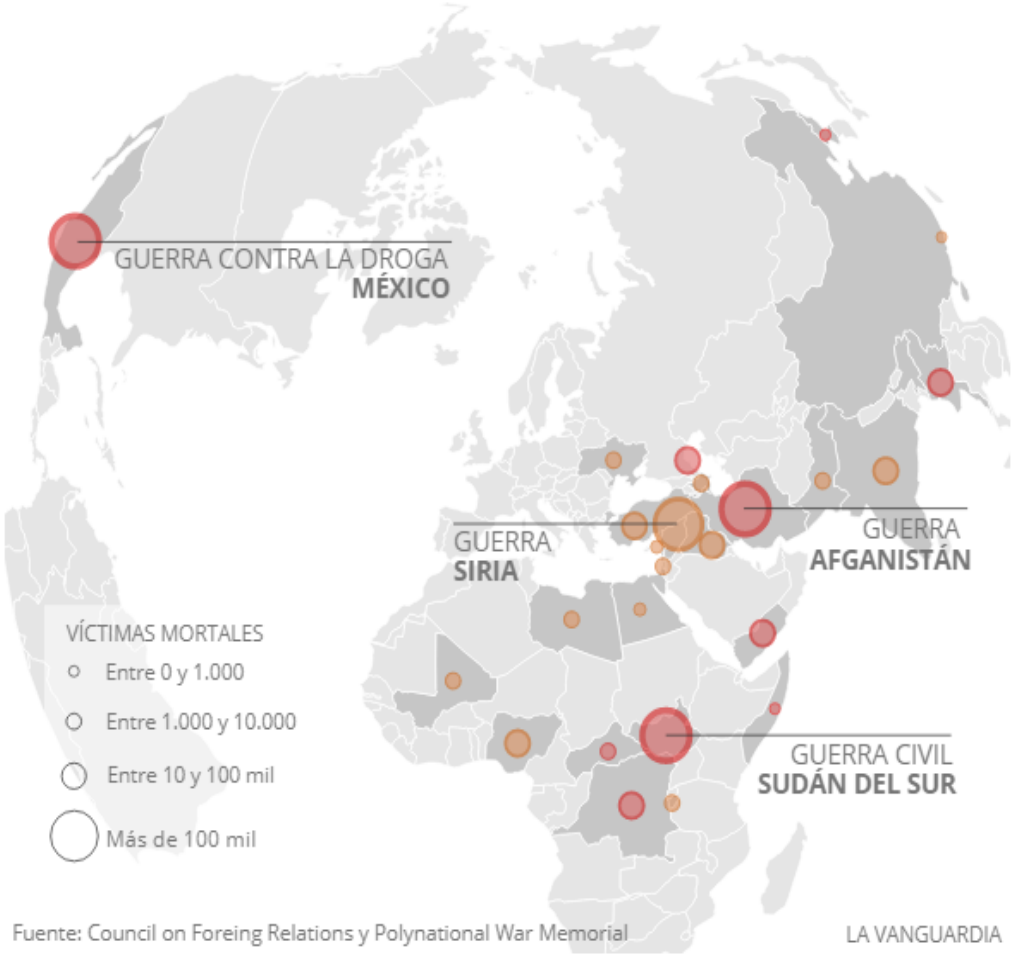

Figura 3. Conflictos activos al año 2019

En la actualidad prevalece la concomitancia de múltiples variables en el dominio operacional:

- Guerra de información
- Nueva matriz conceptual
- Adecuación institucional
- Prevalecen los ataques de precisión
- Prevalece el uso de armas de baja letalidad

- Disminución de los tiempos en el ciclo decisorio
- Dominio de los sistemas de Reconaissance, Surveillance and Target Adquisition (RSTA)
- Asimetrías temporales en los campos de batalla
- Introducción de tecnologías no armamentistas en el ciclo de batalla (Dos Reis y de Brito, 2018)

2. Operatividad: Los conceptos operativos de seguridad y defensa sufrieron procesos de redimensionamiento estableciéndose denominaciones como *Network Centric Warfare* (NCW) en EE.UU. y *Network Enabled Capability* en Europa. Mundialmente se usa el término Netwar. El concepto operativo Netwar refiere optimización de los procesos en sincronía, diagnóstico, proyección de letalidad y supervivencia de las fuerzas en operaciones terrestres, aéreas, marinas, submarinas, espaciales y virtuales. El concepto operacional Transformación, tematizado por La Quadrenial Defense Review (QDR) en el 2001 vino a reestructurar el concepto antiguo de operacionalización, para dar una nueva dimensión a la operatividad militar, bajo la teleología de fortalecer y dar trascendencia a la preeminencia militar de EE.UU. en la dinámica global caracterizada por la irrupción de nuevas tecnologías y reducción drástica en los tiempos de obsolescencia (US Departament of Defense, 2019). Desde el 2018 la QDR fue reemplazada por la National Defense Strategy (Garamone, 2018). En las últimas dos décadas, el Warfare se posicionó como concepto que alude a las renovadas maneras como se desempeña la guerra y el despliegue de la capacidad militar de las potencias. En el mismo orden, *transformation* significa una revolución profunda de los enfoques estratégicos, desplazando las doctrinas ad hoc ligadas a las operaciones de contrainsurgencia, para abrir paso a la "Tercera Estrategia de Compensación (*Third Offset Strategy- TOS*). La tercera estrategia TOS se proyecta como una estrategia fundamentada en la competitividad a largo plazo entre las potencias mundiales. El objetivo del TOS es la consolidación y trascendencia del poderío militar de EE.UU. adecuando los sistemas de defensa a la dinámica tecnológica y estableciendo una red interactiva donde los sistemas de inteligencia, control, mando, computación, reconocimiento y vigilancia se

integren en tiempo real. Estos objetivos se desplegaron en el denominado *Proyecto Marven o Algoritmo de Guerra*, basado en la aplicación de inteligencia artificial a la dinámica de los sistemas de defensa y ataque. El algoritmo contribuye a la toma de decisiones fundamentada en escenarios potenciales, no obstante, los elementos éticos y morales que inciden en la toma de decisiones exigen que el algoritmo de guerra continúe constituyendo una herramienta que construye escenarios mas no emite decisiones inapelables. En ese orden, dentro del grupo de nuevos conceptos operativos que lograron posicionarse dentro de la dialógica militar se encuentran:

- Guerra de información: Se expresa como la lucha por el dominio en el ciberespacio y los flujos de información que circulan en la web, posicionando tema y agendas (Ropers, 2008).
- Dominio de la información: En sus dos dimensiones alude al control de la información y al posicionamiento de un nombre en internet (Ropers, 2008).
- Campo de batalla vacío: Donde las fuerzas armadas no ocupan el espacio de conflicto, el conflicto sucede sin la presencia de actores (Ropers, 2008).
- Campo de batalla digitalizado: Aquel que se sucede en los ámbitos de la red, fundamentalmente en los ámbitos de Tor y la Deep web (Elizalde, 2016).
- Enfoque sistémico del combate y la paz: Donde convergen todas las variables que generan escenarios potenciales de conflicto (Ropers, 2008). Ver Figura 3.
- Operaciones sobre la información: Mecanismos para incidir en la opinión pública y posicionar favorablemente las acciones militares adelantadas en un conflicto (Ropers, 2008).

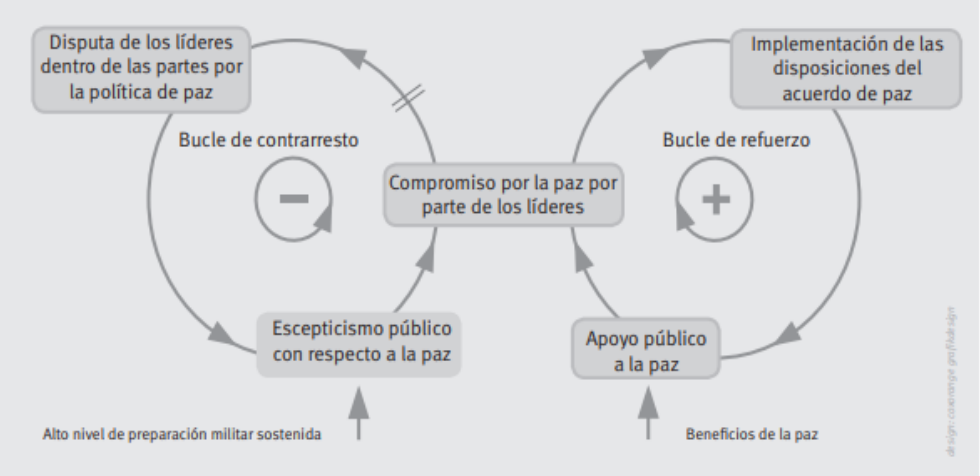

Figura 4. Procesos de paz desde una perspectiva de sistemas

3. Globalidad: El Departamento de Defensa requiere el concurso de los diversos departamentos e instituciones públicas y del sector civil. El sector civil aporta agilidad, motivación y actualización al Departamento, por lo que se persigue la captación de personal altamente calificado en las áreas científicas y tecnológicas, quienes complementan al personal militar.

4. Alianzas: Comprende la integración de las diversas agencias gubernamentales y actores privados, en el establecimiento de alianzas fundamentadas en la teoría de los juegos, donde prevalece el establecimiento de alianzas estratégicas asimétricas. Estas alianzas se fundamentan en la defensa de los principios: libertad, disuasión de la guerra y mantenimiento de la paz. El establecimiento de alianzas demanda de cohesión interna entre los diversos departamentos e instituciones, respondiendo de forma coherente en las acciones frente a los aliados y en contra de los enemigos. Las alianzas proporcionan fuerzas y logística complementaria que posibilita la disminución en los recursos nacionales que deben emplearse en las tareas de prevención y promoción global de la paz y de los objetivos comunes en las relaciones regionales. Orientadas hacia la promoción de este eje se proponen actividades específicas:

- Promoción de mercados abiertos.
- Diseño de la protección de infraestructura crítica: Servicios, defensa, administración.
- Promoción de la consolidación del Estado de Derecho.
- Promoción del desarrollo

- Defensa de los derechos fundamentales y la privacidad (Leiva, 2015).

5. Ingenio: Promueve la captación de las mentes más destacadas en las áreas científicas y de innovación para que se incorporen al Departamento de Defensa.

Obsérvese que la estrategia de EE.UU. persigue fundamentalmente el consolidar la primacía militar del Estado norteamericano en el mundo. No obstante, la perspectiva del sistema de ciberseguridad posee un alcance más amplio, por cuanto comprende la articulación de los principios de seguridad y defensa nacional aunado a la promoción del desarrollo tecnológico. EE.UU. ocupa el primer lugar dentro del ranking ITU con un índice de 0,926 (ITU, 2018)

Países Bajos

La Estrategia Nacional de Ciberseguridad de los Países Bajos fue estructurada en 5 ejes de donde se desprenden estrategias y tareas (Fig 6):

1. Información: Este eje atiende la capitación y la disposición de organismos que desarrollan investigación sobre las amenazas a la ciberseguridad y la ciberdefensa. El Servicio de Inteligencia y Seguridad Militar (MIVD) brinda a la ciudadanía y a los entes públicos información sobre estrategias y herramientas para prevenir los delitos cibernéticos, enfatizando que dada la persistencia de los ciberataques es fundamental asumir medidas preventivas. Dentro de la agenda del MIVD se encuentra la implementación de medidas específicas que emanan de la coordinación con entes públicos y privados. (Ministerie van Defense Netherland, 2018). El MIVD establece como principio la prevención frente a los ataques digitales.

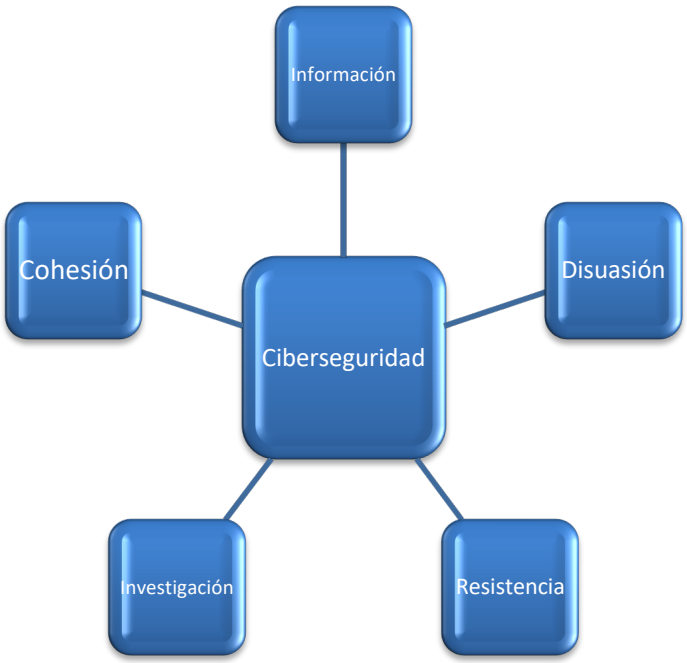

Figura 5. Estrategia Nacional de Ciberseguridad de los Países Bajos
Fuente: Ministerie van Defense Netherland (2018).

