DEPARTAMENTO DE SEGURIDAD Y DEFENSA

TESIS PREVIO A LA OBTENCIÓN DEL TITULO DE ESPECIALISTA EN ESTUDIOS ESTRATÉGICOS DE LA DEFENSA

TEMA: "ESTUDIO PROSPECTIVO DE LA CIBERDEFENSA EN LAS FUERZAS ARMADAS DEL ECUADOR"

AUTOR: CRNL DE E.M.C. EDWIN JAVIER CASTRO PERALVO

DIRECTOR: MSC. EDGAR ARAUZ

SANGOLQUÍ

2015

CERTIFICACIÓN DE TUTORÍA

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

DEPARTAMENTO DE SEGURIDAD Y DEFENSA

CERTIFICADO

MSC. EDGAR ARAUZ SÁNCHEZ

DIRECTOR

CERTIFICA:

Que el proyecto de investigación titulado "ESTUDIO PROSPECTIVO DE LA CIBERDEFENSA EN LAS FUERZAS ARMADAS DEL ECUADOR", realizado por el Crnl. Castro Peralvo Edwin Javier, ha sido guiado y revisado periódicamente, y cumple con las normas estatutarias establecidas por la Universidad de las Fuerzas Armadas ESPE.

El mencionado trabajo consta con un empastado y un disco compacto que contiene los archivos en formato portátil Acrobat (pdf).

Autorizamos al señor Castro Peralvo Edwin Javier que entregue el trabajo a la biblioteca de la institución.

Sangolquí, abril de 2015.

MSC. EDGAR ARAUZ SÁNCHEZ

DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

DEPARTAMENTO DE SEGURIDAD Y DEFENSA

DECLARACIÓN DE RESPONSABILIDAD

Castro Peralvo Edwin Javier

DECLARO QUE:

El proyecto de investigación denominado "ESTUDIO PROSPECTIVO DE LA CIBERDEFENSA EN LAS FUERZAS ARMADAS DEL ECUADOR", ha sido desarrollado respetando los derechos intelectuales de terceros, conforme las citas que se referencian, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría. Las ideas, comentarios, conclusiones, recomendaciones y criterios expuestos en el presente proyecto de grado, son de absoluta responsabilidad del autor.

Sangolquí, abril de 2015.

Castro Peralvo Edwin Javier

CRNL DE EMC.

AUTORIZACIÓN DE PUBLICACIÓN

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

DEPARTAMENTO DE SEGURIDAD Y DEFENSA

AUTORIZACIÓN

Yo, Castro Peralvo Edwin Javier

Autorizo a la Universidad de las Fuerzas Armadas ESPE la publicación, en la biblioteca virtual de la Institución el proyecto titulado “ESTUDIO PROSPECTIVO DE LA CIBERDEFENSA EN LAS FUERZAS ARMADAS DEL ECUADOR”, cuyo contenido y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, abril de 2015.

Castro Peralvo Edwin Javier

CRNL DE EMC.

DEDICATORIA

A Dios Ser Supremo fuente de inspiración para este trabajo, a mi querida esposa e hijos, a mis padres y hermanos.

AGRADECIMIENTO

Un sincero agradecimiento a la Universidad de las Fuerzas Armadas - ESPE, en especial al Departamento de Seguridad y Defensa, a sus oficiales en servicio activo y pasivo quienes han hecho posible ser parte de la I Promoción de la Especialización en Estudios Estratégicos de la Defensa; al Sr. Msc. Edgar Arauz, Director del proyecto de investigación que con sus valiosas orientaciones ha guiado el desarrollo de este proyecto en beneficio de nuestra institución.

ÍNDICE GENERAL

Contenido

INDICE DE TABLAS

INDICE DE GRÁFICAS

ÍNDICE DE ANEXOS

RESUMEN

Las guerras en la actualidad toman otra dimensión, ya no se trata de las clásicas operaciones que se desarrollan en el campo de batalla con las tradicionales armas de las Fuerzas Armadas y sus soldados enfrentándose por ocupar un territorio, actualmente se desarrolla otro tipo de guerra en otro escenario que es el ciberespacio. Existen ejemplos reales que se han desarrollado ciberguerras entre algunos países como el de Rusia y Estonia en el año 2007, Estonia fue atacada su infraestructura critica, se realizaron ciberataques en contra de instituciones públicas y privadas como bancos, periódicos en un país que el uso del internet es mayoritaria en las actividades diarias; Israel y EE.UU desarrollaron un virus llamado “Stuxnet” que dañó y retrasó el programa nuclear de Irán. Las revelaciones de Julián Assange con los cables WikiLeaks dejaron al descubierto los espionajes que realizó EE.UU a la mayoría de países y posteriormente Edward Snowden, agente de la NSA (Agencia Nacional de Seguridad de los EE.UU) hizo público documentos secretos a través de la prensa y confirmó que estamos propensos a ser espiados a través de las redes de internet, paginas sociales, teléfonos celulares, convencionales y otras herramientas que son uso diario de la mayoría de la población. El Ecuador no ha estado exento de este tipo de ataques, páginas del gobierno y correo electrónico del Presidente de la República han sido hackeadas, ante esta realidad el gobierno nacional asignó recursos económicos y dispuso la creación de un Comando de Ciberdefensa con la finalidad de proteger la infraestructura crítica de las Fuerzas Armadas y posteriormente del Estado. La presente investigación se basó en realizar entrevistas y encuestas a un grupo de expertos en el tema, para determinar cuáles son los factores fundamentales en el estudio prospectivo de la Ciberdefensa en las Fuerzas Armadas ecuatorianas para el año 2017, en la construcción de los escenarios y finalmente determinar las estrategias para alcanzar el escenario más óptimo de la Ciberdefensa en nuestro país.

PALABRAS CLAVE:

CIBERDEFENSA.

INFRAESTRUCTURA CRÍTICA.

CIBERGUERRA.

CIBERESPACIO.

PROSPECTIVA.

ABSTRACT

Wars today take another dimension, it no longer is the classic operations taking place in the battlefield with the traditional weapons of the Armed Forces and their soldiers facing occupy a territory, now another kind of war develops in another scenario that is cyberspace. There are real examples that have developed cyber-wars between countries like Russia and Estonia in 2007, Estonia was attacked their critical infrastructure cyber-attacks were made against public and private institutions such as banks, newspapers in a country that use of Internet is majority in daily activities; Israel and US developed a virus called "Stuxnet" which damaged and delayed Iran's nuclear program. The revelations of WikiLeaks Julian Assange with wires uncovered spy reports that US made most countries and later Edward Snowden, agent of the SNA (National Security Agency US), secret documents made public through the press and confirmed that we are likely to be spied through internet networks, social pages, cell phones, conventional and other tools that are daily use of most of the population. Ecuador has not been exempt from such attacks, government websites and email the President of the Republic have been hacked, to this reality, the national government allocated financial resources and ordered the creation of a Cyber Command in order to protect critical infrastructure of the Armed Forces and later the State. This research was based on interviews and surveys with a group of experts in the field, to identify the key factors in the prospective study of Cyber Ecuadorian Armed Forces in 2017, construction of scenarios and finally determine strategies to achieve the most optimal scenario of Cyber in our country.

