Yura: Relaciones internacionales

Departamento de Ciencias Económicas, Administrativas y de Comercio

Revista electrónica ISSN: 1390-938x

N° 23: Julio - septiembre 2020

Ciberdefensa en las Fuerzas Armadas del Ecuador para el 2021 pp.80-98

Jácome Guerrero Juan Carlos

Universidad de las Fuerzas Armadas ESPE

Sangolquí, Ecuador

Av. Gral. Rumiñahui s/n.

jcjjacome@hotmail.com

Ciberdefensa en las Fuerzas Armadas del Ecuador para el 2021

Jácome Guerrero, Juan Carlos
Universidad de las Fuerzas Armadas ESPE
jcjjacome@hotmail.com

Resumen

El nuevo teatro de operaciones virtual asimétrico denominado ciberespacio, de dimensiones infinitas configura el quinto dominio de la guerra junto a la tierra, mar, aire y espacio. Los Estados se preocupan por securitizar el ciberespacio, reivindicando el postulado Weberiano que como en los otros dominios del Estado debe ostentar el monopolio de los medios de coacción. Para enfrentar las amenazas en el ciberespacio, se requieren de planes y capacidades específicas tanto para ciberseguridad y ciberdefensa como para la ciberguerra, dependiendo de los objetivos de cada Estado. El objetivo de la investigación condujo al análisis de un hilo conductor, recogiendo las experiencias en temas de ciberdefensa en Colombia, Chile y Brasil, prácticas que permitan aprovechar los conocimientos y experiencias alcanzados en ciberdefensa, con la finalidad de determinar las capacidades que debe desarrollar las FF.AA. del Ecuador en temas cibernéticos, con proyección al 2021. Los resultados del estudio abordaron hitos nacionales e internacionales que constituyen el punto de partida para estructurar una estrategia nacional que responda al incremento de las amenazas informáticas que afecten al país. Sobre la base estas experiencias externas e internas, se recomienda una organización que permita fortalecer la ciberdefensa, que permita garantizar la integridad de la infraestructura crítica obteniendo como resultado recomendaciones a las instituciones que tienen la responsabilidad directa en ciberdefensa en nuestro país.

Palabras clave

Ciberdefensa, Infraestructura critica, Ciberguerra, Ciberespacio

Abstract

The new asymmetric virtual theater of operations called cyberspace, of infinite dimensions, configures the fifth domain of war together with land, sea, air and space. States are concerned with securitizing cyberspace, claiming the Weberian postulate that, as in other domains of the State, it must have a monopoly on the means of coercion. To deal with threats in cyberspace, specific plans and capabilities are required for both cybersecurity and cyber defense and cyber warfare, depending on the objectives of each State. The objective of the research led to the analysis of a common thread, collecting experiences on cyber defense issues in Colombia, Chile and Brazil, practices that allow taking advantage of the knowledge and experiences achieved in cyber defense, in order to determine the capabilities that must be developed by FF.AA. of Ecuador on cyber issues, with projection to 2021. The results of the study addressed national and international milestones that are the starting point to structure a national strategy that responds to the increase in computer threats that affect the country. Based on these external and internal experiences, an organization that strengthens cyber defense is recommended, that guarantees the integrity of critical infrastructure, resulting in recommendations to the institutions that have direct responsibility for cyber defense in our country.

Keywords

Cyber defense, Infrastructure criticizes, Cyber war, Cyber space,

El vertiginoso crecimiento de la tecnología ha dado lugar al surgimiento de un nuevo teatro de operaciones virtual asimétrico denominado “Ciberespacio”, a este escenario de dimensiones infinitas se lo considera como el quinto dominio de la guerra junto a la tierra, mar, aire y el espacio. (SHAFRAN, 2018)

> El ciberespacio se caracteriza por su bajo costo, el relativo anonimato de la persona y su ubicación, la posibilidad de realizar ataques a la Infraestructura Crítica digital de los Estados; y, fundamentalmente porque su efecto puede ser más devastador que un ataque convencional. En el ciberespacio no existen fronteras, no se requieren medios logísticos, es difícil identificar al enemigo y, consecuentemente, refleja mayores asimetrías que los campos de batalla tradicionales. Ya que para realizar un ciberataque no es necesario desplazarse o atravesar fronteras; el ciberespacio es un ambiente anónimo y asimétrico. (SHAFRAN, 2018) [1]

El Ecuador enfrentó el mayor ataque cibernético de su historia en abril de 2019, luego que el gobierno del “Ecuador decidió retirar el asilo diplomático a Julián Assange, fundador de WikiLeaks”. (Rivadeneira, 2019) Según fuentes oficiales, se registraron 40.000.000 ataques a diferentes instituciones públicas y privadas[2] en pocos días, lo que puso en evidencia la vulnerabilidad del país a este tipo de ataques. (Rivadeneira, 2019).

Ante estos antecedentes hemos visto la necesidad de proponer una estructura organizacional que permita disponer de un sistema integrado de ciberdefensa en FF.AA. que disponga de las capacidades y el equipamiento necesario para neutralizar las posibles amenazas cibernéticas con proyección al 2021. Para esto tenemos que identificar la infraestructura tecnológica que disponen actualmente nuestras FF.AA. para el cumplimiento de su misión y sus posibles vulnerabilidades. Además se describirá las capacidades que el sistema de Ciberdefensa debería alcanzar para el cumplimiento de sus misiones al 2021. Para finalmente proponer una estructura organizacional moderna de ciberdefensa que le permita el cumplimiento de la misión en FF.AA.

