Vol. 1, N° 4, Julio - Octubre 2020 https://bit.ly/37fM6Ef

Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional

Integrated cybersecurity strategies for strengthening national security

Juan Fernando Ormachea Montes[1]

correo: juanferor@gmail.com. **ORCID: https://orcid.org/0000-0002-9119-8846**

PP. 36 - 48

Recibido 03/08/2020 Aceptado 03/09/2020 Publicado 17/10/2020

Resumen

Esta investigación tuvo como objetivo el proponer estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad nacional del Perú. La investigación fue de tipo descriptiva y con enfoque epistemológico; además, el diseño fue no experimental y propositivo. La población estuvo conformada por las estrategias y políticas actuales utilizadas en el ámbito internacional para contrarrestar las ciberamenazas, y la muestra estuvo constituida por las estrategias de ciberseguridad implementadas por los Países Bajos, EE. UU., España y Perú. Las técnicas de recolección de datos fueron la observación y el análisis documental; mientras que los instrumentos utilizados fueron la ficha de registro y la ficha de análisis. Se encontró que, en los indicadores referidos a cooperación regional, bilateral y multilateral, el Perú ha manifestado comportamientos disímiles; además, 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. Por ello, se concluyó que la ciberseguridad constituye un compromiso social que demanda 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.

1 Doctor en Desarrollo y Seguridad Estratégica, CAEN

PALABRAS CLAVE: CIBERSEGURIDAD, CIBERAMENAZAS, ESTADO, SEGURIDAD NACIONAL.

Abstract

This research aimed to propose integrated cybersecurity strategies needed to strengthen Peru's national security. The research was descriptive and epistemologically focused; in addition, the design was non-experimental and purposeful. The population was made up of the current strategies and policies used in the international arena to counter cyberthreats, and the sample was made up of the cybersecurity strategies implemented by the Netherlands, the United States, Spain, and Peru. The data collection techniques were observation and document analysis; while the instruments used were the registration sheet and the analysis sheet. It was found that, in the indicators referring to regional, bilateral and multilateral cooperation, Peru has manifested dissimilar behaviors; furthermore, the Peruvian state and society still transit through the approaches of awareness and development of military cybernetic capabilities, as prevalent indicators in the design of national cybersecurity policies. Therefore, it was concluded that cybersecurity constitutes a social commitment that demands articulation between the public and private sectors, which in Peru is not yet concrete; consequently, the design of the National Cybersecurity Strategy of Peru constitutes a need that demands to be satisfied.

KEYWORDS: CYBERSECURITY, CYBERTHREATS, STATE, NATIONAL SECURITY.

Introducción

El avance tecnológico en el ámbito comunicacional ha representado un reto para la seguridad y defensa de los Estados, pues a la vez que ha tenido un amplio desarrollo, también ha traído consigo grandes desafíos, donde los actores políticos, en todos los niveles, deben asumir la responsabilidad de la seguridad y defensa del país, siendo un reto fundamental, la contención de las amenazas que provienen del ciberespacio, ya que este representa una novedosa plataforma donde la vida de las naciones transcurre más allá del plano físico, pero que ha demostrado ser capaz de alterar la realidad en dicho plano.

Nagurney y Shukla (2017) señalan que las nuevas tecnologías de información y comunicación han dado origen al ciberespacio (Internet). Este constituye el quinto dominio de interacción humana y cada día se hace más extenso, albergando gran cantidad de información y brindando amplia variedad de servicios. Como resultado, este espacio ha dado lugar a la aparición de nuevas amenazas creadas por individuos, organizaciones o Estados, que buscan aprovecharse de esta novedosa forma virtual de interactuar. Las actividades ilícitas en este medio pueden causar efectos negativos en la víctima y reportar sustanciales beneficios al perpetrador, quien, generalmente, no logra ser identificado por las autoridades. Por ello, 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.