La prevención como principio no deriva solo de la voluntad de prevenir, se requiere investigación y el desempeño de tareas de contraespionaje, que orienten al MIVD sobre las amenazas y el diseño de medidas defensivas en acción conjunta con el Servicio General de Inteligencia y Seguridad (AIVD). En ese orden, la ENCS 2019 propone el establecimiento de una plataforma denominada Red Nacional de Detección (NDN) cuya tarea es la detección, contención y defensa contra los ataques digitales. LA NDN cuenta con la colaboración de la Agencia Nacional de Seguridad Cibernética (NCSA), el Comando de Defensa Cibernética (DCC), la Unidad Conjunta de Ciberseñal (JSCU) y el AIVD, el Servicio de Inteligencia y Seguridad Militar (MIVD), el Equipo de Defensa de Emergencia de la Computadora de Defensa (DefCERT), Royal Netherlands Marechaussee. La NDN establecerá una plataforma de cooperación con la NCSC, AVID y la policía. El MIVD posee autonomía para actuar en los casos donde se detecten amenazas (Ministerie van Defense Netherland, 2018).

2. Disuasión: Comprende el inducir al enemigo hacia la ponderación de los costos del ciberataque, por cuanto sean más altos los costos que los logros obtenidos. Esta meta se alcanza en tanto la extensión de las alianzas OTAN (NATO) hasta el

ciberespacio establece que la ciberseguridad y la ciberdefensa son inherentes al dominio militar, tal como lo suscribió la alianza durante la Cumbre de Varsovia del 2016 (NATO, 2016). Los Países Bajos se comprometieron a contribuir con sus capacidades cibernéticas en las misiones de la OTAN. En ese orden, es indispensable el diagnóstico de vulnerabilidades del Ministerio de Defensa para las misiones en el ciberespacio, lo que requiere del concurso de personal capacitado en las más altas competencias de ciberseguridad (Ministerie van Defense Netherland, 2018).

3. Resistencia: Corresponde a la adaptación de las Fuerzas Armadas holandesas a las ciberamenazas, adecuando los sistemas de defensa y ataque a los avances de las tecnologías de información (TI). Los ciberataques pueden ser contenidos y disuadidos en tanto se alcancen altos niveles de resiliencia digital, que induzca al desarrollo de cultura preventiva y mejore los tiempos de respuesta. Aunado a ello se encuentran los niveles de la organización defensiva:

- Gobernanza: Comprende la dirección, enfoques y marcos de las políticas de defensa dentro del dominio cibernético.
- Seguridad por diseño: La seguridad es el eje sobre el que se desarrollan o implementan sistemas TI.
- Evaluaciones de seguridad: Comprendiendo riesgos residuales y el seguimiento de los protocolos y reglamentos de seguridad.
- Vigilancia y seguimiento: Orientada hacia el seguimiento de las conexiones del Ministerio de Defensa con redes externas (Ministerie van Defense Netherland, 2018).

4. Investigación: Persigue establecer las rutas críticas y sensibles ante un ciberataque, mediante el respaldo en redes paralelas, de las que dispone la Red Integrada de las Fuerzas Armadas de los Países Bajos, NAFIN. Aunado a ello, la demanda de personal con las competencias necesarias para responder a los ciberataques deriva en que el Ministerio de Defensa diseña una estrategia de captación y retención de profesionales especializados en ciberseguridad y ciberdefensa, consistente en la oferta de oportunidades de crecimiento profesional y actualización permanente uniformes a todas las instituciones públicas. En ese

orden, el Ministerio de Defensa se incorporó a la Plataforma Holandesa de Seguridad Cibernética para la Educación Superior y la Investigación (Dcypher), que posibilita la coordinación de los estudios en el área de la ciberseguridad, ciberdefensa y criptografía.

5. Asistencia militar: El Ministerio de Defensa asume el compromiso de contribuir al respaldo de las plataformas digitales existentes, así como el diagnóstico de las capacidades y las falencias del propio Ministerio que requieren ser satisfechas.

Los Países Bajos son pioneros europeos en materia de ciberseguridad y ciberdefensa y promotores de la extensión de la alianza de la OTAN hasta el ámbito ciberespacial. Los Países Bajos ocupan el lugar 12 en el ranking ITU 2018 acumulando 0.885 puntos.

España

La Estrategia Nacional de Ciberseguridad fue establecida en España en el 2013, fundamentada en el liderazgo y la coordinación entre los sectores público y privado. En el 2018 fue promulgada por Real Decreto la Ley 12/2018 de Seguridad de Redes y Sistemas de Información. Posteriormente, y gracias a la experiencia acumulada, se han alcanzado importantes avances en materia de ciberseguridad, expresadas en la Estrategia Nacional de Ciberseguridad 2019 que fue estructurada en base a cuatro ejes o principios rectores descritos en la Fig. 6.

Figura 6. Estrategia Nacional de Ciberseguridad de España
Fuente: Gobierno de España (2019)

Los principios rectores se despliegan en el objetivo general contemplado dentro de la estrategia de ciberseguridad nacional, que comprende la garantía por parte del Gobierno de España del uso seguro e íntegro del ciberespacio, amparando los derechos ciudadanos y promocionando el avance socioeconómico (Gobierno de España, 2019: 34). En ese sentido, los cuatro principios se encuentran integrados a la estrategia de seguridad nacional.

Figura 6. Principios rectores. Estrategia Nacional de Ciberseguridad de España
Fuente: Gobierno de España (2019: 33).

Los cuatros principios rectores responden a la búsqueda de coherencia y unificación de criterios y acciones de los diversos entes públicos frente a las contingencias que se presenten en el ámbito virtual. En ese orden, estos principios demandan de liderazgo que posibilite la convocatoria de los actores nacionales públicos y privados, quienes se comprometan con las tareas de anticipación y prevención de riesgos asociados a los espacios virtuales. La prevención a su vez reclama de eficiencia, lo que se traduce en la actualización permanente de los sistemas tecnológicos y la capacitación de los actores responsables de las plataformas virtuales, para contener las amenazas y aprender de ellas.

Los objetivos específicos de la estrategia nacional de ciberseguridad articulan los cuatro principios esbozados:

1. Garantizar la seguridad y resiliencia de las redes y los sistemas de información: Orientado no solo hacia la prevención, enfatiza el aprendizaje a partir de las experiencias críticas, desarrollando una cultura de buenas prácticas en la gestión de la ciberseguridad (Gobierno de España, 2019: 35). Comprende 12 acciones:

i. Ampliación y mejora de las capacidades de ciberacción.
ii. Potenciación de la relación con los centros de investigación abocados al estudio de las medidas de prevención contra las ciberamenazas.
iii. Promoción de las buenas prácticas en ciberseguridad.
iv. Coordinación técnica y operacional entre los sectores público-privados y la sociedad en general.
v. Actualización permanente de la normativa y protocolos de ciberseguridad.
vi. Potenciación de las actividades de ciberdefensa.
vii. Evaluación de riesgos por los actores públicos y privados.
viii. Promoción de las actividades del CSIRT-España.
ix. Desarrollo de plataformas de intercambio de información sobre ciberseguridad.
x. Desarrollo de herramientas preventivas y de respuesta rápida frente a las ciberamenazas.
xi. Promoción del intercambio de información referida a nuevas experiencias en ciberseguridad.
xii. Implementación de medidas de defensa activa contra las ciberamenazas (Gobierno de España, 2019: 44-45).

2. Garantizar el uso fiable y seguro del ciberespacio. Ello comprende la persecución de las actividades ilícitas cometidas a través de la red. Entendiendo que el ciberespacio constituye un ámbito donde los criminales encuentran espacio para sus acciones ilícitas, como medio donde se sucede la comisión de delitos y el ciberespacio como medio de investigación de los hechos delictivos (Gobierno de España, 2019: 36). Comprende 12 acciones:

i. Promoción de las actividades de prevención y defensa.
ii. Promoción en la adecuación y configuración de normativas de protección de infraestructuras críticas.
iii. Promoción del Esquema Nacional de Seguridad y del Sistema Nacional de Infraestructuras Críticas.
iv. Promoción de los principios y estrategias del Esquema Nacional de Seguridad y de la creación de estructuras de ciberseguridad en las comunidades autónomas y los entes regionales.
v. Desarrollo del Centro de Operaciones de Ciberseguridad.
vi. Fortalecimiento de la infraestructura en telecomunicaciones.
vii. Impulso al establecimiento de indicadores que posibiliten medir los niveles de ciberseguridad.
viii. Promoción de compromisos entre los sectores público y privado en materia de prevención de riesgos.
ix. Diseño de catálogos de servicios y productos para la contratación del sector público en servicios y productos de ciberseguridad.
x. Fortalecimiento de los sistemas de vigilancia y seguimiento en materia de ciberseguridad.
xi. Promoción de la ejecución de simulacros de ensayo de los protocolos de ciberseguridad.
xii. Establecimiento de protección de infraestruturas científico-técnicas (Gobierno de España, 2019: 46-47).

3. Proteger el ecosistema empresarial y social de los ciudadanos. Ello constituye una tarea en la que se encuentran comprometidos los actores públicos y privados, quienes están llamados al uso responsable de las tecnologías de la información.

Aunado a ello se promueve el intercambio de experiencias con el sector público y dentro del mismo sector privado, que posibiliten la mejora de las estrategias nacionales de ciberseguridad. Comprende 8 acciones:

i. Reforzamiento del marco jurídico.
ii. Fomento de la participación ciudadana.
iii. Estímulo a la investigación en el ámbito de la información.
iv. Inducción de las instituciones y funcionarios públicos para que reporten ante la justicia penal los delitos cometidos en violación de la ciberseguridad.
v. Promoción de la capacitación de los funcionarios judiciales y policiales orientada a la aplicación de la normativa penal correspondiente en los delitos de cibercriminalidad.
vi. Establecer protocolos de cooperación entre investigadores científicos en el área de la ciberseguridad y los operadores de justicia.
vii. Capacitación de los operadores de justicia, abogados y funcionarios judiciales en todos los niveles en materia de cibercriminalidad, tecnologías asociadas y marco legal.
viii. Impulso a la coordinación de las investigaciones en materia de ciberseguridad entre los entes públicos y privados (Gobierno de España, 2019: 48-49).

4. Promocionar la cultura de ciberseguridad y la capacitación. Esta meta persigue el alcance de la autonomía tecnológica mediante el fomento y la promoción de la instrumentación de los ciudadanos con las competencias necesarias para desempeñar roles activos en los procesos de ciberseguridad y protección del patrimonio tecnológico. Comprende 9 acciones:

i. Suministro de servicios de ciberseguridad óptimos.
ii. Provisión de ciberseguridad y capacitación en las Mypimes.
iii. Difusión de la perspectiva de ciberseguridad como mecanismo de protección de la privacidad.
iv. Suministro de plataformas de denuncias eficientes y seguras para la denuncia de los delitos de ciberseguridad.

v. Estímulo a la cooperación público-privada en materia de ciberseguridad.
vi. Desarrollo de indicadores de riesgo en ciberseguridad.
vii. Promocionar las mejores prácticas de ciberseguridad entre la sociedad en general.
viii. Implantación de sistemas confiables y blindados frente a los delitos de ciberseguridad.
ix. Promoción de las convocatorias anuales del Foro sobre Ciberseguridad (Gobierno de España, 2019: 50-51).

5. Promover la seguridad del ciberespacio a nivel internacional. Comprende la promoción de un ciberespacio abierto, seguro, confiable y plural entre los actores internacionales con quienes sostiene relaciones bilaterales y multilaterales. Ello fundamentado en el respeto a los derechos fundamentales, la Carta de las Naciones Unidas y el Derecho Internacional y en concomitancia con los objetivos del desarrollo sostenible. Comprende 9 acciones:

i. Impulso de los programas de I+D+i en ciberseguridad enfatizando la atención a las Mipymes.
ii. Impulso a la industria de la ciberseguridad enfatizando el respaldo a las Mipymes.
iii. Promoción del desarrollo de productos y servicios de ciberseguridad enfatizando el estímulo a las Mipymes.
iv. Promoción de la exigencia de certificados de ciberseguridad en los productos y servicios.
v. Actualización permanente de las competencias requeridas en los profesionales en ciberseguridad.
vi. Diagnóstico de las demandas de profesionales en el ámbito de la ciberseguridad.
vii. Impulso a los perfiles profesionales en ciberseguridad.
viii. Impulso a políticas de captación y mantenimiento de profesionales especialistas en ciberseguridad.
ix. Impulso a los programas de I+D+i en ciberseguridad y ciberdefensa.

La Estrategia Nacional de Ciberseguridad de España se caracteriza por la vocación de incorporar a los actores públicos y privados en objetivos y actividades comunes orientadas hacia la consolidación de la cultura de la ciberseguridad. España se encuentra en el puesto 7 dentro del ranking ITU 2018, lo que constituye un avance importante en materia de ciberseguridad por cuanto en el 2015 se encontraba en el puesto 9. ITU.

