LA CIBERSEGURIDAD EN EL ECUADOR, UNA PROPUESTA DE ORGANIZACIÓN

Carlos Arturo Tates Almeida **y** Luis Recalde Herrera

[1]Academia de Defensa Militar Conjunta, Sangolquí, Ecuador

[2]Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador

*Autor de correspondencia: llrecalde@espe.edu.ec

Recibido 04 de diciembre 2018, aceptado después de revisión al 26 de febrero 2019

RESUMEN

En esta era de la información digital y el uso las tecnologías de la información, las comunicaciones y los procesos que aportan al desarrollo económico de la sociedad, el gobierno, la empresa pública y la defensa nacional hace que estemos conectados digitalmente, este flujo de la información de los servicios públicos, de emergencia, bancarios y el comercio digital, deben estar asegurados bajo normas y leyes que los estados, las empresas privadas, la academia y los ciudadanos formemos parte de este proyecto incluyente, para enfrentar las nuevas amenazas cibernéticas. En la región países como Colombia, Brasil, Chile, Argentina, Perú han desarrollado sus políticas nacionales y estrategias de seguridad cibernética con el objetivo fundamental de garantizar la seguridad del ciberespacio como parte de la seguridad nacional. Constituye una urgencia para el Ecuador elabore una estrategia nacional de Ciberseguridad como lo han hecho muchos países para proteger su infraestructura informática, de comunicaciones y de importancia crítica. Para el desarrollo de estas políticas deben considerarse a varias instituciones como: Ministerio de Telecomunicaciones, Ministerio de Defensa Nacional, Fiscalía, Ministerio del Interior, la academia entre otros; tomando como referencia la experiencia y estrategias en ciberdefensa de los países de la región. En este estudio he realizado un análisis de las iniciativas que algunos países han tomado para la elaboración de sus estrategias y políticas nacionales para enfrentar esta amenaza hibrida que utiliza el ciberespacio como su campo de batalla.

Palabras clave: Estrategias y Políticas Nacionales de Ciberdefensa, Ciberseguridad, Ciberespacio, Infraestructura Crítica.

ABSTRACT

In this age of digital information and the use of information technologies, communications and the processes that contribute to the economic development of society, government, public enterprise and national defense, we are connected digitally, this flow of information on public services, emergency, banking and digital commerce, must be ensured under rules and laws that states, private companies, academia and citizens are part of this inclusive project, to face new cyber threats. In the region, countries such as Colombia, Brazil, Chile, Argentina, Peru have developed their national policies and cybersecurity strategies with the fundamental objective of guaranteeing the security of cyberspace as part of national security. It is an urgency for Ecuador to develop a national Cybersecurity strategy as many countries have done to protect their IT, communications and critical infrastructure. For the development of these policies, several institutions must be considered: Ministry of Telecommunications, Ministry of National Defense, Prosecutor's Office, Ministry of the Interior, the academy, among others; taking as reference the experience and strategies in cyber defense of the countries of the region. In this study I have made an analysis of the initiatives that some countries have taken to elaborate their national strategies and policies to face this hybrid threat that cyberspace uses as its battlefield.

Key words: Strategies and National Policies of Cyberdefense, Cybersecurity, Cyberspace, Critical Infrastructure.

INTRODUCCIÓN

El uso de las tecnologías de la información en el funcionamiento de todas las actividades de las naciones y de la sociedad en general, han hecho que la dependencia del Internet y el uso del Ciberespacio constituya la puerta de ingreso para que se produzcan ciberdelitos y aparezcan nuevas amenazas tecnológicas (hibridas), en este nuevo escenario de confrontación no existe fronteras, ni actores, ni límites y estas nuevas amenazas pueden afectar a la seguridad del estado y de las personas paralizando la infraestructura crítica del estado ocasionando grandes pérdidas económicas, surgiendo la necesidad de que los estados fomenten las políticas y estrategias en este nuevo dominio de Ciberseguridad y Ciberdefensa como una Política de Seguridad Nacional. El entorno digital en el que se desarrolla el mundo actual debe considerar los riesgos que se presenta en el uso de las redes (internet) en casi todos los procesos de producción. La ciberseguridad representa un dilema de seguridad para todos los estados porque su zona de acción es el ciberespacio que es una zona anárquica.

Los ciberataques a Estonia en la primavera de 2007 marcaron un hito y un reto histórico para la OTAN, fue la primera vez que un país miembro solicitó apoyo a la OTAN por haber sido blanco de un ataque a sus sistemas de información y comunicaciones, en aquel momento la OTAN no disponía de un plan de acción para el caso de un ciberataque a uno de sus Estados miembros, con este antecedente en una reunión desarrollada en el 2007 los ministros de Defensa acordaron trabajar urgentemente sobre este tema, meses después la OTAN recomendaba la implementación de un conjunto de medidas orientadas a mejorar la protección ante los ciberataques de todos sus miembros, surgiendo así la iniciativa de desarrollar una Política de ciberdefensa para los estados miembros de la OTAN. Entre las amenazas no tradicionales actualmente se considera a los ciberataques o ciberguerra y para prevenir sus ataques en las infraestructuras críticas, en Europa y la Unión Europea los ciberataques han puesto en alto riesgo la infraestructura critica del estado, producto que cuenta con 31 millones de internautas, lo que supone una tasa de penetración del Internet del 65,5 % respecto a su población. Situándolo en el puesto 49 a nivel mundial en cuanto a la tasa de penetración de los servicios de la sociedad de la información. En el año 2003 los EE.UU. desarrollaron su primera política de Seguridad Cibernética y su Estrategia de Seguridad para asegurar el ciberespacio estableció tres objetivos estratégicos para la seguridad del ciberespacio nacional: prevención de ataques cibernéticos contra infraestructuras críticas nacionales; reducción de la vulnerabilidad nacional a los ataques cibernéticos; y reducción al mínimo los daños y el tiempo de recuperación de los ataques cibernéticos que se puedan producir.