Es preciso señalar que, a nivel global, existe dependencia de los Estados respecto a sistemas de información, constituyendo la gran fortaleza de los mismos, así como también su gran debilidad. Sin embargo, a pesar de los riesgos que conlleva una sociedad cada vez más interconectada, esta tendencia es imparable, lo que significa

que se debe afrontar el futuro y gestionar los riesgos derivados de estos (Parada, Flórez y Gómez, 2018). El contexto a raíz de las amenazas del ciberespacio es variado, ya que se puede observar una mayor y más compleja actividad criminal desarrollada por grupos organizados y por delincuentes individuales, así como mayor actividad de espionaje, ya sea industrial, militar o político; 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 (Singh et al., 2018). Como dato no menor, se puede observar una mayor participación de individuos en acciones maliciosas, ya sea por ignorancia, curiosidad, diversión, reto o 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 esta clase de actividades.

Los ciberataques son una realidad que, potencialmente, puede destruir en cuestión de horas, la economía, las instituciones y las estructuras de los Estados vulnerables, ya que la interconexión global genera riesgos que se constituyen en peligros inminentes de ser ejecutados por ciberterroristas o, incluso, por *hackers,* quienes experimentan con nuevas herramientas de *software* sin medir la destrucción que pueden causar. Como reacción a esta avalancha de 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 corresponde al desarrollo de capacidades y habilidades en la prevención, defensa, detección, análisis, investigación, recuperación y respuesta a las amenazas, así como también la gestión de riesgos asociados. En ese orden de ideas, es indispensable que los Estados asuman la responsabilidad de contener las amenazas potenciales y reales, lo que ha derivado en 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; ya que esta representa un reto de competencia mundial.

El Perú es un país con escasa conciencia en términos de protección y riesgos en materia de seguridad informática; además, es uno de los países que menos ha legislado en temas de seguridad de la información y seguridad informática y, sobre todo, en planeamiento de ciberdefensa y ciberseguridad. Cabe indicar que estos términos no solamente hacen referencia a proteger una página web, sino también a contar con estrategias de seguridad nacional; como se ha señalado, la ciberseguridad es parte de la seguridad nacional, 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.

Establecer estrategias nacionales e integrales de ciberseguridad en un país está relacionado, necesariamente, con 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. En ese sentido, se revisó el estudio de Machín y Gazapo (2016), quienes tuvieron como objetivo presentar estrategias de ciberseguridad que sean realmente capaces de integrar a las diferentes estrategias nacionales para Europa; concluyendo 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, se comprueba lo dañinos que son; por ello, proponen desarrollar recursos de carácter digital en colaboración con empresas públicas y privadas, para proteger las infraestructuras criticas; además, la protección del ciberespacio no debe dañar la libertad ni los derechos de los usuarios.

Por otro lado, se tomó en cuenta la investigación de Camps (2016), destacando que Uruguay ha modernizado su

marco legal y terminado con las amenazas provenientes del ciberespacio, sobre todo las que pueden afectar el bienestar de la población, pasando esta a ser objeto de la defensa nacional. Estas acciones han sido evaluadas positivamente por el Banco Interamericano de Desarrollo y la Organización de Estados Americanos. Finalmente, en el ámbito internacional, Villalba (2015) desarrolló una investigación enfocada en proponer modelos de gobernanza en el ámbito de la ciberseguridad en España, resaltando propuestas de políticas estructuradas en materia de ciberseguridad y recomendando crear el más alto nivel organizacional para enfrentar las nuevas amenazas. Cabe destacar que este estudio identificó como aspecto primordial fomentar el gobierno electrónico y, a la vez, estructurar a nivel nacional, redes que permitan brindar seguridad cibernética y garantizar el uso de los recursos reales y virtuales.

