CIBERDEFENSA Y CIBERSEGURIDAD EN EL PERÚ: REALIDAD Y RETOS EN TORNO A LA CAPACIDAD DE LAS FF. AA. PARA NEUTRALIZAR CIBERATAQUES QUE ATENTEN CONTRA LA SEGURIDAD NACIONAL

CYBER DEFENSE AND CYBERSECURITY IN PERU: REALITY AND CHALLENGES REGARDING THE CAPACITY OF THE ARMED FORCES TO NEUTRALIZE CYBERATTACKS THAT THREATEN NATIONAL SECURITY

PP. 55-76

Christian Rafael Quevedo Lezama
41325016@caen.edu.pe
Centro de Altos Estudios Nacionales
ORCID: https://orcid.org/0000-0002-5216-7895

Magíster en Educación Inclusiva e Intercultural por la Universidad Internacional de La Rioja en México y Magíster en Lingüística Aplicada a la Enseñanza del Español como Lengua Extranjera por la Universidad Europea del Atlántico en España. Bachiller en Ingeniería Electrónica por la Universidad San Martín de Porres en Perú, y Licenciado en Educación con Especialidad en Ciencia y Tecnología por la Universidad San Ignacio de Loyola en Perú. Cursa el Doctorado en Educación por la Universidad Autónoma de Baja California en México y el de Políticas Públicas y Gestión del Estado en el Centro de Altos Estudios Nacionales.

Recibido: 23 Oct 22	**Aceptado:** 30 Ene 23	**Publicado:** 17 Feb 23

DOI: https://doi.org/10.58211/recide.v4i1.99

Resumen

La ciberdefensa y la ciberseguridad se han convertido en pilares para mantener la estabilidad y el normal funcionamiento de cualquier país, por ende, se consideran áreas clave dentro de los estudios estratégicos. Frente a esa demanda, el Perú no ha sabido desarrollar este sector. Actualmente, el país no cuenta con una inversión destinada a promover los sistemas de seguridad y la defensa cibernética. Si bien la región Latinoamericana tiene poca incidencia en conflictos cibernéticos a gran escala, es importante destacar que la seguridad nacional podría verse vulnerada de no nivelarse a las exigencias actuales. La metodología empleada para el desarrollo del presente texto constó en la revisión documental, concluyéndose que para alcanzar eficientes estrategias de ciberdefensa y ciberseguridad es necesario un sistema que permita la integración y cooperación de los sectores público, privado y militar para alcanzar los objetivos de seguridad nacional.

***Palabras Clave*:** ciberdefensa, Ciberseguridad, Estrategia, Ciberataque, Cooperación.

Abstract

Cyberdefense and cybersecurity have become pillars of maintaining any country's stability and normal functioning; therefore, they are considered vital areas within strategic studies. Unfortunately, faced with this demand, Peru has not been able to develop this sector. Currently, the country does not have an investment aimed at promoting security systems and cyber defense.

Although the Latin American region has little impact on large-scale cyber conflicts, it is essential to note that national security could be violated if it does not level with current demands. The methodology used for the development of the present was delimited in this documentary review, concluding that to achieve efficient cyber defense and cybersecurity strategies, a system is necessary that allows the integration and cooperation of the public, private and military sectors, which makes possible the union of isolated forces to achieve the objectives of national security.

***Keywords*:** cyber defense, Cyber security, Strategy, Cyber Attack, Cooperation.

Introducción

Hoy la ciberdefensa y la ciberseguridad han adquirido un rol protagónico debido a la coyuntura. Una aproximación a su importancia se reconoce en la actual guerra entre Ucrania y Rusia, sumado con las tensiones en ascenso entre China y Taiwán, todos países con una tecnología altamente desarrollada, la cual se ha puesto a prueba en virtud de defender su imagen como potencias mundiales.

El enfoque relacionado a la seguridad cibernética se refiere a la capacidad que tiene cada país para protegerse ante ataques cibernéticos, sea provenientes del interior o exterior, los cuales buscan vulnerar información confidencial. Desde una perspectiva histórica, se puede decir que la finalidad de la seguridad cibernética no es un interés reciente. Su origen proviene de la tabla mesopotámica y la encriptación de información registrado en el año 1500 a. C. Este método de anotación fue evolucionando con el tiempo, asumiendo diferentes modelos hasta llegar al terreno de las plataformas tecnológicas. La creación del ciberespacio en 1984 y la creación de los primeros algoritmos de acceso informático serían los primeros antecedentes de lo que hoy entendemos por la seguridad cibernética (Bay, 2016). Warner (2012) menciona que la seguridad cibernética y la ciberdefensa son el resultado de la evolución de la encriptación de la información. El primer antecedente se dio con la protección básica de acceso de los dispositivos

tecnológicos, la cual se fue desarrollando tras la aparición de diferentes plataformas o redes con códigos diferenciados.

