CONCEPCIÓN POLÍTICO – ESTRATÉGICA DE CIBERDEFENSA

Por: **Crnl. de E.M.C. Robert Vargas Borbúa**

RESUMEN

El ciberespacio es una nueva dimensión del desarrollo de la humanidad; pues influye en todas sus actividades personales, laborales, académicas y sociales. El estudio de la seguridad del ciberespacio es aún un tema en discusión y debate, en los ámbitos académicos de seguridad y defensa. El presente artículo pretende contribuir al proceso académico, analizando la seguridad en el ciberespacio con enfoque multidimensional, la concepción de seguridad en el ciberespacio en el contexto de la seguridad integral y finalmente, la reciente política nacional de ciberseguridad, aterrizando en la estrategia de ciberdefensa de reciente emisión.

Palabras clave: ***ciberespacio / ciberdefensa / ciberseguridad / seguridad integral/ seguridad multidimensional.***

La Seguridad en el ciberespacio con enfoque Multidimensional

La pandemia de COVID-19 resalta como los ciudadanos, las instituciones y los Estados se han vuelto críticamente dependientes del Internet y de las Tecnologías de la Información y las Comunicaciones (TIC); son vitales en la prestación de servicios esenciales, como la energía, las telecomunicaciones, la banca, y otros; su influencia se incrementa en la transformación continua de nuestras sociedades, economías y en los derechos fundamentales de las personas. Por el contrario, existe mayor violación a los datos personales, fuga de información de instituciones privadas y de organismo del Estado, incremento de las actividades delictivas en cantidad y variedad, interrupción del servicio y destrucción de su propiedad; exponiéndonos a la incertidumbre y la impredecible naturaleza de las amenazas cibernéticas. Colectivamente, nuestra inseguridad está creciendo, cada vez hay más actores y personas no estatales que pueden causar daños a las infraestructuras en red de Estados, industrias y las personas en sus diferentes actividades. (Hathaway, 2018)

En este contexto, es por demás acertada la concepción de seguridad multidimensional en el Hemisferio americano, incluyendo múltiples aspectos políticos, económicos, sociales, de salud y otros; incorpora, además de las amenazas tradicionales [amenazas militares externas], nuevas amenazas, preocupaciones y otros desafíos a la seguridad de los Estados del Hemisferio, como: el terrorismo, la delincuencia organizada transnacional, el problema mundial de las drogas, la corrupción, el lavado de activos, el tráfico ilícito de armas y las conexiones entre ellos; los desastres naturales y los de origen humano; los ataques a la seguridad

cibernética; la posibilidad del acceso, posesión y uso de armas de destrucción masiva por parte de terroristas; entre otros (Organización de los Estados Americanos, 2003, págs. 2-3). Fenómenos que se encuentran estrechamente interrelacionados, por lo que deben ser encarados con un enfoque integral, de acuerdo a las prioridades de cada Estado.

El enfoque multidimensional de la seguridad hemisférica, se introduce con la Declaración de la Asamblea General de la O.E.A de Bridgetown, en el 2002 y la Conferencia Especial sobre Seguridad llevada a cabo en México en el 2003. En esta conferencia los países se comprometieron a identificar y combatir las amenazas emergentes, tales como amenazas a la seguridad cibernética, el terrorismo biológico y amenazas a la infraestructura crítica. A la vez, existió el compromiso de desarrollar e implementar una cultura de seguridad cibernética y una estrategia integral de la OEA sobre seguridad cibernética en las Américas, adoptando medidas de prevención eficaces para prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas (Ministerio de Telecomunicaciones y Sociedad de la Información, 2021).

En tales circunstancias, se puede distinguir que existen definiciones y ámbitos superpuestos de seguridad en relación con su enfoque en el estado o en el individuo y en una orientación interna o externa. Conceptos como seguridad nacional, seguridad pública, la seguridad ciudadana y la seguridad humana se traslapan, dejan brechas o se complementan, lo que dificulta su aplicación especialmente cuando se requiere: normativa legal apropiada, capacidades, doctrina de empleo y organización. Según el Dr. Mark Hamilton la seguridad multidimensional engloba esta problemática en cuatro ámbitos de acción (Hamilton, 2020):

a) Las amenazas tradicionales específicamente la defensa frente amenazas externas estatales.