En el ámbito nacional, se revisó la investigación de Taipe (2018), quien determinó que el nivel de conocimiento del personal de las áreas de computación, informática y diseño de políticas de seguridad, de la Fuerza Aérea del Perú, posee bajos niveles de conocimiento de ciberseguridad. Asimismo, Rodríguez (2017) realizó una investigación, con el fin de establecer los mecanismos implementados por los países para el logro de una serie de objetivos establecidos por una doctrina política, concluyendo que la innovación consiste en la relación temporalmente determinada que existe entre los medios y los fines, con el argumento de que, en China, la conformación y desarrollo del Sistema Nacional de Innovación (SNI) ha permitido comprender las nuevas tecnologías, procesarlas y producir nuevos medios de diversa índole, concluyendo que existe una relación interdependiente en la creación de conocimiento, que implica la obtención de conocimientos y tecnologías de otros países. Además, se tomó en cuenta el estudio de Seclén (2016), quien determinó que es necesario encontrar un punto de equilibrio entre el lineamiento 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 Norma Técnica Peruana (NTP) ISO/IEC 27001, y cómo estos terminan afectando a la gestión de los procesos de negocio de las organizaciones.

Asimismo, es preciso resaltar la reciente promulgación de la Ley N.º 30999, Ley de *Ciberdefensa,* la cual constituye un avance en el tema de ciberseguridad y ciberdefensa; no obstante, es indispensable establecer un diagnóstico eficiente en materia de 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. Por ello, este estudio tuvo como objetivo principal proponer estrategias integradas de ciberseguridad, necesarias para fortalecer la seguridad nacional del Perú.

GEOPOLÍTICA Y CIBERAMENAZAS

Ferro y Castaño (2017) definen la geopolítica como la disciplina que estudia las relaciones de poder entre actores de todo tipo, quienes desarrollan acciones orientadas a ejercer el dominio sobre territorios y poblaciones. Entonces, la geopolítica triangula la toma de decisiones, el territorio y el espacio, donde las decisiones políticas son inherentes, tanto a actores estatales como no estatales.

Históricamente, la geopolítica ha experimentado cambios en relación con su objeto de estudio, ya que este se transforma en una dinámica constante. Al respecto, Cabrera (2017) indica que la geopolítica y seguridad clásica incluía como actores al Estado y al sistema internacional, siendo su objeto de estudio el Estado y las amenazas convencionales, quienes tenían como finalidad prever amenazas y disuadirlas; sin embargo, actualmente, los nuevos enfoques de seguridad tienen como objeto de estudio la percepción de inseguridad en la sociedad, por lo cual, la finalidad es analizar la naturaleza del proceso conflictivo con base en múltiples actores.

Actualmente, el avance tecnológico ha propiciado que el mundo de las tecnologías de información y comunicación (TIC) genere esferas de conflictos y amenazas, las cuales fueron identificadas por el Foro Económico Mundial (2019), siendo los principales riesgos actuales, jerárquicamente, los siguientes: confrontación entre potencias por temas económicos; erosión de los acuerdos multilaterales; confrontaciones políticas entre las mayores potencias; ciberataques, plataformas comerciales y fatos; interrupción en operaciones e infraestructura; pérdida de confianza en la seguridad colectiva; populismo y agendas étnicas; noticias falsas, entre otros.

CIBERSEGURIDAD

Hoy en día, el avance tecnológico ha producido grandes beneficios, pero también diversas amenazas, puesto que se ha usado la tecnología para almacenar información de diversos ámbitos, lo que conlleva a riesgos y amenazas del ciberespacio, si estos no se aseguran eficientemente. Al respecto, Signorino (2019) señala que los riesgos "van más allá de la acción de un hacker y se relaciona con actividades informáticas ilegales para sustraer, alterar, modificar, manipular, inutilizar o destruir información o activos" (p. 38), para lo cual se utiliza medios electrónicos. A partir de ello, surge la necesidad de desarrollar la ciberseguridad, la cual, de acuerdo con la UIT (2010), se conceptualiza como el conjunto de herramientas, políticas, acciones, directrices, métodos y medidas idóneas de gestión de riesgos respecto a seguridad, utilizadas con el fin de proteger los activos de la organización y a los usuarios del ciberespacio, garantizando que se mantengan las propiedades de seguridad de los individuos, así como de las organizaciones privadas o estatales.