[1] La seguridad tiene cinco dominios: aire, tierra, mar, espacio y ciberespacio
[2] Entre las entidades atacadas están Cancillería de Ecuador, Presidencia de la República, Banco Central del Ecuador, ministerios y GAD´s.

Materiales y Métodos

Durante la Investigación se empleó el método cartesiano, al descomponer el fenómeno de estudio en sus partes integrantes, con un enfoque cualitativo, por sus fuentes de información, con unidad de análisis es mixta, utilizando el método inductivo y las técnicas documental y bibliográfica. Se partió de lo específico a lo general para definir el procedimiento requerido para seleccionar el personal, equipo y medios necesarios.

La investigación fundamenta el análisis de la información existente tanto en el Comando Conjunto de las Fuerzas Armadas (C.C.FF.AA), en los procesos del Comando de Ciberdefensa (COCIBER), también se realizaron encuestas y entrevistas al personal que cumple las actividades de ciberdefensa en las tres ramas de las Fuerzas Armadas: Fuerza Terrestre (F.T), Fuerza Naval (F.N) y Fuerza Aérea (F.A). También se consideró la organización, la estructura y los procedimientos que se emplea en Colombia, Chile y Brasil países de la región con realidades similares a la nuestra.

Resultados

En el desarrollo de la presente investigación se analizó la evolución que ha tenido la ciberdefensa en Colombia, Brasil y Chile, ya que son países de la región con realidades similares a las nuestras. Encontrando algunas características particulares, como el hecho que Colombia en el año 2009 a través del Consejo Nacional de Política Económica y Social (Conpes) como máxima autoridad nacional de planeación en coordinación con el Ministerio de Defensa de Colombia ha desarrollado las políticas públicas en lo referente a ciberdefensa y ciberseguridad. (Planeacion, 2011).

En el Plan Nacional de Desarrollo 2014-2018, incluye el fortalecimiento de las capacidades en ciberdefensa y en el 2016 se publica el documento CONPES 3854 como parte de la Política Nacional de seguridad digital, considerando como organismos encargados de la ciberdefensa y ciberseguridad en Colombia a la Presidencia de la República, Ministerio de Defensa Nacional y al Ministerio de Tecnologías de la Información y Comunicaciones. Manteniendo como organismos especializados al Comando Conjunto Cibernético de las Fuerzas Militares, al Centro cibernético policial y al Grupo de respuesta a emergencias cibernéticas de Colombia (COLCERT). Con el objetivo “garantizar la soberanía e integridad del territorio nacional, protegiendo los intereses nacionales”. (Planeación, 2015).

Colombia puso en marcha su estrategia de Ciberseguridad y Ciberdefensa a través del "CONPES 3701", con el que buscó fundamentar los mecanismos normativos, organizacionales e institucionales que le permitan afrontar los nuevos retos en seguridad cibernética en el país. Fundamentándose en tres pilares fundamentales que son:

1. Coordinar adecuadamente las operaciones ya que no existen un organismo a nivel nacional constituido para coordinar y desarrollar operaciones de Ciberdefensa. Por lo tanto, no ha sido posible implementar los mecanismos suficientes y adecuados para contrarrestar ataques cibernéticos y proteger los intereses del Estado en el ciberespacio. (PLANEACIÓN, 2016)
2. La capacitación especializada en Ciberseguridad y Ciberdefensa requiere de revisión ya que el conocimiento en estas dos áreas es limitado tanto en el sector público como en el privado. Si bien en Colombia existen algunas instituciones de educación superior que ofrecen especializaciones en seguridad informática y derecho informático, se ha identificado que la oferta académica en programas especializados en estas áreas es reducida. (PLANEACIÓN, 2016)
3. La normativa legal requiere de revisión. El Ministerio de Justicia en la actualidad realiza una revisión integral del Código Penal, específicamente para el tema de tipificación de los delitos informáticos. Existe debilidad en la legislación de la protección de la información y datos. (PLANEACIÓN, 2016).

Colombia cuenta con un sistema de inteligencia que controla y vigila la seguridad y la defensa nacional en el campo digital estarán mejor armadas a la hora de recabar información y datos que permitan disminuir los riesgos para la Nación.

En Brasil la política de ciberseguridad se ha desarrollado en un contexto de creciente preocupación ante el incremento del número de ataques cibernéticos, como también por no quedar detrás de las principales potencias mundiales en el enfrentamiento de las amenazas cibernéticas. Brasil es uno de los países más afectados por el cibercrimen, tanto por el origen de actividades criminales, como por el número de víctimas (Lobato, 2017)

En agosto de 2001 el tema cibernético se trata inicialmente con el desarrollo de la Seguridad de la Información, creándose el Gabinete de Seguridad Institucional de la Presidencia de la República (GSI / PR). A este organismo, le corresponde la coordinación de las actividades de Seguridad de la Información. En 2006, se creó el Departamento de

Seguridad de la Información y Comunicaciones (DSIC), en el GSI / PR, con la misión de planificar y coordinar la ejecución de las actividades de Seguridad de la Información.

En el 2008 con el establecimiento del sector cibernético, se aprueba la Estrategia de Defensa Nacional, reconocieron dos campos distintos: la ciberseguridad, bajo control de la Presidencia de la República (PR), y la ciberdefensa, a cargo del Ministerio de Defensa, a través de FA.