KEY WORDS:

CYBERDEFENSE.

CYBERWAR.

CYBERESPACE.

CRITICAL INFRAESTRUCTURE.

PROSPECTIVE.

INTRODUCCIÓN

Una vez revelada la información secreta que mantenía en especial Estados Unidos sobre los países en el mundo a través de la Agencia Nacional de Seguridad, denunciada por Edward Snowden, se supo la real magnitud de los documentos clasificados como secretos y programas de vigilancia masiva que se infiltró en internet para obtener todo tipo de información convirtiendo al ciberespacio en una herramienta para hallar todos los recursos de información digital. La soberanía de los Estados ha sido violada sistemáticamente a través del medio tecnológico cuya infraestructura crítica puede ser atacada y podría causar el caos en cualquier país a través de ataques cibernéticos que podrían paralizar su sistema financiero, sistema eléctrico, sistema de comunicaciones, sistemas de armamento de las Fuerzas Armadas o sistemas de oleoductos, que pueden ser vulnerables sino se dispone de un equipo de Ciberdefensa que pueda enfrentar este tipo de amenazas. En nuestro país se ha visto la necesidad de crear un Comando de Ciberdefensa a cargo de las Fuerzas Armadas para proteger la infraestructura critica digital del Estado en razón que somos vulnerables en comparación con varios países de la región; varias páginas oficiales ya han sido hackeadas, incluso el Presidente en varias reuniones sabatinas ha mencionado que su cuenta ha sido hackeada en busca de información de su gestión de gobierno y de Fuerzas Armadas, el gobierno asignó cierta cantidad de dinero para su organización que estará conformada por personal militar y civil que ayudará a enfrentar una eventual ciberguerra y que permitirá salvaguardar la seguridad y la soberanía ante posibles ciberataques. El principal objetivo de esta investigación es determinar el escenario del Comando de Ciberdefensa en las FF. AA para el año 2017, para establecer la situación en la que se encontrará y tomar las medidas y estrategias necesarias para que cumpla su misión en óptimas condiciones, se utilizó el método prospectivo FAR apoyado en técnicas de investigación de encuestas y entrevistas, a través de instrumentos como entrevistas, cuestionarios y fichas de observación. El capítulo I plantea el problema del proyecto de investigación, el capítulo II contiene el marco referencial donde consta el estado de arte, el capítulo 3 describe el diseño metodológico, el capítulo IV abarca el procesamiento, análisis, interpretación y presentación de datos sobre la investigación

y finalmente el capítulo V se refiere a la construcción de los escenarios para finalizar con las conclusiones y recomendaciones.

CAPITULO 1

1. EL PROBLEMA

1.1. Planteamiento del problema

Luego de las revelaciones que hicieran Julián Assange y posteriormente Edward Snowden, se confirmó el espionaje por parte de EE.UU a países de todo el mundo incluido Latinoamérica. El gobierno del Ecuador a través del Ministerio de Defensa Nacional ha asignado inicialmente 8 millones de dólares para la creación de un Comando de Ciberdefensa. Ecuador es uno de los 10 países que están en el blanco de ataques cibernéticos **(www.eltelegrafo.com.ec, 2014)**.

La revolución tecnológica y digital en esta época favorece la rapidez de las comunicaciones y la interconexión con los sistemas de información sin embargo es evidente la vulnerabilidad del Estado y de la sociedad ante nuevas formas de ataques cibernéticos, en los últimos años se han presenciado en el mundo una variedad de intrusiones informáticas, revelaciones de información secreta como las de WikiLeaks, así como, ataques cibernéticos, con la actual tecnología se pierde la privacidad, la confidencialidad y resguardo de la información del Estado ante el aparecimiento de actores como los hackers virtuales, en contraposición con los esfuerzos del Estado en la conformación de plataformas tecnológicas para la consolidación de un gobierno eficaz y transparente, lo que implica desarrollar capacidades de control, vigilancia y respuesta para proteger los intereses nacionales de ataques virtuales. **(PNSI, 2014 - 2017).**

Las FF.AA, de acuerdo a la Constitución, tiene como misión fundamental la defensa de la soberanía y la integridad territorial, en la Agenda Política de la Defensa 2014-2017 se impone a las Fuerzas Armadas cuatro misiones: 1) Garantizar la defensa de la soberanía e integridad territorial, 2) Participar en la seguridad integral, 3) Apoyar al desarrollo nacional en el ejercicio de las soberanía y 4) Contribuir a la paz regional y mundial.

Como parte de la misión de Garantizar la defensa de la soberanía e integridad territorial, se encuentran las operaciones de protección del espacio cibernético, al crear la capacidad de la Ciberdefensa protegerá la defensa del Estado ante cualquier ataque cibernético que a través de hackers virtuales traten de vulnerar

el funcionamiento normal de las instituciones, el sistema de Mando y Control de las FF.AA y su infraestructura crítica.

El no disponer de un comando de Ciberdefensa sería un atentado contra la seguridad del Estado, de sus instituciones y por ende de las Fuerzas Armadas, la información, los sistemas de armas aéreos, navales y terrestres serian vulnerables a los ataques cibernéticos por lo que se debe determinar la situación del comando cibernético de FF. AA para el año 2017 con el cual se contrarrestaría las amenazas a fin de proteger la infraestructura crítica y los recursos estratégicos que permita al país ser productivo y funcionar adecuadamente.

Actualmente la situación de la Ciberdefensa en nuestro país es incipiente, se ha responsabilizado a las Fuerzas Armadas su creación asignándole una importante cantidad de recursos económicos para su organización y manejo deseándose conocer cuál sería el escenario del Comando de Ciberdefensa al año 2017.

1.2. Formulación del problema

¿Cuáles son las variables de cambio, hechos portadores de futuro y actores más trascendentales que configurarían los escenarios alternativos que en el ámbito de la Ciberdefensa enfrentarían las fuerzas Armadas ecuatorianas en el año 2017?

