FRIEDRICH NAUMANN FOUNDATION For Freedom.

POLICY PAPER

“Investigación de factores relevantes para la generación de Políticas de Gestión de Seguridad de la Información y Ciberseguridad del Estado Peruano, a nivel estratégico”

Italo Orihuela Oré

Hernán Díaz Añasco

Martina Marangunich Rachumi

Luis Recalde H

ANALYSIS

Imprint

Publisher
Friedrich-Naumann-Stiftung für die Freiheit
Truman Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg
Germany

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit

Authors
ITALO JESÚS ORIHUELA ORÉ
Licenciado en Ciencias Militares, Licenciado en Derecho y Ciencia Política, Abogado en ejercicio, Magíster en Administración Pública, con estudios de post-grado en Ciencias Políticas y Marketing Turístico por la Universidad Nacional Mayor de San Marcos UNMSM), Gobernabilidad y Gerencia Política por la Universidad Católica del Perú y George Washington University, Desarrollo Sostenible por la Universidad de Hiroshima-Japón, Estrategia y Política de Defensa por la Universidad Nacional de Defensa W.J. Perry de USA, Guerra Híbrida y Conflicto en Zona Gris por la Universidad de Operaciones Especiales Conjunta de USA, Online Trainer por la Cámara de Comercio e Industria Peruano-Alemana AHK Perú. Ha finalizado estudios de Doctor mención en Gestión Pública. Conferencista Internacional en Inteligencia Estratégica UNMSM, Catedrático en la UNMSM en Post-Grado y Pre-Grado, profesor invitado en la Academia de la Magistratura del Poder Judicial, en la Escuela Superior de Guerra del EP, Escuela de Alto Mando de la FAP y en las Escuelas de Especialización del Comando de Educación y Doctrina del Ejército.

MARTINA GISELLA MARANGUNICH RACHUMI
Economista, estudios concluidos MBA del Neumann Business School; certificada en PM4R, protección de datos personales IAGIT-España, Policy Maker en Ciberseguridad –INCIBE-OEA Universidad de León-España y Diplomado Internacional en Ciberseguridad CAEN; Cursos de Administración de Crisis para la Defensa del William J. Perry -Center of Hemispherics Defense Studies, at the National Defense University; desarrollándome en gestión, asesoría e implementación de estrategias para programas y proyectos nacionales y/o privados; planificación estratégica, Reingeniería de procesos y acompañamiento del cambio para la mejora continua, gestión de la calidad de los servicios públicos, incorporando componentes de Transformación, Economía y Seguridad Digital. Implementación de mecanismos para la Ciberseguridad y Ciberdefensa, muchos de ellos con mecanismos de cooperación internacional, con aporte no reembolsable, asistencia técnica, intercambio de expertos y mejores prácticas. Miembro del Comité CADE-DIGITAL 2021.

HERNÁN ALBERTO DIAZ AÑASCO
Bachiller, Licenciado y Magister en Comunicación Social, Oficial del Ejército del Perú en la especialidad de Ciencia y Tecnología, Catedrático de Operaciones de Información, Inteligencia y Ciencias de la Comunicación en la Escuela Nacional de Inteligencia - ENI, Escuela de Operaciones Sicológicas del Ejército- EOSE, Escuela Superior de Inteligencia - Ministerio del Interior, Escuela Superior de Guerra del Ejército- ESGE, Escuela de Inteligencia del Ejército-EIE, entre otros; expositor y conferencista. Gestor de Inteligencia Estratégica acreditado por la Dirección Nacional de Inteligencia del Perú. Experiencia en Análisis de Contenido de Inteligencia, Semiología de la Comunicación, Teorías de la Comunicación, Sintaxis y Lenguaje Audiovisual, Análisis Multimodal, Campañas y Gestión de Reputación Política, Institucional y Empresarial, Operaciones de Información y Campañas de Comunicación Multimediaticas en plataformas tradicionales y virtuales. Proactivo para la elaboración de investigación cualitativa y desarrollo de contenidos teóricos y prácticos en el campo de las operaciones de información, manejo de crisis, comunicación, política e inteligencia. Jefe de la Sección Planeamiento en la OIE Oficina de Informaciones del Ejército.

ERNESTO CASTILLO FUERMAN
General del Ejército del Perú, especialista en Ciberseguridad y Ciberdefensa por la UNI-INICTEL, Doctor y Magister en Gestión y Desarrollo, Magister en Gestión Pública e Ingeniero Electrónico. Director del Centro de Entrenamiento Táctico Computarizado de Ejército, fundador del Centro de Ciberdefensa del Ejército y jefe de operaciones de Ciberdefensa y Telemática del Ejército; ha formulado el Manual de Guerra Electrónica y Ciberdefensa del Ejército. Comandante General de Ciberdefensa y Telemática del Ejército; catedrático en el Centro de Altos Estudios Nacional (CAEM) en Ciberseguridad y Defensa.

Editor
[Editor]

Contact

Phone: +49 30 22 01 26 34
Fax: +49 30 69 08 81 02
email: service@freiheit.org

Date
[Monat Jahr]

Notes on using this publication
This publication is an information offer of the Friedrich Naumann Foundation for Freedom.
It is available free of charge and not intended for sale. It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

Tabla de Contenidos

1. Introducción

Los seres humanos asistimos de forma irreversible, a los eventos que se suscitan en el espacio a través de las ondas electromagnéticas y su conexión con aquella gestión colaborativa, de nuevas tecnologías e innovación para la gestión de información más conocida como: internet. En ese contexto la información que se gestiona es compleja y en cantidades exponenciales, lo que la convierte en la era de las informaciones en el ciberespacio, ámbito de riesgos y amenazas, pudiendo ser direccionadas contra el individuo, las organizaciones y contra el Estado; en este caso, contra el Estado Peruano.

Byung-Chul Han, filósofo coreano-alemán, en el prólogo de su libro "*En el Enjambre*", alude al teórico de los medios, Marshall Mc Luham, que, en 1964, advertía: "La tecnología eléctrica ya está dentro de nuestros muros y estamos embotados, sordos, ciegos y mudos ante su encuentro con la tecnología de Gutenberg". Luego, Han, desarrolla su tesis al manifestar que nos encontramos en "una nueva crisis, una transición crítica, de la cual parece ser responsable otra transformación digital: la revolución digital". En ese orden de ideas, no existe en el mundo, un individuo y menos los Estados tal y como los concebimos, que no se encuentren inmersos dentro de la vorágine de aquella *revolución digital.*

El mismo Han, que es uno de los filósofos más leídos del mundo, el año 2021, en su libro "*No-Cosas*", nos dice: "No vivimos en un régimen totalitario con una policía del pensamiento[1] que despoja brutalmente a la gente de sus cosas y sus recuerdos. Es más bien nuestro frenesí de comunicación e información lo que hace que las cosas desaparezcan. La información, es decir, las no-cosas, se colocan delante de las cosas y las hacen palidecer. No vivimos en un reino de violencia, sino en un reino de información que se hace pasar por libertad". Estas premisas socavan, debilitan, la Seguridad Nacional de cualquier Estado, por lo que se hace necesario e indispensable, determinar los factores para establecer Políticas de Gestión y Seguridad de la Información; dentro de ellas la Ciberseguridad como política específica.

Es cierto que la digitalización de la información es un factor tecnológico; al respecto dice Han: los seres humanos estamos "embotados" de "el enjambre digital", por lo que el Estado Peruano no puede ser indiferente y tiene que gestionar Redes y Tráfico de Información, que es el hábitat del dominio de la Seguridad y Defensa de la Información, de lo contrario podría afectar la *data digital* del Estado, en consecuencia, nuestra soberanía y la Seguridad Nacional.

Por su lado, Alvin Toffler, en su libro clásico "*El Shock del futuro*", en la década de los 70, presagiaba y definía el futuro como "demasiado cambio en un periodo muy corto de tiempo". Somos todas las generaciones que convivimos en el siglo XXI, seamos nativos o inmigrantes digitales, los que estamos experimentando ese cambio radical, en una vertiginosa carrera de nunca acabar, cumpliéndose en estricto los escenarios planteados y los cambios disruptivos promovidos por la tecnología en todos los campos del saber y quehacer humano.

El Perú, no es la excepción, por el contrario, se convierte, considerando el factor geopolítico, en uno de los países más importantes de la región en aceptar las TICs, como los fundamentos para cumplir con sus fines y alcanzar el desarrollo nacional que merece como país; nuestro estudio servirá de guía para la mejora del enfoque en ciberseguridad, así como en la identificación de las instituciones y/o personal clave para poder fortalecer dichos conceptos y su ejecución.

De modo que el estado peruano debe de considerar a la información que transita por sus medios y canales digitales oficiales como un "Activo Crítico Sensible"; por lo que se hace necesario generar Políticas de Gestión de Seguridad de la Información del Estado Peruano, a nivel estratégico. Para ello es necesario identificar los diversos sectores claves y puntos vulnerables a reforzar, desarrollando así procedimientos y políticas claras que puedan ser ejecutadas a lo largo de los diversos actores del estado. El previo concepto en mención involucra no solo aspectos de infraestructura tecnológica, sino también las consideraciones que el personal operativo y no técnico debería tener para poder mantener altos estándares de seguridad.

2. Antecedentes y Conceptos Generales

El especialista en temas digitales, Ragi Burhum, en el periódico *La República* del 09 de octubre de 2022, escribió un artículo bajo el título de **"¿Cómo hackearon al Ejército Peruano?"**, señalando que el hackeo a las Fuerzas Armadas peruanas por parte del grupo *Guacamaya*, a más de 283,000 e-mails publicados, de forma abierta, donde se revelaron datos clasificados como, por ejemplo, los planes de guerra con el país vecino del Sur, "lamentablemente no fueron hechos usando un proceso sofisticado".