Perú

El Decreto Supremo N° 012-2017-DE aprobó la Política de Seguridad y Defensa Nacional del Perú. Dentro de esta política se incluye las políticas en materia de ciberseguridad, que comprenden la concepción integrada de la defensa nacional como un compromiso del Estado y de la sociedad. En ese orden, la política nacional de ciberseguridad en el Perú comprende no solo la estructura de lo compendiado en la Ley Nº 27444, el Decreto Supremo N° 012-2017-DE referido a la seguridad y defensa nacional, y la Ley 30999 o Ley de Ciberdefensa; fundamentalmente comprende el compromiso de la sociedad peruana por fortalecer la defensa nacional y la peruanidad. En ese sentido, la política de ciberseguridad nacional se encuentra en constante actualización con el concurso de los sectores público y privado, estimulando especialmente la participación activa de las comunidades urbanas y rurales.

La difusión de información y la capacitación de los funcionarios públicos para que sirvan de multiplicadores y sensibilizadores en materia de ciberseguridad constituyen uno de los pilares de las políticas públicas peruanas. En ese sentido fue constituida la Secretaría de Gobierno Digital. Dicha Secretaría se rige por el artículo 47° del Decreto Supremo N° 022-2017-PCM o Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros. La Secretaría de Gobierno Digital es responsable y posee las competencias necesarias para el diseño y proposición de políticas públicas nacionales, regionales y locales con el objetivo de modernizar y actualizar el Estado en un proceso permanente de adecuación frente a los acelerados procesos de innovación tecnológica mundial. Las funciones de la Secretaría de Gobierno Digital comprenden:

1. Rectoría del Sistema Nacional de Informática.
2. Diseño y proposición de políticas públicas en materia de gobierno digital.
3. Aprobación de normativas en el ámbito de su competencia.
4. Supervisión de los lineamientos en materia de gobierno digital.
5. Ejecuta y supervisa tareas y acciones de promoción y consolidación del Sistema Nacional de Informática.
6. Seguimiento y coordinación de la interoperabilidad de los sistemas informáticos.
7. Seguimiento y coordinación de los portales Web del Estado, sus dependencias y evaluación sobre el seguimiento de las buenas prácticas.
8. Administración del portal Web nacional.
9. Acompañamiento de los organismos públicos en materia digital.
10. Diseño de innovaciones.
11. Asesoramiento técnico a las instituciones públicas.
12. Diseño de propuestas de innovación.
13. Seguimiento y diseño de indicadores de digitalización estatal.
14. Promoción de seguridad digital.
15. Fomentar la cooperación y coordinación público-privada instando a la participación ciudadana en materia de innovación y adecuación digital de las instituciones públicas.
16. Asesorar a los organismos en materia tecnológica.
17. Emitir opinión técnica en el ámbito de su competencia.

Aunado a la Secretaría de Gobierno Digital se encuentra el Sistema de Coordinación de Emergencias en Redes Teleinformáticas de la Presidencia del Consejo de Ministros - PeCERT, fundado en el 2007 mediante Resolución Ministerial N° 360-2009-PCM. Posteriormente, en el 2012 el PeCERT fue asociado por el CERT CC (Computer Emergency Response Team - Coordination Center) como CSIRT (Computer Security Information Response Team) nacional para el Perú (Presidencia del Consejo de Ministros, 2012). El reconocimiento de PeCERT por la comunidad más importante en ciberseguridad a nivel mundial, constituyó la entrada del Perú en el sistema mundial de la ciberseguridad, lo que

brindó la disponibilidad de recursos provenientes de los centros más experimentados en la materia quienes conforman los CERT de todo el mundo. No obstante, el ingreso dentro de la comunidad de los CERT no ha detenido los riesgos inherentes al uso de plataformas virtuales. La Anti-Phishing Working Group - APWG, adscrita a la Universidad de Oxford, EE.UU., diagnosticó en el 2016 que el Perú era el quinto Estado más susceptible a infección por programas virales, sin embargo, el Perú logró escalar posiciones al 2018, con un índice de 0.401 ubicándose en el puesto 95 a nivel mundial y en el puesto 12 en el ranking regional (ITU, 2018).

Dentro de esta estructura institucional, el Perú adelanta políticas de ciberseguridad orientadas hacia la protección de la infraestructura cibernética y las bases de datos del Estado. El Estado se compromete a la protección de la data nacional conservando la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. En ese orden, se implementa la Política Nacional de Ciberseguridad (Fig. 8).

Figura 7. Política Nacional de Ciberseguridad del Perú.

La política nacional de ciberseguridad peruana se encuentra estructurada en torno a seis ejes:

1. Fortalecimiento: Comprende el desarrollo de las capacidades de protección de las instituciones estatales para contener y confrontar las amenazas provenientes de las plataformas virtuales. Este eje comprende la incorporación de la sociedad civil en sus diversas dimensiones: académica, comunitaria, industrial, comercial, para que participen en el desarrollo de estrategias de ciberseguridad y ciberdefensa. Se propone el alcance de esta meta mediante la sensibilización de la población y la profundización de los nexos con expertos internacionales en la materia.

2. Capacitación: Incorpora la formación de los funcionarios de la administración pública en el desarrollo de las competencias necesarias para la implementación de políticas de ciberseguridad. Se propone el alcance de esta meta utilizando las plataformas PeCERT, CERT internacionales y del Comité Interamericano contra el Terrorismo (CICTE) de la OEA. En primera fase atiende la reforma curricular de la escuela de formación de oficiales y suboficiales, incorporando materias en el área de la ciberseguridad y la ciberdefensa.

3. Difusión: Mediante la implementación de un plan de sensibilización ciudadana en materia de ciberseguridad. Comprende conferencias y foros sobre buenas prácticas en ciberseguridad y las normativas vigentes en la materia.

4. Cooperación: Incluye el fortalecimiento de la legislación en materia de ciberseguridad mediante el apoyo de organismos internacionales y la incorporación en organismos multilaterales orientados hacia la ciberseguridad, y la suscripción de los convenios existentes en la materia y la satisfacción de los compromisos inherentes a los objetivos del desarrollo sostenible.

5. Integración: Comprende la coordinación entre las oficinas regionales adscritas al PeCERT en procesos continuos de adecuación y actualización.

Planeación: Estructuración del Plan de Acción Nacional en Ciberseguridad donde participen los diversos actores de los sectores público y privado, organizados en el Comité Nacional de Ciberseguridad.

CAPÍTULO VI

Diálogo teórico-empírico

Ciberseguridad en el Perú

Las diferentes estrategias y políticas nacionales de ciberseguridad tienen en común el objetivo de preservar la integridad del Estado frente a las amenazas provenientes desde el mundo virtual (Figura 9). No obstante, persisten diferencias en cuanto a la perspectiva de los Estados y los fines que se persiguen en la implementación de políticas públicas de ciberseguridad. Obsérvese que la vocación hegemónica global y regional de EE.UU. deriva en que las estrategias de ciberseguridad respondan hacia la contención de sus principales competidores y la trascendencia de sus ejes de influencia. En el caso de los Países Bajos, sus intereses se identifican con los de la Unión Europea y la OTAN bajo la teleología de la consolidación del Estado continental europeo. Otro es el caso de España, que pese a formar parte de la Unión Europea persigue fundamentalmente objetivos endógenos que garanticen la perpetuación del Estado español y sus comunidades autónomas. Por último, el caso peruano expresa la situación de un país en vías de desarrollo con altos niveles de penetración tecnológica y vulnerabilidades evidentes en materia de ciberseguridad.

Los casos mencionados por su naturaleza no permiten comparaciones aplicando indicadores que expresen niveles de desarrollo de las estrategias nacionales de ciberseguridad.

Figura 8. Ciberamenazas y acciones maliciosas.
Fuente: Gobierno de España (2019).

No obstante, es posible identificar la presencia de elementos que orienten cuáles son las vulnerabilidades que requieren de políticas públicas que satisfagan las brechas abiertas en materia de ciberseguridad. Es así como se procedió a aplicar los indicadores recomendados por Leiva (2015), con el objetivo de identificar los indicadores que expresen vulnerabilidades en las políticas nacionales de ciberseguridad del Perú.

Tabla 2
Estrategias Nacionales de Ciberseguridad 2019

	País	Países Bajos	EE.UU.	España	Perú
PROTEGE	Infraestructuras criticas	x	x	x	x
	Economía	x	x	x	
	Seguridad nacional	x	x	x	x
	Bienestar social		x		
ENFOQUE	Concientización		x	x	x
	Conocimiento	x	x	x	
	Educación	x	x	x	
	Capacidades cibernéticas militares	x	x	x	x
SECTOR PUBLICO	Liderazgo/coordinación	x	x	x	
	Marco jurídico	x	x	x	
SECTOR PRIVADO	Participación en la estrategia	x	x	x	
COOPERACIÓN INTERNACIONAL	Cooperación en su grupo	x	x	x	x
	Cooperación con otros países	x	x	x	x

Fuente: Diseño propio basado en Leiva (2015)

Estados Unidos lidera la satisfacción de los indicadores de ciberseguridad según el ranking mundial ITU (2018). Los Países Bajos, aun siendo pioneros en Europa en el ámbito de la ciberseguridad, en la actualidad ocupan el lugar 12 del índice ITU (2018), siendo superados por Inglaterra, Francia, Lituania, Estonia, España, Noruega y Luxemburgo. Los Países Bajos no han logrado satisfacer los indicadores de bienestar social y concientización. En cuanto al indicador bienestar

social, los Países Bajos otorgan prioridad a la seguridad nacional y la seguridad del Estado continental de la Unión Europea, por sobre la protección del bienestar y la concientización de la sociedad nacional, lo que refiere la prioridad entre indicadores en el ámbito de la ciberseguridad y no el detrimento de un indicador por otro.

La ventaja comparativa de España frente a los Países Bajos se explica en el enfoque sobre la resiliencia. España otorga prioridad a la concientización ciudadana en materia de ciberseguridad y en el aprendizaje de las experiencias infortunadas de los CERT a nivel mundial. Esa decisión estratégica posiciona a España en el lugar 7 del índice ITU, superado solo por EE.UU., Canadá y cuatro países europeos.

En el marco de lo expuesto, Perú se ubica en el lugar 95 del índice ITU (2018). Regionalmente se ubica en el lugar 12 superando a países como Panamá, Ecuador, Venezuela, Guatemala y Nicaragua, entre otros. Según refiere la investigación de Leiva (2015), los países de la OEA emprendieron tareas conjuntas de fortalecimiento en materia de ciberseguridad desde el 2004. En 15 años, desde la adopción de la Estrategia Interamericana Integral de Ciberseguridad, esta iniciativa continúa evidenciando profundas asimetrías regionales donde existen grupos de países con capacidad mínima de respuesta ante ciberataques, otros se encuentran en niveles intermedios con capacidades de respuestas que fluctúan entre medias y altas. El Perú se ubica entre los países con capacidad de respuesta de media a baja.

El caso peruano es singular, por cuanto dispone de una profusa legislación en materia de ciberseguridad dispersa entre múltiples instrumentos legales. En el 2019 fue sancionada la Ley de Ciberdefensa, mientras que la Ley de Ciberseguridad esperaba por su promulgación. Ambas legislaciones contienen novedosos aportes al mejoramiento del índice de ciberseguridad, sin embargo, solo la Ley de Ciberdefensa se encuentra vigente. Para la fecha de la evaluación ITU, los dos instrumentos legales se encontraban en discusión y la aprobación de la Ley de Ciberdefensa aún demanda tiempo para que demuestre su efecto sobre los índices de ciberseguridad.

Es fundamental distinguir entre ambos instrumentos. Mientras que la Ley de Ciberdefensa tiene por objeto la regulación de operaciones militares en el ámbito de la ciberdefensa, la Ley de Ciberseguridad atañe a medidas preventivas ante amenazas cibernéticas. Tanto el instrumento vigente como el que está en proyecto poseen la vocación de satisfacer los indicadores ITU y con ello blindar al Estado y a la sociedad peruana frente a las ciberamenazas y al rezago tecnológico derivado de la acelerada dinámica en el desarrollo de las fuerzas productivas digitales. No obstante, la legislación por sí misma es insuficiente en materia de protección de la estructura económica y el bienestar social, en tanto la celeridad de los desarrollos TIC tiende a la obsolescencia normativa, aun antes del alcance de los efectos de novísimas legislaciones. Ello no deriva en el indefectible rezago normativo, solo induce hacia la adecuación permanente en materia reglamentaria que responda a las buenas prácticas en ciberseguridad y ciberdefensa. Para los latinoamericanos estas dinámicas constituyen un desafío titánico, por cuanto el peso de la burocracia de raíces hispanas es un coloso que debe ser derrotado.

Es así como el Estado y la sociedad peruana aún transitan por los enfoques de la concietización y del desarrollo de las capacidades cibernéticas militares como indicadores prevalentes en el diseño de las políticas nacionales de ciberseguridad. Aun cuando el liderazgo descanse, en principio, en el Estado, la ciberseguridad constituye un compromiso social que demanda de articulación entre el sector público y el sector privado, lo que en el Perú aún no se concreta. Las debilidades estructurales y las fluctuaciones de la gobernabilidad y la gobernanza virtual demandan la construcción de plataformas donde concurran los ámbitos público y privado para la configuración de estrategias nacionales de ciberseguridad que respondan a las demandas de internautas civiles y militares, públicos y privados, académicos, investigadores, industriales, comerciantes y en general de la sociedad peruana en su conjunto.