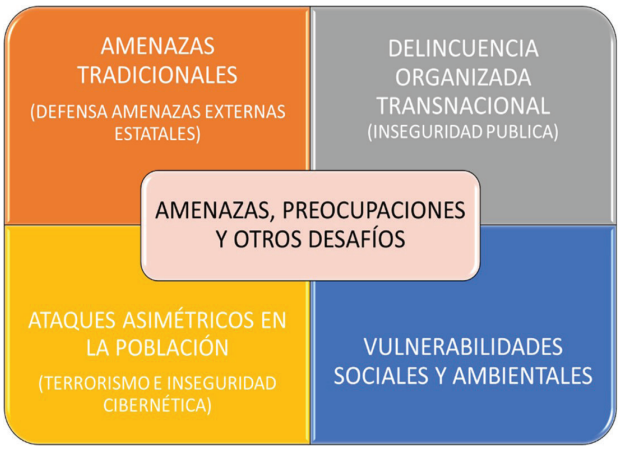
b) La delincuencia organizada transnacional que provoca la inseguridad pública, es la principal preocupación por los saltos niveles de violencia, conflicto social y crimen organizado; identificando la fácil disponibilidad de armas de fuego y el tráfico ilícito de drogas, armas como los principales factores asociados.

c) Las vulnerabilidades sociales y ambientales, que se relacionan con la desigualdad en el crecimiento económico, los esfuerzos regionales por incrementar la resiliencia ante desastres naturales, y la sostenibilidad sin afectar el medio ambiente.

d) Los ataques asimétricos a la población, son punto de confluencia entre el terrorismo y la inseguridad cibernética.

Figura 1

Temas planteados en la Declaración sobre seguridad en las Américas, OEA, 2003.



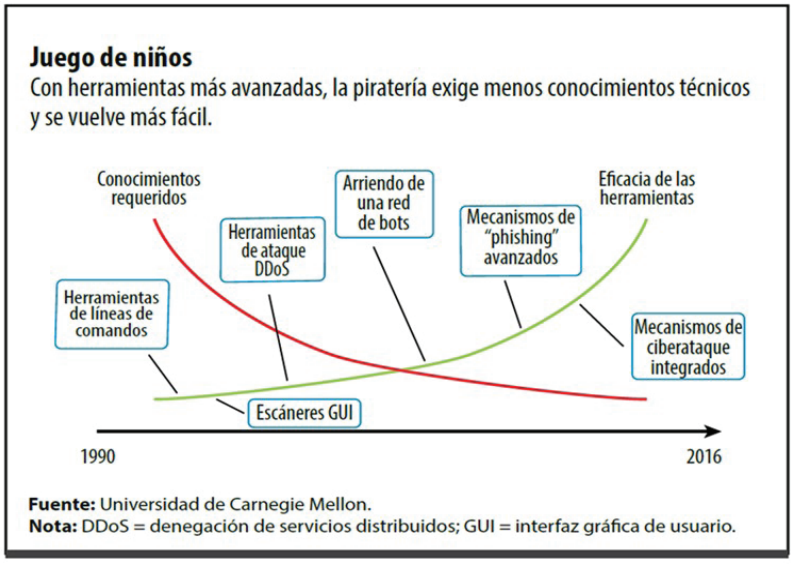
Nota: Tomado de: Dr. Mark Hamilton. CID, Conferencia dictada ADEMIC, noviembre 2020.

La confluencia se da porque el terrorismo y la inseguridad cibernética comparten las características de un campo de batalla o escenario de confrontación asimétrico, la utilización de ataques dirigidos a la población y

un enlace relevante con el crimen organizado. En la última década, los ataques cibernéticos han aumentado en frecuencia e ingenio, a menor costo y riesgo mínimo, la eficiencia de las herramientas utilizadas para los ciberataques ha aumentado mientras los conocimientos requeridos para manipularlas han disminuido, pudiendo causar grandes efectos en la población, instituciones e incluso en el Estado; mientras permanecen relativamente anónimo.

Figura 2

Evolución de la eficacia de las herramientas y conocimientos requeridos para ciberataques.



Nota: Tomado de, La industrialización de la ciberdelincuencia, Gaidosch T, 2018

Asimismo, los derechos de libertad de expresión y privacidad personal se contraponen la capacidad y legitimidad del Estado para brindar a la sociedad.de las herramientas y conocimientos requeridos para ciberataques.

La seguridad cibernética es una prioridad para la OEA desde el 2004 y se esfuerza por garantizar un ciberespacio abierto y seguro en todos los Estados miembros. El Informe "*Ciberseguridad: riesgos, avances, y el camino a seguir en América Latina y el Caribe"* edición 2020, preparado por la Secretaria de Seguridad Multidimensional de la OEA en colaboración con el Banco Interamericano de Desarrollo (BID) y el Centro de Capacidad de Seguridad Cibernética Global de la Universidad de Oxford, proporciona una descripción de las capacidades nacionales de los países de América Latina y el Caribe (ALC) para combatir el ciberterrorismo y analiza la capacidad de seguridad cibernética de los Estados miembros (Banco Interamericano de Desarrollo BID, 2020).