En función a lo descrito, la seguridad informática se puede reconocer como un proceso evolutivo, la cual se mantendrá en cambio constante en función a los nuevos elementos que vayan formando parte del ciberespacio y las redes. Es decir, su adopción implica una actualización persistente.

Considerando la importancia que tiene la información confidencial para cada país u organización, la seguridad y la defensa informática se identifican como una de las tareas más importantes que requieren un mayor desarrollo e inversión. *Secure Connections* (2022) menciona que en la actualidad los países más ciberseguros del mundo son Dinamarca, Suecia, Alemania, Irlanda y Japón. A estos les sigue Francia, Canadá y Estados Unidos con puntuaciones menos significativas. En la misma línea, Abomhara y Koien (2015) mencionan que el incremento en la inversión de ciberseguridad y ciberdefensa ha sido considerable debido a que en la actualidad las acciones de tipo físico no son la primera medida que consideran los países ante situaciones de conflicto. En su lugar, son los ataques cibernéticos la primera acción ofensiva. Por otro lado, Aranda (2018) mencionó que la seguridad cibernética ha mostrado un crecimiento constante en los países desarrollados, los cuales han manejado un modelo de trabajo en conjunto entre el Estado y el sector privado para desarrollar una arquitectura de ciberdefensa y ciberseguridad eficiente.

En consecuencia, la seguridad cibernética se ha convertido en una de las principales prioridades de ciertos países desarrollados para salvaguardar su integridad. Estos han incrementado la inversión en este campo. Por el contrario, existe un avance tardío en ese mismo sector por parte de los países menos desarrollados.

Aranda (2018) señala que Latinoamérica es una de las regiones que recién se encuentra atendiendo la ciberseguridad y la ciberdefensa producto de que es una zona con una clara ausencia de conflictos entre naciones. Es natural por tanto que los gobiernos no hayan promovido este sector y no dirijan la inversión necesaria al mismo. Por su parte, Álvarez (2018) sostiene que, aunque los países de Latinoamérica no se han visto inmersos en conflictos internacionales, estos aun así han sido presas de ataques cibernéticos externos e internos. Es producto de ello que recién se viene impulsado el crecimiento de este sector, aunque vale agregar que en determinados países este compromiso se ha pospuesto. Asimismo, Vargas, Recalde y Reyes (2017) han indagado que algunos países en Latinoamérica han emprendido una iniciativa para crear estrategias de ciberseguridad y ciberdefensa. Tal es el caso de Colombia mediante la estrategia del Consejo Nacional de Política Económica y Social (CONPES) para la ciberseguridad y ciberdefensa. Por su lado, el Perú ha propuesto políticas y estrategias nacionales para la ciberseguridad y ciberdefensa.

La situación del Perú en el campo de la ciberseguridad se ha visto rezagada al no dar la importancia e inversión necesaria para este sector, el Perú se ha visto afectado por innumerables ciberataques durante el 2021, colocándolo como el primer país de Latinoamérica más atacado en la región, dejando en evidencia la debilidad en su infraestructura de seguridad cibernética.

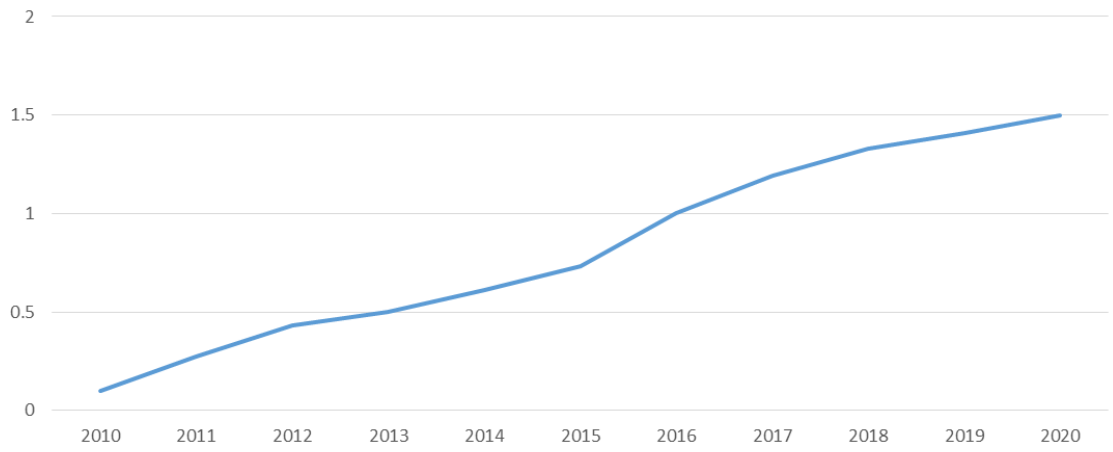
A pesar de que los programas de ciberseguridad y ciberdefensa es un tema que ha sido postergado en el Perú, Bonilla y Ortiz (2020) comentan que los lineamientos en la estrategia de ciberdefensa y ciberseguridad se concentran en el desarrollo de capacidades ofensivas, disuasivas, defensivas e inteligencia para el cuidado del Estado aclarando estándares y compromisos para asegurar el manejo de la información digital a fin de gestionar y mitigar un posible ciberataque manteniendo la capacidad de resiliencia para responder, recuperar y restaurar las áreas afectadas, ello se vería reflejado si se invierte en programas de ciberseguridad y ciberdefensa.