CONTEXTO DE CIBERDEFENSA Y CIBERSEGURIDAD DE AMERICA LATINA Y ECUADOR

El uso de la información digital en la actualidad hace que la sociedad esta hiperconectada, a través del uso de internet permite que todas las personas que se conectan a través de las redes seamos blancos potenciales de los delincuentes, por lo que para inducirnos en el estudio de este campo debemos conocer algunos términos como:

Ciberdefensa: el término posee dos acepciones. (A) En un sentido amplio, son acciones contempladas en el marco de una política nacional de ciberseguridad orientadas a proteger el ciberespacio ante cualquier acción que pueda dañarlo. (B) En un sentido restringido, es el conjunto de políticas y técnicas de la Defensa Nacional destinadas a enfrentar los riesgos y amenazas propias del ciberespacio, de acuerdo con sus atribuciones constitucionales y legales. (Chile, 2015)

Ciberseguridad: La definición de ciberseguridad por parte de ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información) es la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (Azcona, 2017). Para el gobierno español la Ley de Protección de Infraestructuras criticas (2011) diferencia entre Infraestructuras Estratégicas, que son aquellas… "sobre las que descansa el funcionamiento de los servicios esenciales" e Infraestructuras Críticas que son aquellas que… "su funcionamiento es indispensable y no permite soluciones alternativas". (Sanchez, 2016).

Ciberespacio En el artículo publicado por BBC en 2001, se considera al ciberespacio como el nuevo ámbito de la guerra para el Pentágono, e indica que: es un campo de operaciones igual a la tierra, mar, aire o espacio y, por ende, igualmente sujeto a ser escenario de maniobras defensivas y, si es necesario, ataques preventivos y represalias. Frente a este nuevo escenario global es prioritario que los estados tomen medidas de Ciberseguridad y Ciberdefensa considerando que este tipo de ataques pueden afectar a la seguridad nacional como a la seguridad internacional. La UIT (Unión Internacional de Telecomunicaciones) en la guía de Ciberseguridad para los países en desarrollo (UIT, 2007, pág. V) indica que: Para evitar dar oportunidades al incremento de la delincuencia, las infraestructuras de telecomunicaciones existentes deben contar con medidas de seguridad adecuadas de naturaleza tanto técnica como jurídica. Los ataques procedentes del ciberespacio pueden adoptar diversas formas: el secuestro clandestino de un sistema, la denegación de servicio, la destrucción o robo de datos sensibles, la piratería de las redes de telecomunicaciones (hacking), la penetración en la protección de los programas informáticos (cracking) y la manipulación fraudulenta de las conexiones telefónicas (phreaking) (entre las que se encuentran entre otros el sabotaje y secuestro de las centrales telefónicas); todos ellos tienen consecuencias negativas para las organizaciones e individuos que los padecen.

Los países que son parte de la Organización de Estados Americanos frente a estas nuevas amenazas en materia de Ciberseguridad han formulado algunas estrategias con la participación de la empresa pública, la academia y los organismos estatales creando los Centros CERTs que son Equipos de Respuesta ante Emergencias Informáticas. En Latinoamérica la falta de presupuesto, formación universitaria y técnica impide que los estados hayan implementado en forma eficaz las políticas y capacidades técnicas para enfrentar estas nuevas amenazas. El Índice Global de Ciberseguridad (GCI), emitido por la Unión Internacional de Telecomunicaciones (UIT), publicado en el 2017, ubicó al Ecuador en el puesto 66 de 193 países a nivel mundial, y lo posicionó en el sexto lugar entre los países de la región. El Índice Global de Ciberseguridad gira en función de la Agenda de Ciberseguridad Global de la UIT (GCA) y sus cinco pilares: jurídico, técnico, organizativo, creación de capacidades y cooperación, siendo categorizado como intermedio en los tres primeros. Por esta razón, la encuesta del GCI consideró que Ecuador tiene un nivel intermedio de compromiso con la seguridad cibernética (UIT, 2007). Países como Estonia, Israel, Corea del Norte y EE.UU entre otros han elaborado sus estrategias y políticas de ciberdefensa basándose en las consideraciones del BID y de las Experiencias avanzadas en políticas y prácticas de Ciberseguridad del año 2012 en donde los argumentos desarrollados para la elaboración de estas políticas consideran el nivel estratégico y dinámico. Estos temas pueden servir de referencia para la elaboración de una propuesta de estrategia de seguridad en ciberdefensa en el Ecuador como se observa en la tabla No.1

Tabla No. 1 Estrategias y Políticas de Ciberdefensa basadas en las consideraciones del BID. Fuente: BANCO INTERAMERICANO DE DESARROLLO (Experiencias avanzadas, 2016)

	ESTONIA	**ISRAEL**	**COREA DEL NORTE**	**EE.UU**
Política y Estrategia de Ciberseguridad	Dinámico	Estratégico	Estratégico	Establecido
Cultura Cibernética y Sociedad	Estratégico	Dinámico	Dinámico	Dinámico
Educación Formación y Competencia en Seguridad	Estratégico	Dinámico	Estratégico	Estratégico
Marco Jurídico y Leyes	Estratégico	Establecido	Establecido	Dinámico
Normas, Organización y Tecnologías	Estratégico	Estratégico	Estratégico	Estratégico