El estudio analiza la capacidad de seguridad cibernética de cada país identificando cinco dimensiones:

(i) Política y estrategia de ciberseguridad (Diseño de estrategia y resiliencia de ciberseguridad);

(ii) Cibercultura y sociedad (Fomentar una cultura de ciberseguridad responsable en la sociedad);

(iii) Habilidades de educación, capacitación y ciberseguridad (Desarrollo del conocimiento de ciberseguridad);

(iv) Marcos Legales y Regulatorios (Creación de marcos legales y regulatorios efectivos); y

(v) Normas, organizaciones y tecnologías (Control de riesgos a través de estándares, organizaciones y tecnologías).

Cada una de estas dimensiones se divide en factores e indicadores más específicos, de acuerdo al Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), que son: inicial, formativa, consolidada, estratégica y dinámica.

En el perfil del Ecuador (Banco Interamericano de Desarrollo BID, 2020, pág. 92)se hace referencia de manera general a los avances significativos de sus capacidades cibernéticas y en el enfrentamiento de ciberamenazas, apoyado por el establecimiento de un grupo de trabajo para el desarrollo de la estrategia nacional de ciberseguridad. Resalta el

establecimiento del EcuCERT[1], el equipo de respuesta ante incidentes cibernéticos del país que depende de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) como miembro CSIRT[2] Américas, por lo que se beneficia de la red de colaboración, intercambio, estímulo y participación en proyectos técnicos entre los CSIRT nacionales, de defensa, policiales y gubernamentales de los países miembros que proporciona la OEA.

Se menciona que el presupuesto para la ciberseguridad es la barrera más importante con que se enfrentan las organizaciones, así como el déficit en profesionales de seguridad cibernética. La normativa nacional ha mejorado considerablemente con el establecimiento de la Ley sobre comercio electrónico, firma electrónica y mensajes de datos, las reformas del Código Integral Penal para el tratamiento de los delitos contra los activos de los sistemas de información y comunicación, la protección constitucional de datos y la privacidad y el Plan de Gobierno Electrónico, cuyo objetivo es ejecutar un modelo de gobierno electrónico sostenible e inclusivo que tenga en cuenta los aspectos políticos, sociales y ambientales. Menciona que la Dirección de Arquitectura Tecnológica y Seguridad de la Información es responsable de la coordinación de la seguridad cibernética del país y tiene, como una de sus tareas, la formulación, evaluación, coordinación y gestión de los programas gubernamentales de seguridad cibernética, lo cual en caso de un incidente cibernético con repercusión nacional podría ser un error de apreciación del ámbito de responsabilidad.

En el dominio *D1* Política y estrategia de seguridad cibernética, se encasilla la Defensa Cibernética; los resultados no son muy alentadores debido a que los indicadores de organización y coordinación se mantienen en iguales del 2016 al 2020 (1/5); mientras que el indicador de estrategia denota un avance (2/5).

El reporte de ciberseguridad aporta datos cuantificados a la comunidad internacional de la capacidad de seguridad cibernética, que a la vez deber servir de guía para la elaboración de la estrategia, la política y la asignación racional de recursos en cada país, a fin de lograr niveles aceptables de seguridad cibernética y el desarrollo de capacidades fundamentales.

Por su parte, la Seguridad multidimensional agrega un valor diagnóstico y discursivo, que permite entender la complejidad de los desafíos en el ciberespacio, su interrelación con otras dimensiones, para aunar esfuerzos que permitan construir una cibersociedad resiliente y la necesidad de garantizar la ciberseguridad a nivel mundial.

La Secretaría de Seguridad Multidimensional (SSM) de la OEA promueve y coordina la cooperación entre los Estados Miembros, en el Sistema Interamericano y otras instancias del Sistema Internacional, para evaluar, prevenir, enfrentar y responder efectivamente a las amenazas a la seguridad. Siendo el Comité Interamericano contra el Terrorismo (CICTE), la instancia para contrarrestar el terrorismo, con pleno respeto a la soberanía de los países, al estado de derecho y al derecho internacional. Este comité ha creado el programa de Ciberseguridad con los objetivos de desarrollar las capacidades técnicas y políticas que permitan responder y recuperarse con exitosamente de incidentes cibernéticos, centrado en tres (3) pilares: desarrollo de políticas, desarrollo de capacidades (incluyendo capacitación y ejercicios cibernéticos), e investigación y divulgación.