Desarrollo

La ciberseguridad y la ciberdefensa son dos de las áreas más importantes en la seguridad actual considerando la continua alza en la frecuencia de ataques cibernéticos. La función de esas acciones implica preservar la estabilidad de cualquier estado a partir de la creación de una estructura que pueda garantizar la seguridad de la información clasificada de cada uno de sus organismos públicos. Vale mencionar que el espacio cibernético es un entorno en constante evolución y crecimiento. Cada vez es mayor la información disponible y son más los usuarios que se unen, quienes van de personas comunes a empresas privadas o entidades públicas. Se considera que desde el 2010 hasta el 2020 la cantidad de usuarios ha aumentado en un 150% (Díaz, 2021).

Figura 1

Crecimiento porcentual de usuarios en la Internet



Nota: Adaptada con datos de Díaz (2021).

La ciberseguridad, según Becerril (2021), está definida como el conjunto de métodos, procedimientos e implementación de herramientas tecnológicas que buscan mantener bajo confidencialidad la información de una institución. Asimismo, se encarga de garantizar la continuidad, integridad y disponibilidad de los sistemas y redes informáticas ante situaciones de ataques cibernéticos o de acceso no autorizado. Por su parte, Córdoba y Pérez (2021) definen a la ciberdefensa como el conjunto de actividades, sean activas o pasivas, enfocadas a fortalecer la funcionalidad del ciberespacio, su sistema de redes, equipos, personal y enlaces a fin de mantener la defensa de su información y asegurar el cumplimiento de las acciones que estas tengan que desempeñar, evitando que terceros puedan interceder para utilizarlas de manera errada. Por otro lado, Vargas, Recalde y Reyes (2017) indican que existe una diferencia clara entre ciberseguridad y ciberdefensa, la cual se puede reconocer en los siguientes aspectos:

- La ciberseguridad crea mecanismos de protección ante ciberataques, mientras que la ciberdefensa busca proteger y a la vez generar ataques a modo de respuesta.
- La ciberseguridad es complementaria a la ciberdefensa.
- La ciberdefensa se enfoca en prevenir e impedir ataques o amenazas cibernéticas que generen inestabilidad sobre un Estado y su población, mientras que la ciberseguridad es el conjunto de normativas y políticas que protege la información de los usuarios cibernéticos.
- La ciberseguridad busca crear los mejores mecanismos que impiden el acceso a la información, mientras que la ciberdefensa tiene como finalidad repeler los ataques creando mecanismos de defensa que den una respuesta directa a los ataques.

Es importante reconocer la diferencia entre estos dos enfoques, dado que así se puede tener una percepción más clara sobre qué tipo de mecanismo se está utilizando para salvaguardar la integridad cibernética de cada organización o estado.

El ciberespacio y las nuevas amenazas

La humanidad siempre ha buscado encontrar nuevos medios que le ayuden a facilitar su rutina diaria. Es ante esa iniciativa que se ha contemplado al mundo de la tecnología como el escenario más apto para administrar sus diversas funciones cotidianas, lo que a su vez la ha expuesto a adentrarse al mundo del ciberespacio. Es mediante este complejo universo que autoridades de diversas sociedades han podido obtener, por ejemplo, el control de sus sistemas de transporte y comunicación, monitorear sus redes de servicios básicos y almacenar información de interés nacional (Cujabante et al, 2020). Muy a pesar de sus beneficios, esta nueva realidad ha traído consigo nuevas amenazas que pondrían en riesgo la estabilidad y el normal funcionamiento de esos sectores o de una nación entera (Asencio, 2018).

El ciberespacio es un término hoy en día popularizado. Estrategas de la tecnología, gobernantes, militares, empresarios, líderes de industrias y profesionales de la seguridad lo definen como un entorno digital interconectado muy extendido, en donde agentes cibernéticos pueden interactuar por medio de una conexión a la red (Robles, 2015) haciendo posible que el mundo se mantenga en contacto sin barreras. Vargas, Recalde y Reyes (2017) comentan que el ciberespacio es un conjunto de elementos. Estos lo conforman la Internet, las redes de telecomunicaciones, computadoras, softwares, máquinas, las redes sociales, páginas web y los cibernautas, y es un espacio que tiene como función intercambiar servicios y conocimientos. Por su parte, Valdés y Cabrera (2013) se refieren al ciberespacio como una plataforma abstracta, estratégica y operativa constituida por redes informáticas que son captadas mediante el uso de aparatos digitales a fin de dar lugar a procesos sociales y culturales alternativos.