En los estudios realizados por la empresa (Isdefe S.A., s.f.) (Ingeniería de Sistemas para la Defensa de España S.A) consultora que trata sobre seguridad nacional y ciberdefensa del año 2.009 analiza que, las actividades de ciberfensa de Francia, Estados Unidos, Reino Unido, Alemania, España, Noruega, la Unión Europea y la OTAN basan su organización considerando los siguientes puntos: 1) Contexto 2) Legislación, planes y estrategias 3) Organización y Responsabilidades 4) Ciberdefensa en donde se engloba la 4.1)Estrategia Nacional de Seguridad 4.2)Protección de Infraestructuras Nacionales 4.3) Estrategia Nacional de Seguridad de la Información 4.4)Programa Técnico de Seguridad de la Información 4.5) Manual contra el Cibercrimen 4.6) Otras Iniciativas Civiles en Ciberdefensa 4.7)Esfuerzos del Ministerio de Defensa. Este instituto formula un nuevo concepto de seguridad y defensa tomando en consideración el desarrollo de las TICs, e involucra a todos los sectores tanto públicos como privados como actores en la protección de la seguridad del territorio, de las infraestructuras críticas y de los ciudadanos. Los países latinoamericanos considerando este nuevo escenario geopolítico tecnológico han iniciado la incorporación de una cultura de seguridad que sensibilice el cumplimiento de normas que fomenten la seguridad de la información, se puede observar que Colombia junto con Brasil son las naciones más completas en el área de Ciberseguridad. En el informe Ciberseguridad 2016 del Observatorio de la Ciberseguridad en América Latina se establece el porcentaje de acceso al internet y se recoge la siguiente información respecto al desarrollo de las políticas y estrategias en el ámbito de la ciberdefensa expresada en la Tabla No. 2

Tabla No. 2 Organismos encargados de la elaboración de las Políticas y Estrategias de Ciberdefensa en países de América del Sur. Fuente: OBSERVATORIO DE LA CIBERSEGURIDAD EN AMÉRICA LATINA Y EL CARIBE (DESARROLLO & AMERICANOS, 2016)

ECUADOR 43 %	**COLOMBIA 53 %**	**BRASIL 58 %**	**CHILE 72 %**	**ARGENTINA 65 %**
NO ha desarrollado una **ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA**, Ecuador ha hecho avances en los últimos años para fortalecer su capacidad para abordar las amenazas informáticas	El Consejo Nacional de Política Económica y Social del Gobierno de Colombia estableció **LA POLÍTICA NACIONAL DE SEGURIDAD CIBERNÉTICA CONPES** 3701 bajo el auspicio del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa, el Departamento Nacional de Planeación y otras instituciones nacionales clave	En 2010 el Departamento de Seguridad de la Información y Comunicaciones publicó la Guía de Referencia para la Protección de Infraestructuras Críticas de Información y el Libro Verde de Seguridad Cibernética en Brasil. **ESTRATEGIA NACIONAL DE SEGURIDAD DE LAS COMUNICACIONES DE INFORMACIÓN Y SEGURIDAD CIBERNÉTICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL**	El Ministerio del Interior y Seguridad Pública, el Secretario General de la Presidencia y la Subsecretaría de Telecomunicaciones son los principales organismos nacionales que establecen **LA POLÍTICA DE SEGURIDAD CIBERNÉTICA A NIVEL GUBERNAMENTAL**	Programa Nacional de Infraestructuras Criticas de Información y Ciberseguridad (ICIC) y en coordinación con diversos organismos, instituciones académicas y el sector privado, el Gobierno de Argentina ha desarrollado un proyecto de **ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA** Argentina se distingue por haber formado el primer CSIRT nacional en 1994, que desde 2011 ha funcionado bajo el ICIC. ICIC-CERT
El Centro de Operaciones Tecnológicas Estratégicas y Contrainteligencia de la Secretaría de Inteligencia se encarga de los aspectos técnicos de la seguridad cibernética del país y un CSIRT nacional, el EcuCERT, entró en funcionamiento en noviembre de 2013	Las fuerzas del orden y el Poder Judicial tienen la capacidad de investigar y manejar casos de delincuencia cibernética	Las Fuerzas Armadas brasileñas también discuten las preocupaciones sobre defensa cibernética en su Libro Blanco de Defensa Nacional 2012. Recientemente crearon un Comando de Defensa Cibernética formal y una Escuela Nacional de Defensa Cibernética, además del Centro para la Defensa Cibernética del Ejército (CD-Ciber)	Las ramas de las Fuerzas Armadas de Chile comparten responsabilidades de defensa cibernética e información pero no tienen una estructura central de mando y control.	2015 la Presidencia de la República de Argentina emitió el Decreto nº 1067/2015 que reestructuró el control gubernamental de la ICN, y estableció una Oficina Nacional bajo la dirección de la **Subsecretaría de Protección de Infraestructuras Críticas de Información y Ciberseguridad** bajo la Jefatura del Gabinete de Ministros y Secretaría del Gabinete

En muchos países la Presidencia de la República ha delegado esta función a los Ministerios de la Defensa como BRASIL en donde las Fuerzas Militares estan presentes en todos los niveles de conducción del estado como se puede observar en la figura 1.