El autor, nos recuerda que, en su cuenta personal de Twitter detalló las herramientas que se utilizaron para

[1] Han alude a la "policía del pensamiento" de Orwell.

extraer dicha información; pero lo cierto, nos dice, es que "el hackeo se debió a que las personas responsables de mantener los servidores utilizados para mandar e-mails por el Comando Conjunto de las Fuerzas Armadas (FFAA) y el Ejército del Perú no habían instalado una actualización publicada por Microsoft en julio del año pasado".

Añade Ragi Burhum, a modo de conclusión, "la realidad es que este no fue un problema por falta de conocimiento o entrenamiento, de parte de los responsables del sistema de seguridad de la información", pues parte de su trabajo todas las mañanas antes de iniciar labores, "es de revisar los comunicados de seguridad (30 minutos), y ver si alguno de ellos aplica al *software* que están usando. Si es así, instalarlo; es un trabajo extremadamente monótono, y existen muchas herramientas que automatizan esto, pero si se ignora por mucho tiempo, abre la ventana de ataque para que cualquier curioso pueda fácilmente atacarte como vimos en este caso".

Cabe preguntarnos: ¿Cómo fue posible no actualizar el software de ciberdefensa en nuestras FFAA? ¿Quiénes son los responsables? Lo sucedido, con el hackeo a nuestras FFAA, y de la forma "rutinaria" que se habría producido, nos alerta a lo que podría sucedernos como país. El mejor ejemplo de lo que puede pasarnos como Estado, es la experiencia de Estonia, país que fue atacado en todas sus instituciones, públicas y privadas, peligrando literalmente la supervivencia del Estado; fue el primer país, que afrontó una guerra cibernética. Para contrarrestar dicho ataque generalizado, se tuvo que apagar todos los sistemas de información, bloqueando las redes y las líneas de comunicación; luego de una oportuna reacción del Estado Estonio, y la generación y aplicación de adecuadas políticas de ciberseguridad, a nivel estratégico, por la toma de decisiones de ese país, hoy es reconocido como el país más digitalizado del mundo.

MARCO LEGAL:

En ese orden de ideas propuestos, se hace necesario revisar el marco legal vigente para nuestro tema de investigación, y encontramos lo siguiente:

1.1. La **Ley N° 30618**, de fecha 27 de julio de 2017, modificó el **Decreto Legislativo 1141**, Decreto Legislativo de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia – DINI, con la finalidad de regular la Seguridad Digital, definiéndose en el Artículo 2° como sigue:

*"**Seguridad Digital:** Es la situación de confianza en el entorno digital, frente a las amenazas que afectan las capacidades nacionales, a través de la gestión de riesgos y la aplicación de medidas de ciberseguridad y las capacidades de ciberdefensa, alineada al logro de los objetivos del Estado".*

En el Artículo 8°, de la mencionada Ley, en objetivos, se añade el 8.3. "Realizar actividades destinadas a alcanzar la seguridad digital en materia de seguridad nacional".

La duración de la ley mencionada, tiene una vigencia de solamente cinco (05) años, es decir, el Estado Peruano, se encuentra en plena implementación de todos los procesos necesarios, para alcanzar el objetivo nacional de la Seguridad Digital, y todo lo que representa convivir en un país globalizado.

1.2. El **Decreto Legislativo N° 1412**, publicado el 13 de setiembre de 2018, Decreto Legislativo que aprueba la Ley de Gobierno Digital, tiene por objeto:

"Establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno".

El inciso 6.1. del artículo 6°, Gobierno Digital, señala: "El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público".

En el artículo 8°, la Presidencia del Consejo de Ministros, es el ente Rector en materia de Gobierno Digital, "a través de la Secretaría de Gobierno Digital, que comprende tecnologías digitales, identidad digital, interoperabilidad, servicio digital, datos, seguridad digital y arquitectura digital. Dicta las normas y establece los procedimientos en materia de gobierno digital y, es responsable su operación y correcto funcionamiento".

En el Capítulo VI, se desarrolla todo lo relacionado a la Seguridad Digital, y señala en el artículo 30° que "la seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno.

En el artículo 32°, se regula el Marco de Seguridad Digital del Estado Peruano, considerándose los siguientes ámbitos:

a. **Defensa:** El Ministerio de Defensa (MINDEF) en el marco de sus funciones y competencias dirige, supervisa y evalúa las normas en materia de ciberdefensa.

b. **Inteligencia:** La Dirección Nacional de Inteligencia (DINI) como autoridad técnica normativa en el marco de sus funciones emite, supervisa y evalúa las normas en materia de inteligencia, contrainteligencia y seguridad digital en el ámbito de esta competencia.

c. **Justicia:** El Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ) en el marco de sus funciones y competencias dirigen, supervisan y evalúan las normas en materia de ciberdelincuencia.

d. **Institucional:** Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI).

1.3. El 27 de agosto de 2019, se publicó la Ley N° 30999, Ley de Ciberdefensa, señalando en el artículo 1°, el objeto de la Ley, a saber:

"La presente ley tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado Peruano, regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley".

Al respecto, la presente ley, limita las acciones al ámbito exclusivo del Ministerio de Defensa, como consecuencia, los demás sectores del Estado estarían en una situación permanente de indefensión digital; no es suficiente lo normado en la Ley de Gobierno Digital, para normar las acciones que deben realizar las demás instituciones del Estado, resulta insuficiente, y menos siendo el ente rector la Presidencia del Consejo de Ministros (PCM); se aprecia una relación de acciones, que terminan en buenas intenciones, pero que exponen nuestro ciberespacio, a las amenazas y ataques en los diferentes campos y niveles; por lo que se hace imperativo una política de ciberseguridad, para lo cual es necesario determinar los factores necesarios para la implementación de la política de estado.

3. Fundamentos de la Ciberseguridad y buenas prácticas internacionales

Para poder diseñar e implementar un adecuado plan en ciberseguridad, es necesario comprender los distintos componentes que forman parte del circuito de la información. Al referirnos a un intangible, es importante comprender cómo este mismo es manejado dentro de un espacio no físico y cómo se traduce al ser gestionado por un operador final que logra acceder a dicha información.

El primer componente que establece las bases para el flujo, gestión y guardado de la información es la infraestructura tecnológica con la que se va a contar. Dentro de esta misma se definen aspectos vitales como la base de datos, servidores, interfaces de usuarios, aplicativos, entre otros. Aspectos claves como la escalabilidad de la solución, costos de mantenimiento, nivel de seguridad y facilidad de acceso ayudarán a definir qué solución sería la mejor a articular. Es importante mencionar que en la actualidad existen proveedores que pueden brindar toda la infraestructura necesaria sin necesidad de adquirir equipos de manera física, siendo gestionados a través de la nube. Dichos proveedores, tales como AWS, Google o Microsoft, cuentan con todas las certificaciones de seguridad además de contar con personal experimentado y constantemente en actualización respecto a temas de seguridad. De modo que mediante su contratación uno se puede enfocar en los aspectos relevantes de su operación, teniendo que enfocarse solamente en cumplir con los aspectos referentes a su lado, disminuyendo sustancialmente los potenciales riesgos y costos de implementar toda la infraestructura de manera propia.

A la infraestructura previamente mencionada, se le suma como segundo fundamento clave el uso de protocolos de seguridad, los cuales van a encargarse de definir los parámetros de seguridad para el envío y la recepción de información. En el caso previo, contamos con que el proveedor de infraestructura debería contar con las más altas certificaciones de seguridad, teniendo como ejemplos al ISO 27001 y al SOC 2 Tipo 2, de modo que la pregunta relevante ronda respecto a cómo se transmiten los datos a este mismo. Usualmente, este proceso es determinado por la organización usuaria de los datos, la cual debe definir con su equipo técnico las mejores configuraciones para asegurarse que al recibir la información por su sistema esta pueda llegar sin problemas a su infraestructura tecnológica, sea propia o en la nube.

En tercer punto se encuentra un fundamento trascendental y que usualmente puede socavar todos los

procedimientos de seguridad ya implementados si no se gestiona adecuadamente, involucra la capacitación del personal operativo (técnico o no técnico). Con relación a este punto, al final quienes se encargan de gestionar la información son los individuos, de modo que es sumamente importante que estén adecuadamente capacitados y sepan todos los procedimientos necesarios para asegurar la seguridad digital. Esta carencia de detalle sobre lo relevante de los procedimientos para el flujo y acceso a la información, suele venir del personal no técnico ya que en muchas ocasiones no se les da el suficiente entrenamiento para comprender las diversas maneras en las que un sistema puede ser vulnerado. Uno de los métodos más frecuentes es el phishing, mediante el cual se busca conseguir los accesos del personal a través de enlaces o correos donde se les solicita ingresar datos o pueden activar la descarga de diversos tipos de malware.

Es considerando lo previamente mencionado que un plan de ciberseguridad debe incluir no solo la infraestructura tecnológica, sino comprender los diversos puntos desde los cuales fluye la información así como el personal que puede tener acceso a la misma. Para ello se han establecido diversas normativas internacionales que buscan priorizar la ciberseguridad, en especial la protección de información confidencial o personal. Un punto altamente requerido es contar con un nivel de encriptación para datos en transferencia y en reposo tipo AES-256, usando como mínimo un protocolo de seguridad TLS 1.2. Ambos conceptos son algunas de las buenas prácticas requeridas por el Reglamento General de Protección de Datos (RGPD), el cual busca brindar el mayor nivel de seguridad para el manejo de información. A su vez, certificaciones como el ISO 27001 y el SOC 2 tipo 2, requieren una serie de capacitaciones continuas para el personal operativo, así como el desarrollo de evaluaciones de penetración o vulneración del sistema (Pen Tests) para definir los diversos niveles de riesgo, establecer los protocolos respectivos y plantear un modelo de mejora continua.

4. Cadena de Valor Público para la generación de la Política de Ciberseguridad

Siendo el concepto de “valor público”, aquel *valor* que los y las ciudadanos dan a los bienes y servicios recibidos del estado; siempre y cuando, satisfacen una necesidad, con calidad y oportunidad; por lo que, es un mecanismo potente para el logro del desarrollo sostenible.