El espacio cibernético se encuentra inmerso en la red de ordenadores, los móviles, los aparatos digitales, todo un mundo amplio y confuso de entender. A propósito, Asencio (2018) menciona las siguientes características para comprender la naturaleza del espacio cibernético:

- Es un entorno continuamente dinámico y en constante crecimiento.
- Impacta y produce cambios en las sociedades que acceden al ciberespacio. De hecho, las generaciones que han accedido tempranamente al ciberespacio presentan motivaciones y deseos distintos a las generaciones que no tuvieron ese acercamiento prematuro.
- Las operaciones que se llevan a cabo en el espacio cibernético tienen una amplitud ilimitada. Esta no presenta fronteras por lo que puede llegar a cualquier parte del mundo.
- Debido a la utilización de identidades virtuales, las operaciones efectuadas se pueden realizar bajo anonimato.
- Las acciones efectuadas en el ciberespacio generan un efecto inmediato.

Es importante mencionar que el espacio cibernético ha sido de gran ayuda para fortalecer el desarrollo social, ya que mediante sus procesos se puede establecer un orden y control de grandes sistemas sociales. En tanto, conocer las características esenciales del ciberespacio es fundamental para crear planes de defensa y seguridad ante amenazas que pueden conllevar al caos, los que por ejemplo son ejecutados por los cibernéticos. Estos pueden causar apagones eléctricos, fallas en equipos militares, violaciones a secretos de seguridad nacional, robar datos confidenciales, interrumpir las redes telefónicas e informáticas, logrando paralizar los sistemas obligando a que los datos no se encuentren disponibles. Es por esta razón que no es una exageración decir que las amenazas cibernéticas pueden afectar el funcionamiento diario de la vida tal como lo conocemos.

El espacio cibernético proporciona la posibilidad de anonimato por medio de la Internet. Esta sería una característica ventajosa para generar los actos delictivos, dado que dificulta la identificación y rastreo del usuario ante la ejecución de una amenaza o ataque (Ramírez, 2016). Por ende, esta realidad se convierte en un reto de gran relevancia para cada nación, en donde cada uno deberá enfocarse a impulsar una infraestructura y mecanismos de seguridad para la defensa cibernética. Una amenaza cibernética es un acto malicioso que busca dañar o robar datos, e interrumpir la vida digital en general. Los ataques cibernéticos incluyen amenazas como virus informáticos, filtraciones de datos y ataques de denegación de servicio (Pauli y Franco, 2020).

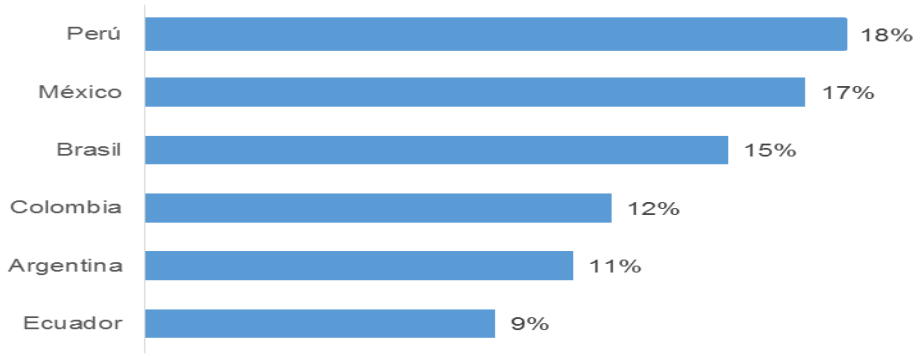
Es un hecho que hoy día salvaguardar la integridad de un estado o nación no solo implica un enfoque físico, sino también cibernético. Muy a pesar, si en teoría ambos tienen un alto nivel de importancia, ese último rubro ha sido postergado en la mayoría de los países subdesarrollados (Medeiros y Franco, 2020). En extensión, Aranda (2018) comenta que en Latinoamérica se registra una variedad de crímenes cibernéticos. Entre ellos se encuentra un reciente robo de alrededor de 10 millones de dólares efectuado a una entidad financiera chilena. Entonces, el haber invertido una fracción de esa cantidad al rubro de la ciberseguridad, tranquilamente hubiera evitado tal desfalco. Aranda añade además que lo ocurrido no es un tema propiamente de un país, sino que se trata de un asunto global, pues las pérdidas anuales debido al cibercrimen oscilan entre un 0,8 a 1,0 por ciento del producto global bruto.