1. Concepción de seguridad en el Ecuador

La Seguridad Integral es la base de la concepción de seguridad en el Ecuador. La Ley de Seguridad Pública y del Estado (LSPE) regula la seguridad integral del Estado, "garantizando la soberanía e integridad territorial, la seguridad de las personas, comunidades, pueblos, nacionalidades y colectivos, e instituciones,

1 EcuCERT: Centro de respuesta a incidentes informáticos del Ecuador
2 CSIRT: Computer Security Incident Response Team.

la convivencia ciudadana de una manera integral, multidimensional, permanente, la complementariedad entre lo público y lo privado, la iniciativa y aporte ciudadanos, y se establecerán estrategias de prevención para tiempos de crisis o grave conmoción social. Se protegerá (…) en el ámbito de la seguridad del Estado la protección y control de los riesgos tecnológicos y científicos, la tecnología e industria militar, el material bélico, tenencia y porte de armas, materiales, sustancias biológicas y radioactivas, etc.".

Esta LSPE crea el Sistema de Seguridad Pública y del Estado, el Consejo de Seguridad Pública y del Estado COSEPE, y a la vez dispone la elaboración del Plan Nacional de Seguridad Integral (PNSI) en concordancia con el Plan Nacional de Desarrollo (PND), con el aporte mancomunado de otras entidades del Estado y de la ciudadanía.

El PNSI asume la multidimensionalidad y complejidad de las amenazas, peligros y desafíos a la seguridad en el Hemisferio, considerados en la Declaración de Bridgetown 2002 y la Declaración de seguridad de las Américas en 2003. Las amenazas de seguridad incluyen problemas que tienen impacto directo en la vida de las personas, seguridad humana, como son, entre otras, el crimen cibernético, el tráfico ilegal de drogas, armas de fuego, seres humanos, el terrorismo en sus diferentes formas, extorsivo y reivindicativo político, siendo el Ciberespacio una dimensión propicia para estas afectaciones a los derechos, libertades y garantías de los ciudadanos se lleven a cabo, con anonimato, autonomía y secreto.

El PNSI articula la defensa y seguridad, con alcance multidimensional, determinando ejes estratégicos para la construcción de la concepción de la seguridad (PNSI 2019-2030, pp. 33-41):

a) De la defensa de la soberanía del Estado y la integridad territorial, frente agresión de amenazas tradicionales externas al Estado (representadas generalmente por otros Estados) y nuevas amenazas intraestatales, que es materia de seguridad nacional. En este campo la rectoría está en el Ministerio de Defensa y Ministerio de Relaciones Exteriores; corresponde a las Fuerzas Armadas su ejecución para cumplir con su misión fundamental de defensa de la soberanía e integridad territorial.

b) De la seguridad ciudadana y el orden público, en el cual el Ministerio del Interior es el Rector y a la Policía Nacional corresponde su ejecución. Ejecutará todas las acciones para proteger a los habitantes en situaciones de violencia, delincuencia común y crimen organizado, proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional; a través del respeto al estado de derecho (reglas) y la autoridad para imponerlo, a fin de lograr una coexistencia segura y pacífica. Coordinará su actuación con los órganos correspondientes de la función judicial.

c) La seguridad de las personas frente a los riesgos naturales y antrópicos. Es decir, de la gestión de riesgos (calamidad pública y desastres naturales); la prevención y las medidas para contrarrestar, reducir y mitigar los riesgos de origen natural y antrópico o para reducir la vulnerabilidad, corresponden a las entidades públicas y privadas, nacionales, regionales y locales. La rectoría la ejercerá el Estado a través de la Secretaría Nacional de Gestión de Riesgos.

Transversalmente a estos ejes el Estado consolida el Sistema Nacional de Inteligencia, manteniendo al Centro de Inteligencia Estratégica (CIES) como ente rector. La Inteligencia es definida como la obtención, sistematización y análisis de la información específica referida a las amenazas, riesgos y conflictos que afecten a la seguridad integral, destacando que la información de inteligencia

Figura 3

Ejes de seguridad y su correspondencia en la Constitución de la República.

<table>
<tr><td rowspan="2">Entidades</td><td>DEFENSA (MDN)</td><td>SEGURIDAD PÚBLICA (MG)</td><td>GESTIÓN DE RIESGOS</td><td rowspan="2">COMPLEMENTARIEDAD</td></tr>
<tr><td>FF.AA</td><td>P.N</td><td>SNGR</td></tr>
<tr><td></td><td colspan="3">PROBLEMAS DE SEGURIDAD</td></tr>
<tr><td rowspan="3">Art. 164</td><td>Agresión</td><td rowspan="3">Grave conmoción Interna</td><td rowspan="2">Calamidad pública</td><td>Insuficiencia</td></tr>
<tr><td>Conflicto armado Interno</td><td>Inexistencia</td></tr>
<tr><td>Conflicto armado Externo</td><td>Desastres naturales</td><td>Imposibilidad</td></tr>
<tr><td></td><td colspan="2">Art. 158</td><td>Art. 389</td><td></td></tr>
<tr><td>Art. 162</td><td>Apoyo Desarrollo</td><td colspan="2">Económico (Industrias de defensa)</td><td>Social (Contingente)</td></tr>
<tr><td>Art. 276</td><td>Paz mundial</td><td colspan="3">Misiones de paz</td></tr>
<tr><td>Disp. legales</td><td colspan="3">COE, LAM, LCAME, LM.</td><td>Autoridad</td></tr>
</table>

Nota: Tomado de, Crnl. de E.M.C. Robert Jiménez, PhD.

es sustancial para la toma de decisiones en materia de seguridad.