En ese contexto, la seguridad digital, en un mundo globalizado, se convierte en valor público fundamental, para la convivencia de todos los peruanos; por lo que se hace necesario revisar los diferentes procesos de producción para la Política de Estado de Ciberseguridad.

1.1. Insumos. - tenemos los siguientes:

- Ciberespacio.
- Ondas electromagnéticas
- Información digital
- TICs.
- Activo crítico sensible.

1.2. Actividades:

- Procesos de gestión de las redes de información digital.
- Servicios digitales.

1.3. Producto:

- Seguridad digital y defensa de la información.

1.4. Resultados Específicos:

- Ciberseguridad o Seguridad Digital.

1.5. Resultado Final:

- Seguridad Nacional.
- Gobernanza en los tres niveles de gobierno.
- Mejora los estándares de vida de los peruanos.

Se hace indispensable, para generar una política de ciberseguridad, desarrollar todos los factores planteados en la cadena de valor de la seguridad digital en el Perú. Consideramos que la clave, se encuentra en los insumos; esto es, determinar nuestra ***soberanía espacial*** (nuevo concepto para la Constitución Política) y administrar el ciberespacio peruano, en las mejores condiciones de seguridad.

5. Operaciones de información en el contexto de la guerra de las informaciones para el estado peruano

Los estados del mundo se ven en la necesidad de establecer políticas claras y definidas para la ***Gestión de la Información***, enmarcadas dentro del dominio de la **Información**.

En el contexto de la globalización, los escenarios se caracterizan por la disposición y accesibilidad de información de fuentes oficiales; originando lo que se denomina un "tráfico" de información híbrido y difuso, por las exponenciales cantidades de información que discurren en la red (nube) y en los servidores de almacenamiento a los cuales; no todos los estados tienen control y exclusividad de uso.

En la actualidad convivimos en un ambiente *informacional* donde se hace necesario comprender como las informaciones son obtenidas, creadas, procesadas, interpretadas y distribuidas. Todo ello se encuentra dividido en 3 componentes: el físico (ALMACENAMIENTO), el lógico (INFORMACIONAL) y el psicológico (COGNITIVO).

El tráfico de información, genera a su vez una "guerra de informaciones" entre los actores y grupos de interés propios de los factores económicos, militares, políticos, sociales y culturales; a su vez la difusión y disponibilidad de la información genera competencia entre las fuentes, los medios y las agencias encargadas de la obtención de la información, para formar un "***mercado informacional***" (fuente abierta y fuente cerrada).

De acuerdo a la doctrina militar y a nivel estratégico del estado el objetivo es la obtención de la denominada **Superioridad de Información**, que es la conquista de una ventaja tanto en términos de obtención, procesamiento y difusión de un flujo continuo de información, como también en términos de explotación o negación del uso de estas mismas capacidades por parte de cualquier adversario.

Las **Operaciones de Información**, a su vez, son definidas por el Comando Conjunto de las FFAA del Perú como "…el uso integrado de las capacidades principales de Guerra Electrónica, Operaciones en el Ciberespacio y Operaciones Sicológicas, Engaño Militar y Operaciones de Seguridad; en conjunto con las capacidades de apoyo y relacionadas, para influenciar, interrumpir, degradar o usurpar la toma de decisiones adversarias humanas y automatizadas protegiendo al mismo tiempo las nuestras".

Hoy el día, la sociedad de la información hace referencia a la creciente capacidad tecnológica para almacenar cada vez más información y hacerla circular rápidamente y con mayor capacidad de difusión; mientras que la sociedad del conocimiento se refiere a la apropiación crítica y selectiva de la información protagonizada por ciudadanos que saben cómo aprovechar la información.

Este tráfico de información ha generado se empiece a construir una **Sociedad de la Información**, alimentada por el manejo de la opinión pública por grupos de interés estratégico; por ello confluyen tiempos de *Fake News*, *Post Verdad*, *Trading Topic* e *Influencer*, donde la virtualización de mano con la inteligencia artificial propone escenarios paralelos llamados: ***metaverso*.**

Nacen así en el mundo organizaciones oficiales (agencias de inteligencia o militares de control y seguridad de información) y no oficiales (organizaciones delictivas como hacker o redes extorsivas) que trafican con la información y desinformación encargadas de implementar procedimientos de guerra de las informaciones para objetivos de nivel estratégico, tácticos y operativos.

Finalmente, el Estado Peruano necesita establecer **Políticas de Gestión de Seguridad y Defensa de las Informaciones**, mediante la aplicación de **Operaciones de Información** a nivel estratégico, que le garanticen la soberanía y el dominio de sus informaciones para la supervivencia del **Estado Informacional**.

6. Nuevas amenazas en el enfoque de la Seguridad y el Gasto Público e Inversión sostenible para las capacidades de Ciberdefensa

El enfoque de la seguridad multidimensional, para hacer frente a las nuevas amenazas, ponen escenarios conectados para acciones del desarrollo con seguridad en diferentes planos.

Estos son, el plano del ciberespacio y el aeroespacial, donde la economía digital está impactando de manera escalonada en el crecimiento de las economías de los países por las nuevas tendencias disruptivas y el cambio generacional en el uso masivo de nuevas tecnologías, debido a que estamos en un mundo digital hiperconectado y que una de las amenazas más potentes hoy en día son las relacionadas al ámbito del ciberespacio y el aeroespacial.

Entonces ¿Qué se requiere como gran paso para una estrategia sostenida de país, a fin de hacer frente a estas nuevas amenazas? Una de las respuestas que se vislumbradas en los estudios el Banco Interamericano de Desarrollo (BID), es referente a que los países cuenten con instituciones fuertes; donde gastar bien sea un prerrequisito para instituciones sólidas, y ello lleva en acompañar el gasto en inversión en mecanismos para la seguridad con enfoque multidimensional, que considere unidades de gestión estratégica (*delivery units*), cultura, sistemas tecnológicos que ayuden en la transformación digital como abanico de oportunidades; datos como herramientas para las toma de decisiones acertadas en el diseño de las políticas públicas y sobre todo el valor del capital humano especializado y entrenado en esta temática.

7. Análisis de las tendencias a nivel mundial para las nuevas amenazas

En 2003, el Perú suscribió “La Declaración sobre Seguridad en las Américas”, instrumento de la cooperación internacional cuyo principal aporte es el compromiso de fortalecer las relaciones para hacer frente a las nuevas amenazas a nivel mundial.

Asimismo, otro de sus aportes es elaborar estrategias coordinadas y planes de acción relacionados con las nuevas amenazas, preocupaciones y otros desafíos a la seguridad hemisférica.

Por esta razón, la misión de la Secretaría de Seguridad Multidimensional (SSM) es promover y coordinar la cooperación entre los estados miembros de la Organización de Estados Americanos (OEA) y de estos con el Sistema Interamericano y otras instancias del Sistema Internacional, para evaluar, prevenir, enfrentar y responder efectivamente a las amenazas a la seguridad, con la visión de ser el principal referente hemisférico para el desarrollo de la cooperación y el fortalecimiento de las capacidades de los Estados Miembros de la OEA .

Este marco nos pone en carrera a partir de 2004, sin embargo, 15 años más tarde, los avances tangibles son los normativos y otros instrumentos importantes, pero no suficientes para cerrar la gran brecha del cómo proyectar a la ciberdefensa y la ciberseguridad, como instrumentos de poder en el ámbito espacial y del ciberespacio; para la seguridad y defensa nacional; así como el desarrollo sostenible.

Estos vacíos presentados en cuanto a los mecanismos para implementar su institucionalidad deben de ser considerados y estructurados. Así, tomando en consideración lo descrito en la Ley N° 29158 y todos los mecanismos disponibles para estructurar y potenciar una estrategia en conjunto que sea sostenible y que pueda hacer frente a estas nuevas amenazas en el ciberespacio y espacio aéreo, que afecten al desarrollo nacional.

La 13ª edición del Informe Global de Riesgos del Foro Económico Mundial (2018), realizado en asociación con Marsh & McLennan Companies, examina el cambiante panorama de riesgo a nivel macro y resalta las amenazas sistémicas que pueden alterar las expectativas. De dicho informe, la segunda amenaza mundial en términos de probabilidad ubica a los ciberataques, como riesgo

sistémico de gran nivel, al igual que los riesgos que representan los desastres naturales, ubicados entre los cinco principales riesgos sistémicos.

Resaltamos que, el enfoque de medición de riesgos, pueden ser de carácter: económicos, geopolíticos, tecnológicos, sociales y medioambientales.

Visto el panorama mundial de las tendencias en relación a los mapas de riegos y la conectividad entre sí, el estudio muestra la metodología basada en la medición de la intensidad del impacto ocasionado en los diversos enfoques; sin embargo, hay necesidad de entender que estas amenazas afectarán según el grado de preparación del país, y la estrategia que aplique.

8. Elementos para el poder aeroespacial y ciberespacio que aportan a la seguridad multisectorial

La Fuerza Aérea del Perú (FAP), cuenta con diversos sistemas y herramientas para la defensa del espacio y del ciberespacio, entendiéndose que dentro de sus funciones según el artículo 4to. del DL 1139 está la defensa del espacio aéreo y en función a los objetivos de las Políticas de Seguridad y Defensa Nacional , que vincula al desarrollo económico y social de manera segura y sostenible con múltiples instrumentos; algunos de ellos enmarcados en los instrumentos y sistemas que desarrolla la FAP.

- CONIDA.
- La Agencia Espacial del Perú y el Perú SAT-1
- Centro Internacional de Investigación Meteorológica y Tropical –CIIMAT, (Proyecto Perú Brasil).
- Sistema de Vigilancia Amazónico y Nacional (SIVAN).
- Programa ante Riesgos y Desastres, con estrategia conectividad aérea.
- Centro Nacional de Vigilancia Amazónico y Nacional –CEVAN.