No solo Chile ha sido el único país de la región víctima de ataques cibernéticos. Además de ser uno de ellos, el Perú ha registrado una gran cantidad de ciberataques (Quiroga, 2021), un dato bastante preocupante y negativo para los usuarios y empresas del país. Ya de por sí esa es una muy buena razón para que sus gobernantes le den una mayor importancia a la implementación de sistemas de seguridad sólidos y robustos para la protección de la información. Así mismo, Poma y Vargas (2019) explican que las modalidades más comunes de los ciberdelincuentes se hacen mediante el robo y venta de

la información de tarjetas; seguido de la sextorsión —la cual se refiere a la publicación no autorizada de imágenes íntimas—; el robo de dinero de cuentas bancarias y; ventas falsas en línea.

Figura 2

Ranking de ciberataques en Latinoamérica



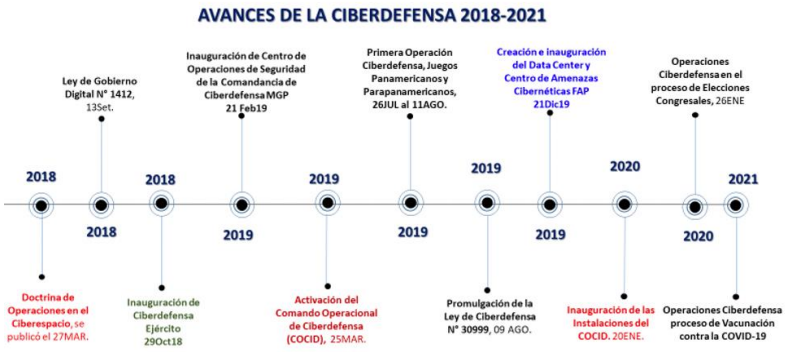
Es importante destacar que mientras el espacio cibernético siga creciendo a nivel comercial, los cibercriminales se verán más interesados en buscar nuevas estrategias para llevar a cabo sus estafas (Álvarez, 2018). Estos delincuentes estarán atentos a escenarios que le den acceso a terrenos fértiles en los que puedan captar víctimas potenciales, tal como se observó durante el principio de la pandemia del COVID 19, en donde el mayor porcentaje de denuncias por parte de los ciudadanos peruanos se relacionaban a delitos informáticos bajo una modalidad en donde los delincuentes se hacían pasar por entidades financieras por medio de diversas vías, tales como llamadas, mensaje de WhatsApp y correos electrónicos (Quiroga, 2021).

Por otro lado, Jardín, Carneiro y Silva (2017) sostienen que las estrategias de defensa deben ser vistas desde un punto militar. En este sentido, de ser necesario, se debe considerar la utilización de todas las fuerzas de una nación, que, a través de operaciones a gran escala, planificación y desarrollo a largo plazo, se garantice la seguridad. Al respecto, Castillo (2021) menciona que las FF. AA. del Perú deben actuar de forma integral ante una amenaza cibernética. Es por esa razón que en el tiempo se ha orientado a la creación de una política sectorial de ciberdefensa. En el 2017, la Dirección de Política y Planeamiento Estratégico para la Defensa del Ministerio de Defensa formuló un proyecto de directiva que establecía las Políticas del Sector Defensa en Ciberdefensa. Aunque no fue aprobada, fue el inicio de una serie se decisiones que permitieron reforzar la Defensa Nacional del Perú.

Es necesario también, tomar en cuenta el costo que implica implementar sistemas de defensa. Galinec, Možnik y Guberina (2017) comentan que mientras que el costo por defender las estructuras cibernéticas y los beneficios de los ataques exitosos siguen aumentando, el costo por lanzar un ataque simultáneo se encuentra disminuyendo.

Figura 3

Línea de tiempo de los avances de la ciberdefensa en el Perú



Nota: Castillo (2021)

Por otra parte, Broeders (2021) comenta el desajuste existente en la evaluación de amenazas por parte del gobierno y corporaciones que indican un entorno en alto riesgo. Se manifiesta así una capacidad gubernamental limitada y una poca voluntad política para proteger a las empresas en línea. Si bien las empresas pueden defender sus propias redes, no pueden tomar represalias ni recopilar pruebas ante fraudes más allá del perímetro de sus propias redes. A propósito, Cujabante et al (2020) alegan que cuando se enfrenta a un atacante criminal de otro país o patrocinado por un Estado extranjero, la defensa cibernética pasiva a menudo parece solo una parte de la solución, algunos abogan por una postura de autodefensa cibernética más agresiva.

La desterritorialidad del ciberespacio

A diferencia de los territorios tradicionales, las acciones en el ciberespacio no están limitadas por controles fronterizos debido a que la inmaterialidad del ciberespacio es demostrable en la red de flujo del espectro electromagnético. Sin embargo, el ciberespacio está anclado por dispositivos móviles operados en dominios usuales, pero al mismo tiempo impregna simultáneamente y abarca otras potestades (Pauli y Franco, 2020). La inmaterialidad del ciberespacio permite la transposición de límites por diferentes flujos de información. Esta es la peculiaridad más evidente del ciberespacio en cuanto a su ruptura con los conceptos tradicionales de territorio como el espacio físico delimitado por fronteras (Medeiros y Franco, 2020).