1.3. Justificación e importancia

El desarrollo de esta investigación es de importancia en vista que el Comando de Ciberdefensa de las FF.AA no cuenta con estudios prospectivos que le permita visualizar un panorama sobre su futuro, por lo que es necesario determinar el escenario de la Ciberdefensa en el año 2017 para enfrentar las amenazas y riesgos cibernéticos en contra de la infraestructura crítica de las FF.AA, colaborar en la protección de la infraestructura critica del Estado, determinar las debilidades y amenazas que afectarán el normal cumplimiento de la misión del Comando de la Ciberdefensa, determinar las variables o factores de cambio para la metodología de levantamiento de escenarios para la Ciberdefensa y proponer las estrategias que permitan desarrollar su capacidad de respuesta.

Se considera el estudio prospectivo para el año 2017 por dos razones fundamentales, el fin de periodo de gobierno y por lo tanto se abre dos

posibilidades, la reelección o el inicio de un nuevo gobierno lo que en cierta manera genera incertidumbre para el apoyo de la Ciberdefensa y por otro lado el avance tecnológico es impresionante como incrementa constantemente sus capacidades en muy poco tiempo.

1.4. Factibilidad

La presente investigación es factible desde el punto de vista que puedo acceder a la información sobre la nueva concepción del Comando de Ciberdefensa, que actualmente ocupa un lugar en el edificio del Comando Conjunto de las Fuerzas Armadas, además, es factible realizar entrevistas a los expertos. Asimismo, en función del tiempo es posible llegar a determinar un escenario prospectivo de mayor probabilidad de ocurrencia en determinado año. El financiamiento para el presente trabajo de investigación será cubierto por el investigador.

1.5. Objetivos de la investigación

1.5.1. Objetivo general

Determinar las variables de cambio, hechos portadores de futuro y actores más trascendentales que configurarían los escenarios alternativos que en el ámbito de la Ciberdefensa enfrentarían las Fuerzas Armadas ecuatorianas en el año 2017

1.5.2. Objetivos específicos

- Determinar el Estado del Arte del Comando de Ciberdefensa en las FF.AA ecuatorianas.
- Determinar las variables y los hechos portadores del futuro que influyen en el ámbito de la Ciberdefensa.
- Diseñar el escenario más probable de la Ciberdefensa en las Fuerzas Armadas ecuatorianas para el año 2017, empleando el método FAR.
- Establecer las amenazas y oportunidades a enfrentar para alcanzar el escenario optimista.

CAPITULO 2

2. MARCO DE REFERENCIA

2.1. Estado del Arte

La historia de internet se inicia en la década de los 60, en plena guerra fría entre Estados Unidos y la Unión Soviética, con la amenaza de una guerra nuclear, los Estados Unidos creó una red exclusivamente militar que en caso de un ataque ruso pudieran tener acceso a la información militar desde cualquier sitio del país. Esta red se creó en 1962 y se llamó ARPANET (Advanced Researchs Projects Agency), conformado por muchos científicos de alto nivel, inicialmente esta red contaba con cuatro ordenadores ubicadas en varias universidades del país, un par de años después ya contaban con 40 ordenadores conectados, tanto fue el incremento de esta red que este sistema de comunicación pasó a ser obsoleto, investigadores crearon el Protocolo de Control de Transmisión/ Protocolo de Internet TCP/IP que pasó a constituirse en un estándar de comunicaciones en las redes informáticas, posteriormente esta red se abrió al campo académico y de investigación mientras que los militares crearon una nueva red llamada MILNET desligándose de ARPANET.

La NSF (National Science Fundation) crea una red informática llamada NSFNET que luego absorbió a ARPANET posteriormente se crearon nuevas redes de libre acceso y que se unieron a NSFNET iniciando así lo que hoy conocemos como INTERNET. En 1985 ya se mencionó la palabra “ciberespacio” que con el pasar del tiempo pasó a ser un sinónimo de internet, desde entonces creció mucho más que cualquier medio de comunicación con varios servicios como el correo electrónico, transmisión de archivos, conversaciones en línea, acceso remoto a otras máquinas, transferencia de archivos y otros más que antes era inimaginable creer que se conviertan en una realidad que facilita la comunicación desde cualquier lugar del mundo. (http://www.cad.com.mx/historia del internet.htm, s.f.)

A inicios de la década de los 80 se dio una transición de ARPANET a World Wide Web (WWW) en que se desarrollaron ordenadores de manera exponencial. El crecimiento fue de tal manera que se creía que la red se bloquearía por la gran cantidad de usuarios y la información transmitida debido al uso del correo

electrónico. El World Wide Web es una red que puede ser buscado o mostrado a través de un protocolo llamado Hyper Text Transfer Protocol (HTTP) que a partir de la aplicación de esta tecnología y de los navegadores se dio acceso a un público mucho más amplio que además con la fabricación de nuevos ordenadores más baratos y potentes lo que permitió un rápido y masivo crecimiento de internet. (Barcelona, 2002)

Una consideración muy importante para el crecimiento de internet en el mundo entero es el acceso abierto y gratuito a las actividades comunes de las personas que primordialmente se trata de intercambio de información, sin embargo existe la comercialización de publicidad con millones de dólares de inversión, el internet en la actualidad se ha convertido en una herramienta que nos permite conectarnos con cualquier persona sin importar la distancia física a través del correo electrónico y otras aplicaciones como el Skype, Messenger, Twitter, Facebook, WhatsApp, que facilita las actividades diarias de nuestras vidas y puede ser enriquecedor si lo usamos correctamente. A nivel de instituciones públicas se ha dado mucho impulso a fin de poder realizar cualquier gestión pública a través de internet sin necesidad de asistir físicamente a las instalaciones de igual manera el sistema financiero ya no será necesario hacer largas filas en los bancos para realizar nuestras transacciones sino simplemente lo podremos realizar a través de una computadora.

En los últimos tiempos aparece un nuevo concepto político debido a los avances de la tecnología y las comunicaciones, las denominadas *guerras cibernéticas* como un nuevo enfoque de seguridad. Se han revelado hechos que marcan el nuevo contexto geopolítico internacional con la globalización de la vigilancia permanente, clandestina e indiscriminada, incluyendo el espionaje masificado como estrategia de defensa de los Estados. Debe ser compromiso del Estado trabajar en temas de Ciberseguridad y Ciberdefensa a fin de garantizar la seguridad de la información y la infraestructura tecnológica frente a estas nuevas amenazas (PNSI, 2014).