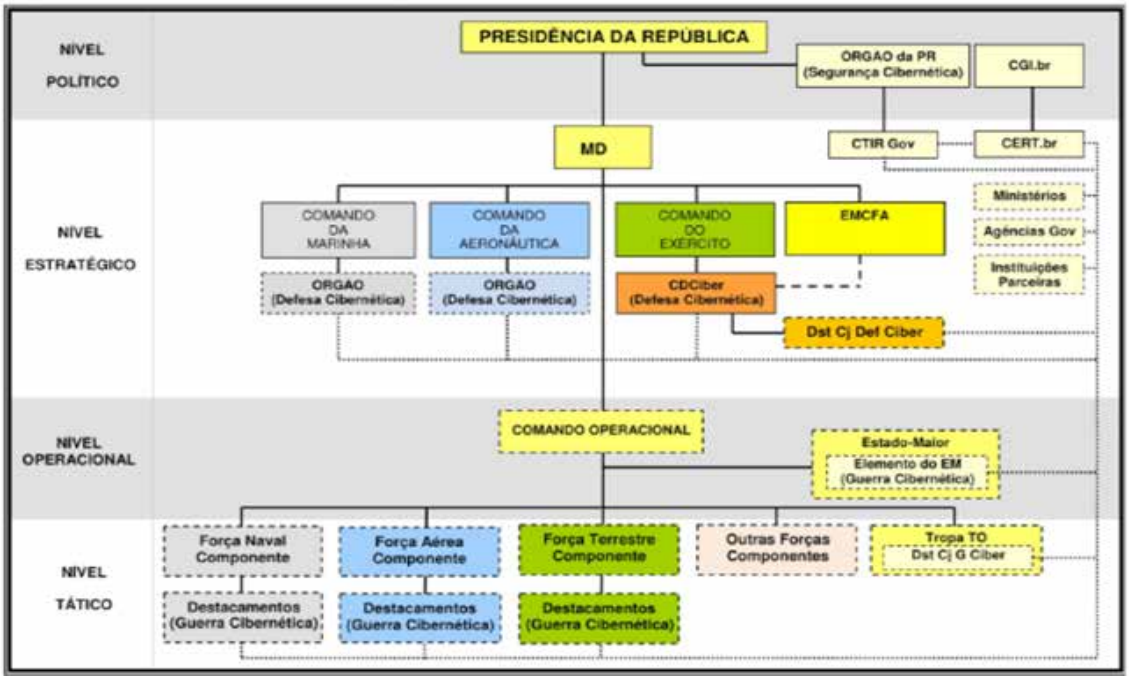

Figura 1: Estructura de Defensa Cibernética según lo establecido por el Ministerio de Defensa de BRASIL. Fuente Ministerio de Defensa Brasil

El Ecuador carece de la implementación de una Política y Estrategia Nacional de Ciberseguridad como tal. Sin embargo a través de los Acuerdos Ministeriales Nos. 804 y 837 de 29 de julio y 19 de agosto de 2011 de la Secretaría Nacional de la Administración Pública, se crea la COMISIÓN PARA LA SEGURIDAD INFORMÁTICA Y DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN integrada por miembros de los siguientes Ministerios: de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública, cuyos objetivos son los de: establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, considerando la información contenida para las instituciones de la Administración Pública Central e Institucional. El Gobierno ecuatoriano, en su esfuerzo por minimizar estos problemas, tomó algunas decisiones de tipo político-coyuntural. Por ejemplo, conformó un Centro de Operaciones Estratégico Tecnológico que operó desde las 12AM del 4 de noviembre hasta las 21PM del 5 de noviembre de 2013, con el fin de realizar un monitoreo de ataques informáticos sobre los equipos de seguridad de varias instituciones públicas (Ministerio Coordinador de Seguridad 2014). Asimismo, se ejecutaron proyectos como: la implementación del Ecucert para el tratamiento de los incidentes Informáticos, iniciado a partir del año 2012. Algunas instituciones incorporaron en sus planes estratégicos institucionales objetivos para incrementar la ciberseguridad como: la Secretaria Nacional de Inteligencia en su planificación 2015-2017.

Marco Legal. - En el Ecuador podemos indicar que en los siguientes documentos se establece normas para garantizar la seguridad de la información:

- Constitución de la República del Ecuador
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Ley Orgánica de Transparencia y Acceso a la Información Pública

- Ley del Sistema Nacional de Registro de Datos Públicos
- Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva
- Ley Orgánica y Normas de Control de la Contraloría General del Estado
- Leyes y normas de control del sistema financiero
- Leyes y normas de control de empresas públicas
- Ley del Sistema Nacional de Archivos
- Decreto Ejecutivo No. 1014 sobre el uso de Software Libre en la Administración Pública
- Decreto Ejecutivo No. 1384 sobre Interoperabilidad Gubernamental en la Administración Pública

Otras normas cuya materia trate sobre la gestión de los activos de información en las entidades de la Administración Pública

Esquema gubernamental de seguridad de la información (EGSI). - La Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación ha desarrollado el ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION **EGSI**, elaborado en base a la norma NTE INEN-ISO/IEC 27002 "Código de Práctica para la Gestión de la Seguridad de la Información".

Comando de Ciberdefensa del Comando Conjunto de FF.AA.- Las Fuerzas Armadas del Ecuador para proteger su información creó el COCIBER cuya misión es: defender, explotar el dominio cibernético y responder ante incidentes o amenazas que atenten la infraestructura crítica estratégica digital de FF. AA. y del estado; a través de la conducción de operaciones de ciberdefensa, a fin de contribuir a la misión del Comando Conjunto.