Para crear un sólido sistema de defensa y seguridad cibernético es necesario entender a profundo de qué se trata el ciberespacio. Analizar su territorio físico si bien no es el conducto más amplio para alcanzar este entendimiento, sí es una dirección para entender una parte de su constitución. Este terreno físico se refiere a la capa conformada por los dispositivos, los cuales permiten la inserción en el espacio cibernético (Pauli y Franco, 2020).

Propuesta de estrategia para la ciberseguridad en el Perú

En la actualidad, los ataques cibernéticos cada vez son más frecuentes consecuencia de la exposición de sus sistemas de seguridad. Esto ha generado el aumento en la inversión para salvaguardar la información. Para una empresa pequeña podría resultar un atentado contra un patrimonio de 100 mil dólares, mientras que en caso el ataque sea en contra a una institución, organismo social o hacia el mismo Estado, el daño sería irreparable, lo que conllevaría a no solo la pérdida de activos, sino también la confianza de los inversionistas (Ormachea, 2020).

El principal objetivo de los delincuentes cibernéticos es acceder a la información confidencial, ya sea de las instituciones privadas o del estado, obtener secretos militares, rastrear movimientos de tropas en conflictos armados entre países o exponer a agentes de contrainteligencia. Por ende, es de suma importancia asistir a este tema de manera minuciosa y contar con estrategias que se adapten a las exigencias actuales permitiendo contrarrestar cualquier diversidad de ciberataques que puedan perturbar o buscar destruir las infraestructuras estatales o hasta generar una ciberguerra (Aguilar, 2019).

De acuerdo con Aguilar (2021), una estrategia sólida de ciberseguridad puede proporcionar una buena postura de seguridad contra ataques maliciosos diseñados para acceder, alterar, eliminar, destruir o extorsionar sistemas y datos confidenciales de una organización o usuario. En extensión, la ciberseguridad también es fundamental para prevenir ataques que tienen como objetivo deshabilitar o interrumpir las operaciones de un sistema o dispositivo.

La propuesta de estrategia para la ciberseguridad del estado peruano se debe caracterizar por estar cimentada en un sistema participativo y cooperativo, alentando e integrando la participación conjunta de diversos agentes, tales como la ciudadanía, instituciones y organizaciones públicas y privadas, así como militares activos y hasta la comunidad internacional, todo ello con la finalidad de que se desarrolle un programa

eficaz ante cualquier ataque y que procure reducir la brecha en la capacidad de respuesta (Sheth, Bhosale y Kurupkar, 2021). Para reforzar la capacidad cibernética nacional es necesario que exista la separación de las redes internas del Estado de la Internet pública. Al mismo tiempo, contar con una organización que se encargue de lidiar y gestionar la ciberseguridad de la nación, así como de un sistema tecnológico de alta calidad para detectar y responder a los ciberataques en tiempo real. Esto se puede alcanzar mediante las siguientes tres fases propuestas por Ormachea (2020):

- Planificación: Por lo general, los efectos que se generan de un cibercrimen se conocen una vez que es ejecutado. Por ende, la fase de planificación involucra una exploración inteligente e ingeniosa que permita evaluar el alcance asociado a la amenaza, permitiendo crear mecanismos de defensa suficientes. Es fundamental además contar con equipos actualizados que no generen una falsa sensación de seguridad y más bien permiten que las amenazas se materialicen.

  La fase de planificación debe cumplir con medidas tales como establecer un dominio basado en la confianza y la cooperación público-privado-militar, en donde se compartan responsabilidades en materia de ciberseguridad. Se debe promover además un ecosistema innovador que permita un crecimiento sostenido y constante del sistema de ciberseguridad nacional. Finalmente, se debe de fomentar arduamente una cultura de seguridad cibernética en la población que dé a reconocer su importancia.
- Ejecución: En esta fase se debe replantear de manera constante nuevas formas o vías de acción para robustecer la infraestructura de la seguridad nacional. En tanto, se debe establecer la forma de la implementación de un plan básico en la ciberseguridad nacional a nivel táctico y operacional, de modo que se persigan los objetivos establecidos en la estrategia. Lo antes mencionado debe ser llevado a cabo considerando medidas tales como incrementar la seguridad de la infraestructura central nacional, diseñar un sistema de ciberseguridad de alta

tecnología y mejorar las capacidades de respuesta ante ataques cibernéticos. Aquí es crucial que las fuerzas armadas tengan un papel activo en las medidas defensivas contra los ataques cibernéticos masivos.

- Evaluación: En esta fase se lleva a cabo una revisión de las fases anteriores. Se realiza la supervisión periódica de los aspectos comprendidos en la estrategia, así como la subsanación de las deficiencias a fin de brindar mejoras que permitan elevar la calidad de la ciberseguridad de las personas, empresas y la entidad gubernamental. Es fundamental que esta fase ejecute el paradigma de la medida: enriquecimiento de los sistemas de cooperación bilateral y unilateral.