Existen claros ejemplos que se han registrado a nivel mundial con los cuales podemos tener una idea de la seriedad de las guerras cibernéticas, podemos mencionar lo que sucedió en Estonia en el año 2007 que sufrió ataques

cibernéticos en represalia por el traslado en Tallin del monumento a los soldados soviéticos caídos durante la II Guerra Mundial, estos ataques e iniciaron a fines de abril poco después que el gobierno estonio trasladara desde el centro de la capital a un cementerio apartado el conocido como Soldado de Bronce, monumento erigido a los militares soviéticos caídos combatiendo el nazismo, que para muchos estonios representaba el monumento a quien durante medio siglo ocupó su país, se realizaron ataques electrónicos contra instituciones públicas y privadas como bancos, periódicos en un país que el uso del internet en las actividades diarias es mayoritaria, la página web del gobierno estonio normalmente recibía entre 1000 y 1500 visitas al día, cuando se iniciaron los ataques en la primera semana de mayo llegaron a recibir entre 1000 y 1500 por segundo, eso hace caer cualquier sistema, hubo versiones que los ataques cibernéticos provenían de Rusia, existieron claros indicios que fue así, sin embargo no es posible probar estos ataques electrónicos en vista que cualquier experto en la materia puede apropiarse de cualquier computador para lanzar desde él sus ataques, este hecho fue algo espectacular y se creó conciencia que existe realmente una amenaza de este tipo, con estos hechos se alarmaron a la OTAN y a la Unión Europea. (Martinez, 2007)

Según la publicación realizada por el periódico “The New York Times” manifiesta que Israel y los EE.UU desarrollaron el virus que dañó y retrasó el programa nuclear iraní, la central nuclear de Dimona ubicado al sur de Israel se convirtió en el laboratorio para examinar y ensayar el virus llamado “Stuxnet” que fue desarrollado para sabotear las centrifugadoras nucleares en Irán. En la central nuclear Dimona Israel logró desarrollar el mismo tipo de centrifugadoras que la central iraní de Natanz donde se produce el enriquecimiento de uranio. La razón por la que el gusano tuvo éxito es porque se probaron en el mismo tipo de máquinas que disponía la central nuclear iraní, razón por la cual ha sido muy efectivo el virus informático, según expertos, este virus informático paralizó la quinta parte de las centrifugadoras de enriquecimiento de uranio de la central nuclear iraní, según Israel existen entre 4.000 y 5.000 centrifugadoras en la planta de Natanz, el régimen de Teherán insisten en que continuarán sin pausa su programa nuclear confirmando que tiene fines pacíficos y no militares como

creen muchos países. Israel ha manifestado varias veces que su principal reto y amenaza existencial es un Irán nuclear por lo que no descartan una opción militar, sin embargo Israel cree que todavía no es el momento y por ahora está recurriendo a las opciones políticas, económicas y tecnológicas para retrasar el programa nuclear iraní. Hasta ahora el desarrollo del virus informático "Stunxnet" podría considerarse como el arma más sofisticada en la historia y que fue el principal origen para que se retrase el plan atómico de Irán. (The New York Times, citado por El Mundo, 2011)

A nivel nacional ya se han registrado actividades de hackeo a páginas oficiales en el año 2010, la Secretaria Nacional de Inteligencia instaló herramientas en los equipos de altos funcionarios del gobierno, se ha monitoreado y revisado logs de los equipos de seguridad perimetral, se han detectado y analizado las vulnerabilidades de los servidores de la presidencia y además la aplicación de encriptación de datos, para complementar estas actividades en el campo legislativo para el combate de los ciberdelitos, la Asamblea Nacional aprobó el Código Orgánico Integral Penal y junto a la Ley de Comercio electrónico incluyen sanciones a los ataques a la integridad de datos y sistemas, a la falsificación y al fraude informático (PNSI, 2014).

La soberanía está siendo violada sistemáticamente, sin que el público e incluso los organismos de seguridad y defensa, tengan clara conciencia o respuesta a esa situación. La amenaza a la seguridad interna y externa a través del medio tecnológico, no está aun cabalmente asimilada en toda su magnitud por los ciudadanos y por los responsables de establecer las respectivas políticas, regulaciones y estrategias para cuidar la privacidad de las personas y la información, servicios e infraestructura sensible del Estado.

El problema es muy complejo, ahora es posible que un país sea vulnerado por un enemigo o por la ciberdelincuencia en sus redes e infraestructuras informáticas desde cualquier país del mundo, uno de los factores que facilita la ciberguerra es que todos los dispositivos que se conectan a internet son fabricados por múltiples empresas y realmente no conocemos lo que contienen, de igual manera sucede con los programas informáticos que en su elaboración de los software participan varias personas y compañías.

> En la última cumbre de jefes de Estado de Unasur se dio el mandato al Consejo de Defensa suramericano de trabajar en una propuesta compartida a nivel regional de Ciberdefensa. La idea es crear una especie de anillo de seguridad que proteja las comunicaciones entre los jefes de Estado y que permita salvaguardar la seguridad y soberanía ante posibles ciberataques y ciberespionajes. (Telegrafo, 2014)

En la actualidad no existe una entidad o institución que se encargue de contrarrestar ataques cibernéticos o ciberdelitos que afecta la seguridad de la información o las actividades diarias de las instituciones del Estado, ante esta realidad es evidente la necesidad de proteger la información y la infraestructura digital del Estado y de las Fuerzas Armadas, como bien consta en el Plan Nacional de Seguridad Integral y en la Agenda Política de la Defensa, la preocupación del gobierno en este tema que incluyen nuevas misiones en las que se menciona las operaciones de protección del espacio cibernético por lo cual es necesario crear una nueva capacidad de defensa, cuya responsabilidad es de las Fuerzas Armadas, que como es de conocimiento público, el gobierno nacional dispuso la creación del Comando de Ciberdefensa con los recursos económicos asignados para tal efecto.

La creación del Comando de Ciberdefensa en nuestro país ayudará a enfrentar el ciberespionaje y una eventual ciberguerra, este Comando estará a cargo de personal civil y militar con un perfil adecuado.

2.2. Marco Teórico

Existen varias disciplinas que analizan y estudian el futuro: el forecasting y la prospectiva (foresight). Hay una estrecha interrelación entre información e incertidumbre a mayor información menor incertidumbre y viceversa, el forecasting es de origen norteamericano que surgió en la década de los años cincuenta y su traducción al español sería “pronóstico”, históricamente el forecasting es anterior a la prospectiva con el nacimiento del método Delphi en 1848, analizar el futuro por medio del forecasting se asume que se dispone de información y por lo tanto se reduce la incertidumbre, mientras que con la prospectiva ingresa en el futuro mediante conjeturas y construir la mejor opción. (Mojica, 2008) Un método prospectivo consiste en ubicarse mentalmente en el

futuro por medio de un acto de anticipación, la prospectiva no consiste en adivinar sino en preparar un futuro deseable.