En este contexto el Ministerio de Defensa, determina que las acciones cibernéticas deben tener las siguientes denominaciones según el nivel de decisión

1. Nivel político - Seguridad de la información y las comunicaciones (SIC) y Seguridad cibernética - coordinado por la Presidencia de la República y que abarca la administración pública federal directa e indirecta (FPA), así como las infraestructuras de información crítica inherentes a las infraestructuras críticas nacionales.
2. Nivel estratégico - Defensa cibernética: a cargo del MD, Jefes de Estado Mayor Conjunto de las Fuerzas Armadas (EMCFA) y los Comandos de la FA, que interactúan con la Presidencia de la República y la APF; y
3. Niveles operativos y tácticos - Guerra cibernética: nombre restringido al alcance interno de las FF.AA. (DEFESA, 2017).

Con la publicación, de la Estrategia Nacional de Defensa (END) en 2008, se establece prioridades en tres sectores estratégicos para la Defensa Nacional: Nuclear, Cibernético y Espacial. El Ministerio de Defensa por medio de directrices, a los sectores estratégicos de la defensa, estableciendo en el 2009, las responsabilidades para cada una de las Fuerzas. Correspondiendo al Ejército la responsabilidad de la coordinación y la integración del Sector Cibernético, activando el 2 de agosto de 2010, el Núcleo del Centro de Defensa Cibernética. (Hernandez, 2014)

En 2014, por medio de una ordenanza Interministerial del Ministerio de Ciencia, Tecnología e Innovación y Ministerio de Defensa, se instituyó el Programa de Investigación, Desarrollo e Innovación en Defensa Cibernética, que, entre otros, tiene como objetivos, el fomento de soluciones nacionales en Ciberdefensa, la creación de laboratorios de análisis de programas maliciosos y gestión técnica, de negocios y gobernanza y en el año 2015, se creó el Comando de Defensa Cibernética y la Escuela

Nacional de Defensa Cibernética, con la activación de sus núcleos, a partir del 1 de enero de 2015. Además, fue elaborada por el GSI / PR la Estrategia de Seguridad de la Información y Comunicaciones de Seguridad Cibernética de la Administración Pública Federal - 2015/2018. Finalmente, en abril de 2016, el Comando de Defensa Cibernética fue activado. (Lobato, 2017)

De lo expuesto, se puede evidenciar un encadenamiento lógico de acciones políticas, estratégicas y operativas que facilitó la implantación de estructuras y normalizó el sector cibernético en Brasil. Se identifica la participación de otros organismos del estado a más de la estructura militar, alcanzando una participación nacional en el proceso, manteniendo la base ejecutiva en manos del Ejército Brasileño, como una Estrategia Nacional de Defensa.

En Chile se aprobó el Plan Nacional de Ciberseguridad para el periodo 2017-2022, en abril del 2017 Constituyéndose en el primer instrumento de política pública del Estado de Chile tendiente a desarrollar una estrategia nacional en esta materia, con el propósito de contar con un ciberespacio libre, abierto, seguro y resiliente.

La masificación en el uso de tecnologías de información y comunicaciones (TIC), a más de servir al desarrollo del país, conlleva riesgos que pueden afectar a la seguridad pública, las infraestructuras críticas, el gobierno digital, los intereses esenciales y la seguridad exterior de Chile. (Aranguiz, 2018)

Estos riesgos pueden provenir de múltiples fuentes y se pueden manifestar atreves de actividades de espionaje, sabotaje, fraudes o ciberataques realizados por otros países, por grupos organizados o por particulares, entre otros.

Chile con este documento, busca contar con una política que oriente la acción del país en materia de ciberseguridad, junto con implementar y poner en marcha las medidas que sean necesarias para proteger la seguridad de los usuarios del ciberespacio, considerando estrategias educativas orientadas al autocuidado y prevención en el ambiente digital, a fin de lograr una cultura de seguridad digital que proteja a los usuarios privados y públicos. (Asesoría Técnica Parlamentaria, 2018)

Chile cuenta con un conjunto de normas legales y reglamentarias que se hacen cargo directa e indirectamente del fenómeno de ciberseguridad que resulta necesario revisar y actualizar conforme a las directrices que plantea esta política, por ejemplo, la ley Nº

19.223 sobre delitos informáticos o la ley Nº 19.628 sobre protección de la vida privada, entre otras. (Chile, 1993)

Panorama de riesgos.- Los riesgos y amenazas son de carácter externo e interno, y se originan tanto en causas naturales como en actividades delictivas, por ejemplo, en labores de espionaje y vigilancia llevadas a cabo con diversos fines, afectando la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, y con ello, los derechos de las personas.

La política de ciberseguridad tiene dos componentes centrales: una política de Estado, diseñada con objetivos orientados al año 2022, y una agenda de medidas específicas, que serán implementadas entre los años 2017 y 2018 (lo que resta del gobierno de la presidenta Bachelet). El objetivo de este diseño es proponer una visión general de hacia dónde debe moverse Chile en el mediano y largo plazo.

La política para el año 2022. se enmarca en un conjunto de políticas que el Gobierno Chileno ha implementado o se encuentra desarrollando en materia digital, con el objeto de contar con definiciones claras y sistémicas sobre el ciberespacio: (CIBERSEGURIDAD, 2017)

1. Agenda Digital 2020.- Es una hoja de ruta para avanzar hacia el desarrollo digital de Chile, mediante la definición de objetivos de mediano plazo, líneas de acción y medidas concretas. busca transformar el uso masivo de las tecnologías en un medio para reducir las desigualdades, abrir más y mejores oportunidades de desarrollo, respetando los derechos de todos los chilenos. En la agenda existe una medida específica, que apunta a la elaboración de una estrategia de ciberseguridad. (CIBERSEGURIDAD, 2017).
2. Política nacional de ciberdefensa.- considerando que las redes y sistemas de información de la Defensa Nacional constituyen una infraestructura crítica para la seguridad exterior y el ejercicio de la soberanía de Chile, y a las atribuciones constitucionales y legales de la Defensa Nacional, el Ministerio de Defensa, durante el año 2017 preparará y publicará políticas específicas de ciberdefensa, en torno a cómo serán protegidas estas redes, y cómo las capacidades de la Defensa Nacional pueden colaborar en la formación de un ciberespacio libre, abierto, seguro y resiliente para el país. (CIBERSEGURIDAD, 2017).