La FAP cuenta con funciones de carácter multisectorial que aportan al desarrollo del país. Por ello, es importante su participación y aporte a las estrategias para la lucha a las nuevas amenazas, tales como la tala ilegal, la minería ilegal y el narcotráfico; entre las principales; su participación es indispensable para el desarrollo nacional, considerando que la seguridad es parte de ello.

Cabe resaltar la gran importancia que significa el valor de su factor humano; por las capacidades inherentes al ámbito de acción; demostrables por años de experiencia y entrenamiento continuo en estrategias en el ciberespacio y aéreo espacial.

9. Análisis de riesgos para el plan nacional de infraestructura para la competitividad

Esta preocupación es una realidad para muchos sectores, pero principalmente para el Sector Defensa ya que pone en evidencia la ausencia de proyectos en Plan Nacional de Infraestructura para la Competitividad 2019 (PNIC 2019); como los de la Mejora y Mantenimiento del Satélite Perú SAT-1 y los del Sistema CEVAN, este último como mecanismo de control de la Amazonía, donde muchas de las nuevas amenazas se dan.

¿No son estos instrumentos una inversión para la sostenibilidad de los proyectos del PNIC 2019, o representa un gasto? A la vista están relacionados con la sostenibilidad de la seguridad de los proyectos de inversión, así como ser un instrumento para la reducción de riesgos en el ámbito digital.

Por ello, en los análisis de gestión de riesgos para los proyectos priorizados en el PNIC 2019, está ausente el análisis de peligro, de exposición, de vulnerabilidades y estimación del riesgo; para los ataques cibernéticos o la *seguridad digital*.

Asimismo, se puede observar que varios de ellos son de infraestructuras críticas. Ante ello, la pregunta es ¿El nivel de riesgo ante amenazas del ciberespacio o aeroespacial, están considerados en función al tipo de

impacto, nivel de afectación o de intensidad por algún sector?

¿Con qué instrumentos se cuenta para hacer una evaluación de ese tipo, y qué sector debe contar con mecanismos de unidad gestión estratégica para ello?

10. Visibilidad de la inversión en elementos de poder aeroespacial y ciberespacio para la prevención de ataques en el medio digital

Visto los antecedentes mencionados, entonces, podemos cuestionarnos dos preguntas: ¿Qué se está ejecutando para la prevención de los riesgos en el ámbito digital, a pesar que, contamos con capacidades de la FAP? y ¿Cómo se puede visibilizar el presupuesto de inversión en ello?

Para responderlas, una propuesta viable sería considerar una unidad estratégica de gestión en el ámbito del ciberespacio y aeroespacial; a la FAP, considerando sus capacidades para la seguridad multidimensional.

Ello permitirá reducir los riesgos en las estrategias y proyectos a nivel nacional, que consideran instrumentos para la formulación como el PMO y el BIM. También observamos que el modelo econométrico aplicado considera variables del tipo de terreno en las siguientes variables: elevmeg, y agreste1; (anexa el modelo econométrico para su visualización) que justamente son datos que aportan los instrumentos de la FAP mencionados anteriormente.

"El empleo de los medios aéreos durante los primeros instantes de la emergencia son de vital importancia sobre todo para salvar vidas y evitar que el desastre genere efectos irreversibles"; trasladando esta frase a un caso de ciberataques a cualquiera de los activos críticos o las capacidades nacionales en el ámbito digital; hagamos a continuación los siguientes cuestionamientos; ¿Qué capacidad de reacción es la que se tiene para una Seguridad Digital a nivel nacional?

¿Se está invirtiendo en ello adecuadamente? ¿Los mecanismos con que cuenta la Ley 30225 del OSCE, está preparada para ello?;

¿Qué tendría que hacer el MEF para incluir la inversión para la ciberseguridad y ciberdefensa con mecanismos sostenibles, según el DL N° 1440?

A manera de conclusión, es recomendable presentar una estrategia que incorpore los instrumentos con los que cuenta la FAP, para las capacidades de la prevención de las nuevas amenazas en el ciberespacio y espacio aéreo, así como, el soporte de información para los proyectos de inversión pública para el desarrollo nacional y la seguridad multidimensional, con institucionalidad y recursos para su sostenibilidad.

11. Política Sectorial de Ciberdefensa: una necesidad impostergable

Las infraestructuras críticas de un país, los sistemas de comando y control, así como los sistemas de armas cuentan con plataformas informáticas para su funcionamiento; sin embargo, como resultado de un ciberataque, estas plataformas podrían quedar inservibles y paralizar a un país, poniendo en riesgo la Seguridad, la Defensa y el Desarrollo Nacional. Por consiguiente, resulta imprescindible contar con una Política Sectorial de Ciberdefensa, cuyos objetivos y lineamientos permitan fortalecer el desarrollo de capacidades para neutralizar las amenazas y ataques en y mediante el ciberespacio, impulsando la cultura, la educación, así como la Investigación, Desarrollo e Innovación (I+D+i) en ciberdefensa entre las Instituciones Armadas. En este artículo se analiza la situación de la Ciberdefensa en el Perú y se propone el enunciado, así como los objetivos y lineamientos de la necesaria Política Sectorial de Ciberdefensa que el Estado peruano debería poseer.

El incremento de amenazas en el ciberespacio, así como el uso de nuevas tecnologías para generar amenazas informáticas constituyen preocupaciones comunes en todos los países, dado que impactan de manera significativa en la seguridad de la información (en los ámbitos públicos y privados) e, inclusive, en los activos críticos nacionales y recursos claves de un

Estado. En el Perú, la Ley N° 30999, Ley de Ciberdefensa, aprobada el 26 de agosto de 2019, define a la Ciberdefensa como la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio, cuando estos afecten la Seguridad Nacional. Por lo tanto, el desarrollo de capacidades en las Fuerzas Armadas (FF. AA.) para enfrentar los ciberataques y la ciberguerra es una necesidad impostergable en el Estado peruano ya que, de lo contrario, se ponen en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y los recursos claves del Estado. Sin embargo, en el Perú, se carece de una Política Sectorial de Ciberdefensa que oriente el desarrollo de dichas capacidades en las FF. AA.

El ataque cibernético a Estonia

El primer ataque cibernético de gran envergadura contra un Estado se realizó en abril de 2007 en Estonia. A consecuencia de ese ataque, las principales instituciones públicas y privadas de Estonia se vieron paralizadas por una avalancha de ciberataques que tuvieron como objetivos a numerosas instituciones, entre las cuales el Parlamento y varios ministerios, además de bancos, partidos políticos y medios de comunicación. Ante ello, Estonia tuvo que cortar toda la línea de internet y formatear todos sus sistemas.

El ataque cibernético a Estonia reveló una nueva forma de hacer la guerra, pudiéndose asegurar que la dificultad para la identificación de quienes llevaron a cabo el ataque y la naturaleza de los medios empleados cambiaron la imagen de lo que serían los conflictos del futuro. Al respecto, el Director del Centro de Seguridad Informática de Estonia indicó que todo fue muy confuso en los días precedentes al ataque debido a que no entendían lo que estaba pasando; asimismo, afirmó que la magnitud y el impacto del ataque fueron mucho mayores de lo que podrían haber imaginado. Durante dichos eventos, los *hackers* atacaron sustituyendo los portales de las páginas oficiales por imágenes insultantes contra el Primer Ministro estonio. El tráfico en internet se disparó bruscamente hasta saturar los servidores y la población de Estonia salió a tomar las calles de la capital ya que sentían que su gobierno perdía poco a poco el control de la situación. Cuando el Ministerio de Defensa intentó averiguar lo que pasaba, descubrió que no solo las agencias de noticias habían sido atacadas sino, también, los grandes bancos comerciales lo que, en un país pequeño como Estonia, fue una gran preocupación a todo nivel. El ataque cibernético estuvo a punto de generar una revuelta, ya que los estonios de origen ruso invadieron el centro de la capital, mientras los sistemas informáticos se bloquearon, la distribución de la gasolina y del pan fueron interrumpidos y la anarquía se propagó por el país.

Como respuesta a este ataque cibernético, la Organización del Tratado del Atlántico Norte (OTAN) implementó en Tallin, la capital de Estonia, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, siendo considerado actualmente un referente en ciberdefensa a nivel mundial. Asimismo, en enero de 2008, la OTAN promulgó la Política de Ciberdefensa con el objetivo de mejorar la capacidad de la Alianza para proteger sus sistemas de información y comunicaciones, de importancia crítica frente a los ciberataques.

Posteriormente, en Varsovia, en julio de 2016, los Jefes de Estado y de Gobierno miembros de la OTAN se comprometieron -a través del documento *Cyber Defence Pledge*- a mantenerse alertas ante las ciberamenazas y a ser capaces de defenderse en el ciberespacio, tal y como ocurre en el dominio terrestre, aéreo y marítimo, reconociendo al ciberespacio como un nuevo dominio de las operaciones militares.

La ciberdefensa en el Perú

Tras el caso descrito, resulta indudable afirmar que el Estado peruano requiere crear el ambiente y las condiciones necesarias para brindar efectiva protección en el ciberespacio y enfrentar las amenazas que atentan contra su seguridad. En ese sentido, tomando en consideración que las FF. AA. requieren actuar de forma integral frente a las amenazas cibernéticas, es necesario que el Perú cuente con una Política Sectorial de Ciberdefensa.

Al respecto, en el año 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. Este proyecto de Directiva –aunque no fue aprobado con Resolución Ministerial- fue tomado en consideración para la formulación del Plan Estratégico Sectorial Multianual (PESEM) 2017-2021, el mismo que para alcanzar su Objetivo Estratégico 1 (Garantizar la Defensa Nacional) contemplaba la implementación de la Acción Estratégico 1.7 (Desarrollar la Ciberdefensa protegiendo la infraestructura critica del Estado de ciberataques). Incluso, el Plan Estratégico Institucional (PEI) 2018-2020 del Sector Defensa contempla alcanzar el Objetivo Estratégico 6 (Desarrollar la Ciberdefensa institucional). Para ello, tanto el Comando Conjunto de las Fuerzas Armadas (CCFFAA) como las Instituciones Armadas han creado sus entidades de ciberdefensa, lográndose promulgar la Ley N° 30999, Ley de Ciberdefensa.