En el forecasting existe un solo futuro que puede ser levantado mediante paneles de expertos y extrapolación de tendencias, es decir, utiliza la historia para identificar la tendencia, su realidad es lineal, este método reúne argumentos de personas conocedoras del tema para aseverar la ocurrencia de eventos en el futuro, pertenece a la escuela determinista, es decir, aceptar que el futuro es único y no puede ser cambiado por el hombre lo que implica resignación y la preparación del hombre para ese futuro basado en el cálculo matemático del comportamiento de un patrón histórico. (Ibidem) En nuestro caso de la Ciberdefensa en las Fuerzas Armadas ecuatorianas prácticamente no existe historia en vista que recientemente se encuentran creando esta nueva capacidad por lo que mal se podría proyectar el futuro de algo que no dispone de un patrón histórico.

El método FAR es un método prospectivo que se encuentra clasificado entre los estructurados que sirve para la elaboración y el diseño de escenarios múltiples, su autor lo denominó Field Anomaly Relaxation, debido a que estructura sus opiniones expertas en diferentes campos de interés, este método parte de la premisa que el mundo no puede ser descrito por un solo aspecto y por lo tanto es indispensable pensarlo en diferentes campos o dimensiones como el Político, Económico, Social y Tecnológico, pudiendo agregar otros campos de acuerdo al problema específico como las influencias externas que puedan afectar la visualización de los diferentes escenarios posibles futuros.

Este método funde dos conceptos el de la “relajación” de la ingeniería matemática que va conduciendo a un entendimiento cada vez más refinado en función de un patrón de circunstancias. Al eliminarse combinaciones ilógicas (anomalías) van quedando solo aquellas factibles hasta completar un conjunto coherente, el otro concepto se refiere a la Teoría de Campo Social (Social Field Theory) que se refiere al campo del cual se va a investigar el futuro. Se necesita un contexto futuro coherente, donde los eventos tomen sentido, de las infinitas variables de la realidad quedan al final siete variables con posibles valores para cada una, la combinatoria y el análisis tiene niveles de complejidad. Se

denominan Factores los estados alternativos que cada sector puede tener, los Sectores y Factores se ubican de manera matricial donde cada sector encabeza una columna que se completa hacia abajo sus respectivos factores. (Gallardo, 2009)

Para el presente trabajo de investigación se utilizará el método FAR porque permite determinar los escenarios optimista, probable y pesimista en base del análisis del tema desde diferentes campos, esta escuela de carácter estructuralista o sistémica que a diferencia de la escuela determinista no observa al futuro como único sino que es producto de la suma de las acciones individuales de los hombres. Además, este método es sencillo, práctico y objetivo, ya que permite al decisor en cada uno de los niveles, disponer de una matriz gráfica que facilita la visualización del escenario probable, además permite determinar estrategias para alcanzar los objetivos proyectados.

2.3. Marco Conceptual.

Ciberespacio.-

Ciberespacio tiene su origen en la palabra griega "cibernao"(pilotear una nave), se empleó por primera vez en la novela de ciencia ficción "Neuromante" escrita por William Gibson en 1984, el ciberespacio, como inteligencia colectiva. Es un espacio virtual que "contiene" todos los recursos de información y comunicación disponibles en la red, donde los sujetos interactúan entre sí, a través de las nuevas tecnologías. Las barreras físicas desaparecen, tiempo y espacio toman una nueva dimensión, y un individuo puede comunicarse con otros individuos en diferentes lugares del planeta al mismo tiempo. (Miranda, 2011)

Para el presente trabajo de investigación a fin de estar acorde con el tema y con la misión que la Agenda de la Defensa impone a las Fuerzas Armadas en la creación de una nueva capacidad de la Ciberdefensa, tomaremos las definiciones que constan en el Plan Nacional de Seguridad Integral 2014 – 2017.

Ciberespacio: Dominio virtual, global y dinámico donde se hallan los recursos de información digital, a los que se puede acceder a través de las tecnologías de la información y comunicación. (PNSI, 2014)

Ciberdefensa.-

El prefijo “ciber” está tomada de la palabra *cibernética* que a su vez tiene una raíz etimológica griega, procede de *kybernetike*, cuyo significado es el de arte de la navegación. Por su parte la palabra “defensa” proviene del latín defensa que significa acción o efecto de proteger algo contra una ofensiva o daño, para la investigación utilizaremos la siguiente definición:

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (PNSI, 2014)

Ciberseguridad.-

La palabra seguridad proviene del latín *securitas* que a su vez se deriva de *securus* (sin cuidado, sin precaución, sin temor a preocuparse), que significa libre de cualquier peligro o daño, y desde el punto de vista psicosocial se puede considerar como un estado mental que produce en los individuos (personas y animales) un particular sentimiento de que se está fuera o alejado de todo peligro ante cualquier circunstancia. La seguridad es la garantía que tienen las personas de estar libre de todo daño, amenaza, peligro o riesgo; es la necesidad de sentirse protegidas, contra todo aquello que pueda perturbar o atentar contra su integridad física, moral, social y hasta económica. (Orozco, 2011)

Para la presente investigación la definición de Ciberseguridad será la siguiente: Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional. (PNSI, 2014)

Hacker.-

Etimológicamente, la palabra hacker deriva del vocablo inglés "hack" (cortar, golpear), el cual comenzó a adquirir su primera connotación tecnológica a principios del siglo XX, cuando pasó a formar parte de la jerga de los técnicos telefónicos de los EE.UU, quienes a veces lograban arreglar de inmediato las cajas defectuosas mediante un golpe seco, un hack. A mediados de los años 60, el término comenzó a formar parte de la cultura informática al ser utilizado para definir un perfil de conocimientos y capacidad con las computadoras que tenían determinadas personas. Gente que a diferencia de los demás podía resolver las

tareas de programación de forma más rápida, como si sólo le hubieran dado un golpe (un hack) a la computadora.

Para la presente investigación la definición de hacker será la siguiente: Es alguien que descubre las debilidades de una computadora o de una red informática. (Wikipedia)

Infraestructura crítica Estratégica.-

Aquella donde se dispone de información estratégica digital, requerida para mantener la gobernabilidad de la nación o la efectiva operación de una organización. (PNSI, 2014)

Prospectiva.-

La palabra prospectiva proviene del latín *prospectivus* (relativo a mirar hacia delante, al futuro). Para la presente investigación la definición de la palabra prospectiva será la siguiente: Conjunto de análisis y estudios realizados con el fin de explorar o de predecir el futuro, en una determinada materia. (RAE)

2.4. Marco Legal.

Constitución Política del Ecuador.