En los indicadores referidos a cooperación regional, bilateral y multilateral, el Perú ha manifestado comportamientos disimiles. Ha establecido acuerdos de asesoría militar con los EE.UU. que le permiten fortalecer sus sistemas de ciberdefensa y ciberseguridad fundamentado en la experiencia norteamericana.

Además, cuenta con acuerdos regionales dentro de la plataforma OEA, que promueven la cooperación con los socios regionales.

Según los mencionados indicadores, el Estado peruano confronta el reto de satisfacer los indicadores ITU, lo que se resume en:

i. Construcción de plataformas de alta seguridad que protejan los sistemas del Estado y de la sociedad en general.
ii. Capacitación de fuerza de trabajo altamente especializada.
iii. Fortalecimiento de los CERT regionales.
iv. Convocatoria eficiente a la ciudadanía para que se incorpore al desarrollo de planes y protocolos de ciberseguridad.
v. Adecuación normativa y firma de convenios internacionales novedosos en materia de ciberseguridad.
vi. Consolidación y reimpulso del PeCERT.
vii. Democratización de la participación ciudadana en materia de ciberseguridad.

Todo ello con el objetivo de alcanzar la transformación digital del Estado peruano bajo la premisa del blindaje cibernético (Figura 10).

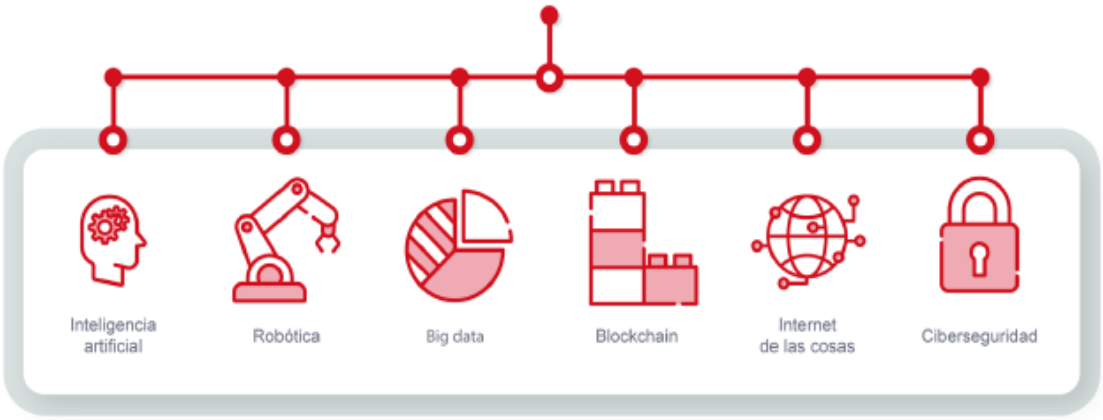

Figura 9. Transformación digital
Fuente: Gobierno de España (2019).

Conclusiones

Al comenzar esta tesis se propuso un objetivo general que se constituyó en "Proponer estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad nacional del Perú, 2019", aunado a un conjunto de objetivos específicos que se tratarían de alcanzar al finalizar el estudio, que fueron: Analizar las estrategias integradas de ciberseguridad más eficientes implantadas en tres países seleccionados al 2019, evaluar el marco normativo legal respecto a la ciberseguridad en el Perú, identificar las limitaciones referentes al desarrollo de la ciberseguridad en el Perú, establecer las brechas en materia de desarrollo, evaluación y actualización de una estrategia integradas de ciberseguridad en el Perú, y abordar las brechas para optimizar el desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú.

La ciberseguridad constituye un aspecto fundamental para la consecución de los objetivos socioeconómicos de las economías modernas, así mismo, las estrategias están formuladas para ser implementadas conforme al sistema de categorización específico que ha decidido cada país para aplicarla de tal modo que estas puedan presentarse a la población mediante una norma, un reglamento, políticas o programas generales nacionales existentes en relación con la ciberseguridad. Es importante también mencionar que una de las estrategias de ciberseguridad está configurada por el resultado del esfuerzo multidisciplinario de colaboración en provecho de los conocimientos, experiencia y pericia de las organizaciones públicas y privadas a favor de las políticas nacionales y reconocimiento de la necesidad de reforzar por convenios participativos de cooperación de la comunidad internacional en materia de constante capacitación para dar respuesta oportuna en relación con los índices de respuestas ante ciberataques de cualquier índole. Cabe mencionar que, en 15 años desde la adopción de la Estrategia Interamericana Integral de Ciberseguridad, esta iniciativa continúa evidenciando profundas asimetrías regionales donde existen grupos de países con capacidad mínima de respuesta ante ciberataques, otros se encuentran en niveles intermedios con capacidades de respuestas que fluctúan entre medias y altas. El Perú se ubica entre los países con capacidad de respuesta de media a baja.

Asimismo, se observó que la Constitución Política del Perú en su artículo 44°, concatenado con el artículo 163°, establece que son deberes primordiales del Estado brindar la seguridad tanto en relación con la protección de la población, garantizar derechos humanos, y entre otros, la defensa de la seguridad y la soberanía de la nación, dejando expuesto que el acceso a contenidos y materiales gráficos del internet puede ser perjudicial por no ser apto tanto para menores de edad (por el contenido sexual, violencia y de drogas al que se expone) como para la sociedad que está expuesta al "hackeo" de información personal, entre otros. Por otro lado, en el 2011 se aprobó un Plan Estratégico de Desarrollo Nacional, denominado Plan Bicentenario, el cual se proyectó hasta el 2021, en función de mejorar tanto el aspecto del ciberespacio como el comercial inclinándose hacia este último. Por lo que, aun cuando se plantean proyectos y planes estratégicos de acciones estratégicas cuyo despliegue se proyecta en tres fases, en las cuales se pretende visionar cómo abordar las áreas vulnerables deducidas en la tabla N° 2 inserta en la sección 5.4 del capítulo V, se enfocó en dar respuesta a las amenazas y riesgos que pudieran presentarse a la seguridad nacional, bajo tres lineamientos, según la época claves, ya que tendían a la modernización y reforma de las Fuerzas Armadas, el fortalecimiento de las acciones sociales y la lucha contra el narcotráfico, actividades exclusivas del Ejercito del Perú, por lo que dista de la fusión de la actividad civil, mientras que el Estado y la sociedad peruana transiten por el largo camino de plano táctico del desarrollo y análisis de riesgo, y los enfoques de la concientización en el desarrollo de las capacidades cibernéticas, tanto de la sociedad civil y militar como indicadores prevalentes en el diseño de las políticas nacionales de ciberseguridad, demanden un verdadero compromiso social que involucre la articulación entre el sector público y el sector privado, lo que en el Perú aún no se concreta, razón por la cual no se aprecian avances.

En cuanto a las limitaciones resaltantes en el desarrollo de la ciberseguridad en el Perú, se señala que las debilidades estructurales y las fluctuaciones de la gobernabilidad en la vía virtual requieren la construcción de plataformas donde concurran los ámbitos público y privado para la configuración de estrategias nacionales de ciberseguridad que respondan a las demandas de internautas civiles y militares, públicos y privados, académicos, investigadores, industriales,

comerciantes y en general de la sociedad peruana en su conjunto. En ese orden, el diseño de la Estrategia Nacional de Ciberseguridad del Perú constituye una necesidad que demanda ser satisfecha, desde la palestra de la planificación para la prevención y no como respuesta a los ciberataques, lo cual amerita intencionalmente un cambio en la postura de la política nacional que sustenta erradamente la idea que las estrategias se irán definiendo en relación a los logros alcanzados.

En cuanto a las brechas en materia de desarrollo, se concluye que son un efecto de más interesante que la megatendencia del uso del ciberespacio y las facilidades que presenta se obtiene en un gran impacto para la reducción de las brechas de acceso a la información en el acceso de bienes y servicios que auguran nuevas oportunidades de negocios y de desarrollo, pero a su vez configura la apertura de una gran brecha a los ladrones de información que acechan el ciberespacio, esto afecta a los sectores de bajos ingresos de los países en vías de desarrollo. Así mismo, indicar que la principal brecha que se presenta es una gran carencia de tecnologías adecuadas y/o novedosas que permitan el funcionamiento y mantenimiento del orden interno, orden público y seguridad ciudadana. Y debido a la carente tecnología de punta, la inestable y crítica infraestructura de protección y gestión del riesgo de desastres, por contener programas ya obsoletos e ineficaces evita una articulación en tiempo real, bien por la ausencia de un ente rector que verifique, promueva y canalice estas acciones a través de tecnologías de la información y comunicación que contribuyan a garantizar la seguridad nacional.

Por último, para abordar las brechas y optimizar el desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú, es preciso mencionar los diversos elementos tecnológicos de los que se sirven los hackers para lograr el ingreso y fin de dichos ciberataques, por lo que es inminente concluir que la principal brecha es la que ha de combatirse con el ajuste y actualización de tecnología de avanzada para afrontar las amenazas desde la perspectiva preventiva y no de la de solucionar el mal ya causado. La segunda es la falta de integración de intereses personales y unificarlos por el bienestar del país en general.

Recomendaciones

1. De acuerdo al profundo estudio en materia de ciberseguridad realizado se sugiere aplicar la propuesta desarrollada en la investigación con el fin de fortalecer la seguridad nacional a través de estrategias de ciberseguridad configuradas por el resultado del esfuerzo multidisciplinario de colaboración en provecho de los conocimientos, experiencia y pericia de las organizaciones públicas y privadas. Igualmente, reconocer la necesidad de reforzar, a través de convenios participativos de cooperación de la comunidad internacional, la capacitación constante para dar respuesta oportuna en relación con los índices de respuesta ante ciberataques de cualquier índole.

2. Investigar y mejorar el sistema de intercambio de información, investigación y respuesta con los países e instituciones privadas que aporten avances para la previsión de un ataque o crisis cibernética.

3. Evaluar y mejorar la capacidad del gobierno para identificar, detener y ajustar el ordenamiento jurídico nacional al marco normativo internacional para enjuiciar a los autores de delitos cibernéticos con base en expertos con conocimientos fusionados en materia legal y especializados en programación para investigar esos delitos conjuntamente con la cooperación de organismos, tanto dentro del país como del extranjero.

4. Se recomienda una constante evolución de los recursos normativos, los recursos humanos y los recursos tecnológicos y crear espacios de integración de las alianzas estratégicas que permitan la coordinación para afrontar en el preciso instante en que se identifique cualquier limitante.

5. Ampliar el alcance de la detección de ciberataques para permitir la detección y el bloqueo en tiempo real, y desarrollar tecnologías de respuesta basadas en la IA.

6. Para abordar las brechas, desde la óptica preventiva, mas no de respuesta ante el ataque, es recomendable fortalecer la gestión de las instalaciones, novedosas, de tecnología de avanzada para la interface y los servicios de dominio, o adoptar el buen acceso a un VPN de acceso remoto para gestión centralizada hasta firewalls de sistema de detección de amenazas, con los cuales coadyuvar e imposibilitar los delitos cibernéticos y establecer una red de seguridad cibernética, con la participación de todos los organismos, empresas e instituciones gubernamentales pertinentes.

Propuesta de Estrategia Nacional de Ciberseguridad del Perú

6.1 Presentación

La seguridad siempre ha sido una gran preocupación para los Estados y las organizaciones. Fue crucial incluso en los días de las tarjetas perforadas y la presentación manual de datos en formato impreso. Un solo archivo perdido en esos días podía costar mucho a la industria y también con mayor afectación a la seguridad nacional. Hoy, sin embargo, las apuestas son aún mayores porque la información circula por el ciberespacio donde existen demasiados riesgos y ahora amenazas.

Con la creciente frecuencia de los ataques cibernéticos, el costo también ha aumentado. Informes recientes revelan que el costo de una sola violación cibernética es de alrededor de 84,000 a 148,000 dólares para una pequeña empresa. Esto ni siquiera incluye el costo de remediación y recuperación; si el ataque es al Estado, a una infraestructura crítica u organización estatal, agregue la pérdida de confianza de los inversionistas y el daño será irreparable. En la banca y la empresa privada, con un golpe tan grande, no es de extrañar que el 60% de estas empresas cierren en los seis meses posteriores a un ciberataque. Una sola violación puede resultar fatal para un negocio y también para la seguridad nacional, por lo tanto, la mejor estrategia es la prevención.

La ciberseguridad no es solo una palabra de moda. No es un truco de marketing para vender servicios y soluciones. Con un número creciente de amenazas cibernéticas que también se están volviendo más sofisticadas cada día, la seguridad cibernética o ciberseguridad es la necesidad imperiosa de hoy. Cualquier país podría estar a solo una brecha de un ciberataque que comprometa seriamente la economía, el bienestar de su población y hasta la seguridad en todas sus dimensiones, hay mucho más en juego que dinero, por lo tanto, debemos de contar con políticas adecuadas y con estrategias integradas para lograr la anhelada seguridad digital, y al referirme a que deben ser integradas es consecuencia de que si estas amenazas afectan a la seguridad, se entiende ahora que esta seguridad es multidimensional, por lo tanto, las estrategias y acciones coordinadas que se proponen en esta investigación deben de ser de competencia política, económica,

social, medioambiental y militar inclusive, aun sabiendo que las FF.AA. son responsables de la ciberdefensa.