Al respecto, el 25 de marzo de 2019, el CCFFAA activó el Comando Operacional de Ciberdefensa (COCID), inaugurando sus instalaciones el 20 de enero de 2020. El COCID cuenta con tres Componentes (terrestre, naval y aéreo). Por una parte, el Componente Terrestre lo conforma el Centro de Ciberdefensa del Ejército, inaugurado el 29 de octubre de 2018. Por otra parte, el Componente Naval lo conforma la Comandancia de Ciberdefensa de la Marina de Guerra, inaugurado el 21 de febrero de 2019. Asimismo, el Componente Aéreo lo conforma el Grupo de Operaciones en el Ciberespacio de la Fuerza Aérea, inaugurado el 21 de diciembre del 2019.

Línea de Tiempo de los Avances de la Ciberdefensa en el Perú

A la fecha, el COCID ha realizado operaciones de ciberdefensa durante la realización de los XVIII Juegos

Panamericanos y VI Juegos Para panamericanos de Lima 2019, las Elecciones Congresales de enero de 2020 y la ejecución del Plan de Vacunación COVID- 19 del año 2021. Todas estas experiencias han servido para conocer e identificar las debilidades del Estado Peruano en el entorno digital, sobre todo en los activos críticos nacionales del sector público, lo que conllevaría a poner en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves del Estado.

En ese sentido, el Artículo 12 (sobre el control y la protección de los activos críticos nacionales y recursos claves) de la Ley N° 30999, Ley de Ciberdefensa, señala que *"el CCFFAA está a cargo de la Ciberdefensa de los activos críticos nacionales y recursos claves, cuando la capacidad de protección de sus operadores y/o del sector responsable de cada uno de ellos y/o de la Dirección Nacional de Inteligencia sea sobrepasada, a fin de mantener las capacidades nacionales, en el ámbito de la seguridad nacional"*[12]. Por consiguiente, para cumplir eficazmente esta función, el Gobierno debe asignar los recursos necesarios que permitan fortalecer y desarrollar capacidades en Ciberdefensa tanto del COCID, como de sus Componentes.

Asimismo, resulta imprescindible la formulación, aprobación e implementación de una Política Sectorial de Ciberdefensa que señale los objetivos y lineamientos que deberán ser alcanzados por el Sector Defensa. Para ello, a continuación, se brinda una propuesta del enunciado de dicha Política, así como de sus objetivos y lineamientos con la finalidad de brindar ideas y facilitar su necesaria formulación. En ese sentido, el enunciado de la Política de Ciberdefensa podría ser: *"Contar con FF. AA. con una capacidad de Ciberdefensa adecuada para hacer frente a las amenazas o ataques realizados en y mediante el ciberespacio, que pongan en riesgo la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales, considerando las debilidades del Estado en el entorno digital"*.

Asimismo, tomando como referencia el proyecto de Directiva formulado por la Dirección de Política y Planeamiento Estratégico para la Defensa del Ministerio de Defensa y las experiencias obtenidas durante estos últimos años, los objetivos y lineamientos de la Política Sectorial de Ciberdefensa podrían ser los siguientes:

- **Objetivo 1:** *"Fortalecer la capacidad de Ciberdefensa de las FF. AA. para neutralizar las amenazas y ataques en y mediante el ciberespacio cuando afecten la seguridad nacional"*, proponiéndose –para ello- los siguientes **Lineamientos**: (1) Fortalecer el COCID a fin de neutralizar la ciberamenazas y responder los ciberataques que atenten a la seguridad nacional. (2) Potenciar las capacidades militares de las organizaciones de ciberdefensa de las Instituciones Armadas, asegurando el ciberespacio que emplean las fuerzas terrestres, navales y aéreas, así como el ciberespacio de los activos críticos y recursos claves designados. (3) Mejorar las capacidades de las FF. AA. para contar con información oportuna ante una posible ciberamenaza, desarrollando alertas tempranas y apoyo a las operaciones ante ciberataques.

- **Objetivo 2:** "Impulsar la cultura y la educación en ciberdefensa en las FF. AA.", proponiéndose los siguientes **Lineamientos**: (1) Concientizar al personal que labora en el Sector Defensa de los riesgos derivados de las actividades en el ciberespacio, en busca de consolidar la cultura de ciberdefensa. (2) Desarrollar conocimientos, habilidades, experiencia y capacidades tecnológicas en las instituciones del sector para soportar y cumplir los objetivos de ciberdefensa, certificando la calidad educativa. (3) Impulsar la formación, capacitación, especialización del personal en cursos y programas de pre y post grado en Ciberdefensa.

- **Objetivo 3:** "Desarrollar Investigación, Desarrollo e Innovación (I+D+i) en Ciberdefensa colaborativa entre las FF. AA". Para ello, se proponen los siguientes **Lineamientos**: (1) Mejorar las Políticas para I+D+i en ciberdefensa a fin que sean adecuadas y oportunas. (2) Implementar Infraestructura y equipamiento adecuado para la I+D+i en ciberdefensa. (3) Promover proyectos de I+D+i culminados en las FF. AA. (4) Fomentar la colaboración en I+D+i entre las Instituciones de las Fuerzas Armadas.

- **Objetivo 4:** "Impulsar la cooperación nacional e internacional a fin de contar con una seguridad cooperativa en el entorno digital", proponiéndose los siguientes **Lineamientos**: (1) Incrementar la presencia del Sector Defensa del Perú en organizaciones y foros internacionales en ciberdefensa. (2) Suscribir acuerdos con organizaciones nacionales e internacionales de países con quienes el Perú comparta intereses. (3) Fomentar la participación coordinada con otras instituciones públicas y privadas en simulacros y ejercicios internacionales de ciberdefensa. (4) Aumentar la cooperación con organismos nacionales e internacionales en materia de ciberdefensa, buscando la estandarización y alineamiento de procesos.

12. La Ciberdefensa en el Desarrollo y Seguridad Nacional

Los ciberataques comienzan silenciosamente, alguien hace clic en un enlace de un correo electrónico y al principio parece que no pasa nada, pero ese clic abre la puerta a los intrusos y cuando llega el momento atacan. Nada funciona creando caos y confusión, pero si ese sistema es necesario para que funcione un país entero, si ese sistema es un activo crítico nacional que afecte el desarrollo, seguridad y defensa nacional ¿qué se puede hacer para protegerlos? En el presente artículo analizaremos cómo la tecnología digital se ha vuelto indispensable para el funcionamiento de nuestras sociedades y cómo gracias a esto, los *hackers* pueden dejarnos fuera de combate en cuestión de milisegundos; explicaremos cómo funcionan los ataques informáticos sobre una red importante, veremos cómo los ciberdelincuentes han convertido al ciberdelito en una industria y negocio más rentable que el narcotráfico y tráfico de armas (Lozano, 2022), ganando miles de millones de dólares, afectando a infraestructuras y activos críticos nacionales. Por los avances tecnológicos, cada vez más, los activos críticos nacionales dependen de los sistemas informáticos y cuando estos son atacados y es sobrepasada la capacidad de ciberseguridad de sus operadores, sectores responsables o la Dirección de Inteligencia Nacional, la ciberdefensa actúa, siempre que afecta la seguridad nacional (Ley Ciberdefensa, art. 4. Congreso de la República de Perú).

¿Imaginas tu vida sin poder tener alimento y agua, sin poder movilizarte, cobrar tu sueldo o tener garantizada la atención de tu salud, o sin energía eléctrica, internet y redes de telecomunicaciones?, sería un caos.

Para garantizar nuestro bienestar cotidiano, están los activos críticos nacionales y los ciudadanos debemos valorarlos. Pero, ¿qué son los activos críticos nacionales? Son las principales infraestructuras, recursos y sistemas del país que garantizan la atención de nuestras necesidades vitales y el desarrollo nacional de nuestra vida cotidiana; son esenciales, sin estos los peruanos resultaríamos muy afectados, es por eso que el estado busca protegerlos y nosotros los ciudadanos debemos valorarlos. Tengamos en cuenta que los activos críticos nacionales nos permiten atender nuestras necesidades vitales, como los servicios públicos, agua, energía, transporte, saneamiento, salud entre otros. Nos permiten el servicio de instituciones del estado y la administración pública, nos permiten garantizar nuestra integridad física, la seguridad ciudadana, la gestión de riesgo de desastres y la defensa nacional, de igual forma, nos permiten todo aquello que contribuye al bienestar social y económico.

Los activos críticos nacionales son esenciales para satisfacer nuestras necesidades vitales; y, para que nuestro Perú pueda alcanzar sus objetivos nacionales, es realmente importante que todos los peruanos tengamos garantizada la atención de nuestras necesidades vitales, por eso el valorar los activos críticos nacionales, está en nuestras manos.

Para la protección y defensa de los activos críticos nacionales, la ciberdefensa cumple un rol muy importante, pues es el último bastión cuando estos sufren ciberataques, porque actúan una vez que ha sido sobrepasada la capacidad de protección de sus operadores, sector responsable o la Dirección de Inteligencia Nacional nacional (Ley Ciberdefensa, art. 4. Congreso de la República de Perú), haciendo uso de sus fortalezas y capacidades, realizando ciberoperaciones (JID, 2020).

En muchos sentidos las sociedades avanzadas son como el cuerpo humano: en ellas ocurren simultáneamente miles de procesos diferentes e, igual que algunos órganos, son fundamentales para nuestra supervivencia; algunas infraestructuras o activos son tan vitales que todo se derrumbaría sin ellas. Tradicionalmente estos activos críticos se construyen para que puedan funcionar de forma autónoma, pero en las dos últimas décadas, gran parte de ellas se conectaron a Internet y ahora dependen del acceso a la tecnología digital; como si un cuerpo humano estuviera conectado a un cerebro artificial externo, millones de veces más potente. Esto ha creado una capa silenciosa e invisible de tecnología digital que conectan nuestros activos críticos, permitiendo que funcionen con más eficacia, pero, también, hace que sea cada vez más interdependiente.