Art. 158.- Las Fuerzas Armadas y la Policía Nacional son instituciones de protección de los derechos, libertades y garantías de los ciudadanos.
Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial.

La Constitución de la República no constituye un obstáculo para la presente investigación sino al contrario va a contribuir a la misión fundamental que es la defensa de la soberanía, al estudiar sobre la implementación de una nueva capacidad estratégica con la creación del Comando de Ciberdefensa a fin de proteger la infraestructura crítica de las Fuerzas Armadas.

Esta investigación de igual forma no vulnera la protección a los derechos de los ciudadanos en los artículos relacionados que constan en la Constitución sobre el acceso universal a las tecnologías de información y comunicación ni tampoco el derecho a la protección de datos de carácter personal que son los derechos relacionados al tema de la investigación.

Código Orgánico Integral Penal (COIP)

El Código Orgánico Integral Penal (COIP) entró en vigencia a partir del mes de agosto de 2014 en la cual ya se incluyen algunos artículos relacionados con los delitos contra la seguridad de los activos de los sistemas de información y comunicación, a partir del artículo 229 se especifica delitos que son sancionados con prisión.

Artículo 229.- Revelación ilegal de base de datos.

Artículo 230.- Interceptación ilegal de datos.

Artículo 231.- Transferencia electrónica de activo patrimonial.

Artículo 232.- Ataque a la integridad de sistemas informáticos.

Artículo 233.- Delitos contra la información pública reservada legalmente.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

El Código Orgánico Integral Penal contribuye en el tema de la investigación al haber tipificado en sus artículos varios delitos relacionados a los sistemas de información y comunicación que el antiguo Código Penal no lo contemplaba, si bien es cierto, no es suficiente para la realidad que vivimos actualmente con el impulso acelerado de la tecnología a nivel mundial mientras que la legislación informática avanza a pasos muy lentos, pero al menos ya existe legislación que podría servir para contrarrestar los ataques por parte de hackers que quieran ingresar a la información digital de Fuerzas Armadas.

Ley orgánica de transparencia y acceso a la información pública (LOTAIP) su Reglamento y sus reformas.

Su objeto es garantizar el derecho a acceder a las fuentes de información, como mecanismo para ejercer la participación democrática y está sujeto a todos los funcionarios y entidades del Estado, establece que no existirá reserva respecto de informaciones que reposen en archivos públicos, excepto de aquellas que por seguridad nacional no deben ser dadas a conocer.

En las Fuerzas Armadas existen directivas disponiendo el control y seguridad de la información en especial la documentación militar calificada.

Para la presente investigación no influirá ninguna ley en particular en vista que la información a la cual se ingrese y obtenga será legal y aquellas que se

tenga reserva por la naturaleza del tema se pedirá la autorización respectiva para tener acceso a la misma, en conclusión no se tendrá limitaciones legales que puedan interferir en la investigación de la Ciberdefensa y tampoco existe un marco legal en donde se determine hasta donde tiene la competencia esta nueva capacidad de la Ciberdefensa.

2.5. Preguntas de investigación

- ¿Cuál es el Estado del Arte del Comando de Ciberdefensa en el Ecuador?
- ¿Cuáles son las variables y los hechos portadores del futuro que determinan escenarios alternativos en el ámbito de la Ciberdefensa en Ecuador?
- ¿Cuál es el escenario más probable de la Ciberdefensa en las Fuerzas Armadas ecuatorianas para el año 2017?
- ¿Cuáles son las amenazas y oportunidades a enfrentar para alcanzar el escenario optimista?

CAPITULO 3

3. DISEÑO METODOLÓGICO

3.1. Alcance de la Investigación

La presente investigación es de tipo correlacional porque se utilizó la metodología del método prospectivo FAR para el levantamiento de escenarios en la cual interrelaciona dos o más variables que generan cambios en el campo de la Ciberdefensa, además de las variables disponen de actores y hechos portadores del futuro que podrían cambiar un escenario, se describieron relaciones entre dos o más variables en un momento determinado, en este diseño se evaluó-analizó la asociación entre variables.

Es además transeccional porque los datos fueron recopilados una sola vez y en un tiempo único, las variables que constituyeron parte del escenario, fueron determinadas por una sola vez y sometidas al proceso de estructuración de los escenarios complementada con la investigación bibliográfica y documental relacionada al tema de investigación.

3.2. Tipo de estudio

Por los objetivos.

Es una investigación aplicada porque se diseñó entrevistas y encuestas que fueron aplicadas a juicio de expertos orientados a los objetivos de la investigación.

Por el lugar.

Es una investigación de campo, porque se realizó las entrevistas a diferentes personajes que laboran o han laborado en el tema de la Ciberdefensa en diferentes instituciones públicas y privadas quienes aportaron con su experiencia y conocimiento que sirvieron para el establecimiento de las variables y así se pudo iniciar con el método prospectivo en el levantamiento del escenario.

Por su naturaleza.

Esta investigación se realizó a través del método prospectivo FAR, un método práctico, sencillo y objetivo que permitió disponer de una matriz gráfica muy práctica para la toma de decisiones.

3.3. Población y muestra

La población y la muestra no fueron aplicables estrictamente en este caso porque se aplicó el método prospectivo FAR.

En los primeros pasos para determinar las variables, hechos portadores del futuro y actores, se realizó una exploración bibliográfica, no se utilizó muestreo probabilístico sino el muestreo no probabilístico, en esta investigación fue necesario la opinión de expertos en el tema de la Ciberdefensa que se realizó a través de talleres, juicios de expertos o talleres tipo Delphi, es decir, es más probable que la opinión de los expertos, especialmente cuando ellos están de acuerdo, sea más correcta que la de quienes no son expertos, sobre todo en su especialidad.

De aquí en adelante no se aplicó rigurosamente el método científico de investigación sino que a partir de este punto nos referimos al método FAR que consideró los siguientes pasos:

Paso No 1

Identificación de las fuerzas principales (definición de las principales variables que modelan la realidad-sectores).

Se definieron no más de siete sectores

Paso No 2

Establecimiento de los estados alternativos de cada sector (factores).

Se realizó una breve definición de cada concepto.

Paso No 3

Construcción de la matriz Sectores/Factores.

Se definió con un lenguaje simbólico, se representó cada sector con una letra que mejor lo caracterizó.

Paso No 4

Calibración de la matriz.