3. Política internacional para el ciberespacio.- Uno de los objetivos hace referencia a la cooperación y relaciones internacionales en torno a la ciberseguridad en el contexto global.

Siendo imprescindible que el país integre estos objetivos con otros tales como el desarrollo, los derechos humanos, la defensa y otros relacionados, para consolidarlos e integrarlos en la política exterior de Chile. Para ello, la presente política contempla una medida específica vinculada con la elaboración de una estrategia en estos aspectos por parte del Ministerio de Relaciones Exteriores, que apunta a generar una visión país sobre gobernanza de internet. (CIBERSEGURIDAD, 2017)

En Ecuador, existe una norma constitucional y legal; inclusive procesos e instituciones responsables de promover, planificar, ejecutar y supervisar las medidas relacionadas con la ciberseguridad y ciberdefensa; podemos decir que no contamos con una estrategia nacional de ciberseguridad. Esta afirmación se fundamenta en que las diferentes instituciones públicas y privadas, no se encuentran articuladas, ni operan en forma coordinada para cumplir este cometido. Según (Murdock, 2004), la estrategia nacional consiste en saber cómo actuar y con qué recursos se cuenta para conseguir sus fines; dar una idea general de cómo se esperan conseguir los resultados buscados.

Para que exista una estrategia nacional de ciberseguridad, es indispensable que la ciberseguridad y ciberdefensa, sean consideradas como una Política de Estado. Se requiere disponer de una Estrategia de Seguridad Nacional que se establezcan propósitos, principios rectores, políticas, objetivos a corto, mediano y largo plazo, contar con medidas específicas, líneas de acción, tener un diseño institucional que establezca funciones mínimas, como también contar el con una normativa con leyes adecuadas. Es fundamental que las instituciones públicas y privadas trabajen coordinadamente, que cuenten con las capacidades e infraestructura necesaria y que cuenten con los recursos presupuestarios necesarios para ejecutar su planificación.

Como resultado del análisis realizado de a las encuestas y entrevistas realizadas durante la investigación podemos concluir que la infraestructura de ciberdefensa con la que actualmente cuenta nuestro país y las FF.AA., es insuficiente para el cumplimiento de sus misiones. Quedando en evidencia la vulnerabilidad de la infraestructura crítica nacional, a los ataques cibernéticos. Siendo entre otras causas, una consecuencia de un presupuesto reducido para ciberdefensa. (NRD Cyber Security, 2019)

El Ecuador no dispone de una normativa en Ciberdefensa, en la actualidad se ha presentado en la Asamblea Nacional los proyectos de: Ley Orgánica de Seguridad del Estado, el proyecto de Ley de Seguridad Pública y del Estado y especialmente el proyecto de Ley de Seguridad Digital introducen cambios en los requisitos de capacidad de ciberdefensa de Ecuador que van desde el empleo de las Fuerzas Armadas para la protección de empresas públicas y privadas que operan en sectores estratégicos en tiempos de emergencia para la detección, prevención, contención y respuesta a los ataques cibernéticos contra todas las IC nacionales. (NRD Cyber Security, 2019)

Las Fuerzas Armadas, en la actualidad, no cuentan con suficiente personal capacitado en Ciberdefensa y el existente no tiene una articulación intra - fuerzas. Las Escuelas e Institutos de Formación, Perfeccionamiento y Especialización no tienen programas en ciberdefensa lo que incide negativamente en las operaciones, ya que el personal no tiene los conocimientos suficientes para enfrentar esta amenaza específica.

El sistema de ciberdefensa en el 2021 deberá integrar al Comando Conjunto con las tres ramas de las Fuerzas Armadas; Fuerza Terrestre, Fuerza Naval y Fuerza Aérea, así como también con las otras instituciones del estado consideradas como infraestructura critica, para garantizar la prevención, detección, respuesta ante posibles ciberataques. Ya que en la actualidad solamente el CC.FF.AA. dispone de una unidad de Ciberdefensa.