Conclusiones

Perú presenta un déficit en temas de ciberseguridad y ciberdefensa debido a que no se han ejecutado adecuadamente los procesos o medios tecnológicos que permitan fortalecer la protección de datos o información de entidades u organismos tanto privados como públicos. Esta deficiencia se justifica ante la ausencia de amenazas de conflictos a gran escala, lo que provoca el desinterés respecto al tema por parte de los gobernantes de estado. En ese sentido, esa desmotivación representa uno de los retos de mayor relevancia para cambiar el rumbo de esta situación. Por otra parte, Perú es considerado como el país que registra un mayor número de ataques cibernéticos en la región relacionados al hurto de información personal de los ciudadanos.

Por su parte, los países desarrollados han considerado la importancia que representa contar con sólidos sistemas de seguridad y defensa cibernética, ya que la estabilidad de estos depende en gran medida de la protección de información o datos oficiales del estado. Mientras tanto, los países menos desarrollados manifiestan un avance tardío. Tal es el caso del Perú que, a pesar de haber tenido la iniciativa de crear políticas y estrategias nacionales enfocadas a la ciberseguridad y ciberdefensa, no dirige la inversión suficiente

para la continua actualización de estas, valiéndose de tecnologías obsoletas que vulneran la seguridad nacional.

Por otro lado, el cuerpo de las FF. AA. peruanas posee una capacidad limitada para contrarrestar un ataque cibernético de importancia al no contar con el equipamiento ni la tecnología necesaria que cumplan con las exigencias actuales, además de una estrategia de ciberseguridad y ciberdefensa eficiente, la cual es la que integra la cooperación de los sectores público, privado y militar. Cabe destacar que el desconocimiento y la falta de investigación en esta área es una de las barreras que debe ser cubierta, a fin de ir disminuyendo la amenaza de un posible caos ante la eventualidad de un ataque de este tipo.

Se debe considerar al ciberespacio, militarmente hablando, como un medio o dominio en el que existe amenazas reales que pueden llegar a ocasionar mucho daño y en donde la vulnerabilidad ante los ataques va en aumento, no solo por la expansión de la Internet, sino por cómo la sofisticación de los ciberataques aumenta en mayor medida. Adicionalmente, si bien cualquier estrategia debe ser constantemente estudiada para evaluar su efectividad, en el caso del Perú es necesario un modelo de gobernanza en ciberseguridad y ciberdefensa que acople y materialice de forma efectiva los esfuerzos de los diversos sectores del estado.

La seguridad nacional en el Perú hoy en día no solo depende de salvaguardar las fronteras terrestres, marítimas y aéreas, que era lo habitual en tiempos pasados. Ahora también se deben velar y fortalecer los sistemas de seguridad cibernéticos, aquellos que sepan contrarrestar un ciberataque en caso de que este tenga lugar. Es por ello por lo que las FF. AA. tienen como desafío capacitarse en cada uno de estos sectores, logrando así convertirse en un organismo integral en cuando a defensa y seguridad se refiere.

Referencias

Álvarez, D. (2018). *Ciberseguridad en América Latina y ciberdefensa en Chile*. Revista chilena de derecho y tecnología, 7 (1), 1 – 2. https://rchdt.uchile.cl/index.php/RCHDT/article/view/50416/53050

Aranda, O. (2018). *Ciberseguridad y ciberdefensa: prioridad nacional postergada*. Revista de Marina, 956 (1), 1 – 15. https://revistamarina.cl/revistas/2018/4/oarandam.pdf

Abomhara, M. y Koien, G. (2015). *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks*. Information and communication, 1 (1), 1 – 24. https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_414.pdf

Asencio, A. (2018). *El Ciberespacio como sistema y entorno social*. Comunicación y sociedad, 31 (1). 23 36. https://dialnet.unirioja.es/servlet/articulo?codigo=6336401

Aguilar, J. (2019). *Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. URVIO*. Revista Latinoamericana De Estudios De Seguridad, (25), 24 - 40. https://doi.org/10.17141/urvio.25.2019.4007

Aguilar, J. (2021). *Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior.* Undefined, 53 (198). 169 – 197. https://doi.org/10.5354/0719-3769.2021.57067

Bonilla, H. y Ortiz, F. (2020). *Estrategia Nacional de Ciberdefensa y Ciberseguridad - ECDCS- 2020 - 2030*. Sello Editorial ESDEG. 1 14. 10.25062/9789585254558.