Los aerogeneradores de Alemania, por ejemplo, pueden necesitar estar conectados a satélites estadounidenses, para que funcionen bien, por eso, una disrupción en esta capa invisible ocasionaría posiblemente efectos en cascada y en el peor de los casos dejar sin control y fuera de juego la infraestructura o activo crítico de toda una sociedad.

Caso Ciberataque al Distrito de Anhalt-Bitterfeld, Alemania, 2021.

Anhalt-Bitterfeld es una ciudad en el centro de Alemania que se vio afectada por una forma de ciberdelincuencia que acecha en las sombras del internet: a las seis y media de una mañana del verano del 2021, llegó la primera llamada al departamento de informática, sus funcionarios habían prendido su computadora y no funcionaba nada, los archivos estaban encriptados. Los responsables de los servicios digitales pensaban que era un ataque que se resolvería en poco tiempo, que lo aclararían en los próximos días, pero las llamadas seguían llegando con empleados de todo el distrito quejándose de que sus computadoras estaban muertas. Alarmados, los informáticos revisaron el sistema y encontraron una nota de rescate que les helo la sangre, se dirigía directamente a ellos, alguien lo había preparado muy bien, fue entonces cuando comprendieron que se no se trataba de un ciberataque más, esto era mucho más serio y cuando

la computadora del jefe informático de Anhalt-Bitterfeld, que tiene todos los derechos y accesos, se encriptó, conocieron que tenían un problema grave. ¿Quiénes eran los intrusos?, ¿qué querían? y ¿cómo saldría el distrito de esta situación?

El segundo día del ciberataque en Anhalt-Bitterfeld, la noticia ya estaba en la prensa, indicando que habían hackeado a la administración y no se sabía cuándo podrían volver a trabajar. Los programas de las distintas oficinas estaban conectados entre sí a través de la infraestructura informática. Nada funcionaba, ni la caja registradora, ni el sistema de alarma; oficinas enteras, desde la asistencia social, hasta los servicios de inmigración tuvieron que cerrar y a medida que las noticias sobre el apagón cibernético se extendían, también se extendía el temor de los residentes. La gente se preguntaba si la oficina sería capaz de pagar la asistencia social, las dietas, la ayuda a los ancianos, etc. ¿Qué sucedió?, en pocas horas las autoridades se dieron cuenta de que la comunidad había sido víctima de la ciberdelincuencia organizada con un ataque de *ransomware*.

¿Qué se conoce de un ataque de ransomware; qué sabemos exactamente; cómo funcionan estos ataques? Suelen seguir un guión similar: en primer lugar, los intrusos acceden a una red informática, al igual que los virus biológicos encuentran varias formas para entrar en nuestro cuerpo, los intrusos tienen un arsenal de herramientas para entrar en el sistema, a menudo se disfrazan de contactos de confianza y convencen a las personas para que compartan sus credenciales de acceso; una vez dentro del sistema, suelen pasar semanas o incluso meses a la caza, buscan información los suficiente sensible como para que la gente pague para recuperarla. Cuando encuentran lo que buscan, encriptan los datos y envían un mensaje a su víctima, ofreciéndole una clave a cambio de un rescate. Las víctimas tienen dos opciones, pagar y confiar en que les devolverán los datos o negarse e intentar recuperar por su cuenta parte de los datos secuestrados.

En la sala de operaciones técnica o sala de guerra, los responsables de los servicios digitales de Anhalt-Bitterfeld buscaban soluciones. Tenían mucha adrenalina, mucho estrés, con jornadas de diez y seis o diez y ocho horas, y con discusiones por culpa del estrés. Olivert Rumpt, jefe de Tecnologías de la Información (TI) de Anhalt-Bitterfeld, reflexionaba sobre la situación, indicando que «teníamos que actuar, tenían que encontrar soluciones, mis pensamientos y miedos, oh dios mío, qué va a pasar, cuánto durará esto» (Canal DW, 2021).

Poco a poco se dieron cuenta de la magnitud de lo que había sucedido, todos los correos electrónicos de los últimos 20 años se habían perdido, todos perdidos, imposibles de recuperar. Cómo comunicar esto a los empleados, indicarles que «lo sienten, pero su cerebro se borró», muchos utilizan sus sistemas de email como un archivo donde guardan todos sus correos.

¿Cómo lograron acceder los intrusos al sistema; dónde está la brecha que utilizaron? El ataque inicial se produjo a través de un correo electrónico de *phishing*. Meses antes, un empleado había hecho clic en un enlace infectado dentro de un correo electrónico y había introducido su contraseña, en este momento, al parecer, los atacantes ingresaron al sistema. El atacante estuvo en el sistema al menos unos seis meses, aproximadamente.

Ataques de ransomware como el de Anhalt-Bitterfeld, se han convertido en algo habitual y cada vez es peor, es el cibercrimen organizado. En Alemania, los sistemas informáticos de más de cien comunidades e instituciones públicas fueron tomados como rehenes en los últimos dos años. Es una industria en auge y es una industria que tiene gestores, planificadores, promotores, etc. Los grupos criminales aprovecharon la pandemia del COVID-19 y los cambios en nuestras vidas para atacar las instituciones públicas sanitarias, tal como ocurrió con el sistema de salud de Irlanda (ABC, 2021).

El ciberataque a Anhalt-Bitterfeld lo realizó un grupo que se llamaba «Pay or gruibe» y el importe del rescate era de quinientos millones de euros, una cantidad exacerbada para un distrito como ese. El ciberataque debía ser cubierto por el distrito, tenían que cubrir todos los costos de recuperación. En algún momento pensaron en pagar para que todo volviera a la normalidad, sin embargo, no tenían el presupuesto, ni contaban con un seguro en caso de ciberataque, por lo que decidieron no pagar ese rescate, pues, además, el sector público no puede entrar en este tipo de juego. En un escenario del pago de rescate, ¿les darán la clave? y no olvidemos que el virus estaba en este sistema, ¿quién asegura que no dejarán una puerta trasera para volver a atacar y encriptar?, se conocen casos de entidades públicas y privadas que han accedido a pagar, sin embargo, el 92 % no han logrado recuperar el total de sus archivos (Computerworld, 2021).

La comunidad de Anhalt-Bitterfeld analizó a detalle la situación y la decisión que se tomó fue algo nunca antes visto. Por primera vez en la historia de Alemania, las autoridades declararon el estado de emergencia por un ciberataque, lo cual no fue fácil. Normalmente esto sólo se hace cuando la vida y la integridad física están en peligro. Por ejemplo, cuando durante las inundaciones de 2002 y 2013 se declaró catástrofe en el distrito. Pidieron consejo a muchos expertos y cuando quedó claro que se trataba de un asunto muy importante, dieron el paso para enviar una señal clara, para poder actuar rápidamente y para poder generar ayuda externa. Esto significaba, entre otras cosas, que las fuerzas armadas alemanas podrían enviar a sus ciber expertos para ayudar a los funcionarios a recuperar el control del sistema, lo cual ayudó enormemente, ya que el departamento de informática no disponía de suficiente personal, sin embargo, su lucha estaba lejos de terminar.

Cuando las autoridades del distrito de Anhalt-Bitterfeld, decidieron no pagar el rescate, en los días que siguieron a esa decisión, empezaron a sentir las consecuencias. A pocos días de recibir la petición de rescate, los primeros datos fueron publicados, eran datos de carácter interno, informaciones personales de los miembros del consejo del distrito. Todo esto se publicó en la *dark web*. Los

archivos incluían información sensible, como datos de cuentas bancarias, o la situación laboral de más de noventa personas.

La paralización de la administración tuvo efectos inesperados en todo el distrito. Por ejemplo, un concesionario Auto-Center-PFUHL, necesitaba la aprobación oficial del distrito para que los vehículos circularan por las carreteras; sin ella, los autos se quedaban en el concesionario y no podían utilizarse; por eso, después que el ciberataque dejara fuera de combate a la administración, el concesionario no pudo entregar más vehículos a sus nuevos propietarios, ocasionando un periodo de tres a cuatro semanas de inactividad. La concesionaria reanudó lentamente, pero, casi un año después, todavía siente las consecuencias: en este trimestre perdió setecientos cincuenta mil euros de facturación.

El daño financiero del ciberataque en Anhalt-Bitterfeld fue de entre 1.7 a 2 millones de euros, presupuesto que se había reservado para la digitalización y para renovar el sistema informático en los próximos años. Fue muy doloroso para los funcionarios del distrito, porque tenían una estrategia focalizada en objetivos y tuvieron que gastar el dinero para volver al punto de partida. El distrito tardó casi un año en volver a poner todo en marcha, y más para recuperar la confianza de los ciudadanos en su administración y la seguridad de que el Estado estará ahí siempre que lo necesiten. Esto es esencial y un problema enorme; Anhalt-Bitterfeld es, posiblemente, sólo un aviso y lo ocurrido aquí es más que el presagio de lo que está por venir.

Panorama General

Tomando el caso anterior como ejemplo, vale la pena preguntarse qué pasaría si los ciberataques en vez de realizarse a una pequeña ciudad, lograron hackear los activos críticos de todo un país. Los hackers lo han intentado recientemente: en el 2019 los ciberatacantes irrumpieron en la red de la mayor central nuclear de la India (El País, 2019); el 2021 un ciberataque a un proveedor de gasoducto provocó compras de pánico y escasez de gas en Estados Unidos, declarando el estado de emergencia (BBC, 2021); finalmente, en 2022 los hackers paralizaron los sistemas informáticos del gobierno de Costa Rica, declarando también el estado de emergencia (Bit2Me News, 2022). Cada uno de estos ciberataques tuvo un impacto local o regional en el territorio donde se produjo; sin embargo, si un grupo decidiera lanzar varios ciberataques simultáneamente en muchos países distintos de todo del mundo, el impacto sería potencialmente devastador. Ahora bien, supongamos que los atacantes no lo hacen sólo por dinero: podrían actores estatales y no estatales, por ejemplo, utilizar métodos similares como un arma para sembrar el caos en su enemigo; esto es un auténtico problema, pues si los ciberdelincuentes cooperan con los actores estatales y no estatales, la combinación es explosiva. Cabe mencionar que increíblemente difícil decir con total precisión, quién está detrás de un ciberataque.