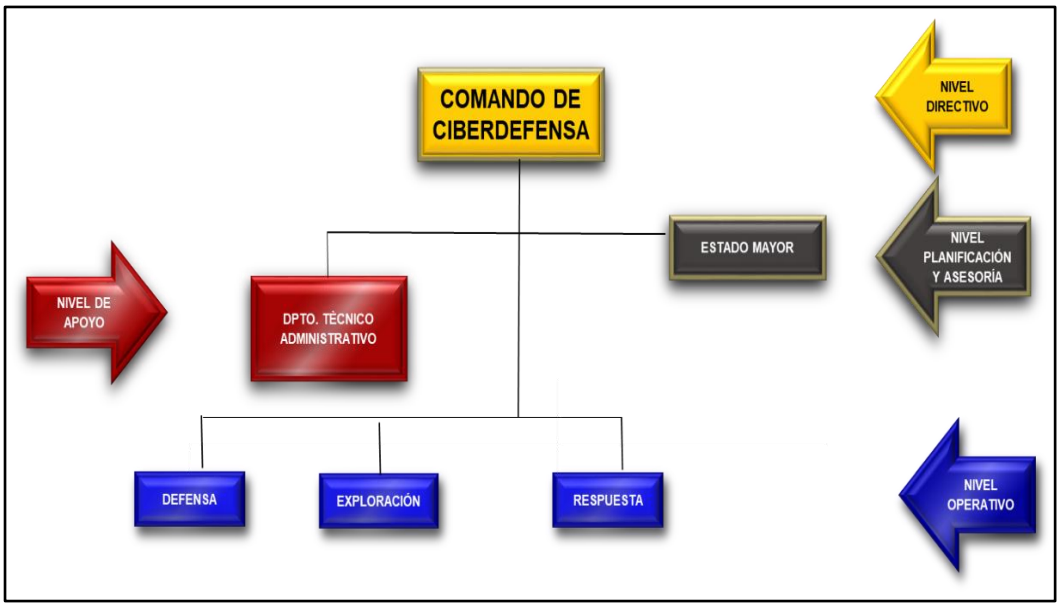

ILUSTRACIÓN 1. Organización del COCIBER

Fuente: (COCIBER, 2014)

Para solucionar este necesidad es necesario disponer de personal capacitado y entrenado permanente, también contar con infraestructura tecnológica adecuada y moderna que permita realizar el monitoreo permanente de las posibles amenazas desde cada una de las Fuerzas, como lo realiza el COCIBER., con procedimientos estandarizados, con seguridad en el interior de FF.AA. de manera que permitan prevenir y mitigar ciberataques que pudieran afectar a Fuerzas Armadas y a la Infraestructura Critica del país. Para que esto sea posible se deben:

1. Cumplir con los principios de disponibilidad, confidencialidad e integridad de la información.
2. Planificar y ejecutar la ciberdefensa para las Fuerzas Armadas y la Infraestructura Crítica Digital, con el apoyo de todas las instituciones gubernamentales y, posteriormente.
3. Desarrollar capacidades suficientes de respuesta y resiliencia ante cualquier tipo de ciberataque.

El recurso humano es esencial, por lo tanto se requiere contar con personal capacitado en seguridad de la información, seguridad informática, análisis forense, respuesta de incidentes, ciberinteligencia entre otras especialidades; para que puedan actuar en manera oportuna ante cualquier incidente que se pudiera presentar en el ciberespacio. Este personal deberá ser seleccionado y contar con un perfil debidamente analizado y validado que garantice contar con las personas más idóneas para el manejo de información clasificada.

Este personal deberá estar acompañado de una infraestructura tecnológica que le permita prevenir, detectar y mitigar ciberataques. Deberíamos contar de un COS (Centro de Operaciones de Seguridad) que permita monitorear las redes de datos de cada una de las Fuerzas; Fuerza Terrestre, Fuerza Naval y Fuerza Aérea con la finalidad de brindar la alerta oportuna y prevenir cualquier tipo de ciberataque.

Es necesario, establecer un perfil profesional y un plan de carrera para el personal militar en el ámbito de la ciberdefensa, para especializarlo en función de las necesidades específicas, se deberá realizar un análisis del personal en cuanto a su desempeño profesional en su carrera militar, que al menos deberían tener diez (10) años en la institución. Posteriormente, se debe seleccionar personal calificado que disponga conocimientos básicos y sólidos en áreas tales como: Switching, Routing, Linux,

Windows server, cableado estructurado y comunicaciones inalámbricas; es decir, durante los primeros 10 años se debe enfocar los esfuerzos para que los técnicos (oficiales y tropa) vayan adquiriendo estos conocimientos y sean expertos en el conocimiento de la infraestructura de cada una de las tres Fuerzas. Con esto deben someterse a un entrenamiento especializado en CIBERDEFENSA bajo el control del COCIBER que les permita contar personal capacitado, entrenado y con el perfil que esta nueva especialidad requiere.

Esto permitirá que exista un equipo homogéneo con personal especializado en el CC.FF.AA.[3] y en cada una de las tres Fuerzas, que sabrán entenderse y actuar con sinergia ante las amenazas y riesgos de un ciberataque, mejorando las condiciones de protección de la infraestructura crítica y tecnológica de las FF.AA. así como permitirá optimizar los recursos humanos, materiales y económicos de la institución.

Adicionalmente se requiere contar con asignaturas en las Escuelas de Formación y Perfeccionamiento que permitan mantener a todo el personal de FF.AA. de la importancia que tiene la ciberdefensa, algo muy importante es mantenernos en contacto de manera permanente con la Academia para actualizar los conocimientos del personal, coordinando con la ESPE- CICTE en la realización de cursos. La creación de líneas de investigación que permita evitar la dependencia de empresas privadas extranjeras para la adquisición de herramientas.

Actualmente se cuenta con equipos para realizar análisis forense, equipos para monitoreo de disponibilidad de servicios. El COCIBER se encuentra en proceso de ejecución del proyecto de “Implementación de la Capacidad de Ciberdefensa de las Fuerzas Armadas”. Se estima que para el 2020 el Ecuador contará con un inmueble con su respectivo centro de datos y con un simulador de ciberdefensa que permitirá vitalizar la infraestructura digital de Fuerzas Armadas. Para el año 2021 se estima ya disponer con un Centro de Operaciones de Seguridad. Pero en las tres remas de Fuerzas Armadas no se dispone de personal, ni material para realizar operaciones de ciberdefensa, solamente disponen de sistemas que les permite proteger la información de los servidores centrales y los accesos al internet.