La Figura 3 detalla la concordancia de estos ejes estratégicos de seguridad con la Constitución de la Republica en sus diferentes artículos.

Con este enfoque se articula una respuesta interinstitucional coherente y coordinada del Estado, inclusiva con la participación del sector privado y la sociedad en general, como la manera óptima de enfrentar los desafíos de seguridad actuales y futuros. Estas áreas específicas, interactúan integralmente a través de coordinación, planificación y ejecución de acciones en todos los niveles del Estado; pues, actualmente no existe una frontera claramente definida entre los diversos asuntos – interno, externo, regional, global – siendo esta relación y sus efectos cada vez más significativos (PNSI, p. 35).

El PNSI se adentra en el ciberespacio al mencionar al crimen cibernético, ciberamenazas y ciberataques, como aspectos claves de seguridad. Incluye un amplio detalle de la tecnología como el aporte del conocimiento humano para mejorar las condiciones de vida del hombre y el crecimiento económico de los países: la evolución tecnológica principalmente digital, reconfigura las interacciones del trabajo, los sistemas económicos e inclusive los sistemas sociales y permiten que elementos con la inteligencia artificial, Internet y las redes de comunicaciones ponen al alcance de la mano el conocimiento y la información; siendo nuestra principal vulnerabilidad la dependencia tecnológica extranjera en los campos de las telecomunicaciones, computación, los sistemas que utilizan un software y la automatización.

Debido a la frecuencia y creciente sofisticación de los ciberataques y a sus efectos políticos, económicos, sociales, militares, ambientales y de decisión, y sus efectos negativos y destructores, la seguridad en el ciberespacio es una prioridad actual. Sin embargo, los problemas para adquirir la capacidad (en sus componentes

MIRADO[3]) adecuada, la necesidad de mejorar la planificación y coordinación de la respuesta interinstitucional (CSIRT), y la falta de legitimidad del Estado en el ambiguo límite de la privacidad y el derecho a la comunicación, no han permitido una respuesta contundente del Estado.

Esto se agrava pues el desarrollo tecnológico no se detiene; e influye de manera compulsiva en nuevas actividades de la sociedad y de los Estados. Incluso los grupos delincuenciales, narcotraficantes y terroristas se han embarcado, yo diría de forma eficiente, en el empleo eficiente de la tecnología del ciberespacio.

Estos actores configuran un escenario de confrontación digital, que no descarta una ciberguerra en un escenario asimétrico. Según William S. Lind, la cuarta generación de la guerra está marcada por el retorno un mundo de culturas, no solamente de estados, en conflictos, en donde la legitimidad del estado puede entrar en crisis, lo que significa que muchos países desarrollarán una guerra de cuarta generación en su suelo, debido a la creación de verdades sesgadas a intereses particulares. (Lind, 2004). Se configura la amenaza del ciberterrorismo en la que los grupos agresores emplean medios digitales para atacar sistemas, redes, servidores, telecomunicaciones e información privada con el objetivo de intimidar y coaccionar a un Estado o a su población, y crece en relación proporcional con el aumento de su dependencia tecnológica. Cualquier fallo, intrusión o ataque en los sistemas informáticos puede causar daños irreparables en infraestructuras básicas de la comunidad, y los terroristas aprovechan esta vulnerabilidad como elemento de presión (El Orden Mundial, 2021).

La vulnerabilidad latente al desarrollo tecnológico externo, especialmente en cuanto a redes de comunicaciones digitales de conectividad permanente, la gestión de grandes volúmenes de datos, la robotización y automatización de procesos críticos en la provisión de servicios esenciales y la afectación de “bienes públicos”, el desarrollo de la comunicación interactiva en audio y video, la rapidez de la difusión de los mensajes con información o desinformación, el acceso y uso de tecnologías útiles y eficaces, a menor costo y de fácil adopción por actores estatales y no estatales difuminan este límite entre los peligros a la seguridad interna y externa, creando un escenario conflictivo marcado por la ambigüedad, la zona gris. (Moral, 2019)

2. Política de Ciberseguridad nacional.

El artículo 140 de la Ley orgánica de Telecomunicaciones (LOT) especifica que el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información. A dicho órgano le corresponde el establecimiento de políticas, directrices y planes aplicables en tales áreas para el desarrollo de la sociedad de la información.