En este paso se puso a prueba la matriz, al menos se puso representar el tiempo presente tiempo cero (T0).

Paso No 5

Construcción de escenarios.

Se realizaron las combinaciones y a través del proceso de relajación se eliminaron las combinaciones que no cuadraron, los escenarios no debieron ser extremos sino explicables secuencialmente, tuvieron lógica y consistencia, se obtuvieron así una especie de visión de futuro más no una descripción de eventos privilegiando el sentido de contexto sobre la exactitud.

Paso No 6

Narración del escenario más probable.

El escenario debe ser relatado, expuesto en prosa y en lenguaje coloquial logrando el sentido de contexto, es decir, una visión holística deseada, señalando las secuencias que define la trayectoria desde el presente hacia el futuro.

Paso No 7

Identificación de oportunidades y amenazas.

Se debió aprovechar los beneficios del método FAR en la vinculación de la prospectiva con la planificación estratégica, la identificación de las oportunidades y amenazas se determinaron observando las coincidencias que existieron de los factores entre el escenario más probable, el optimista y el pesimista.

Cuando un factor es coincidente entre el escenario más probable y el escenario pesimista, lo más probable es que ocurra lo peor.

Cuando un factor es coincidente entre el escenario más probable y el escenario optimista, lo más probable es que ocurra lo mejor.

Paso No 8

Conclusiones y recomendaciones.

El método prospectivo debe concluir y recomendar con el fin de ilustrar el proceso decisional. (Gallardo, Prospectiva Estratégica Aplicada, 2009)

3.4. Técnicas de recolección de datos

La etapa de recolección de datos implica tres actividades estrechamente relacionadas entre sí:

1) Seleccionar uno o varios instrumentos o métodos de recolección de datos, los cuales deben ser válidos y confiables, de lo contrario no se puede basar en sus resultados.

2) Aplicar esos instrumentos o métodos para recolectar datos y
3) preparar las observaciones, registros y mediciones obtenidas para que se analicen correctamente. (Hernandez, 2002)

En la presente investigación en cuanto a la recolección de datos, los instrumentos utilizados fueron básicamente la entrevista y encuesta orientadas a juicio de expertos los que se aplicaron únicamente en el primer paso del método prospectivo FAR: Identificación de fuerzas principales o definición de variables (sectores).

Las técnicas de recolección de datos se clasifican también en primarias y secundarias, las primeras, son aquellas que toman información de primera mano, de fuente directa, del origen, en el mismo sitio de los acontecimientos en este caso se tomará información del Comando de Ciberdefensa recientemente creado en el Comando Conjunto de las Fuerzas Armadas ecuatorianas, mientras que las secundarias toman información de fuentes indirectas, es decir de segunda mano, permiten realizar investigación bibliográfica o documental, como efectivamente se ha realizado para tener un conocimiento acertado del tema de investigación.

La entrevista se define como una conversación entre una persona (el entrevistador) y otra (el entrevistado) u otras, es más flexible y abierta, las entrevistas se clasifican en estructuradas, semiestructuradas o no estructuradas o abiertas, las primeras, el entrevistador realiza su trabajo en base a una guía de preguntas específicas, las entrevistas semiestructuradas se basan en una guía de asunto o preguntas en donde el entrevistador tiene libertad de incluir preguntas adicionales para obtener mayor información sobre los temas deseados, las entrevistas abiertas se basan en una guía general con temas o específicos en donde el entrevistador tiene toda la libertad para manejarla. (Ibídem)

La encuesta es una técnica que se sirve de un cuestionario debidamente estructurado, mediante el cual se recopilan datos provenientes de la población frente a una problemática determinada, se clasifica en: 1) por los asuntos que aborda y 2) por el número de personas encuestadas. Por los asuntos que aborda se divide: en descriptiva, explicativa y mixta. Por el número de personas encuestadas se divide en: censo o encuesta general y por muestreo.

En la presente investigación se utilizó la entrevista semiestructurada y la encuesta por muestreo dirigido a juicio de expertos, es decir, los entrevistados y encuestados fueron expertos en el tema de la investigación para identificar las principales variables que se aplicó únicamente en el primer paso del método prospectivo FAR.

CAPITULO 4

4. PROCESAMIENTO, ANALISIS, INTERPRETACION Y PRESENTACION DE DATOS.

El grupo de expertos en el tema que fue entrevistado pertenecen a diferentes instituciones del país que se encuentran ligados al manejo de software, hardware, redes, internet, herramientas, tanto en el campo laboral como en el campo académico, es importante conocer como estuvo conformado este equipo de expertos que dieron sus comentarios a través de las entrevistas y encuestas sobre la creación de la Ciberdefensa en las Fuerzas Armadas.

Tabla 1

Funciones del grupo de expertos e instituciones a las que pertenecen.

ORD	GRADO/TITULO	INSTITUCIÓN
01	Crnl del Ejército	Director de Sistemas y Comunicaciones del Ejército.
02	Crnl del Ejército	Subdirector de Sistemas y Comunicaciones del Ejército.
03	Capt del Ejército	Sistemas y Comunicaciones del Ejército.
04	Ing. Sistemas	SP de Sistemas y Comunicaciones del Ejército.
05	Crnl del Ejército	Comandante del Comando de Ciberdefensa
06	Tcrn de la FAE	Jefe de Estado Mayor del Comando de Ciberdefensa.
07	Mayo del Ejército	Grupo de Ciberdefensa
08	Capt del Ejército	Grupo de Ciberdefensa
09	Tnte del Ejército	Grupo de Ciberdefensa
10	Crnl(SP) Ejército	Director del Dpto. de Ciencias de la computación ESPE.
11	Ing. Sistemas	PHD Ciencias de Computación. ESPE
12	Ing. Sistemas	Planificador Académico de Ciencias de Computación. ESPE
13	Msc. Informática	Docente de la Facultad de Ciencias de Computación. ESPE

CONTINÚA ➡

14	Ing. Sistemas	Docente de la Facultad de Ciencias de Computación. ESPE
15	Tcrn del Ejército	Ing. Sistemas. Comando de Inteligencia Militar Conjunta.
16	Ingeniero	Telecomunicaciones. CERT SUPERTEL.
17	Ingeniero	Telecomunicaciones. SUPERTEL. Analista de seguridad
18	Ingeniero	Telecomunicaciones. CERT SUPERTEL.
19	Ingeniero	Telecomunicaciones. CERT SUPERTEL.
20	Ing. Sistemas	CERT UTPL.

4.1. Resultados

De acuerdo a las entrevistas se ha realizado la tabulación correspondiente obteniendo los siguientes resultados.