También se debería considerar a la ciberdefensa como una capacidad estratégica de Fuerzas Armadas, como también se ve la necesidad de crear un sistema de ciberdefensa

[3] Comando Conjunto de las Fuerzas Armadas

con un plan de carrera definido, que permita contar con el personal capacitado y especializado en ciberdefensa, este personal especialista debería ser empleado solamente en su especialidad, rotar únicamente en las unidades y áreas de ciberdefensa,

Discusión

La resiliencia como como estrategia ofrece una visión de equilibrio de los sistemas y nos indica la manera de cómo responder ante diversas circunstancias. A partir de esto y usando el análisis de riesgos, nos permite reducir las amenazas o las vulnerabilidades. Considerando que no existe ningún sistema cien por ciento seguro y siempre existe la probabilidad de ocurrencia de un efecto de riesgo que puede ser reducido por la resiliencia.

El ataque a una Infraestructura Crítica por el nivel de impacto que puede acarrear la interrupción en su funcionamiento o daño en sus sistemas, produciría graves consecuencias en el normal desempeño de las actividades cotidianas de la población y de las instituciones públicas y privadas del país. La Infraestructura Crítica del país como: los sistemas de generación y distribución de energía, las redes de telecomunicaciones, el control del oleoducto, entre otros, pueden ser el blanco de los ciberataques. El impacto económico en las empresas, el costo que tendría para el estado el recuperar estas infraestructuras, así como la presión regulatoria para mitigarlas, incrementa la importancia de la ciberdefensa.

Durante la investigación se ha evidenciado como los países de la región han incrementado el uso de tecnologías de informática y comunicación para bloquear, prevenir y contrarrestar los ataques cibernéticos, que cada día son más comunes. Pese a que han avanzado mucho en este campo, sus debilidades son muy similares a las nuestras.

Se han establecido lineamientos para la Ciberseguridad y Ciberdefensa a través de la estrategia que establece mecanismos normativos, organizacionales e institucionales que le permitan afrontar los nuevos retos en seguridad cibernética en sus respectivos países. Como por ejemplo la activación del COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), que busca articular y coordinar el desarrollo de medidas preventivas y reactivas de Seguridad Digital, ya que responde al máximo nivel del Gobierno. Adicionalmente se considera en cada ministerio y departamento administrativo

de orden nacional la creación de un enlace sectorial en términos de Seguridad Digital. Es fundamental contar con ley de Protección de Datos.

En nuestro país la Ciberseguridad inicia en el año 2011 año en el que la Secretaría Nacional de la Administración Pública crea la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional.

Los países en los cuales se hizo una revisión bibliográfica, coinciden en mantener dos sistemas. Un sistema de seguridad externa (ciberdefensa)[4] y otro de políticas internas (ciberseguridad)[5]. Ambos mantienen una coordinación unificada y enlace directo con la Presidencia. Es muy importante mantener una coordinación similar en el Ecuador, tanto para un adecuado intercambio de información como para desarrollar protocolos similares de defensa.

En nuestro país el 12 de septiembre de 2014, por el Acuerdo Ministerial No. 281 se crea el Comando de Ciberdefensa dentro de las Fuerzas Armadas, 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, mediante operaciones de protección del espacio cibernético, acciones de prevención, disuasión, explotación y respuesta ante eventuales amenazas, riesgos e incidentes a fin de contribuir a la misión del Comando Conjunto.

En el Ecuador contamos con el centro de respuesta a incidentes informáticos del Ecuador (ECUCERT) que tiene como finalidad brindar a su comunidad objetivo apoyo

[4] "Es el conjunto de recursos, actividades, técnicas y procedimientos para preservar la seguridad de mando y control de las Fuerzas Armadas y la información que manejan así como permitir la explotación y respuesta sobre los sistemas necesarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos." (Fernández, 2016)

[5] Es el conjunto de técnicas o procedimientos que velan por la seguridad de los usuarios que comparten información entre sistemas computables. (economia simple.net , 2016)

en la prevención y la resolución de incidentes de seguridad informática, a través de coordinación, capacitación y soporte técnico. (ARCOTEL, 2019).

El Ecuador todavía no cuenta con una estrategia en ciberdefensa y ciberseguridad, pero el gobierno se encuentra comprometido con desarrollar la ciberdefensa y ciberseguridad. Por lo que ha adoptado de algunas políticas y estrategias en las que se definen los lineamientos con respecto a la ciberdefensa y ciberseguridad. (NRD Cyber Security, 2019)

En la Política de Defensa Nacional, publicada en el 2018, se considera a la ciberseguridad y la ciberdefensa como elemento integral de la defensa nacional, por lo que se han estableciendo requisitos y capacidades para ser desarrolladas por las Fuerzas Armadas. (Ministerio de Defensa Nacional, 2018)

Con la finalidad de fortalecer y asegure el entorno digital, funcionarios del Ministerio de Telecomunicaciones y miembros de la Sociedad de la Información (MINTEL), se reunieron con representantes del Banco Interamericano de Desarrollo (BID) y la consultora NRD Cyber Security, para la "Elaboración de la Estrategia Nacional de Ciberseguridad". Al finalizar esta consultoría, Ecuador obtendrá una metodología adaptada al contexto cultural y organizacional; que permitirá fortalecer y asegurar el entorno digital. (Información, 2019)

Mantener un compromiso internacional es clave ya que por medio de esta técnica es posible observar la evolución en materia de ciberespacio en el ámbito internacional, para mejorar la coordinación de la ciberdefensa con los estados aliados, Ecuador ha establecido acuerdos de cooperación bilateral con Chile, Perú, Colombia y España, pero, a nivel nacional, la coordinación es en gran medida ad hoc y no está formalizada. Es importante mantener la coordinación ya que a más de ser una herramienta de desarrollo con la que cuenta el país, se convierte en un punto clave para la protección de posibles ataques cibernéticos. (NRD Cyber Security, 2019).