Centro de respuesta a incidentes informáticos del Ecuador (Ecucert, s.f.)**. -** Este centro de respuesta tiene como compromiso contribuir a la seguridad de las redes de telecomunicaciones de todo el país, así como del uso de las redes de internet; para esto ofrecerá productos relevantes, respuestas ágiles y servicios de calidad a la sociedad. Además, coopera con otros CSIRT dentro y fuera del Ecuador. El Ecuador en este nuevo contexto geopolítico debe integrar esfuerzos para desarrollar una Política Nacional de Ciberseguridad que involucre en forma multidisciplinaria a los sectores de la sociedad "lideradas" bajo la Presidencia de la Republica y sea el Ministerio de la Defensa amparado en el artículo 118 de la constitución del año 2008 que indica que "Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial" que coordine esta propuesta.

Considerando lo estipulado en la Agenda Política de la Defensa del Ecuador en vigencia, se establece claramente los objetivos y misiones a cumplir respecto a la protección de las áreas de infraestructura estratégica y la realización de operaciones de protección del espacio cibernético. Ante la falta de una política estatal en materia de Ciberseguridad es imprescindible y urgente fortalecer la gestión tecnológica de infraestructura e información digital, en todos los niveles a través de un Organismo de Ciberdefensa que permita articular y elaborar normas y leyes que fortalezcan la seguridad de la infraestructura de las áreas críticas del estado en forma preventiva y no reactiva.

METODOLOGÍA DE DESARROLLO DEL ESTUDIO

El presente estudio, plantea una metodología cualitativa, que permita observar los elementos de la problemática planteada en el objeto fenómeno de investigación, permitiendo la

planificación del diseño de la investigación, con la utilización de diferentes estrategias para obtener la información de manera precisa y su respectivo análisis de los resultados. Además, Sampieri (2006), menciona a la metodología cualitativa como la "la recolección de datos sin medición numérica para descubrir o afinar preguntas de Investigación en el proceso de interpretación" (p. 16), y (Hernández, Fernández & Baptista, 2012) considera que existen diferentes técnicas de recolección de datos, cuyo propósito es obtener información de los participantes, entre los que se encuentran la entrevista, grupo focal, entre otros. La metodología cualitativa, permite la utilización de métodos y técnicas que ayudan a reunir datos que se emplearan en la investigación de diferentes criterios, los cuales se articulan para la interpretación, explicación y predicción de resultados planteados desde la problemática del tema a tratarse.

PROPUESTA GENERAL DE ORGANIZACIÓN DE LA ESTRATEGIA NACIONAL DE CIBERDEFENSA (ESCD) PARA EL ECUADOR

La estrategia en el ámbito de la seguridad nacional hace referencia a las decisiones sobre el empleo de los diferentes instrumentos estatales del poder para resolver el problema de la seguridad. Proporciona las líneas de acción o respuestas al problema de seguridad planteado y que tienen que ver con la previsión (Felix Arteaga y Enrique Fojón, 2007). De acuerdo con (Murdock, 2004), la estrategia nacional consiste en saber cómo actuar y con qué recursos para conseguir los fines de la política; dar una idea general de cómo se esperan conseguir los resultados buscados. La estrategia está asociada a la complejidad de los contextos, es así como, vistos desde la perspectiva del componente militar, la estrategia ha trascendido desde las dimensiones terrestre, naval y aérea de los siglos XIX y XX, a nuevas dimensiones aeroespaciales y ciberespaciales que determinan un campo de batalla complejo (Gray, 1999), y en estas circunstancias, es más necesario que nunca contar con estrategias que integren el número y complejidad de los problemas de seguridad en estas nuevas dimensiones. A pesar de que, en Ecuador, existe una norma constitucional y legal; procesos e instituciones responsables de promover, planificar, ejecutar y supervisar las medidas relacionadas con la ciberseguridad; podemos afirmar que no existe una estrategia nacional de ciberseguridad en el país; dicha afirmación se fundamenta a que, las instituciones e instrumentos mencionados, no se encuentra articulados ni operan en forma coordinada para cumplir este cometido.

Para que exista una estrategia nacional de ciberseguridad, es indispensable elaborar una Política de Estado; considerándola como una Estrategia de Seguridad Nacional en donde se establezcan propósitos, principios rectores, políticas, objetivos a largo plazo, medidas específicas o líneas de acción, un diseño institucional con funciones mínimas, leyes y normativa, instituciones coordinadas y con capacidades, infraestructura, presupuesto, etc., para enfrentar las nuevas amenazas cibernéticas. Una estrategia nacional de ciberseguridad, debe involucrar al Estado (Administración Pública), a la empresa privada, la sociedad, la academia y las relaciones internacionales, quienes deben orientar sus esfuerzos en un mismo sentido, que permita, conocer las amenazas del ciberespacio, sus fuentes, origen, formas de manifestación y afectaciones; así como gestionar los riesgos y obtener las capacidades adecuadas para enfrentarlas, a través de acciones de prevención, detección, análisis, defensa, respuesta y recuperación. La estrategia en el ámbito de la seguridad nacional hace referencia a las decisiones sobre el empleo de los diferentes instrumentos estatales del poder para resolver el problema de la seguridad. Proporciona las líneas de acción o respuestas al problema de seguridad planteado y que tienen que ver con la previsión (Felix Arteaga y Enrique Fojón, 2007). Considerando el Política Nacional de Ciberseguridad de

Chile para el periodo 2017-2022 el mismo que contiene los lineamientos políticos de Chile que apunta al año 2022, para contar con un ciberespacio libre, abierto, seguro y resiliente, (Chile G. d., s.f.) nuestro país debería formularse las siguientes interrogantes e incorporarlas a la construcción de su política de ciberdefensa.

¿Por qué se requiere una política nacional de ciberdefensa y ciberseguridad?

Para resguardar la seguridad de las personas en el ciberespacio. - Es necesario brindar a las personas un nivel de seguridad que les permita el normal desarrollo de sus actividades personales, sociales y comunicacionales en el ciberespacio, junto al ejercicio de derechos fundamentales como la libertad de expresión, el acceso a la información, la protección de la vida privada y la propiedad.