Asimismo, el artículo 8 de esta misma Ley, da potestad que: *en caso de agresión; conflicto armado internacional o interno; grave conmoción interna, calamidad pública; o desastre natural o emergencia nacional, regional o local, cuando el Decreto Ejecutivo de Estado de Excepción que emita el Presidente o Presidenta de la República, involucre la necesidad de utilización de los servicios de telecomunicaciones, los prestadores que operen redes públicas de telecomunicaciones tienen la obligación de permitir el control directo e inmediato por parte del ente rector de la defensa nacional, de los servicios de telecomunicaciones en el área afectada. Por lo que se puede entender que existe una correlación de los objetivos de desarrollo, seguridad y defensa en los casos permitidos por la Leyes nacionales.*

El MINTEL, emitió el Libro Blanco de la Sociedad de la Información y del Conocimiento (LSIC),

3 MIRADO: Material, Infraestructura, Recursos humanos, Adiestramiento, Doctrina, Organización.

para fortalecer el sector mediante el desarrollo y explotación de las TIC, que permita al Estado alcanzar un desarrollo con el propósito de dar una mejor calidad de vida a los ciudadanos, a fin de impulsar el crecimiento económico, la equidad e inclusión y la eficiencia de la administración pública. Para poder cumplir con este objetivo se propone cinco ejes de acción: i) Infraestructura y conectividad, ii) Gobierno Electrónico, iii) Inclusión y habilidades digitales, iv) Seguridad de la información y protección de datos personales, v) Economía digital y tecnologías emergentes.

El eje de seguridad de la información y protección de datos personales tiene directa relación con el Índice Global de Ciberseguridad (GCI), emitido por la Unión Internacional de Telecomunicaciones (UIT), que en el 2017 posicionó al Ecuador en el puesto 66 de 193 países a nivel mundial, y en el sexto lugar entre los países de ALC. El GCI gira en torno a la Agenda de Ciberseguridad Global de la UIT (GCA) que a su vez consideró que Ecuador tiene un nivel intermedio de compromiso con la seguridad cibernética (MINTEL-LB, 2018)

Se nota pues, la LOT y el libro Blanco LSIC establecen la conexión entre desarrollo, seguridad y defensa del conjunto de tecnologías que permiten el funcionamiento de la sociedad de la información y conocimiento.

En este contexto se ha emitido la Política de Ciberseguridad Nacional (PCN) en el Ecuador (Ministerio de Telecomunicaciones y Sociedad de la Información, 2021), definiendo a la ciberseguridad como la capacidad del Estado para proteger a las personas, sus bienes activos de información y servicios esenciales ante riesgos y amenazas que se identifican en el ciberespacio.

Es necesario explicar que de forma paralela y aplicable a un nivel operativo y táctico la ciberseguridad está definida como el conjunto de herramientas, conceptos, salvaguardas, directrices, métodos de gestión de riesgos, acciones, formación, practicas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de información de la institución y a los usuarios en el ciberespacio.

La PCN toma en consideración los intereses nacionales, vitales y estratégicos; considerando como objetivo: *construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio; y, ejecutar acciones para garantizar el ciberespacio seguro.*

El logro de este objetivo contribuirá de manera directa al desarrollo social, económico y humano del país, creando un escenario de confianza digital fundamental para favorecer el intercambio de información y, en consecuencia, de bienes y servicios en línea, además que establecerá las instituciones que garantizarán el ejercicio de los derechos y libertades en el ciberespacio. Es la muestra más fehaciente que el desarrollo va de la mano con la seguridad y con un estamento que permita defenderla.

La PCN se aplica al espectro radioeléctrico y en las infraestructuras digitales, incluyendo dominios, plataformas y programas desde un manejo de la información de carácter estatal y privado, así como información personal de la población; más las infraestructuras de los servicios automatizados y servicios esenciales del Estado como parte de los bienes jurídicos a proteger; abarca todas las industrias y todos los sectores, tanto vertical como horizontalmente. Su implementación conlleva un proceso de seguimiento y evaluación, que permitirá verificar el impacto de las acciones de la PCN y ajustarla en función de los rápidos cambios en el entorno digital.

En el marco de la prevención de incidentes cibernéticos se ha priorizado la protección de infraestructuras criticas digitales y servicios esenciales. Salvaguardar estas infraestructuras y servicios no es una tarea nueva, por cuanto

desde la óptica de soberanía y seguridad del Estado ya se identificaban áreas estratégicas a defender. Los nuevos enfoques de la seguridad implican un cambio en la óptica de estos espacios vitales para el Estado, los cuales, en torno a consideraciones de desarrollo, económicas, ambientales y de seguridad, amplían el alcance y la concepción de estas infraestructuras.