La educación y capacidades de investigación y desarrollo, es fundamental ya que los delincuentes cibernéticos continuamente desarrollan nuevas formas para realizar ataques cibernéticos. Es por esto, que la investigación sobre el tema es indispensable para estar acorde a las exigencias que presenta cada una de las funciones, pero para realizar una adecuada investigación primero hay que educarse con la finalidad que la investigación sea prospera. Una de las herramientas del gobierno para combatir este fenómeno, se

concentra en la especialización de su talento humano por medio de diferentes cursos sobre Ciberdefensa y Ciberseguridad. En esta temática se puede observar su evolución y desarrollo en cuanto a estos dos temas, ya que se cuenta con herramientas de educación que dan pasó a la especialización.

En lo que se refiere a la Doctrina podemos evidenciar que la mayoría de países han desarrollado su propia doctrina basados en su realidad, considerando las amenazas, estructura y medios disponibles. También podemos identificar que de igual manera su normativa está acorde con su organización, considerando tanto a las entidades públicas y privadas que actúan coordinadamente. Obteniendo como resultado la generación de una doctrina conjunta propia de cada país. Para ello entregan la responsabilidad de la ciberseguridad a la policía y la ciberdefensa a las FF.AA. También hemos podido observar la asignación de responsabilidades en los diferentes niveles, tanto político, estratégico, operativo y táctico.

Entre las premisas sobre el sector cibernético, se considera que la protección del espacio cibernético abarca un gran número de áreas, como: capacitación, inteligencia, investigación científica, doctrina, preparación y empleo operacional; y gestión de personal.

Manteniendo Programas de Investigación, Desarrollo e Innovación en Defensa Cibernética, que, entre otros, tiene como objetivos, el fomento de soluciones nacionales en Ciberdefensa, la creación de laboratorios de análisis de programas maliciosos y gestión técnica, de negocios y gobernanza, es muy importante ya que fue creado con la finalidad de desarrollar una estrategia nacional en esta materia, trabajan en la Política nacional de ciberdefensa, la política internacional para el ciberespacio y la Ley sobre delitos informáticos con el propósito de contar con un ciberespacio libre, abierto, seguro y resiliente. Nuestro país todavía no cuenta con doctrina propia, ni con centros especializados en capacitar y especializar al personal en Ciberdefensa, la ESPE está incursionando en esta nueva especialidad y planifica la creación de una carrera con esta especialización.

Considerando las experiencias de los países analizados en la región podemos concluir que la infraestructura con la que actualmente cuenta FF.AA. del Ecuador, es insuficiente para el cumplimiento de su misión. Ya que el nivel de riesgo al que está expuesta la infraestructura crítica del país es alto.

Es por esto que proponemos una nueva organización en las tres ramas de las Fuerzas Armadas; Terrestre, Naval y Aérea que en la actualidad no disponen de una unidad ni de equipo especial rara realizar operaciones de ciberdefensa, crear una sección de ciberdefensa orgánica en los comandos de cada fuerza, que permita disponer de una estructura orgánica flexible, que se encuentre articulada entre los comandos de las tres fuerzas inicialmente, para en una segunda fase se dote de estas unidades a los comandos operacionales, a las Divisiones y a las Brigadas, lo que permitirá estar en condiciones de realizar ciberdefensa en todos los niveles y estar acordes a los avances tecnológicos.