Así mismo, se debe tener presente que los costos de los ciberataques llegan a ser equivalentes a presupuestos estatales, llegando a seis billones de dólares en el 2021 y creciendo año con año, con un escenario posible de alcanzar para 2025 los 10.5 billones de dólares (Diario Libre, 2022).

Ciberseguridad en los Activos Críticos Nacionales

¿Cómo pueden las comunidades mejorar la protección en sus sistemas informáticos para evitar este tipo de ciberataques?

En primer lugar, dejar atrás las ideas anticuadas sobre ciberseguridad que se han mantenido durante décadas. El modelo clásico es como un castillo con un foso, todo lo de dentro sería valioso y lo de fuera peligroso; ese modelo no funciona en la era post covid en la que todos nos conectamos desde cualquier lugar. La pregunta ya no es si entrará un ciberatacante, porque todos sabemos que entrará; para protegerse debemos descubrir cuándo entra alguien y en el mejor de los casos descubrirlo en una fase muy temprana. La ciberprotección de hoy en día, no consiste tanto en defender la muralla del castillo, si no en tener guardias dentro de él que estén preparados para luchar contra los invasores y sacarlos cuanto antes. Así es como se puede mantener cierto control, incluso cuando ya se está siendo atacado. Esta resiliencia es muy importante, pues quienes han experimentado la pérdida del control total de sus sistemas informáticos dicen que las huellas que dejan los ataques pueden ser muy graves.

Ciberguerra Entre Rusia y Ucrania

La guerra Rusia y Ucrania se inició con ciberataques el 14 de enero del 2022, antes del ataque físico, con masivos ataques de denegación de servicios (DDos) a setenta sitios web gubernamentales de Ucrania. El 14 y 15 de febrero los sitios web de las Fuerzas Armadas, Ministerio de Defensa, así como de medios financieros como Oschadbank, y el Pribatbank fueron también ciber atacados.

Igualmente, tanto el 24 como el 25 de febrero, que se inició el ataque con tropas, el parlamento ucraniano denunció una campaña de *phishing* (Newtral, 2022).

Del mismo modo, al inicio de la guerra con tropas, el 24 de febrero mediante una cuenta en Twitter, *anonymous* le declaró la guerra a Rusia, apoyando a Ucrania.

Durante los primeros días de la guerra se desencadenó un conflicto al interior del ecosistema de *ransomware* criminal. Esto puede sonar complicado, pero lo más importante es entender que antes de la invasión, grupos rusos que se dedicaban al secuestro de datos habían estado trabajando también con personas dentro de Ucrania. Cuando estalló el conflicto, estos operativos ucranianos no estuvieron contentos con lo que estaban haciendo las bandas de *ransomware*, así que prefirieron filtrar información para ayudar a las fuerzas del orden en todo el mundo a localizar y detener a estas bandas.

Hoy tenemos que despertar ante una realidad

contundente: las guerras se libran también en el ciberespacio, que es un nuevo domino donde se realizan operaciones militares y donde el comandante de una fuerza debe emplear todas sus capacidades, incluida la ciberdefensa, para logra el objetivo de su misión.

La Ciberdefensa

La ciberdefensa es la capacidad militar que se emplea si se afecta la seguridad nacional cuando existen ciberamenazas o ciberataques (Ley Ciberdefensa, art. 4. Congreso de la República de Perú). Es también el último bastión en la protección de activos críticos nacionales o recursos claves cuando sufren ciberataques, porque actúan haciendo uso de sus capacidades una vez que ha sido sobrepasada la capacidad de protección de sus operadores, sector responsable o la Dirección de Inteligencia Nacional (Ley Ciberdefensa, art. 12. Congreso de la República de Perú). En el Perú el responsable de la planificación, dirección y conducción de las operaciones de ciberdefensa es el Comando Conjunto de las Fuerzas Armadas, a través del Comando Operacional de Ciberdefensa (CCFA, s. f.).

Comando Operacional de Ciberdefensa

El Comando Operacional de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas es una fuerza militar con capacidad de ciberdefensa y es el responsable de realizar el planeamiento, organización, dirección y conducción de las operaciones militares conjuntas de ciberdefensa, defendiendo, explotando y respondiendo las ciberamenazas y ciberataques que alteren o impidan el normal funcionamiento de nuestras redes digitales, sistemas de información, telecomunicaciones, activos críticos nacionales y recursos claves que minan la seguridad nacional (CCFA, s. f.).

Los componentes de ciberdefensa de las Fuerzas Armadas, es decir, aquellos elementos que componen el Centro de Ciberoperaciones (CCO) (JID, 2020), son los siguientes:

1. Componente de Ciberdefensa del Ejército del Perú: es el Centro de Ciberdefensa, cuyo ámbito de responsabilidad es el ciberespacio que emplean las Fuerzas Terrestres y los activos críticos nacionales y recursos claves asignados para la seguridad.

2. Componente de Ciberdefensa de la Marina de Guerra del Perú: es la Comandancia de Ciberdefensa, cuyo ámbito de responsabilidad es el ciberespacio que emplean las fuerzas navales y los activos críticos nacionales y recursos claves asignados para la seguridad.

3. Componente de Ciberdefensa de la Fuerza Aérea del Perú: es el Grupo de Operaciones en el Ciberespacio, cuyo ámbito de responsabilidad es el ciberespacio que emplean las Fuerzas Aéreas y los activos críticos nacionales y recursos claves asignados para la seguridad.

Es importante mencionar que el empleo de la capacidad de ciberdefensa se realiza en estricto cumplimiento del capítulo II de la Ley de ciberdefensa (Ley Ciberdefensa, art. 12. Congreso de la República de Perú) y las ciberoperaciones (JID, 2020). El empleo de la fuerza por parte de los componentes de Ciberdefensa de las Fuerzas Armadas se puede dar en legítima defensa o en cumplimiento de la misión asignada. El empleo de la fuerza en legítima defensa surge en respuesta a un ataque (acto hostil) o amenaza de un ataque inminente (intención hostil), que ponga en riesgo y atente contra la soberanía, los intereses nacionales, los activos críticos nacionales o recursos claves para mantener las capacidades nacionales (Ley Ciberdefensa, art. 10. Congreso de la República de Perú).

La ley de Ciberdefensa fue pública el 9 de agosto del 2019, siendo muy urgente cumplir con la disposición complementaria primera de la ley, que da un plazo máximo de noventa días para formular el reglamento, habiendo transcurrido hasta la fecha tres años. Este reglamento es muy importante, a fin de poder emplear la capacidad de ciberdefensa con el paraguas legal correspondiente, como lo realizaron las fuerzas armadas alemanas cuando se apoyaron de ciber expertos para recuperar el control de los sistemas informáticos de la comunidad de Anhalt-Bitterfeld.

Hay que tener presente que la capacidad de ciberdefensa de las Fuerzas Armadas permite también apoyar en el Orden Interno, realizando coordinaciones interinstitucionales y cooperado operativamente con la Policía Nacional del Perú, el Ministerio Público y el Poder judicial, en la lucha contra los delitos informáticos, de acuerdo a la 4ta y 5ta Disposición Complementaria Final de la Ley de Delitos Informáticos Nº 30096 y la Ley Modificatoria N° 30171.

Formación en Ciberseguridad y Ciberdefensa

A fin de tener una nueva generación de expertos en Ciberseguridad y Ciberdefensa, el Centro de Altos Estudios Nacionales desde el año 2018 imparte un diplomado en Ciberseguridad y Ciberdefensa, habiendo hasta la fecha formado más de medio centenar de especialistas. Por otro lado, en el presente año, 2022, se inició la I MAESTRÍA en Ciberseguridad y Ciberdefensa con mención en Transformación Digital, con base en el diplomado en Ciberseguridad y Ciberdefensa. En ella, se propone un programa con dos semestres en ciberseguridad, un semestre en ciberdefensa y un semestre de transformación digital. Para los cursos de la Maestría en Ciberseguridad y Ciberdefensa con mención en Transformación Digital se ha tomado como referencia la Iniciativa Nacional para Carreras y Estudios en Seguridad Cibernética (NICCS, s. f.), siendo el principal recurso en línea para capacitación, educación e información sobre carreras en seguridad cibernética de la Agencia de Seguridad de Infraestructuras y Ciberseguridad de EE. UU.

Al finalizar el proceso formativo, los estudiantes de la Maestría en Ciberseguridad y Ciberdefensa con Mención en Transformación Digital, estarán cualificados para una función directiva en el área de ciberseguridad y para una ocupación consultiva de nivel estratégico–operativo,

incluyendo riesgos tecnológicos y soluciones de ciberseguridad para el negocio, con herramientas en la capacidad de Ciberdefensa que les permita actuar frente a ciberamenazas o ciberataques que afecten la seguridad nacional. El programa forma líderes en el fenómeno global de la transformación digital de entidades públicas y privadas, con capacidades para aplicar herramientas tecnológicas, gestionar emergencias y realizar investigación y con mira en los objetivos nacionales, el desarrollo sostenible y la defensa nacional.

La realidad hoy en día es que la tecnología es cada vez más sofisticada y los ciberatacantes encontrarán cada vez más formas de lograr su objetivo, por eso, para evitar el peor de los escenarios como que los ciberataques paralicen todo un país, los gobiernos deben atacar el problema de raíz, las infraestructuras o activos críticos deben estar protegidos con plataformas informáticas seguras de la última generación, y, quizás lo más importante, los países deben invertir en la formación de una nueva generación de expertos en Ciberseguridad y Ciberdefensa, lo cual requerirá tiempo, dinero y compromiso político. Estas acciones deben tomarse, pues la amenaza de los ciberataques está aquí para quedarse.