Vargas, Recalde y Reyes (2017) señalan que la ciberseguridad o seguridad cibernética es la suma de esfuerzos conjuntos de los organismos gubernamentales, la comunidad empresarial, organizaciones y ciudadanos, tanto a nivel nacional como internacional. Cabe destacar que, las fronteras entre seguridad externa e interna se difuminan, y las compartimiciones 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). Por su parte, Arreola (2018) también afirma lo anterior e indica, además, que los Estados enfrentan nuevos desafíos a partir del avance tecnológico, ya que, desde la perspectiva de la seguridad, esta ha acelerado procesos, pero también ha aumentado la vulnerabilidad de la seguridad e información, conllevando a que los Estados se enfoquen en buscar estrategias que salvaguarden la ciberseguridad, implementando medidas y políticas tecnológicas que incluyan a todos los actores involucrados, a fin de contrarrestar las amenazas del ciberespacio.

En vista de esta problemática, Álvarez (2018) refiere la necesidad de implementar estrategias nacionales de ciberseguridad (ENC) a nivel mundial, con las cuales se debe intentar 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. Cabe señalar que los objetivos de estas estrategias no se limitan únicamente a garantizar la seguridad de los ciudadanos y de las infraestructuras críticas del país, sino también incluyen la instauración de un ecosistema que fomente la cooperación público-privada y la internacional. Es por esta razón que la ciberseguridad es una necesidad social y económica, ya que la influencia de los sistemas de información y telecomunicaciones en la economía y en los servicios públicos, así como la estabilidad y prosperidad del Perú dependen, en buena medida, de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometidas por causas técnicas, fenómenos naturales o agresiones deliberadas.

MATERIALES Y MÉTODOS

La investigación fue de tipo descriptiva y enfoque epistemológico, puesto que se orientó hacia el establecimiento de las estrategias de ciberseguridad necesarias para fortalecer la seguridad nacional en el Perú. El diseño de la investigación fue no experimental y propositivo; mientras que el método utilizado se fundamentó en la hermenéutica; este se realizó en tres etapas: 1) exploratoria: en esta fase se identificaron las estrategias nacionales de ciberseguridad de los Países Bajos, EE. UU., España y Perú; 2) descriptiva: esta se desarrolló en dos fases o momentos metodológicos; primero, descripción de la situación actual de los Países Bajos, EE. UU., España y Perú; segundo, recopilación de las diversas experiencias en tema de ciberseguridad; 3) la fase estructural: comprendió el estudio, análisis e interpretación de los documentos y fuentes de información, nacionales e internacionales, utilizados en esta investigación.

La población estuvo conformada por las medidas, estrategias y políticas diseñadas a nivel internacional para contrarrestar las ciberamenazas; mientras que la muestra estuvo constituida por las estrategias y políticas respecto a ciberseguridad, implementadas en los Países Bajos, EE. UU., España y Perú. La técnica de recolección de datos fue la observación y el análisis documental; mientras que los instrumentos de acopio de información fueron una ficha de registro y una ficha de análisis. Finalmente, cabe precisar que las variables de análisis fueron las estrategias integradas internacionales sobre ciberseguridad y las estrategias integradas sobre ciberseguridad en el ámbito de seguridad nacional del Perú.

RESULTADOS Y DISCUSIÓN

Las diversas estrategias y políticas nacionales de ciberseguridad tienen en común el objetivo de preservar la integridad del Estado frente a las amenazas provenientes del ciberespacio. No obstante, persisten diferencias en cuanto a la perspectiva de los Estados y los fines que se persiguen al implementar políticas públicas de ciberseguridad. Observar 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 Organización del Tratado del Atlántico Norte (OTAN), bajo la concepción 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.