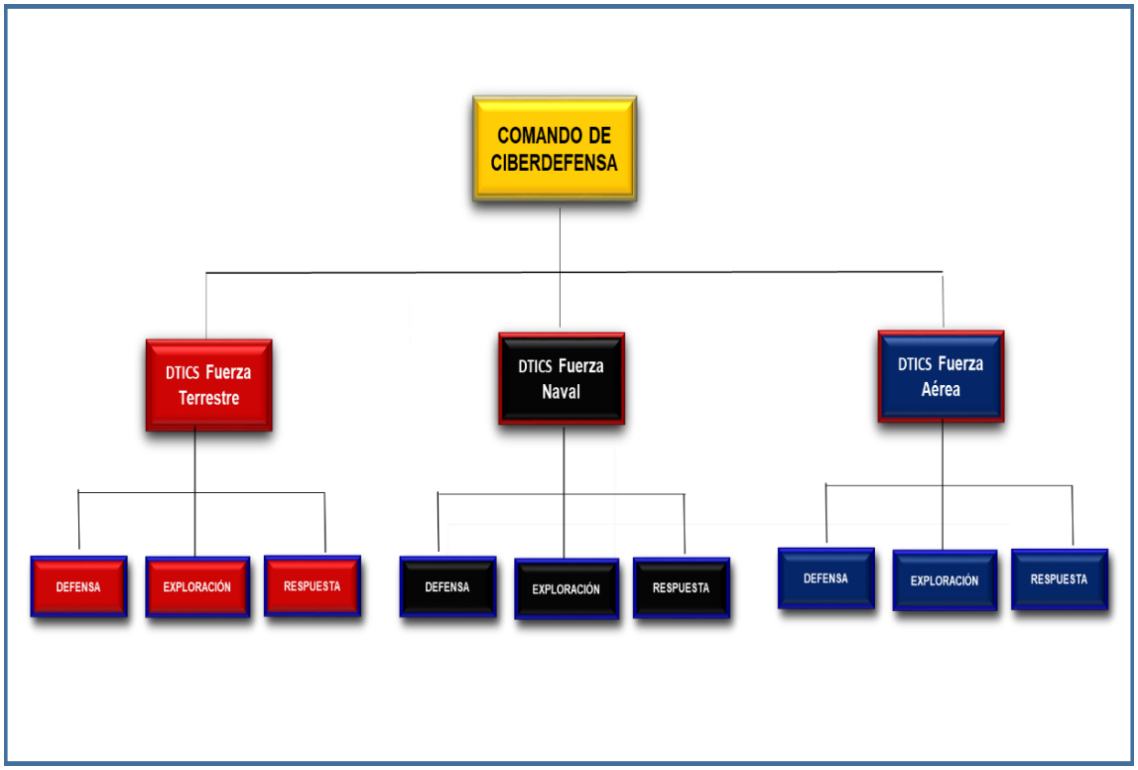

ILUSTRACIÓN 2. Estructura de Ciberdefensa propuesta en FF.AA

Lista de referencias

Aranguiz, O. E. (21 de 03 de 2018). *infodefensa.com*. Obtenido de https://www.infodefensa.com/latam/2018/03/21/noticia-chile-creara-comando-conjunto-ciberdefensa.html

ARCOTEL. (2019). ECUCERT. *Revista Institucional ARCOTEL*, 12.

Asesoría Técnica Parlamentaria. (Julio de 2018). Obtenido de Política Nacional de Ciberseguridad: 2017-2022: https://www.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf

Chile, C. N. (7 de Junio de 1993). *Biblioteca del Congreso Nacional de Chile*. Obtenido de Biblioteca del Congreso Nacional de Chile: https://www.leychile.cl/Navegar?idNorma=30590

CIBERSEGURIDAD, P. N. (2017). *POLíTICA NACIONAL DE CIBERSEGURIDAD*. Obtenido de POLíTICA NACIONAL DE CIBERSEGURIDAD: https://www.ciberseguridad.gob.cl/media/2018/06/PNCS_Chile_ES_FEA.pdf

COCIBER. (2014). Quito.

DEFESA, M. D. (2017). *Manual de Campanha GUERRA CIBERNÉTICA*. MINISTÉRIO DA DEFESA.

economia simple.net . (2016). *economia simple.net* . Obtenido de Definición de Ciberseguridad: www.economiasimple.net/glosario/ciberseguridad

Fernández, A. M. (19 de Febrero de 2016). *Orden ministerial de creación del mando conjunto de ciberdefensa de España*. Valencia: Tirant lo blanch.

Hernandez, D. O. (07 de 10 de 2014). *incibe-cert_*. Obtenido de incibe-cert_: https://www.incibe-cert.es/blog/la-ciberseguridad-de-brasil-una-clave-para-el-progreso

Información, M. d. (28 de marzo de 2019). *Ministerio de Telecomunicaciones y de la Sociedad de la Información*. Obtenido de Ministerio de Telecomunicaciones y de la Sociedad de la Información: https://www.telecomunicaciones.gob.ec/ecuador-trabaja-en-la-estrategia-nacional-de-ciberseguridad/

Lobato, L. C. (26 de abril de 2017). *La política brasileña de ciberseguridad como estyrategia de liderasgo regional* . Obtenido de https://revistas.flacsoandes.edu.ec/urvio/article/view/2576/1604: https://revistas.flacsoandes.edu.ec/urvio/article/view/2576/1604

Ministerio de Defensa Nacional. (2018). Política de la Defensa Nacional. En M. d. Nacional, *Libro Blanco* (págs. 20, 132). Quito: IGM.

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

NRD Cyber Security. (2019). *Revisión de la Capacidad de* . Quito.

Ojeda, J., Jiménez, P., Quintana, A., Crespo, G., & Viteri, M. (2015). Protocolo de investigación. (U. d. ESPE, Ed.) *Yura: Relaciones internacionales, 5*(1), 1 - 20.

Planeacion, D. N. (14 de 7 de 2011). *https://es.slideshare.net/Derechotics/3701*. Obtenido de https://es.slideshare.net/Derechotics/3701: https://es.slideshare.net/Derechotics/3701

Planeación, D. N. (2015). *https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/Colombia_Plan_Nacional_de_Desarrollo_2014_2018.pdf*. Obtenido de https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/Colombia_Plan_Nacional_de_Desarrollo_2014_2018.pdf: https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/Colombia_Plan_Nacional_de_Desarrollo_2014_2018.pdf

PLANEACIÓN, D. N. (16 de 1 de 2016). *https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf*. Obtenido de https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf: https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf

Rivadeneira, G. (15 de Abril de 2019). *EL UNIVERSO*. Obtenido de https://www.eluniverso.com/noticias/2019/04/15/nota/7287215/ecuador-ha-recibido-40-millones-ataques-ciberneticos-revela

SHAFRAN, A. (25 de Junio de 2018). *La seguridad tiene cinco dominios: aire, tierra, mar, espacio y ciberespacio*. Obtenido de www.perfil.com/noticias/internacional/la-seguridad-tiene-cinco-dominios-aire-tierra-mar-espacio-y-ciberespacio.phtml