Así mismo, a fin de cumplir con lo dispuesto por la ley de ciberdefensa, se debe asignar recursos suficientes y necesarios a las Fuerzas Armadas para tener una capacidad de ciberdefensa que sea el último bastión de protección en el ciberespacio, que sea disuasiva y que pueda ser empleada cuando el Estado Peruano lo requiera, ya sea para el desarrollo: actuando en defensa de los Activos Críticos Nacionales y Recursos claves, cuando su capacidad de protección sea sobrepasada, teniendo presente que ellos son esenciales para satisfacer nuestras necesidades vitales y para que nuestro Perú pueda alcanzar sus objetivos nacionales; sea para el orden interno: realizando coordinaciones Interinstitucionales y operativas con la PNP, Ministerio Público y Poder Judicial en la lucha con los Delitos Informáticos; o sea en su rol primordial de garantizar la independencia, la soberanía y la integridad territorial de la República: actuando ante ciberamenazas o ciberataques que afecten la Seguridad Nacional.

13. Ciberseguridad comparada: La Ciberseguridad y la Ciberdefensa en el Ecuador

En el Ecuador la seguridad del Ciberespacio ha venido evolucionando paulatinamente desde el año 2011, el país incursiona incipientemente en el ámbito de la ciberseguridad, para ese entonces la Secretaría Nacional de la Administración Pública crea la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación, la cual estaría conformada por delegados del **Ministerio de Telecomunicaciones y de la Sociedad de la Información** (MINTEL), la Secretaría Nacional de Inteligencia (SENAIN) y la Secretaría Nacional de la Administración Pública (SNAP), otorgándole las atribuciones de articular lineamientos de seguridad informática, protección de infraestructura de redes y sistemas, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional.

Posteriormente en el año 2013, se desarrolló e implementó el Esquema Gubernamental de Seguridad de la Información (EGSI), el cual fundamentalmente se implementó en las instituciones de la Administración Pública Central con el fin de que las Instituciones públicas cuenten con un marco de referencia para la gestión de la seguridad de la información.

Para el año 2014, debido a una serie de incidentes informáticos que se llevaron a cabo en contra de la infraestructura tecnológica de nuestro país, se crea el Centro de Respuesta a Incidentes Informáticos (EcuCERT) como parte de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador (ARCOTEL), con el objetivo de brindar el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, capacitación y soporte técnico a la ARCOTEL, a los prestadores de servicios de telecomunicaciones y a las instituciones del sector público y privado con la finalidad de contribuir a la seguridad de las redes de telecomunicaciones de todo el país y así como del uso de la red de Internet.

Bajo este contexto de inseguridad cibernética y con la finalidad de fortalecer y asegurar el entorno digital, el MINTEL como órgano rector de las Telecomunicaciones y de las Tecnologías de información y Comunicación del país, con el asesoramiento de varias organizaciones internacionales, aprueba y pública la Política Nacional de Ciberseguridad mediante Acuerdo Ministerial 006-2021, con el propósito de construir y fortalecer las capacidades nacionales que permitan garantizar el

ejercicio de los derechos y libertades de la población, así como la protección de los bienes jurídicos del Estado en este dominio; encaminando acciones para garantizar un ciberespacio seguro.

Esta política estableció los siguientes pilares básicos de la ciberseguridad en el Ecuador:

I) Gobernanza de la ciberseguridad.

II) Sistemas de información y gestión de incidentes.

III) Protección de la infraestructura crítica digital y servicios esenciales.

IV) Soberanía y defensa.

V) Seguridad pública y ciudadana.

VI) Diplomacia en el ciberespacio y cooperación internacional.

VII) Cultura y educación de la ciberseguridad.

Posteriormente, en agosto de 2022, se publica la Estrategia Nacional de Ciberseguridad la cual se elaboró conforme lo publicado por el órgano rector del sector, en estrecha cooperación con actores nacionales e internacionales y tiene por objeto establecer la dirección y un marco para alcanzar objetivos específicos y claros para el trienio 2022- 2025.

Los objetivos propuestos en esta estrategia son los siguientes (MINTEL, 2022):

1. Gobernanza y coordinación nacional: establecer un enfoque coordinado de la ciberseguridad nacional.
2. Resiliencia cibernética: mejorar la resiliencia cibernética a nivel nacional y organizacional para prepararse, responder y recuperarse de los incidentes cibernéticos.
3. Prevención y lucha contra la cibercriminalidad: Fortalecimiento de las capacidades para prevenir, investigar y perseguir los delitos cibernéticos.
4. Ciberdefensa nacional: reforzar las capacidades de Ciberdefensa para proteger las Infraestructuras de Información Crítica (IIC) nacionales y los servicios esenciales del Estado y desarrollar capacidades en ciber inteligencia que permitan obtener información útil y oportuna de las amenazas presentes en ciberespacio para la toma de decisiones.
5. Habilidades y capacidades de ciberseguridad: mejorar y ampliar las capacidades cibernéticas de la nación en todos los niveles.
6. Cooperación internacional: maximizar los beneficios de la cooperación internacional.

En cuanto a la Ciberdefensa el 12 de septiembre de 2014, mediante Acuerdo Ministerial No. 281 se creó el **Comando de Ciberdefensa** (COCIBER) dentro de las Fuerzas Armadas del Ecuador, bajo la premisa que el Estado Ecuatoriano identifica los principales riesgos en el campo tecnológico de los ciberataques, tales como: organizaciones criminales, el ciberterrorismo, ciberdelito, cibercrimen, ciberespionaje, infiltración de los sistemas de TICs, entre otros.

Para mayo del 2021, con acuerdo ministerial 199, se publica la Estrategia de Ciberdefensa cuyo propósito fundamental es el de establecer lineamientos que orienten el fortalecimiento de la ciberdefensa como una capacidad necesaria en el cumplimiento de la misión constitucional de la Defensa.

Los objetivos que se establecen en la Estrategia de Ciberdefensa son:

1. Fortalecer la ciberdefensa para cumplir la misión constitucional de Defensa en el ciberespacio, la infraestructura crítica y áreas reservadas.
2. Incrementar las capacidades de defensa activa y respuesta para contrarrestar a las amenazas que puedan afectar a la soberanía e integridad territorial en el ciberespacio, y lograr un impacto estratégico.
3. Articular y coordinar acciones conjuntas para el desarrollo de normativas y fortalecimiento interinstitucional que permita proteger el ciberespacio
4. Intensificar la cooperación internacional con el fin de generar un espacio de intercambio y apoyo en el ámbito de la ciberdefensa.
5. Fortalecer la cultura de ciberdefensa para reducir los incidentes de los sistemas institucionales.

En el siguiente gráfico, de elaboración propia, se presenta un esquema de la estructura actual de la ciberseguridad y Ciberdefensa en el Ecuador:

14. Conclusiones

1.1. El marco legal peruano para la gestión del ciberespacio y sus complementos resulta insuficiente y no define las responsabilidades y el ente rector no tiene capacidad para contrarrestar las amenazas que pueden afectar la soberanía espacial del país.

1.2. El que gane la guerra cibernética cumplirá lo expresado por Sun Tzu: *"Los generales expertos en mando siempre hacen a los ejércitos enemigos doblegarse sin batalla, esa es la máxima victoria"*. En ese sentido, las infraestructuras críticas de un país, los sistemas de comando y control, así como los sistemas de armas cuentan con plataformas informáticas para su funcionamiento; sin embargo, como resultado de un ciberataque, estas plataformas podrían quedar inservibles y paralizar a un país, poniendo en riesgo la Seguridad, la Defensa y el Desarrollo Nacional.

Al respecto, la Política Nacional define el "qué hacer"; por consiguiente, resulta imprescindible contar con una Política Sectorial de Ciberdefensa, cuyos objetivos y lineamientos permitan fortalecer el desarrollo de capacidades para neutralizar las amenazas y ataques en y mediante el ciberespacio, impulsando tanto la cultura y la educación en ciberdefensa en las Fuerzas Armadas, como la Investigación, Desarrollo e Innovación (I+D+i) en ciberdefensa entre las Instituciones Armadas, así como la cooperación nacional e internacional a fin de contar con una seguridad cooperativa en el entorno digital.

1.3. La realidad hoy en día es que la tecnología es cada vez más sofisticada y los ciberatacantes encontrarán cada vez más formas de lograr su objetivo, por eso, para evitar el peor de los escenarios como que los ciberataques paralicen todo un país, los gobiernos deben atacar el problema de raíz, las infraestructuras o activos críticos deben estar protegidos con plataformas informáticas seguras de la última generación, y, quizás lo más importante, los países deben invertir en la formación de una nueva generación de expertos en Ciberseguridad y Ciberdefensa, lo cual requerirá tiempo, dinero y compromiso político. Estas acciones deben tomarse, pues la amenaza de los ciberataques está aquí para quedarse.

Así mismo, a fin de cumplir con lo dispuesto por la ley de ciberdefensa, se debe asignar recursos suficientes y necesarios a las Fuerzas Armadas para tener una capacidad de ciberdefensa que sea el último bastión de protección en el ciberespacio, que sea disuasiva y que pueda ser empleada cuando el Estado Peruano lo requiera, ya sea para el desarrollo: actuando en defensa de los Activos Críticos Nacionales y Recursos claves, cuando su capacidad de protección sea sobrepasada, teniendo presente que ellos son esenciales para satisfacer nuestras necesidades vitales y para que nuestro Perú pueda alcanzar sus objetivos nacionales; sea para el orden interno: realizando coordinaciones Interinstitucionales y operativas con la PNP, Ministerio Público y Poder Judicial en la lucha con los Delitos Informáticos; o sea en su rol primordial de garantizar la independencia, la soberanía y la integridad territorial de la República: actuando ante ciberamenazas o ciberataques que afecten la

Seguridad Nacional.