Para proteger la seguridad del país. - Es necesario promover el resguardo de las redes y sistemas informáticos del sector público y privado, especialmente aquellas que son esenciales para el adecuado funcionamiento del país, velando por la continuidad operacional de los servicios básicos, así como la cadena de mando de los tomadores de decisiones.

Para promover la colaboración y coordinación entre instituciones. - Es necesario mejorar la comunicación, coordinación y colaboración entre instituciones, organizaciones y empresas, tanto del sector público como privado, nacional e internacional, con el propósito de fortalecer la confianza y entregar una respuesta común a los riesgos del ciberespacio.

Para gestionar los riesgos del ciberespacio. - Es necesario considerar el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de capacidades para la prevención y recuperación ante incidentes o ataques de ciberseguridad, configurando un ciberespacio estable y resiliente. A pesar de que, en Ecuador, existe una norma constitucional y legal; procesos e instituciones responsables de promover, planificar, ejecutar y supervisar las medidas relacionadas con la ciberseguridad; podemos afirmar que NO existe una estrategia nacional de ciberseguridad en el país; dicha afirmación se fundamenta a que, las instituciones e instrumentos mencionados, no se encuentra articulados ni operan en forma coordinada para cumplir este cometido. Considerando lo expuesto en la Conferencia realizada en Julio 2018 en la Universidad Andina sobre Mesa de Seguridad en Ciberdefensa considera que los siguientes actores deben estar presentes en el desarrollo y en la elaboración de una Política a nivel Estado: 1) El estado (desarrollo de políticas, normativa legal, planes sociales, regulación y control. 2) Sector privado (inversión, desarrollo y masificación de tecnologías). 3)Organismos internacionales (acuerdos de cooperación, normativa comunitaria e internacional). 4) Academia (formación, capacitación e investigación). (Bolivar, 2018)

En el libro blanco de la Sociedad de la Información y del Conocimiento elaborado por el MINTEL en el año 2018; NO se engloba a la ciberseguridad de una manera puntual sino en forma genérica sin especificar las tareas y objetivos específicos que se deben establecer para eliminar estas amenazas. En el capítulo referente a la seguridad de la información y protección de datos personales del estudio realizado por la empresa DELOITTE (2017) sobre seguridad de la información, establece que: existe brecha en seguridad de información de las empresas que generan una gestión de incidentes, existe la necesidad de elaborar planes de capacitación para mejorar los procesos de seguridad, el estado y las empresas requieren mayor presupuesto para la implementación en seguridad informática, las diferentes instituciones no tienen planes de contingencia para afrontar incidentes de seguridad digital porque no disponen de un SOC (Security Operation Center). Como producto de las revisiones internas y externas de las empresas,

la gestión de usuarios sigue siendo el elemento más tambaleante de la gestión de los CISO (Chief Information Security Officer) de las organizaciones. Y como conclusión de este estudio indica que "debe mejorar la gestión de la seguridad de la información tanto en la Academia, así como en las empresas" y presenta en la figura 2.

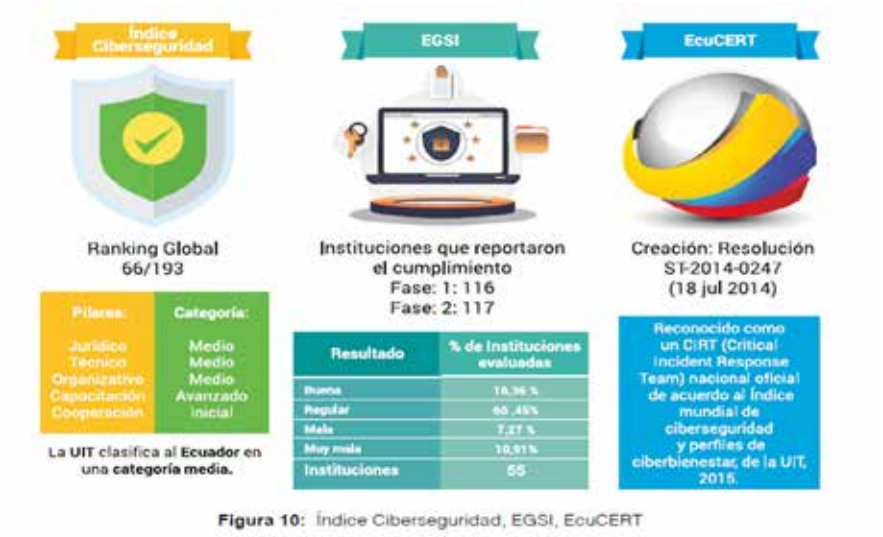

Figura 2. Gestión de la seguridad de la información Fuente: Libro Blanco de la Sociedad de la Información y del Conocimiento (MINTEL, 2018)

En el artículo sobre Ciberdefensa y Ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en Ciberdefensa**,** publicada en la revista latinoamericana de estudio de seguridad en el año 2017, se jerarquiza la gestión de la Ciberdefensa en tres niveles: nivel estratégico, nivel operacional y/o gerencial, y nivel táctico y/o técnico, gerenciada por un organismo denominado Secretaria de Ciberdefensa tal como se muestra en la figura 3.