Por su naturaleza, los casos indicados no permiten comparaciones aplicando indicadores que expresen niveles de desarrollo de las estrategias nacionales de ciberseguridad. No obstante, a partir de estos, fue 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 1.
Estrategias nacionales de ciberseguridad

	Indicadores	Países Bajos	EE.UU.	España	Perú
Protege	Infraestructuras críticas	X	X	X	X
	Economía	X	X	X	
	Seguridad nacional	X	X	X	X
	Bienestar social		X		
	Concientización		X	X	X
Enfoque	Conocimiento	X	X	X	
	Educación	X	X	X	
	Capacidades cibernéticas militares	X	X	X	X
Sector público	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

En la Tabla 1 se puede observar que Estados Unidos ha liderado la satisfacción de los indicadores de ciberseguridad según el *ranking* mundial ITU (2018); mientras que los Países Bajos, aun siendo pioneros en Europa en el ámbito de la ciberseguridad, ocuparon el puesto 12 del *ranking* ITU (2018), siendo superado por Inglaterra, Francia, Lituania, Estonia, España, Noruega y Luxemburgo; esto a causa de que no han logrado satisfacer los indicadores de bienestar social y concientización. Respecto al indicador bienestar social, los Países Bajos dan 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 en 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 Equipos de Respuesta ante Emergencias Informáticas (CERT) a nivel mundial. Esa decisión estratégica posicionó a España en el puesto 7 del índice ITU (2018), superado solo por EE. UU., Canadá y cuatro países europeos.

En el marco de lo expuesto, en el *ranking* ITU (2018), Perú se posicionó en el puesto 95; mientras que, regionalmente, se ubicó en el puesto 12, superando a países como Panamá, Ecuador, Venezuela, Guatemala, Nicaragüa, entre otros. Leiva (2015) señala que los países pertenecientes a la Organización de los Estados Americanos (OEA) han emprendido tareas conjuntas de fortalecimiento en materia de ciberseguridad desde el 2004 y, desde la adopción de la Estrategia Interamericana Integral de Ciberseguridad, esta iniciativa continúa evidenciando profundas asimetrías regionales, ya que existen países con poca capacidad de respuesta ante ciberataques; mientras que, otros se encuentran en niveles intermedios con capacidades de respuestas fluctuantes. En este sentido, el Perú se ubica entre los países con capacidad de respuesta de media a baja.

Cabe precisar que el caso peruano es singular, ya que dispone de una profusa legislación en materia de cibersegu-

ridad 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. Es fundamental distinguir entre ambos instrumentos: 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 de tecnologías de información y la comunicación (TIC) tiende a la obsolescencia normativa, aun antes del alcance de los efectos de novísimas legislaciones. Ello no deriva en el indefectible rezago normativo, solo induce a la adecuación permanente en materia reglamentaria que responda a las buenas prácticas en ciberseguridad y ciberdefensa. Para los latinoamericanos, estas dinámicas constituyen un desafío titánico, ya que el peso de la burocracia de raíces hispanas es un coloso que debe ser derrotado.

De esta manera, el Estado y la sociedad peruana aún transitan por los enfoques de la concienciación y el desarrollo de 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 articulación entre el sector público y 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; además, 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.

Adicionalmente, 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 lo siguiente: construcción de plataformas de alta seguridad que protejan los sistemas del Estado y de la sociedad en general; capacitación de fuerza de trabajo altamente especializada; fortalecimiento de los Equipos de Respuesta ante Emergencias Informáticas (CERT) regionales; convocatoria eficiente a la ciudadanía para que se incorpore al desarrollo de planes y protocolos de ciberseguridad; adecuación normativa y firma de convenios internacionales novedosos en materia de ciberseguridad; consolidación y reimpulso del Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional de la Administración Pública Peruana (PeCERT); 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.

PROPUESTA DE ESTRATEGIA NACIONAL DE CIBERSEGURIDAD EN EL PERÚ

Con la creciente frecuencia de los ataques cibernéticos, los costos también han aumentado, siendo el de una sola violación cibernética de alrededor de 84,000 y 148,000 dólares, para una pequeña empresa, esto sin incluir los costos de remediación y recuperación. En caso de que este ataque sea contra el Estado, infraestructura crítica u

organización social, conlleva a la pérdida de confianza por parte de los inversionistas, ya que el daño causado resulta irreparable. Cabe destacar que, según un estudio llevado a cabo por la compañía de ciberseguridad Kaspersky Lab junto a Ponemon Institute y citado por Portaltic (2020), el 60 % de las empresas que sufren un ciberataque, cierran en los seis meses posteriores a este, por lo tanto, la mejor estrategia para enfrentar los riesgos de la ciberseguridad es la prevención.