La presente propuesta, cónsona con el tema desarrollado, es conducente directamente con la ciberseguridad, cuya actividad se concentra a nivel estratégico en maximizar la participación y atención por parte de este nivel, abordar la planificación para la protección, persecución, detección y sanción de los agentes delictuales en el ciberespacio, y la disminución del nivel de riesgo que permita preservar la confidencialidad, integridad y disponibilidad ante las amenazas, peligros y daños al que está expuesta la información de los ciudadanos en el ciberespacio.

En cualquier área en la que se pretenda resguardar la seguridad y derechos de los ciudadanos, la improvisación es el primer detonante de debilidad y riesgo, por ello, en la ciberseguridad la carente capacidad de enfrentar riesgos cibernéticos (SEDENA, 2030), la carencia de tecnologías de última generación y la ausencia de un ente rector que plasme estas acciones a través de tecnologías de la información y comunicación que contribuyan a garantizar la seguridad nacional, tal y como se enuncia en la Política de Seguridad y Defensa Nacional sustentada en lo expuesto en el Decreto Supremo N° 012-2017-DE, son algunos de los aspectos que impulsan la necesidad de implementar un plan estratégico concentrado en complementar y reducir las brechas en materia de tecnología y ciberseguridad para optimizar el desarrollo, evaluación y actualización de la Estrategia Integrada de Ciberseguridad en el Perú.

La ciberseguridad comprende una cultura multidisciplinaria de conciencia participativa y preventiva de la materia. Ofrecer un grado mínimo de seguridad amerita vigorosamente la participación conjunta de expertos, tecnologías y estrategias integrales de ciberseguridad para obtener un control en las redes que detecte las “alertas tempranas” con base en una estructura de supervisión y monitoreo, para la detección temprana con generación de alertas ante cualquier actividad anómala. Por ello, es menester la existencia de un mecanismo o procedimiento para determinar con precisión qué infraestructuras, plataformas, dispositivos, redes y sistemas deben ser monitoreados permanentemente y de qué

forma se desarrollarán y revisarán los correspondientes informes de resultados de la evaluación de monitoreo, apegados a las líneas de acción en las estrategias de ciberseguridad que involucre el desenvolvimiento del nivel estratégico, regional o local.

El Estado como ente que, mediante la verificación, ejecución de supervisión y diseño de las acciones de mejora, mantiene activo el estado de seguridad, comprende en la presente propuesta comprometerse específicamente en trazar este primer nivel que se ciñe a un plan estratégico de lineamientos, selección de los recursos, modo de acción y ámbito de participación. No obstante, en cuanto a los otros dos niveles restantes se hace ocasionalmente referencia que el desarrollo de estos se fomentará en el devenir del desarrollo de las mismas estrategias.

El plano local o táctico, o nivel usuario, comprende el desarrollo y análisis del riesgo, el diseño de estrategias de acción y sus zonas de aplicabilidad preferencial o piloto, el diseño de ingeniería de seguridad, el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), y el gobierno de seguridad e implementación del SGSI, de los cuales por integración multidisciplinaria se genere la probabilidad de controles de sistema de capas, bien con protección de los DNS o sistemas de tecnologías biométricas, lo que permite pasar al nivel operacional, que consiste en el funcionamiento y plena ejecución de la maniobra del cómo se plantea el empleo y funcionamiento de las herramientas de gobierno de seguridad mediante la monitorización, supervisión y detección de eventos dentro del sistema de intercepción de datos de diferentes capas de seguridad, que genera un impacto como buena estrategia encadenada a la escala de documentación del evento registrado, apropiado en una visión realista que se active, así como también clasificar o categorizar las alarmas permite efectuar un monitoreo y detección.

El panorama de riesgos a abordar es de amplio espectro por el carácter global del ciberespacio, el riesgo y amenazas provienen originariamente tanto del exterior como del interior del territorio peruano, por causa de actividades delictuales, afectando los derechos de las personas y socavando la confidencialidad, integridad y disponibilidad de los activos de información en el

ciberespacio, y otras labores como el espionaje y vigilancia llevadas a cabo con diversos fines.

El principal objetivo de los ciberdelincuentes es acceder a la valiosa información confidencial, tanto de carácter personal como de las instituciones del Estado, como lo son los secretos militares que pueden ser usados para construir armamento, rastrear movimientos de tropas o exponer a agentes de contrainteligencia, siendo una lista interminable de propósitos malévolos, por ello, se hace necesaria cada vez más profundizar y actualizar las estrategias para abordar la gran diversidad de ciberataques que perturban o pretenden destruir las infraestructuras gubernamentales físicas e incluso la posible producción de una ciberguerra.

El objetivo de la propuesta de estrategias integradas nacionales de ciberseguridad en el Estado peruano plantea cimentar un sistema participativo y cooperacional en el que se alienta la participación conjunta de todas las personas, organizaciones e instituciones públicas, privadas y militares a participar en actividades para desarrollar eficazmente un programa de ciberseguridad dentro de la nación que involucre la cooperación con la comunidad internacional, ya que esto exige una atención y acción más proactivas.

El ámbito de aplicación advierte que tiene alcance nacional y está específicamente referido a toda persona natural o jurídica y comunidad integrante del territorio nacional e incluso las instituciones u organismos del Sistema de Seguridad y Defensa Nacional sin que esto sea discriminatorio para las comunidades autóctonas.

Las acciones estratégicas se despliegan en tres fases, en las cuales se pretende visionar cómo abordar las áreas vulnerables deducidas en la tabla N° 2 insertas en la sección 5.4 del capítulo V, donde se deduce la necesidad de una estructuración hacia una visión donde se procure disminuir la brecha en la capacidad de respuesta, reforzando las capacidades cibernéticas nacionales que involucran tanto la separación de las redes internas del Estado y de la internet pública como la creación de una organización única encargada de liderar y gestionar la ciberseguridad a nivel nacional y de un sistema de alta tecnología para

detectar y responder a los ataques cibernéticos en tiempo real. Estas estrategias están distinguidas como: Fase I. Línea de Acción I o planificación; Fase II. Tendente a la ejecución; y Fase III, que ilustra la evaluación de la ciberseguridad como proceso de protección de la información mediante la prevención, detección y respuesta a los ataques (Fig.11).

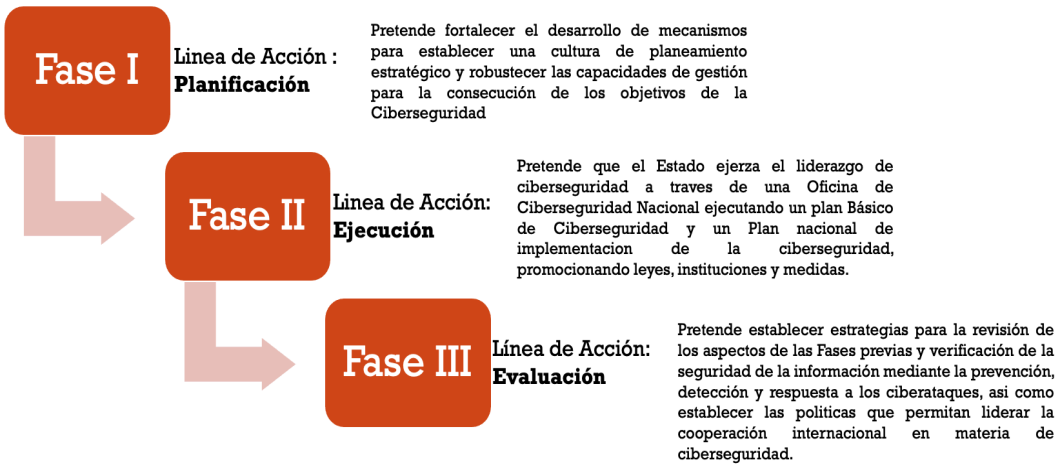

Figura 10. Fases estratégicas de Ciberseguridad Nacional
Fuente: Diseño propio

6.2 Línea de Acción o Fase I

Las líneas de acción se presentan y se ponen a disposición, no solo con la finalidad de contribuir a la postura institucional, sino que también pretenden fortalecer el desarrollo de mecanismos para establecer una cultura de planeamiento estratégico y robustecer las capacidades de gestión en la institución con visión en la consecución de los objetivos de la seguridad nacional.

Generalmente, los efectos de los ciberataques se conocen cuando este ya se ha ejecutado, es decir, el mal siempre está oculto y sale a la luz; es porque algo en su configuración falló, hay muchos eslabones en la cadena de las “mafias organizadas”. La estrategia de planificación involucra una apertura mental que proporcione una técnica con la capacidad de observar a profundidad, con alcance y trascendencia al punto máximo de poder ubicar la actividad del dominio asociado a la amenaza que sirve como conducto para redireccionar con sistemas sofisticados a los servidores y proxys que ocasionan el ciberdelito, sin embargo,

equipos desactualizados y componentes obsoletos permiten que las amenazas se materialicen mediante la falsa sensación de seguridad que ofrecen ciertos cifrados de datos que se almacenan y quedan desprotegidos, esto y mucho más evoca la necesidad del diseño en el ámbito estratégico de "defensa informática" de vías técnicas para minimizar los riesgos del Sistema de Gestión de Seguridad de Información, por lo que involucra las medidas siguientes:

a. El establecimiento de un gobierno basado en la confianza y la cooperación.

b. La construcción de cimientos de la industria de la ciberseguridad.

c. Fomentar la cultura de la ciberseguridad.

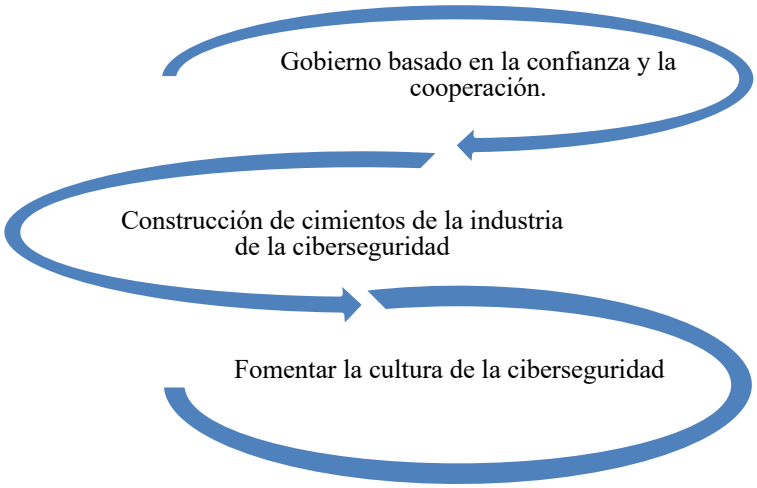

Figura 11. Fase II
Fuente: Diseño propio

A. *Establecer un gobierno basado en la confianza y la cooperación, conlleva:*

1. Facilitar la cooperación e interacción público-privada-militar

   a) Crear un sistema de gobernanza en virtud del cual todas las entidades, incluido el Gobierno, compartan funciones y responsabilidades para cooperar en materia de ciberseguridad.

b) Apoyar a las personas y a las empresas para que compartan la visión nacional de la ciberseguridad y mejoren sus capacidades para cumplir sus funciones.

c) Crear una red de cooperación de expertos nacionales e internacionales para llevar a cabo investigaciones en profundidad sobre estrategias, políticas y otras cuestiones pertinentes en materia de ciberseguridad.

d) Hacer esfuerzos para reducir los puntos ciegos de la ciberseguridad en el sector privado, mejorando la respuesta a los ataques cibernéticos, fortaleciendo la cooperación entre los organismos pertinentes y ampliando los recursos para apoyar a las instituciones.

e) Ampliar las organizaciones y expertos dedicados y facilitar la colaboración con el sector privado para establecer un sistema de autogestión de la seguridad en el sector público.

f) Mejorar la defensa de la ciberseguridad nacional para responder activamente a las amenazas de las redes de información y comunicaciones en las entidades públicas del Estado.

g) Crear la Secretaria de Ciberseguridad Nacional, y a través de ella supervisar la cooperación público-privada-militar, para lo cual se desarrollarán e implementarán políticas de ciberseguridad a nivel nacional.

2. Construir y facilitar una información a nivel nacional con sistema de reparto

a) Construir un sistema nacional de intercambio de información entre los sectores: público, privado y de defensa para facilitar el intercambio de información sobre las amenazas cibernéticas.

b) Desarrollar medidas para compartir al máximo la información sobre las ciberamenazas en los sectores público, privado y militar, y mejorar el funcionamiento de estos sistemas.

c) Elaborar medidas legales para garantizar la confidencialidad y evitar usos no previstos, como la violación de la privacidad cuando se comparte información.

d) Promover activamente el intercambio de información con organizaciones especializadas en el extranjero y compartir la información pertinente con las organizaciones nacionales para responder a las amenazas cibernéticas transnacionales.

3. Reforzar el fundamento jurídico de la ciberseguridad.

a) Mejorar las leyes y las instituciones con el fin de responder sistemáticamente a las amenazas de la ciberseguridad, maximizando las capacidades de ciberseguridad en los sectores público, privado y militar, y concentrar las capacidades nacionales.

b) Elaborar medidas legales que permitan obligatoriamente compartir, analizar y utilizar sistemáticamente la información sobre las ciberamenazas entre los sectores público, privado y militar.

c) Fortalecer la base jurídica para responder al cambiante entorno de ciberseguridad, como la aparición de nuevas vulnerabilidades debidas a la utilización de la tecnología de inteligencia artificial.