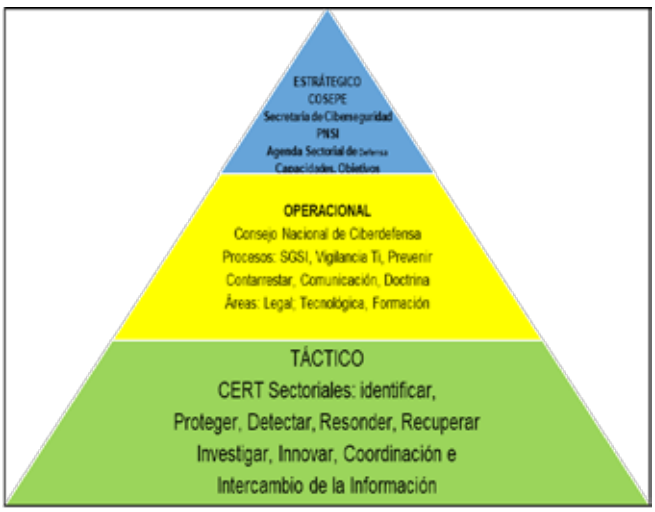

Figura. 3. Secretaria de Ciberdefensa. Fuente; "Pirámide organizacional de la Ciberdefensa" (Vargas R, 2017).

Ahora bien, consideremos como parte de este planteamiento: que para iniciar una discusión nacional de los temas de ciberseguridad y ciberdefensa, es necesario integrar al seno del mencionado Consejo, a los representantes de distintas instituciones ecuatorianas, considerando como énfasis que el ámbito de las TIC es transversal a las organizaciones públicas y privadas del Estado; y que las instituciones citadas en el planteamiento tiene gran relevancia en la gestión de los sectores estratégicos del país y son los órganos rectores de la política pública en sus respectivos ámbitos. La gestión de funcionamiento del organismo de ciberdefensa que regule estas políticas deben estar considerar niveles: nivel estratégico, nivel operacional, y nivel táctico en forma interagencial, como resultados del accionar de este organismo, se dictarán políticas y objetivos, alineados con el Plan Nacional Toda una Vida y que deberán estar plasmadas en el PNSI y en las Agendas Sectoriales como observamos en la Tabla No. 3.

Tabla No. 3 Niveles de Organización y Organismo que constituyen la Ciberdefensa

SECRETARIA/COMITÉ INTERSECTORIAL			
NIVEL	**ACTORES**	**RESPONSABLE**	**FUNCIONES**
Político estratégico	Estado Cosepe	Midena Mintel Ministerio relaciones exteriores Ministerio del interior Centro de inteligencia estratégica Ministerio de justicia Asamblea nacional	Órgano de elaborar las políticas y objetivos de ciberseguridad y ciberdefensa. Elaboración de leyes Supervisar la implementación de la estrategia
		Industrias Empresas de sistemas	Realizar proyectos de investigación orientados A apoyar el desarrollo tecnológico en el ámbito De la ciberdefensa y ciberseguridad.
		Transferencia tecnológica Capacitación	Actualización de conocimientos y procedimientos en el ciberespacio
Operacional	Comites	Comaco	Planificación
Táctico	Coordinador nacional de certs.	Cociber Ecucert	Respuesta a incidentes

Esta propuesta de estrategia planteada debe considerar los objetivos nacionales de seguridad cibernética como un todo con una sección direccionada a la Ciberseguridad y otra a la Ciberdefensa, considerando el contexto estratégico y los factores que pueden afectar las actividades de ciberdefensa frente a las amenazas y riesgos, intereses nacionales y los convenios y tratados vigentes, tomando en cuenta los recursos legales, capacidades técnicas, organizaciones estructural y la cooperación internacional desarrolladas en un plazo establecido, con prioridades

para el estabelecimiento de políticas con objetivos concretos y preciso considerando las amenazas y riesgo informático con un propósito de largo alcance (Figura 4).

Figura 4. Propuesta de Organización Cibernética del Ecuador.

Este organismo o comité de seguridad cibernética debe implementar los ejes de la política nacional de ciberseguridad observando los estándares internacionales de acuerdo a nuestra realidad considerando: 1) la Infraestructura de la información, 2) Prevención y sanción, Sensibilización, formación y difusión, 3) Cooperación y relaciones internacionales y 4) Institucionalidad de la ciberseguridad. En el nivel POLITICO este organismo de ciberdefensa debe articular las instancias permanentes y de conformación que aborden el tema desde el nivel político estratégico a fin de coordinar e implementar políticas y estrategias de ciberseguridad y ciberdefensa. Esta entidad debe considerar lo propuesto por (Vargas R, 2017):

1) Proponer la organización y funcionamiento de la ciberdefensa, en las siguientes áreas: protección de las infraestructuras críticas, manejo de crisis, ciberterrorismo, ciberdefensa militar, inteligencia y contrainteligencia, y gobernanza en internet y ciberdelitos (R. Vargas, L. Recalde y R. Reyes, 2012).
2) Disponer de una red de expertos conformando "observatorios de seguridad de la información" tanto públicos como privados de manera coordinada con cada sector estratégico.
3) Coordinar las actividades de ciberdefensa entre el sector gubernamental, los sectores privados y la población en general, articulando un sistema de intercambio de información y comunicación de incidentes (ISO/IEC27032 2012).
4) Coordinar actividades de ciberdefensa con otros países, y entidades regionales mediante acuerdos y creando estructuras de información de ciberseguridad para propósitos de intercambio (establecido en la Agenda Política de la Defensa).
5) Orientar el desarrollo de políticas del COSEPE, basado en el levantamiento de las "debilidades, vulnerabilidades y riesgos actuales y sobre los dilemas" (Klimburg 2012) existentes en cada ámbito, como son: estimular la economía versus mejorar la seguridad nacional, modernizar la infraestructura crítica o proteger la infraestructura crítica y protección de los datos o compartir información.