El objetivo principal de los ciberdelincuentes es acceder a información confidencial, tanto de instituciones privadas o del Estado, como secretos militares que pueden ser usados para construir armamento, rastrear movimientos de tropas o exponer a agentes de contrainteligencia; por ello, es necesario 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 se enfocó en cimentar un sistema participativo y de cooperación, alentando la participación conjunta de la población, organizaciones e instituciones públicas, privadas y militares, para que estas participen en actividades que permitan el desarrollo eficaz de un programa de ciberseguridad dentro de la nación, que involucre la cooperación con la comunidad internacional. Así, las acciones estratégicas se despliegan en tres fases, con base en 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 encargada de liderar y gestionar la ciberseguridad a nivel nacional, así como de un sistema de alta tecnología para detectar y responder a los ataques cibernéticos en tiempo real.

a) Fase I: Planificación

Generalmente, los efectos de los ciberataques se conocen cuando estos ya se han ejecutado; por ello, la estrategia de planificación involucra una apertura mental que proporcione una técnica con la capacidad de observar a profundidad y ubicar la actividad de 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. A partir de lo expuesto, se 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 siguientes medidas:

Establecer un Gobierno basado en la confianza y la cooperación

Esta medida conlleva a facilitar la cooperación e interacción público-privado-militar, lo que implica compartir funciones y responsabilidades para cooperar de forma conjunta entre las entidades nacionales y estatales, en materia de ciberseguridad; construir y facilitar una información a nivel nacional con sistema de reparto, enfocado en compartir y facilitar al máximo la información respecto a ciberamenazas, tanto en sectores públicos, como privados y militares; reforzar el fundamento jurídico de ciberseguridad, es decir, mejorar las leyes institucionales o elaborar medidas legales, a fin de responder de forma eficaz ante las amenazas de la ciberseguridad.

Construir las bases para el crecimiento del Sistema de Ciberseguridad Nacional

Esta medida conlleva crear un ecosistema innovador para la ciberseguridad, a fin de garantizar la competitividad de la tecnología, los recursos humanos y las industrias, las cuales son fundamentales para la ciberseguridad nacio-

nal. Entre los principales alcances de esta medida se encuentran ampliar la inversión de ciberseguridad, fomentar la competitividad de la seguridad, mano de obra y tecnología, fomentar un entorno de crecimiento para las entidades de ciberseguridad y establecer un principio de competencia ética en las actividades de ciberseguridad.

Fomentar una cultura de ciberseguridad

La población debe reconocer la importancia de la ciberseguridad y esforzarse por aplicar normas básicas de seguridad; además, el Gobierno debe respetar los derechos fundamentales de los ciudadanos, al aplicar las políticas y facilitar la participación ciudadana. En ese sentido, esta medida se encuentra constituida por los siguientes objetivos: incrementar la conciencia de ciberseguridad, reforzar las prácticas de ciberseguridad y asegurar que los derechos fundamentales no sean afectados por la ciberseguridad.

b) Fase II: Ejecución

Esta fase comprende replantear de manera constante una nueva vía o curso de acción para aumentar la infraestructura de seguridad nacional. Por ello, se debe 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, de modo que cada ministerio y organismo persiga los objetivos establecidos en la estrategia, con la finalidad de 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 con las siguientes medidas:

Incrementar la seguridad de la infraestructura central nacional

Esta medida amerita tanto reforzar la seguridad como la resistencia de la infraestructura básica nacional frente a los ataques cibernéticos, con la finalidad de garantizar la prestación continua de servicios esenciales; para ello, es necesario alcanzar los siguientes objetivos: seguridad de la información nacional y redes de comunicación, mejorar el entorno de ciberseguridad en las infraestructuras críticas, y diseñar e implementar un sistema de ciberseguridad nacional de alta tecnología.