Sin embargo, y pese que la pandemia por el COVID-19 obligó a la implementación amplia del teletrabajo, la teleducación, la telemedicina y otras aplicaciones telemáticas, que surgieron como paliativos a la enfermedad, a la economía y a lo social, la cultura de ciberseguridad en el Ecuador no se ha consolidado. Recientemente, con las filtraciones de ataques cibernéticos producidos a la Corporación Nacional de Telecomunicaciones, se está reconociendo como un tema prioritario, en el cual se deberán tomar medidas para mejorarla, invirtiendo en educación en todos los niveles, incorporando en las mallas escolares y universitarias el abordaje de esta temática.

Por su parte, en el sector gubernamental, la obsolescencia e insuficiencia de los equipos (hardware), más las restricciones para adquirir bienes de larga duración, licencias de software configuran una gran vulnerabilidad para la protección de la información, los derechos de las personas y dificulta las tareas de las entidades de seguridad.

Se agrava este escenario con la participación de los competidores estratégicos del Ecuador, que conducen campañas cibernéticas de desinformación para erosionar nuestro ciberespacio, amenazan nuestras infraestructuras críticas, reducen nuestra prosperidad económica y alterar nuestro escenario de paz y seguridad.

Frente a este escenario, la PCN contempla la intervención del Estado en siete pilares que, en coordinación con el sector privado, la academia y sociedad civil, considera los intereses nacionales y mantiene una visión ubicua, holística y compartida a largo plazo de ciberseguridad. Además, establece objetivos y líneas de acción de todas las partes interesadas relevantes de la seguridad cibernética. La Figura 4 explica la correlación de pilares, objetivos y responsables:

Figura 4

Pilares, objetivos y responsables de Ciberseguridad nacional.

PILAR	OBJETIVO	INSTITUCIÓN RESPONSABLE
I. Gobernanza de la ciberde-fensa	OBJETIVO 1	MINTEL
II. Sistema de información y gestión de incidentes	OBJETIVO 2	MINTEL
III. Protección de la Infrae-structura Critica digital y servicios esenciales	OBJETIVO 3	MDN
IV. Soberanía y defensa		
V. Seguridad Publica y ciudadana	OBJETIVO 4	MDG
VI. Diplomacia en el ciber-espacio y cooperación internacional	OBJETIVO 5	MREMH
VII. Cultura y educación de la ciberseguridad	OBJETIVO 6	MINTEL

Nota: Política Nacional de Ciberseguridad

Como se puede apreciar la responsabilidad directa del Ministerio de Defensa Nacional (MDN) está en el tercer pilar: la Protección de la infraestructura critica digital y servicios esenciales y en el cuarto pilar: la Soberanía y defensa; que en su conjunto forman el Objetivo 3: Proteger la infraestructura critica del Estado ante amenazas y riesgos en el ciberespacio para garantizar su adecuado funcionamiento y la entrega de servicios esenciales; y sus diez

(10) estrategias. Sin embargo, su participación es fundamental en todos los pilares como se explicará más adelante.

Las infraestructuras críticas digitales y servicios esenciales (II.CC) se definen como aquellas instalaciones, sistemas y redes, así como servicios y equipos físicos y de tecnología de la información, cuya inhabilitación, interrupción o destrucción tendría un impacto negativo sobre la población, la salud pública, la seguridad, la actividad económica, el medio ambiente, los flujos de servicios esenciales y el funcionamiento de las cadenas de suministros servicios de gobierno o el eficaz funcionamiento de un Estado. (OEA/Ser.L/X.2.15; CICTE/doc.1/15, Comité Interamericano contra el Terrorismo, CICTE). La mayoría de las IICC, tanto públicos como privados, dependen de las TIC y TO para su funcionamiento.

La protección de las II.CC requiere de la identificación y definición a nivel nacional, su protección es responsabilidad de los operadores y del Estado, a través del sector defensa en el Estado (pilar III), y de la sociedad en general, siendo fundamental la complementariedad, coordinación y cooperación entre sectores públicos y privados.

Las acciones que se generan en este pilar están encaminadas a construir las condiciones necesarias de robustez y resiliencia para garantizar su normal funcionamiento, minimizar el impacto de ciberataques y permitir la pronta recuperación del servicio. Por lo que, su defensa se considera parte primordial de la soberanía y la garantía de la integridad territorial en el ciberespacio.

La soberanía y defensa nacional (pilar IV) se fundamenta en el reconocimiento del ciberespacio como un dominio de la guerra, donde las vulneraciones a los activos digitales y sus afectaciones en el entorno físico, pueden atentar contra la soberanía del Estado y a los derechos y libertades de las personas, así como al Estado.