B. ***Construir las bases para el crecimiento del Sistema de Ciberseguridad Nacional***. Crear un ecosistema innovador para la ciberseguridad a fin de garantizar la competitividad de la tecnología, los recursos humanos y las industrias que son fundamentales para la ciberseguridad nacional.

1. Ampliar la inversión en ciberseguridad.

a) Promover la reforma reglamentaria y el apoyo para permitir que el sistema de ciberseguridad desempeñe un papel clave en la mejora del nivel de ciberseguridad del país.

b) Incrementar progresivamente el presupuesto del gobierno orientado a la ciberseguridad y concebir medidas de financiación que puedan

utilizarse en situaciones de emergencia, por ejemplo, para responder a ataques cibernéticos masivos.

c) Promover el sistema de "notificación pública de la seguridad de la información" para fomentar la inversión en el sector privado y ampliar el apoyo fiscal a las inversiones en sistemas de seguridad e I+D.

2. Fortalecer la competitividad de la seguridad, mano de obra y tecnología

   a) Potenciar la experiencia y competitividad del personal de ciberseguridad del sector público con la capacitación permanente.

   b) Fortalecer los programas personalizados de desarrollo de personal para proporcionar a las empresas, el gobierno, FF.AA. y la sociedad una fuerza laboral cibernética equipada con diversas capacidades.

   c) Dictar medidas para mejorar los conocimientos especializados en materia de ciberseguridad y contratar a personal con talento.

   d) Incrementar significativamente el presupuesto de I+D en ciberseguridad para reducir nuestras brechas tecnológicas con los países desarrollados y adquirir tecnologías innovadoras de fuentes básicas para liderar el mercado mundial.

3. Fomentar un entorno de crecimiento para las entidades de ciberseguridad.

   a) Fomentar un entorno de cooperación entre la industria, sistema educativo e instituciones de investigación.

   b) Promover el apoyo gubernamental y la mejora continua de los planes para fomentar la creación de nuevas organizaciones de ciberseguridad.

   c) Fortalecer la competitividad global de la ciberseguridad nacional mediante el fomento de asociaciones estratégicas con entidades

internacionales para intercambio de experiencias y conocimientos técnicos.

4. Establecer un principio de competencia ética en las actividades de ciberseguridad.

   a) Incrementar la capacidad tecnológica de los sistemas de ciberseguridad del Estado con adquisiciones basadas en la calidad de los equipos y no en el precio.

   b) Proponer procedimientos y normas para el establecimiento de los servicios particulares de ciberseguridad y de sus contrataciones de parte de entidades del Estado.

C. Fomentar una cultura de ciberseguridad. La población debe reconocer la importancia de la ciberseguridad y esforzarse por aplicar normas básicas de seguridad, y el gobierno debe respetar los derechos fundamentales de los ciudadanos al aplicar las políticas y facilitar la participación ciudadana.

1. Incrementar la conciencia de ciberseguridad y reforzar prácticas de ciberseguridad.

   a) Definir principios y normas de ciberseguridad para que la población pueda ser consciente de la importancia de la ciberseguridad y ponerlas en práctica en su vida diaria.

   b) Desarrollar y ejecutar programas educativos de cibernética y seguridad adaptados en sectores específicos de la sociedad, tales como estudiantes, funcionarios gubernamentales, personal militar y empleados del Estado.

   c) Fortalecer el concepto de la importancia de la seguridad de las informaciones en todas las entidades públicas y privadas, así como en las FF.AA.

2. Asegurar que los derechos fundamentales no sean afectados por la ciberseguridad.

a) Asegurar que el Perú cuente con un ciberespacio libre y abierto, respetando los derechos y la privacidad del pueblo.

b) Establecer procedimientos para promover la participación de los sectores público y privado, así como de las FF.AA. en el proceso nacional de elaboración de las políticas de ciberseguridad.

c) Mantener informado a los diferentes sectores, público y privado, sobre los riesgos e incidentes de ciberseguridad que afectan la seguridad nacional.

6.3 Línea de Acción o Fase II

Comprende replantear de manera constante una nueva vía o curso de acción para aumentar la infraestructura de seguridad nacional. El Gobierno deberá ejercer el liderazgo y cumplir con sus responsabilidades para alcanzar la visión y los objetivos de la estrategia nacional de ciberseguridad en cooperación con sus ciudadanos y empresas, así como con la comunidad internacional.

Establecer y llevar a cabo el plan básico nacional de ciberseguridad y el plan nacional de implementación de la ciberseguridad (nivel táctico y operacional) para dar forma e implementar esta estrategia con proporcionalidad, racionalidad y eficacia, en la cual cada ministerio y organismo debe perseguir los objetivos establecidos en dicha estrategia, cumplir con los principios básicos y llevar a cabo las tareas estratégicas de promoción de las leyes, instituciones y políticas relacionadas con la ciberseguridad, acorde a las siguientes medidas:

d. El incremento de la seguridad en la infraestructura nacional.

e. La mejora en la capacidad de respuesta a los ataques cibernéticos.

Figura 12. Fase II
Fuente: Diseño propio

D. Incrementar la seguridad de la infraestructura central nacional. Amerita tanto reforzar la seguridad como la resistencia de la infraestructura básica nacional frente a los ataques cibernéticos para garantizar la prestación continua de servicios esenciales, para ello es menester:

1. Asegurar la seguridad de la información nacional y redes de comunicación

    a) Implementar medidas de seguridad por etapas para garantizar que las redes nacionales de información y comunicaciones estén protegidas contra las ciberamenazas en toda entidad del Estado, garantizar la operación y la eliminación de la amenaza.

    b) Desarrollar sistemas para ejecutar fiscalizaciones y mejoras permanentemente a fin de detectar y prevenir cualquier amenaza de vulnerabilidad de seguridad en la red nacional de información y comunicaciones, así como en las redes y equipos conexos.

    c) Adoptar medidas de control estrictas para asegurar el funcionamiento de las redes nacionales de información y comunicaciones, incluyendo los sistemas de rendimiento avanzados

y las instalaciones ampliadas de respaldo, a fin de garantizar la prestación de servicios frente a los diversos ataques cibernéticos.

d) Mejorar los sistemas de seguridad de información, tanto criptográfica como confidencial, para que la información confidencial en general esté protegida contra filtraciones o daños en los datos.

e) Incrementar la capacidad tecnológica y potencial humano del PCERT que permita sea el centro nacional líder e integrador en la gestión de los incidentes informáticos del sector público, privado y de las FF.AA.

2. Mejorar el entorno de ciberseguridad en las infraestructuras críticas.

a) Mejorar los planes para permitir que el Gobierno designe y proteja rápidamente las instalaciones en infraestructuras críticas cuya interrupción en caso de ataque perturbe considerablemente la vida cotidiana de la población.

b) Apoyar a las instituciones que gestionan infraestructuras críticas, para crear departamentos dedicados a la ciberseguridad y asignar un presupuesto suficiente para ello como prioridad del Estado.

c) Suscribir directrices para que las instituciones asuman prioritariamente la seguridad de la infraestructura crítica para el establecimiento y creación de planes pertinentes e inspección.

d) Fomentar un entorno que permita realizar evaluaciones voluntarias e inopinadas de seguridad a las redes o equipos de red e información de las infraestructuras que son críticas del sector privado.

e) Diseñar e implementar procedimientos de evaluación de las vulnerabilidades de la seguridad específicas en cada sector y aplicar medidas correctivas para garantizar la continuidad de los servicios en caso de que se produzca un incidente de seguridad.

3. Diseñar e implementar un sistema de ciberseguridad nacional de alta tecnología.

    a) Ejecutar planes técnicos o multisectoriales para responder eficientemente a las nuevas amenazas contra la seguridad nacional provocadas por la convergencia tecnológica y el advenimiento de nuevas tecnologías en el ciberespacio.

    b) Implementar la "seguridad desde el diseño" del software y servicios de las TIC que pueden afectar directamente a la integridad de las personas, lo que permitirá garantizar su seguridad.

    c) Desarrollar e implementar redes informáticas de alta seguridad en las infraestructuras críticas, que aseguren la eficiente operación y funcionamiento como parte de la seguridad nacional.

    d) Diseñar e implementar a nivel nacional un sistema de autenticacion digital único que permita la utilización de los servicios de las infraestructuras críticas en seguridad.

E. Mejorar las capacidades de respuesta a ataques cibernéticos, implica ampliar la capacidad para vislumbrar eficazmente los ataques cibernéticos por adelantado y conseguir lo antes posible la resiliencia.

1. Asegurar la prevención de los ciberataques.

    a) Contar con capacidades para responder activamente (Defensa pasiva) a todos los ataques cibernéticos que infrinjan la seguridad y los intereses nacionales concentrando las capacidades nacionales.

    b) Fortalecer la capacidad preventiva mediante la creación de un sistema de monitoreo nacional que recopile, gestione y elimine eficazmente las vulnerabilidades del ciberespacio.

    c) Adquirir capacidades técnicas y tecnológicas para analizar y determinar las causas de los ciberataques e identificar la fuente.

2. Reforzar las medidas defensivas contra los ataques cibernéticos masivos.

    1) Evaluar y mejorar el sistema de intercambio de información, investigación, análisis forense y respuesta de los organismos pertinentes en relación con un ataque o crisis cibernética.

    2) Incrementar la capacidad de detección de ciberamenazas para permitir la alerta y el bloqueo en tiempo real, y desarrollar tecnologías de respuesta basadas en la IA.

    3) Mejorar las capacidades de respuesta frente a las crisis cibernéticas en todo el país mediante ejercicios conjuntos público-privados-militares, incluidos ejercicios nacionales de gestión de crisis.

    4) Propiciar y facilitar la cooperación público-privada-militar, incluyendo los deberes de emitir alertas de crisis cibernéticas, compartir información sobre amenazas y realizar exámenes e investigaciones conjuntas.

    5) Normar y establecer la clasificación cuantitativa y la categorización de las alertas de una cibercrisis, que permitan a los individuos, las empresas y el gobierno una respuesta a la crisis de acuerdo a protocolos establecidos con prontitud y eficiencia.

3. Coordinar permanentemente con las FF.AA. (Comando Operacional de Ciberdefensa del CCFFAA) sobre las respuestas activas para ataques cibernéticos.

    a) Revisar y alinear todos los medios de respuesta con las normas internacionales en caso de amenaza importante para la ciberseguridad y ciberdefensa y planificar medidas específicas de manera conjunta con las FF.AA.

    b) Desarrollar varias estrategias y tácticas, a través de los Comandos de Ciberdefensa de las FF.AA. y adquirir tecnologías básicas para

salvaguardar la seguridad nacional y los intereses en la guerra cibernética.

c) Capacitar a especialistas militares en guerra cibernética y apoyar la conformación de unidades de respuesta para llevar a cabo actividades de ciberdefensa de manera eficiente y coordinada con la ciberseguridad.

4. Mejorar las capacidades de respuesta contra la ciberdelincuencia.

   a) Fortalecer la gestión de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la PNP, responsable de investigar los delitos cibernéticos y establecer una red de seguridad cibernética, con la participación de todos los organismos, empresas, organizaciones e individuos pertinentes.

   b) Mejorar la capacidad del Gobierno para identificar, localizar, detener y enjuiciar a los autores de delitos cibernéticos mediante el potenciamiento de los conocimientos técnicos especializados de los responsables de investigar esos delitos, así como asegurar la cooperación con los organismos pertinentes en el país y en el extranjero.

6.4 Línea de Acción o Fase III

Corresponde a la revisión de todos los aspectos comprendidos en las fases previas, proceso que pretende alcanzar la revisión de protección de la información mediante la prevención, detección y respuesta a los ataques, para así evaluar las políticas que permitan liderar la cooperación internacional en materia de ciberseguridad.

La Oficina de Ciberseguridad Nacional, señalada en la fase II, deberá supervisar periódicamente la aplicación de esta estrategia y las mejoras de ciberseguridad de las personas, empresas y entidades gubernamentales; Además, deberá examinar tanto la idoneidad del marco de ciberseguridad necesario para aplicar la estrategia como la eficacia de las estrategias de ejecución e

implementación de la ciberseguridad a la luz de los cambios en el entorno de seguridad, subsanará las deficiencias, tomando siempre en consideración a lo reflejado por deficiencias en la estrategia, perseverando la inserción de mejoras cuando sea necesario, conforme a la siguiente medida:

Figura 13. Fase III
Fuente: Diseño propio

F. Enriquecer los sistemas de cooperación bilateral y multilateral. Cooperación internacional tanto pública como privada necesaria en virtud de la propia naturaleza de las amenazas, para el monitoreo y evaluación de las políticas públicas de ciberseguridad, impulsando la innovación y el desarrollo económico en materia de ciberseguridad a través de la promoción del debate multilateral y bilateral basada en relaciones fluidas en el ámbito de la ciberseguridad y orientada hacia la construcción de capacidades, lo que permite, además, fomentar un criterio unificado de normas internacionales que promuevan la confianza y seguridad en el ciberespacio.