El análisis y la resolución de estos dilemas permitirán establecer los objetivos de seguridad derivados de las necesidades nacionales mediante un balance entre los significativos de libre flujo de información y las necesidades de seguridad del sector público, sector privado y los ciudadanos en general.

El **nivel operacional** materializado por Centro Nacional de Ciberdefensa, que gestione los procesos de resiliencia para desarrollar las capacidades para la defensa cibernética; además, se desarrollaría la doctrina para el empleo de los ciber-defensores, apuntalándolos con los mandatos legales, de formación y desarrollo tecnológico.

Por ello, el marco de trabajo de ciberseguridad y ciberdefensa debe ser pensado como una articulación de esfuerzos privados y públicos, civiles y militares, requeridos para asegurar un nivel aceptable de ciberseguridad del país. Para garantizar su efectividad, debe ser organizado de forma matricial, en donde un eje determine los niveles de decisión y trabajo, mientras se intercalan con los estándares, los sectores que deben atender, la metodología de aplicación y los objetivos de control que se deben aplicar.

El **nivel táctico** que realiza la activación y operación de los Centros de Respuesta de Emergencias Informáticas (CERT, por sus siglas en inglés) en las diferentes áreas (financiero, bancario, energía, telecomunicaciones, infraestructuras críticas y organismos públicos estratégicos) que se encargarán de identificar, proteger, detectar, responder, recuperar, investigar, innovar, coordinar e intercambiar información en cada una de las áreas críticas que potencialmente podrían ser afectadas por amenazas y reportar el incidente para garantizar un nivel de seguridad adecuado.

CONCLUSIONES

Considerando todas las experiencias de muchos países de la región y el mundo en cuanto a las estrategias y leyes creadas en función de las amenazas que circundan en el ciberespacio, es una necesidad imperiosa del estado ecuatoriano frente a estas nuevas amenazas "híbridas", crear un organismo de Ciberseguridad que garantice el principio de individualidad de los ciudadanos y de la infraestructura crítica del estado evitando la pérdida de recursos garantizando la seguridad y paz interna en forma preventiva y proactiva considerando la experiencia de países que lideran este campo y ya tienen en funcionamiento sus políticas nacionales y estrategias de Ciberseguridad.

El Ecuador tiene un acceso al internet del 43 % de la población permitiendo estar conectados a la información que está en el ciberespacio lo cual es una puerta de entrada para los delincuentes aumentando el riesgo a la seguridad, por lo cual se debe adaptar su política y estrategias de Ciberdefensa considerando los modelos implementados en países de la región y en las recomendaciones que entrega la OEA y Chile especialmente respecto a esta nueva amenaza híbrida tomando en cuenta de que el ciberespacio no tiene ni fronteras ni leyes y no requiere una declaración de guerra para iniciarla en donde deben participar el MINTEL, Ministerio de Interior, Ministerio de Relaciones Exteriores, Ministerio de Justicia, el Centro de Inteligencia Estratégica, la Asamblea Nacional entre otros bajo la coordinación del Ministerio de Defensa como institución encargada de la defensa.

Es fundamental que el estado cuente un marco legal contra los delitos informáticos, que puede afectar la infraestructura crítica y proteja la información, este marco jurídico debe estar basado en precedentes tomados de acuerdos internacionales y de la legislación de otros países.

BIBLIOGRAFÍA

BOLIVAR, U. S. (2018). *https://www.uasb.edu.ec/contenido?mesa-de-analisis-sobre-ciberseguridad*.

Chile, G. (2015). Bases para una Politica Nacional de Ciberseguridad.

Ciberseguridad, N. d. (s.f.). *https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf*.

DESARROLLO, B. I., & AMERICANOS, O. D. (2016). Banco Interamericano de Desarrollo (BID); Organización de los Estados Americanos - En https://publications.iadb.org/handle/11319/7449?locale-attribute=es#sthash.aKSZmfpW.dpuf.

Ecucert. (s.f.). *https://www.ecucert.gob.ec/*

ESPAÑOL, G. (2011). LEY DE PROTECCION DE INFRAESTRUCTURA FISICA.

Experiencias avanzadas. (2016). https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7:

Felix Arteaga y Enrique Fojón. (2007). *El planeamiento de la política de defensa y seguridad en España.* Madrid: Reprografía Doppel S.L.

GOBIERNO DE CHILE. (s.f.). *POLITICA NACIONAL DE CIBERSEGURIDAD*. En: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

GRANADA, U. D. (2018). ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN AMERICA LATINA. .

Gray, C. (1999). *Modern Strategy.* Boston: Oxford University Press.

HERNÁNDEZ, J. C. (2018). *ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN AMÉRICA LATINA*. En: http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

ISDEFE S.A., I. d. (s.f.). *https://www.isdefe.es/*.

MINTEL. (2018). *https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/07/Libro-Blanco-de-la-Sociedad-del-Informaci%C3%B3n-y-del-Conocimento.pdf*.

Murdock, C. (2004). *Improving the Practice of National Security Strategy.* Washington D.C.: CSIS.

R. Vargas, L. Recalde y R. Reyes. (2012). National Cyber Security Framework Manual. *URVIO*, 31-45.

Sanchez, M. (2016). *https://manuelsanchez.com/2016/01/29/la-seguridad-y-las-infraestructuras-criticas-sectores-estrategicos-presente-y-futuro/*.

UIT. (2007). *GUIIA DE CIBERSEGURIDAD PARA LOS PAISES EN DESARROLLO*. En: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

Vargas R, R. L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa . *Revista Latinoamericana de Estudios de Seguridad*, 31-45.