Mejorar las capacidades de respuesta a ataques cibernéticos

Esta medida implica ampliar la capacidad para vislumbrar eficazmente los ataques cibernéticos por adelantado, y conseguir lo antes posible la resiliencia; para ello, es preciso alcanzar los siguientes objetivos: asegurar la prevención de los ciberataques, reforzar las medidas defensivas contra los ataques cibernéticos masivos, coordinar permanentemente con las Fuerzas Armadas (Comando Operacional de Ciberdefensa del CC. FF. AA.) sobre las respuestas activas para ataques cibernéticos y mejorar las capacidades de respuesta contra la ciberdelincuencia.

c) Fase III: Evaluación

Esta fase corresponde la revisión de los aspectos comprendidos en las fases previas. La Oficina de Ciberseguridad Nacional, señalada en la Fase II, tiene el deber de supervisar periódicamente la aplicación de esta estrategia, así como las mejoras de ciberseguridad de las personas, empresas y entidades gubernamentales; adicionalmente, esta oficina 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; subsanar las deficiencias, tomando siempre en consideración lo reflejado por deficiencias en la estrategia, perseverando la inserción de mejoras cuando sea necesario, conforme con la siguiente medida: enriquecimiento de los sistemas de cooperación bilateral y unilateral.

CONCLUSIONES

La ciberseguridad constituye un aspecto fundamental para la consecución de los objetivos socioeconómicos de las economías modernas. A su vez, las estrategias están formuladas para ser implementadas conforme con el 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 señalar que las estrategias de ciberseguridad deben estar configuradas 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.

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 seguridad en relación con la protección de la población, garantizar derechos humanos, y entre otros, defender la seguridad y la soberanía de la nación, dejando expuesto que el acceso a contenidos y materiales gráficos de 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, con la finalidad de mejorar, tanto el aspecto del ciberespacio como el comercial, inclinándose hacia este último. Por ello, aun cuando se planteen proyectos y planes estratégicos de acciones respecto a ciberseguridad, es necesario que exista un compromiso social, tanto de la población como de las entidades estatales, privadas y militares, para contrarrestar los efectos de las ciberamenazas, aminorar los riesgos y salvaguardar la seguridad nacional.

En cuanto a las limitaciones resaltantes en el desarrollo de la ciberseguridad en el Perú, se encontró 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 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 con los logros alcanzados.

En cuanto a las brechas en materia de desarrollo, se concluyó que son un efecto más interesante que la megatendencia del uso del ciberespacio y las facilidades que presenta, encontrándose que la principal brecha existente es una gran carencia de tecnologías adecuadas o novedosas, que permitan el funcionamiento y mantenimiento del orden interno, el orden público y la seguridad ciudadana, esto debido a la carencia de tecnología de punta, la inestable y crítica infraestructura de protección y gestión del riesgo de desastres, y al hecho de contar con programas ya obsoletos e ineficaces, lo que evita una articulación en tiempo real, debido a 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 actualiza-

ción de tecnología avanzada, para afrontar las amenazas desde la perspectiva preventiva y no la de solucionar el mal ya causado; mientras que la segunda está relacionada con la falta de integración de intereses personales que se unifiquen por el bienestar del país en general.

RECOMENDACIONES

Aplicar la propuesta desarrollada en la investigación, con la finalidad de fortalecer la seguridad nacional, a través de estrategias de ciberseguridad configuradas por el estudio del esfuerzo multidisciplinario de colaboración, en provecho de los conocimientos, experiencia y pericia de las organizaciones públicas y privadas, así como investigar y mejorar el sistema de intercambio de información, a la vez que evaluar y mejorar la capacidad del Gobierno para identificar, detener y ajustar el ordenamiento jurídico nacional al marco normativo internacional.

Se recomienda, además, una constante evolución de los recursos normativos, humanos y tecnológicos, además de crear espacios de integración de alianzas estratégicas, que permitan la coordinación para afrontar el preciso instante en que se identifique cualquier limitante. Por otro lado, se recomienda ampliar el alcance de la detección de ciberataques, para permitir la detección y bloqueo en tiempo real, y desarrollar tecnología de respuesta basada en inteligencia artificial.