1. Explorar medios que permitan la cooperación práctica (bilateral y multilateral) para así establecer sistemas de asistencia mutua mediante

la celebración de consultas sobre políticas cibernéticas, el fortalecimiento de la asociación con organizaciones internacionales y la adhesión a acuerdos internacionales.

2. Promover la cooperación en sectores como la defensa nacional, la inteligencia y el sistema judicial, así como el intercambio con el sector privado para responder a las amenazas a la ciberseguridad, incluidos los actos de guerra, terrorismo y delincuencia.

3. Proporcionar mecanismos que permitan a los entes u organismos pertinentes proponer orientaciones de política gubernamental para compartir la información recopilada durante todo el proceso de cooperación internacional.

   El desarrollar una fuerza de trabajo de ciberseguridad superior, con alianzas con países como Japón, Corea, etc., y profesionistas a nivel mundial comprometidos en la constante capacitación, creada con el fin de mitigar los riesgos de la seguridad digital, incide directamente como una gran contribución al crecimiento de la economía digital nacional, y esta a su vez permite impulsar una mayor prosperidad social y económica del país, ya que al desarrollar plenamente un vasto grupo de talentos nacionales, al mismo tiempo atraerá a los mejores y más brillantes entre los extranjeros que comparten nuestros valores, todo ello permite contar con una mano de obra altamente cualificada en materia de ciberseguridad, lo que es una ventaja estratégica para la seguridad nacional. Cumpliendo así el propósito de garantizar el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos, y seguridad nacional promovida en la Estrategia de Seguridad Nacional del Perú.

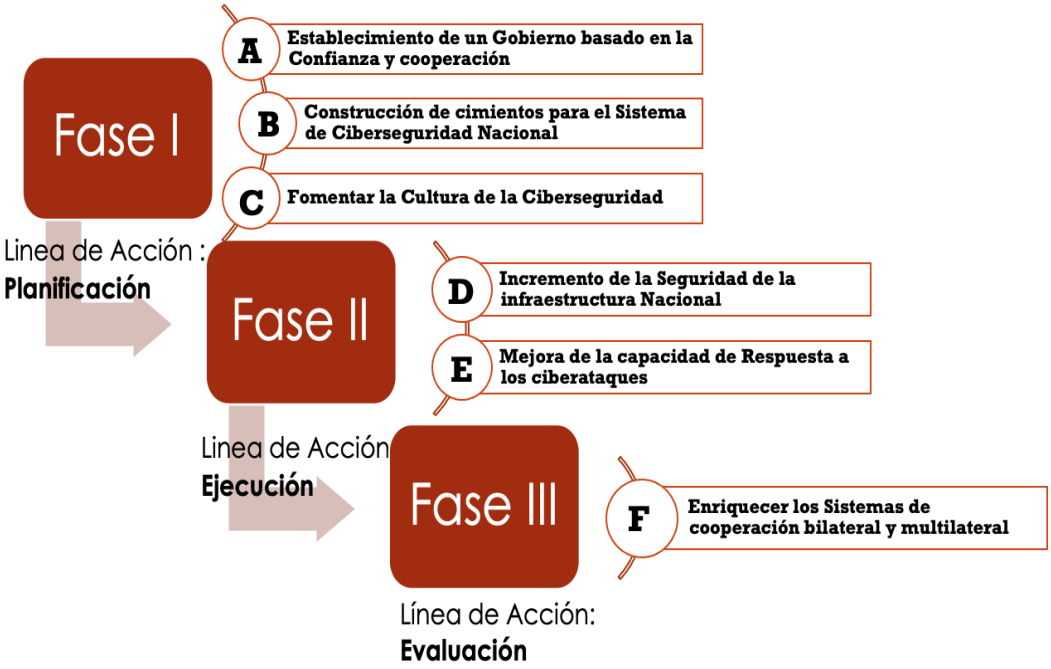

Figura 15. Lineamientos para las Estrategias Integradas de ciberseguridad
Fuente: Diseño propio

Referencias bibliográficas

Accenture Security (2016). *Generar confianza para enfrentar el problema de la ciberseguridad*. Accenture and HfS Research, Ltd. Recuperado de: https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/local/ar-es/pdf-1/accenture-building-confidence-facing-cybersecurity-conundrum-transcript-ar.pdf

Álvarez, D. (2018). *Ciberseguridad en América Latina y ciberdefensa en Chile*. *Revista chilena de derecho y tecnología*, *7*(1), 1-2. Recuperado de https://dx.doi.org/10.5354/0719-2584.2018.50416

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

Amaro, J. A. y Rodríguez, C. R. (2017). *Seguridad en internet*. *PAAKAT: revista de tecnología y sociedad*, *6* (11), 00006. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S200736072017000100006&lng=es&tlng=es.

Ballesteros (2015). *Método para el análisis de regiones geopolíticas* (marg). Revista del Instituto Español De Estudios Estratégicos (IEEE). N°6. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/5281867.pdf

Brose, C. (2019). The New Revolution in Military Affairs War's Sci-Fi Future. Foreing Affaire, 98 (3). Recuperado de: https://www.foreignaffairs.com/articles/2019-04-16/new-revolution-military-affairs

Cabrera, (2017). *Vinculaciones entre los enfoques clásicos y contemporáneos de la geopolítica y la seguridad*. URVIO, Revista Latinoamericana de Estudios de Seguridad, (20), 111-125. DOI: https://doi.org/10.17141/urvio.20.2017.2578.

Camps, P. (2016*). Ciberdefensa y ciberseguridad: Nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito.* Informe. Montevideo: Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC).

Carrillo (2018). *¿Cuánto te cuesta hoy una violación de datos?* Forbes, Recuperado de: https://www.forbes.com.mx/cuanto-te-cuesta-hoy-una-violacion-de-datos/

Claval, P. (2002). El enfoque cultural y las concepciones geográficas del espacio. *Boletín de la age*, (34), 21-39. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=660030

Coello, E., Blanco, N. y Reyes, Y. (2012). *Los paradigmas cuantitativos y cualitativos en el conocimiento de las ciencias médicas con enfoque filosófico-epistemológico*. *EDUMECENTRO*, *4*(2), 137-146. Recuperado de

http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2077-28742012000200017&lng=es&tlng=es.

Constitución Política del Perú (1993). *Ministerio de justicia.* Lima: Recuperada de: https://www.minjus.gob.pe/wp-content/uploads/2019/05/Constitucion-Politica-del-Peru-marzo-2019_WEB.pdf

Convenio contra la Ciberdelincuencia o Convenio de Budapest. Perú se acoge en (1) de febrero 2019. Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Decreto Supremo N° 050-2018-PCM. Estableció la definición de Seguridad Digital Recuperado de: https://www.gob.pe/institucion/pcm/normas-legales/3108-050-2018-pcm

Decreto Supremo N° 012-2017-DE, *Políticas de seguridad y defensa nacional* Recuperada de: https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-la-politica-de-seguridad-y-defen-decreto-supremo-n-012-2017-de-1600032-1/

Decreto Supremo N° 012-2017-DE, mediante el cual se publica la Política de Seguridad y Defensa Nacional El Peruano. Lima. Recuperado de: https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-la-politica-de-seguridad-y-defen-decreto-supremo-n-012-2017-de-1600032-1/

Decreto Supremo N° 063-2007-PCM, Reglamento de Organización y Funciones de la PCM, en el que ONGEI es el Órgano Técnico Especializado que depende jerárquicamente del Presidente del Consejo de Ministros. *El Peruano.* Lima 14 de julio de 2007. Recuperado de: http://www.pcm.gob.pe/transparencia/Doc_Gestion/DS-063-2007-PCM.pdf

Decreto Supremo N° 067-2003-PCM, Reglamento de Organización y Funciones de la PCM, en el cual se crea la ONGEI. *El Peruano.* Lima 22 de junio 2017. Recuperado de: https://www.gobiernodigital.gob.pe/normas/1934/NORMA_1934_DECRETO_SUPREMO_N%C2%B0_067_2017_PCM.pdf

Decreto Supremo N° 066-2003-PCM, mediante el cual se fusiona la Subjefatura de Informática del INEI con la PCM. *El Peruano*. Lima 22 de julio 2013. Recuperado de: http://www.pcm.gob.pe/normaslegales/2013/DS-081-2013-PCM.pdf

Dilthey (1949). *Introduccion a las Ciencias del Espíritu*, Panuco. México, Recuperado de: http://www.posgrado.unam.mx/filosofia/pdfs/Textos_2019-1/20191_Dilthey_Introduccion CienciasEspiritu.pdf

Dos Reis, A. E. y de Brito, R. (2018). No Boots on the Ground': Reflections on the US Drone Campaign through Virtuous War and STS Theories. Contexto Internacional, 40 (1), 53-71 Recuperado de: http://www.scielo.br/pdf/cint/v40n1/0102-8529-cint-2018400100053.pdf

Elizalde, I. (2016). *El "Internet Oscuro", el nuevo campo de batalla digital*. Recuperado de: https://directortic.es/seguridad/internet-oscuro-nuevo-campo-batalla-digital-2016112216962.htm

EY (2019). ¿La ciberseguridad es algo más que protección? *Encuesta Global de Seguridad de la Información 2018-19.* México: EY. Recuperado de: https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf

Ferro, G. y Castaño, Ó. A. (2017). *Geopolítica contemporánea y análisis de factores relevantes a escala global*. *Razón Crítica, 3*, 111-144. Recuperado de: DOI: http://dx.doi.org/10.21789/25007807.1235

Foro Económico Mundial (2019). *Informe Global de Riesgos 2019.* Ginebra: WEF. Recuperado de: https://www.marsh.com/uy/es/insights/research/informe-riesgos-globales-2019.html

Foro Económico Mundial (2015) *Reporte global de tecnología de la información 2015*. Recuperado de: http://www.cdi.org.pe/InformeGlobaldeInformacion/index.html

Fundación Telefónica (2016). *Ciberseguridad, la protección de la Información en el mundo digital*. Madrid, España: Editorial Ariel. Recuperado de: https://publiadmin.fundaciontelefonica.com

Gadamer, H. (1993). *Verdad y método.* Salamanca, España: Edic. Sígueme. 367 p.

Galeano, M. V. (2001). Registro y sistematización de información cualitativa. *Interacciones y Pensamientos.* Recuperado de: https://www.academia.edu/6608261/Registro_y_sistematizacion_de_informacion_cualitativa

Garamone, J. (2018). US Dept of Defense (2018). DoD Official: National Defense Strategy Will Enhance Deterrence. Recuperado de: https://www.defense.gov/Explore/News/Article/Article/1419045/dod-official-national-defense-strategy-will-enhance-deterrence/

Gestión (2018). Ciberataques al sector energético en el Perú cuestan US$ 17.20 millones al año. *Gestión, 31 de julio.* Recuperado de: https://gestion.pe/tecnologia/ciberataques-sector-energetico-peru-cuestan-us-17-20-millones-ano-240175-noticia/

Gobierno de España (2019). *Estrategia Nacional de Ciberseguridad.* Presidencia del Gobierno. Recuperado de: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Heidegger, M. (1926). *Ser y tiempo*. Edición digital. Recuperado de: http://www.afoiceeomartelo.com.br/posfsa/Autores/Heidegger,%20Martin/Heidegger%20-%20Ser%20y%20tiempo.pdf

Hernández, R., Fernández, C. Baptista, P. (2018). *Metodología de la investigación*. México: McGraw Hill. Edamsa impresiones. ISBN: 978-1-4562-6096-5.

Hobsbawm, E. (1997). *Las hegemonías de Gran Bretaña y Estados Unidos, y el Tercer Mundo*. Artículo expuesto en la conferencia dictada en el New School for Social Research, Nueva York. Recuperado de: http://biblioteca.hegoa.ehu.es/downloads/6147/%2Fsystem%2Fpdf%2F431%2Flas _hegemonias_de_Gran_Bretaña_y_EE.UU._y_el_Tercer_mundo.pdf

Instituto Nacional de Estadística e Informática-INEI. (2018). Estadísticas de las Tecnologías de Información y Comunicación en los Hogares. Recuperado de: https://www.inei.gob.pe/media/MenuRecursivo/boletines/01-informe-tecnico-n02_tecnologias-de-informacion-ene-feb-mar2018.pdf

ITU. (2018). Global Cybersecurity Index. Committed to connecting the world. Recuperado de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Křoustek, J. (2017). Ransomware de la familia Petya está usando la vulnerabilidad EternalBlue para infectar computadoras en todo el mundo. *Avastblog.com* Recuperado de: https://blog.avast.com/es/ransomware-de-la-familia-petya-est%C3%A1-usando-la-vulnerabilidadad-eternalblue-para-infectar-computadoras-en-todo-el-mundo

Lacoste, Y. (2008). *Geopolítica: la larga historia del presente*. Barcelona: Síntesis.

Lambert, C. (2006). Edmund Husserl: la idea de la fenomenología. *Teología y vida*, *47*(4), 517-529. Recuperado de: https://dx.doi.org/10.4067/S0049-34492006000300008

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

Ley de Protección de Datos Personales Nº 29733 (2011). El Peruano N° 445746. Recuperada de https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf

Ley de Delitos Informáticos Nº 30090 (2013). El Peruano N° 505484. Recuperada de https://www.peru.gob.pe/docs/PLANES/10434/PLAN_10434_2013_Ley_N%C2%B0_30096-DELITOS_INFORMATICOS.pdf

Ley 30999 o Ley de Ciberdefensa. El Peruano, Lima. 9 de agosto del 2019.