Broeders, D. (2021). *Private active cyber defense and (international) cyber security—pushing the line?* Journal of Cybersecurity, 7 (1). 1 10. https://academic.oup.com/cybersecurity/article/7/1/tyab010/6199903

Bay, M. (2016). *What is cybersecurity? In search of an encompassing definition for the post-Snowden era*. French journal for media research, 1 (1), 1 – 12. https://www.researchgate.net/publication/308609163_WHAT_IS_CYBERSECURITY_In_search_of_an_encompassing_definition_for_the_post-Snowden_era

Becerril, A. (2021). *Cybersecurity and E-commerce in Free Trade Agreements*. Mexican Law Review, 13 (1), 1 – 12. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-05782020000200003

Castillo, E. (2021). *Política Sectorial de Ciberdefensa: una necesidad impostergable*. Centro de Estudios Estratégicos del Ejército del Perú. 1. 1 6. https://ceeep.mil.pe/wp-content/uploads/2021/11/CEEEP-2021-Politica-Sectorial-de-Ciberdefensa-1.pdf

Córdoba, J. y Pérez, L. (2021). *La ciberdefensa en los sistemas de información sanitarios militares.* Sanidad Militar, 76 (3), 1 – 12. https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1887-85712020000300140

Cujabante, X., Bahamón, L., Prieto. J. y Quiroga, J. (2020). *Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares*. Revista Científica General José María Córdova, 18 (30), 357 – 377. http://www.scielo.org.co/pdf/recig/v18n30/2500-7645-recig-18-30-357.pdf

Díaz, R. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe*. Serie Desarrollo Productivo, (228).1 68. https://repositorio.cepal.org/bitstream/handle/11362/47240/1/S2100485_es.pdf

Galinec, D., Možnik, D. y Guberina, B. (2017). *Cybersecurity and cyber defense: a national level strategic approach.* Automatika, 58(3). 273 – 286. https://www.researchgate.net/publication/324777689_Cybersecurity_and_cyber_defence_national_level_strategic_approach

Jardim, D., Carneiro, A. y Silva, F. (2017). *Cyber security governance and management for smart grids in Brazilian energy utilities*. JISTEM *J.Inf.Syst. Technol. Manag,* 14 (3). 385 – 400. https://www.scielo.br/j/jistm/a/RfZk5rzRxD9fML864dJCmfH/

Medeiros, B. y Franco, L. (2020). *The Fundamental Conceptual Trinity of Cyberspace*. Contexto internacional, 42 (1), 31 – 55. https://www.scielo.br/j/cint/a/WYHRGNsY5mpWzjCwsSfrTZv/?format=pdf&lang=en

Ormachea, J. (2020). *Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional*. Defensa-CAEN, 1 (4). 36 – 48. https://orcid.org/0000-0002-9119-8846

Poma, A., y Vargas, R. (2019). *Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo*. SCIÉNDO, 22(4), 275-282. https://doi.org/10.17268/sciendo.2019.034

Pauli, B. y Franco, L. (2020). *The Fundamental Conceptual Trinity of Cyberspace*. Contexto Internacional, 42 (1). 31 53. https://www.scielo.br/j/cint/a/WYHRGNsY5mpWzjCwsSfrTZv/?format=pdf&lang=en

Quiroga, J. (2021). *Ciberseguridad y protección de datos personales en el Perú*. Advocatus, (39). 15 - 21. https://doi.org/10.26439/advocatus2021.n39.5114

Ramírez, E. (2016). *Fuerza Pública, negociaciones de paz y posacuerdo en Colombia*. Análisis Político, 29 (87), 146 - 149. https://doi.org/10.15446/anpol.v29n87.60757

Robles, M. (2015). *El ciberespacio y la ciberseguridad: consideraciones sobre la necesidad de un modelo jurídico*. Documento Opinión, 1 18. https://www.ieee.es/en/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-CIberseguridad_Margarita-Robles.pdf

Sheth, A., Bhosale, S. y Kurupkar, F. (2021). *Research paper on cyber security. Contemporary research in India*, 1 (1). 246 251. https://www.researchgate.net/publication/352477690

Secure Connections (2022*). Cybersecurity in the Philippines: Global context and local challenges*. https://asiafoundation.org/wp-content/uploads/2022/03/Cybersecurity-in-the-Philippines-Global-Context-and-Local-Challenges-.pdf

Vargas, R., Recalde, L. y Reyes, R. (2017). *Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa.* Revista Latinoamérica de estudios de seguridad, 20 (1), 31 – 45. https://revistas.flacsoandes.edu.ec/urvio/article/view/2571/1605

Valdés, J. y Cabrera, E. (2013). *Ciberespacio y cibersociedad, su relación con las formas alternativas de socialización para la apropiación social de las TIC´s.* Revista Iberoamericana para la Investigación y el Desarrollo Educativo, 10. 1 18. https://1-11.ride.org.mx/index.php/RIDESECUNDARIO/article/viewFile/564/553

Warner, M. (2012). *Cybersecurity: A Pre-history. Intelligence and National Security*, 27(5), 781–799.10.1080/02684527.2012.708530