"Se define la Ciberdefensa como: la capacidad militar, intelectual y tecnológica que poseen las FF.AA. para ejecutar operaciones en o a través del ciberespacio que permitan explorar, proteger y defender de ciberataques a la infraestructura crítica e información estratégica del Estado, así como apoyar el cumplimiento de operaciones en los otros dominios"

Los pilares (III y IV) tienen estrecha relación con el fortalecimiento del equipo de respuesta ante incidentes cibernéticos de FF.AA. (CSIRT - FF.AA.) que funciona en el Comando de Ciberdefensa. Este CSIRT – FF.AA. permite cumplir el objetivo 2: Potenciar las capacidades de detección, prevención y gestión de incidentes cibernéticos, al igual que el manejo de crisis de ciberseguridad de manera oportuna, efectiva, eficiente y coordinada; al momento de CSIRT-FF. AA. tiene la capacidad de gestionar incidentes en relación con la infraestructura crítica digital de FF.AA.

La Constitución determina los casos en los cuales el presidente puede decretar los estados de excepción (artículo 164); en cada uno de estos casos, como se explicó en el numeral 2, se ejecutan acciones en el ciberespacio, que deben ser abordadas de una manera integral por los organismos determinados en la Política de ciberseguridad nacional. Aspectos que se deberán especificar en la Directiva de la Defensa Nacional, que establece la actuación de FF.AA. relacionada al ciberespacio.

En base a la PCN se ha emitido la Estrategia de Ciberdefensa y la Guía estratégica política de ciberdefensa. La Estrategia establece objetivos y líneas de acción que le permitirán crecer y adaptarse en función de la ciberamenazas que se presenten (Ministerio de Defensa Nacional,

2021). Por su parte, la guía establece el entorno operativo actual, la conceptualización de los activos a defender, el análisis de las amenazas, el análisis de las políticas nacionales de seguridad y de la sociedad del conocimiento que permitan diagramar posibles escenarios de ciberconflicto para desarrollar las capacidades de ciberdefensa. (Ministerio de Defensa Nacional, 2021)

Es en este contexto, en donde se define la Ciberdefensa como: la capacidad militar, intelectual y tecnológica que poseen las FF.AA. para ejecutar operaciones en o a través del ciberespacio que permitan explorar, proteger y defender de ciberataques a la infraestructura crítica e información estratégica del Estado, así como apoyar el cumplimiento de operaciones en los otros dominios. Es decir, es una capacidad militar para proteger la información digital contra accesos no autorizados, evitando que esta información sea modificada o manipulada, tanto cuando está almacenada, como cuando se está procesando o en tránsito, incluyendo las medidas necesarias para detectar, documentar y hacer frente a tales amenazas.

Bibliografía

Banco Interamericano de Desarrollo BID. (2020). *Reporte de ciberseguridad 2020.* NY: OEA.

El Orden Mundial. (24 de Agosto de 2021). *EOM*. Obtenido de ¿Qué es el ciberterrorismo y cómo se ha vuelto una amenaza latente?: https://elordenmundial.com/que-es-el-ciberterrorismo-y-como-se-ha-vuelto-una-amenaza-latente/

Hamilton, M. (6 de Noviembre de 2020). Un enfoque multidimensional : . *Análisis de las amenazas que afectan la seguridad interna de los países del hemisferio*. Colegio Interamericano de Defensa.

Hathaway, M. (2018). *Gestión del Riesgo cibernético nacional.* OEA.

Lind, W. (15 de Enero de 2004). *Antiwar.com*. Obtenido de Understanding Fourth Generation War: https://original.antiwar.com/lind/2004/01/15/understanding-fourth-generation-war/

Ministerio de Defensa Nacional. (2021). *Estrategia de Ciberdefensa.* Quito: IGM.

Ministerio de Defensa Nacional. (2021). *Guía político - estratégica de ciberdefensa.* QUITO: IGM.

Ministerio de Telecomunicaciones y Sociedad de la Información. (2021). *Política de Ciberseguridad Nacional.* Quito: MINTEL.

Moral, P. (23 de diciembre de 2019). *EOM*. Obtenido de Los nuevos conflictos se libran en la zona gris: https://elordenmundial.com/los-nuevos-conflictos-se-libran-en-la-zona-gris/

Organización de los Estados Americanos. (2003). Declaración sobre seguridad en las Américas. (pág. 14). Mexico: OEA/Ser.K/XXXVIII.

(Footnotes)

1 Ministerio de Telecomunicaciones y de la Sociedad de la información

2 Ministerio de Defensa Nacional

3 Ministerio de Gobierno

4 Ministerio de Relaciones Exteriores