Libro Blanco de la Defensa Nacional del Perú, Ministerio de Defensa, (2005).

Marcos (2018) Ciberseguridad aplicada a la e-democracia: análisis criptográfico y desarrollo de una metodología práctica de evaluación para sistemas de voto electrónico remoto y su aplicación a las soluciones más relevantes. Publicaciones de la Universidad de León, España. Recuperada de: http://riasc.unileon.es/archivos/documentos/tesis/ Tesis_David_Y_Marcos.pdf

Machin y Gazapo (2017). *La ciberseguridad como factor crítico en la seguridad de la unión europea*. Unidad de Investigación sobre Seguridad y Cooperación

Internacional (UNISCI) N°42, Universidad Complutense de Madrid, España. Recuperada de: https://www.ucm.es/unisci/revista-n-42

Ministerie van Defensie Neatherland (2018)). Defensie Cyber Strategie 2018 Investeren in digitale slagkracht voor Nederland. Recuperado de: https://www.defensie.nl/binaries/defensie/documenten/publicaties/2018/11/12 /defensie-cyber-strategie-2018/web_Brochure+Defensie+Cyber+Strategie.pdf

Navarrete, F. (2014). El ciberespacio: Nuevo escenario de confrontación. *Anuario mexicano de derecho internacional*, *14*, 863-868. Recuperado en 15 de octubre de 2019, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-46542014000100027&lng=es&tlng=es.

Marks, P. (2010). Stuxnet: the new face of war. *New Scientist, 208*: 26-27. Recuperado de: https://doi.org/10.1016/S0262-4079(10)62459-1

Nagurney, A. y Shukla, S., (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability, *European Journal of Operational Research,* 260: 588–600. DOI: https://doi.org/10.1016/j.ejor.2016.12.034

NATO (2016). NATO Summit Warsaw 2016. Recuperado de: https://www.nato.int/cps/en/natohq/events_132023.htm

Orden Ejecutiva N° 13800 (2017). Fortalecimiento de la ciberseguridad de las redes federales e infraestructura crítica. Recuperada de: https://www.icex.es /icex/GetDocumento?dDocName=DOC2019822789&urlNoAcceso=/icex/es/registro/iniciar-sesion/index.html?urlDestino=https://www.icex.es:443/icex/es /navegacion-principal/todos-nuestros-servicios/informacion-de-mercados/ estudios-de-mercados-y-otros-documentos-de-comercio-exterior/DOC 2019822789.html&site=icexES

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

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

Parada, D.J., Flórez, A. y Gómez, U.E. (2018). Analysis of the Components of Security from a Systemic System Dynamics Perspective. *Información tecnológica*, *29* (1): 27-38. https://dx.doi.org/10.4067/S0718-07642018000100027

Pastor, O., Pérez, J., Arnaíz, D. y Taboso, P. (2009). *Seguridad nacional y ciberdefensa.* 1ra ed. Madrid: Fundación Rogelio Segovia para las telecomunicaciones.

Piedra, D. (2011). Definición de cibernética. *ACIMED 22* (3): 271-281. Recuperado de: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352011000300008&lng=es.

Congreso de la República. (2018). *Plan Nacional de Ciberseguridad.* Recuperado de: http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Pol%C3%ADtica_Nacional_de_Ciberseguridad_peru.pdf

Presidencia del Consejo de Ministros (2012). Plan Nacional de Gobierno Electrónico, ONGEI. Recuperado de: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/54A7FF44FD2DF7F605257C1200108C2B/%24FILE/10492a55-a315-453e-8fdc-2c908b422d18.pdf

Presidencia del Consejo de Ministros (2012ª). *PeCERT ingresa a la comunidad internacional de CERT y es reconocido como CSIRT nacional para el capítulo Perú.* Recuperado de: https://www.gobiernodigital.gob.pe/noticias /segdi_ noticias_detalle.asp?pk_id_noticia=367

Presidencia del Consejo de Ministros (2018). *Política Nacional de Ciberseguridad.* Recuperado de: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf /54A7FF44FD2DF7F605257C1200108C2B/%24FILE/10492a55-a315-453e-8fdc-2c908b422d18.pdf

Raffestin, C. (2011). *Por una geografía del poder*. Michoacán. Editorial Colegio de Michoacán.

Ratzel, F. (1987). Las leyes del crecimiento espacial de los Estados. *Geopolíticas*, 2, 135-156

Reglamento General de Protección de Datos (GDPR) de la Unión (2018). Web oficial de la Unión Europea. Recuperado de: https://ec.europa.eu/commission/ priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_es

Robinet (2011). *Tradición e historia de la filosofía: la concepción cibernética de A. Robinet.* Recuperado de: https://revistas.ucm.es/index.php/ASEM/article/ download /ASEM9292220853A/ 17636

Rollano, R (2012) *Ataques a la seguridad informática y telecomunicaciones en el contexto internacional*. Artículo publicado en La Razón/Gaceta Jurídica. Recuperada de: https://www.la-razon.com/la_gaceta_juridica/Ataques-seguridad-informaticatelecomunicaciones-internacional1_0_1687031396.html

Roperts, N. (2008). *Transformación sistémica de conflictos: reflexiones acerca del conflicto y del proceso de paz en Sri Lanka*. Berghof Research Center for Constructive Conflict Management. Recuperado de: https://www.berghof-foundation.org/fileadmin/redaktion/Publications/Handbook/Dialogue_Chapters/spanish_ropers_dialogue6_lead.pdf

Rubio, G.J. (2017). *Política de ciberseguridad comparada entre Argentina y Brasil*. Tesis de Maestría. Bs As, Argentina: Universidad de la Defensa Nacional. Recuperado de:

https://www.academia.edu/35640526/Pol%C3%ADtica_de_ciberseguridad_comparada_entre_Argentina_y_Brasil

Ruedas Marrero, M., Ríos Cabrera, M. M. & Nieves, F. (2009). Hermenéutica: La roca que rompe el espejo. *Investigación y Postgrado*, *24*(2), 181-201. Recuperado de: http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1316-00872009000200009&lng=es&tlng=es.

Sanguin, A. (1981). *Geografía política*. Barcelona: Oikos Tau.

SEDENA (2014). Estudio prospectivo de la seguridad y defensa nacional al 2030. Lima.Recuperado de: https://es.calameo.com/read/00566600762a706c3e84f

Socarrás, H.E. , & Santana, I. (2019). Ciberseguridad del Sistema de Control Industrial de la Planta Cloro-Sosa ELQUIM. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (32), 83-6. https://dx.doi.org/10.17013/risti.32.83-96

Seclén, J. A. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001.* Tesis de Maestría. Lima: Universidad Nacional Mayor de San Marcos. Recuperado de: http://cybertesis.unmsm.edu.pe/handle/cybertesis /4884

Taipe, I.D. (2017). *La auditoría de seguridad informática y su relación en la ciberseguridad de la Fuerza Aérea del Perú año 2017*. Tesis Doctoral. Lima: Fuerza Aérea del Perú. http://repositorio.fap.mil.pe/bitstream/handle/fap/49/ARTICULO%20TESIS%20OK.pdf?sequence=1&isAllowed=y

US Departament of Defense. National Defense Strategy. Recuperado de: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Vargas, R., Recalde, L. y Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO, Revista Latinoamericana de Estudios de Seguridad,* (20). Recuperado de: https://www.redalyc.org/jatsRepo/5526/552656641013/html/index.html

Villalba, A. (2015). *"La ciberseguridad en España 2011 – 2015. Una propuesta de modelo de organización". Tesis Doctoral.* Madrid: Universidad Nacional de Educación a Distancia. Recuperado de: http://e-spacio.uned.es/fez/view/tesisuned:CiencPolSoc-Avillalba

Villanueva, Ed. (2015). La incursión digital y la política pública: nuevos actores a partir del conflicto del derecho de autor en el campo digital. Tesis Doctoral. Lima: PUCP. Recuperado de: http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/6208

Weber, M. (2010) *Conceptos sociológicos fundamentales.* España: Alianza editorial.

Anexos

Anexo 1: Matriz de consistencia

Preguntas de investigación	**Objetivos**	**Justificación**	**Observables**	**Metodología**
General	General	1. Necesidad e importancia de proteger el valor de la información estratégica y crítica del Estado. 2. Necesidad e importancia de proteger el valor de la información publicadas por los peruanos en la red. 3. El imperativo que cada sector del Estado sea responsable del uso que hace de la red. 4.Importancia de evitar los delitos cibernéticos y las posibles amenazas que pueden ser desde las que afectan a la seguridad nacional. 5.Necesidad de consolidar una entidad u organización responsable de la normatividad y del planeamiento la Estrategia Integrada de ciberseguridad.	Categoría N° 1.- Estrategias integradas internacionales de ciberseguridad: • Protección: • Enfoque: • Sector público: • Sector privado: Participación en la estrategia. • Cooperación internacional Categoría N° 2.- Estrategias integradas de ciberseguridad en el ámbito de seguridad nacional del Perú. • Protección: • Enfoque: • Sector público: • Sector privado: Participación en la estrategia. • Cooperación internacional	Enfoque: Cualitativo
¿Cuáles son las estrategias de ciberseguridad necesarias para fortalecer la seguridad nacional en el Perú 2020?	Cuáles son las estrategias de ciberseguridad necesarias para fortalecer la seguridad nacional en el Perú 2019			
Específicas	Específicos			Tipo: • Descriptivo. • Analítico. • Propositivo
¿Cuáles son las estrategias integradas de ciberseguridad más eficientes implantadas en tres países seleccionados al 2019?	Analizar las estrategias integradas de ciberseguridad más eficientes implantadas en tres países seleccionados al 2019.			
¿Cuál es el marco normativo legal respecto a la ciberseguridad en el Perú, 2019?	Evaluar el marco normativo legal respecto a la ciberseguridad en el Perú, 2019.			Método: Hermenéutico
¿Cuáles son los límites referentes al desarrollo de la ciberseguridad en el Perú, 2019?	Identificar las limitaciones referentes al desarrollo de la ciberseguridad en el país.			
¿Cuáles son las brechas en materia de desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú, 2019?	Establecer las brechas en materia de desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad en el Perú, 2019			Escenario: Países Bajos, EE.UU., España y Perú.
¿Cómo se pueden abordar las brechas para optimizar el desarrollo, evaluación y actualización de la estrategia integrada de ciberseguridad en el Perú, 2019?	Abordar las brechas para optimizar el desarrollo, evaluación y actualización de una estrategia integrada de ciberseguridad.			Fuentes: • Legislación. • Doctrina. • Convenios. • Estructuras Organizativas • Informes de Gestión

Anexo 2: Instrumentos de acopio de información

A.- Modelo de Ficha de Registro

<table>
<tr><td rowspan="2">Localización</td><td>Virtual</td><td>Url:
https://www.redalyc.org/jatsRepo/5526/552656641013/html/index.html</td></tr>
<tr><td>Física</td><td>Biblioteca:</td></tr>
<tr><td colspan="3">Descripción: Vargas, R. , Recalde, L. y Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, Revista Latinoamericana de Estudios de Seguridad, (20).</td></tr>
<tr><td colspan="2" rowspan="3">Contenido:

La seguridad del ciberespacio no solo constituye una necesidad individual o propia de las compañías, sino que también es un asunto de seguridad y soberanía nacional que influye en la gobernanza nacional (Choucri 2013), en la política nacional e internacional en diferentes grados (Nye Jr. y Welch 2013), en la integridad de la economía y en la protección de la información de sus ciudadanos (Government of Canada 2010). El Estado y sus instancias regionales deben afrontar el reto de la seguridad y defensa del ciberespacio, así como proteger y garantizar el acceso, uso y contenidos a la sociedad civil en el ámbito virtual, siendo conscientes de su repercusión local, nacional y global.</td><td>Palabras clave:
Ciberseguridad
Ciberdefensa
Estrategias</td></tr>
<tr><td>Subcategoría: Protección</td></tr>
<tr><td>Indicador: Seguridad y Defensa</td></tr>
<tr><td colspan="3">Observaciones:
Definiciones y estructura del modelo de ciberdefensa del Ecuador explicando los actores participantes en el proceso de diseño de políticas públicas de ciberseguridad.</td></tr>
<tr><td colspan="2">Tipo de Ficha: Textual</td><td>Investigador: Ormachea, Juan</td></tr>
</table>

B. Modelo de Ficha de Análisis

SUBCATEGORÍA	INDICADOR	PAÍSES BAJOS	EE.UU.	ESPAÑA	PERÚ
PROTECCIÓN	Infraestructuras Críticas				
	Economía				
	Seguridad Nacional				
	Bienestar Social				
ENFOQUE	Concientización				
	Educación				
	Capacidades Cibernéticas Militares				
SECTOR PÚBLICO	Liderazgo y Coordinación				
SECTOR PRIVADO	Participación en la estrategia				
COOPERACIÓN INTERNACIONAL	Cooperación con otros países				

Anexo 3: Autorización de acceso de campo

Anexo 4: Autorización para el levantamiento de información

Anexo 5: Diagrama de investigación