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 interfaz 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, así como establecer una red de seguridad cibernética, con la participación de todos los organismos, empresas e instituciones gubernamentales pertinentes.

REFERENCIAS

Álvarez, D. (2018). Ciberseguridad en América Latina y ciberdefensa en Chile. *Revista Chilena de Derechos y Tecnología,* 7(1), 1-2. http://dx.doi.org/10.5354/0719-2584.2018.50416

Arreola, A. (2018). Ciberseguridad Nacional en México y sus desafíos. *Instituto de Investigaciones Estratégicas de la Armada de México.* https://www.researchgate.net/publication/329253059_Ciberseguridad_Nacional_en_Mexico_y_sus_desafios

Cabrera, L. (2017). La vinculación entre geopolítica y seguridad: algunas apreciaciones conceptuales y teóricas. *URVIO: Revista Latinoamericana de Estudios de Seguridad,* (20), 111-125. https://dialnet.unirioja.es/servlet/articulo?codigo=6110844

Camps, P. (2016). Ciberdefensa y ciberseguridad, nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa a la seguridad nacional, estrategias de ciberseguridad y cooperación interagencias en este ámbito. *Revista Estrategia,* (6), 80-93. https://www.gub.uy/ministerio-defensa-nacional/sites/ministerio-defensa-nacional/files/2020-03/Revista_Estrategia_6.pdf

Ferro, G. y Castaño, Ó. (2017). Geopolítica contemporánea y análisis de factores relevantes a escala global. *Razón crítica,* (3), 111-114. https://revistas.utadeo.edu.co/index.php/razoncritica/article/view/1235

Foro Económico Mundial. (2019). *Informe de riesgos mundial 2019.* WEF.

Fundación Telefónica. (2016). *Ciberseguridad, la protección de la información en el mundo digital.* Editorial Ariel.

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

Leiva, E. (2015). Estrategias nacionales de ciberseguridad: estudio comparativo basado en enfoque *top-down* desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software, 3*(4). 161-176. https://doi.org/10.18294/relais.2015.161-176

Machín, N. y Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI,* (42), 47-68. https://www.redalyc.org/pdf/767/76747805002.pdf

Nagurney, A. & Shukla, S. (2017). Multiform models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research, 260*(2), 588-600. https://doi.org/10.1016/j.ejor.2016.12.034

Parada, D., Flórez, A. & Gómez, U. (2018). Analysis of the components of security from a systemic system dynamics perspective. *Información tecnológica,* 29(1), 27-38.

Portaltic. (2020). *El 60 % de las pymes que sufren un ciberataque desaparece seis meses después, según Kaspersky Lab.* https://www.europapress.es/portaltic/ciberseguridad/noticia-60-pymes-sufren-ciberataque-desaparece-seis-meses-despues-kaspersky-lab-20171002141317.html

Rodríguez, F. (2017). *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)* [tesis de maestría, Pontificia Universidad Católica del Perú, Lima]. http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/9304

Seclén, J. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades púbicas peruanas de acuerdo a la NTP-ISO/IEC 27001* [tesis de maestría, Universidad Nacional Mayor de San Marcos, Lima]. http://cybertesis.unmsm.edu.pe/handle/20.500.12672/4884

Signorino, A. (2019). Ciber riesgos: su dimensión social, funcional y ética. *Revista Ibero-Latinoamericana de Seguros, 28*(51), 33-56. https://doi.org/10.11144/Javeriana.ris51.crsd

Singh, A., Shandhu, 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. https://doi.org/10.1016/j.cose.2017.08.016

Taipe, D. (2018). *La auditoría de seguridad informática y su relación en la ciberseguridad de la Fuerza Aérea del Perú año 2017* [tesis doctoral, Escuela Superior de Guerra Aérea, Lima].

Unión Internacional de Telecomunicaciones. (Noviembre de 2010). Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. *Actualidades de la UIT.* https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx#:~:text=La%20ciberseguridad%20es%20el%20conjunto,los%20usuarios%20en%20el%20ciberentorno.

Vargas, R., Recalde, I. 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), 31-45. http://200.41.82.22/handle/10469/12199

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