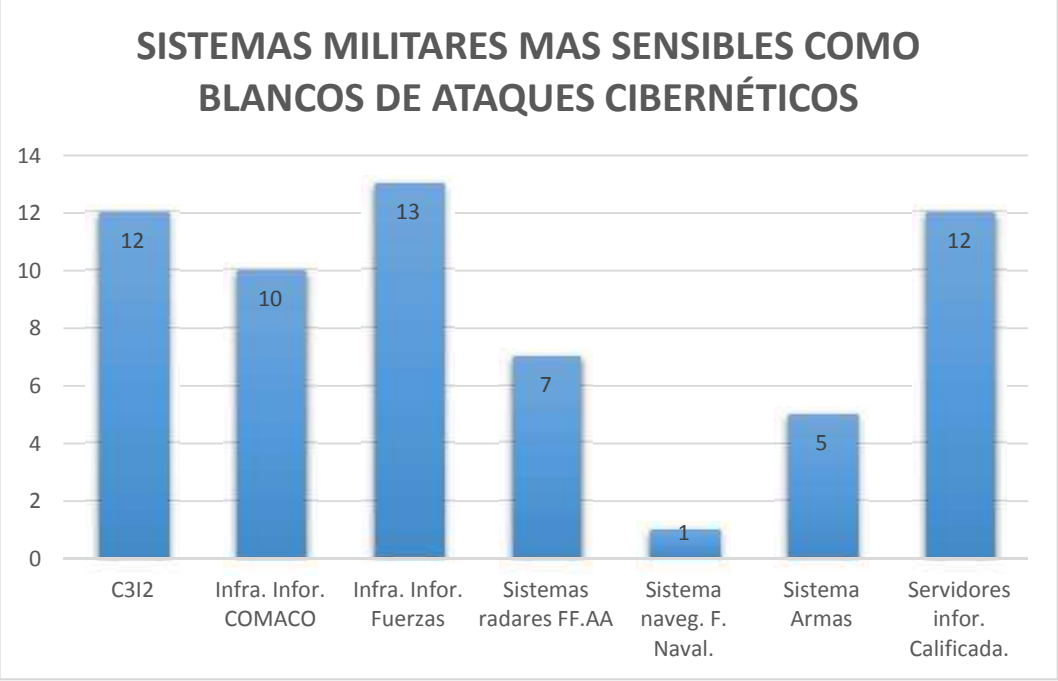


Figura 1 Sistemas Militares sensibles de ataques cibernéticos.

Los sistemas militares más sensibles que pueden ser blancos de ataques cibernéticos de acuerdo a las entrevistas son: la infraestructura informática de las Fuerzas, es decir, de la Fuerza Terrestre, Naval y Aérea con 13 nominaciones,

luego están el C3I2 y los servidores con 12 nominaciones, la infraestructura del Comando Conjunto con 10 nominaciones y en menor importancia de acuerdo a los expertos se encuentran los sistemas de radares de las Fuerzas Armadas, los sistemas de armas y el sistema de navegación de la Fuerza Naval con 7, 5 y 1 nominación respectivamente.

Se puede apreciar que como objetivo de un ataque cibernético está la información clasificada de las Fuerzas, lógicamente en el mando y control del Comando Conjunto de las Fuerzas Armadas y lo servidores que almacenan información clasificada, la diferencia entre estos tres sistemas es mínima, es decir, son los tres más importantes.

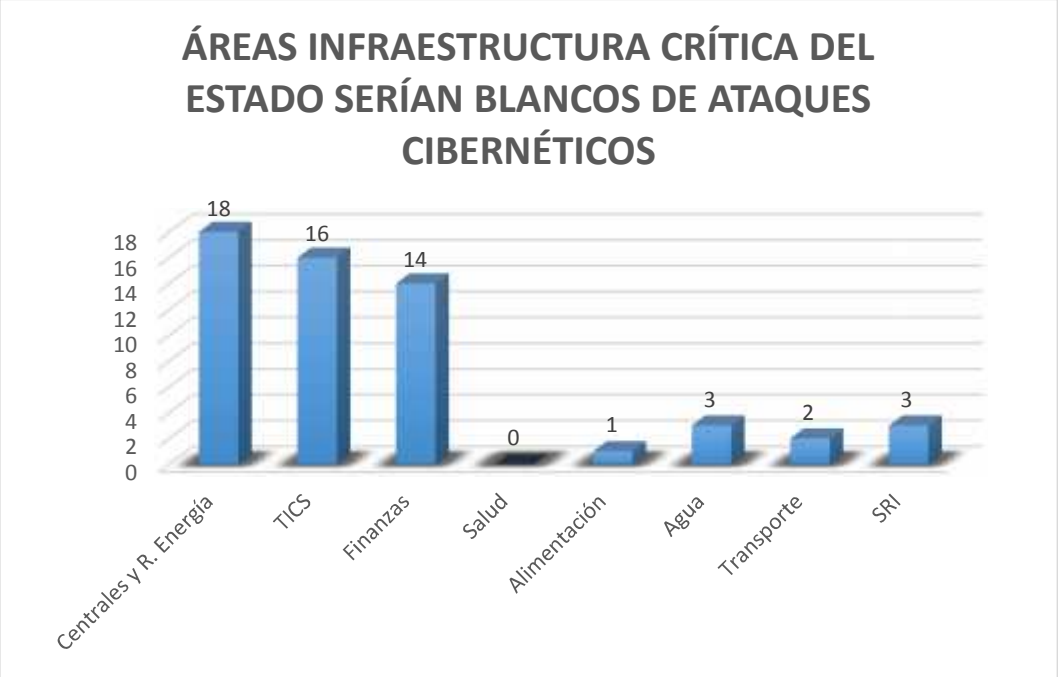


Figura 2. Áreas Infraestructura Critica del Estado posibles blancos

Las áreas de infraestructura crítica del Estado que serían blancos de un ciberataque de acuerdo a expertos en el tema son los siguientes: las Centrales y redes de energía en donde se encuentran inmersos la electricidad, petróleo, gas, instalaciones de almacenamiento y refinerías con sus sistemas de transmisión y distribución con 18 nominaciones, a continuación se encuentra las Tecnologías de Información y Comunicación con 16 nominaciones, luego el Sistema de Finanzas con 14 nominaciones, el Sistema del SRI apenas tiene 3 nominaciones

igual que el Sistema de Agua, luego el Sistema de transporte y por ultimo sin ninguna nominación el Sistema de Salud.

Se puede apreciar que de acuerdo al criterio del grupo de expertos los sistemas más importantes del Estado que podrían ser posibles blancos de un ataque cibernético por su importancia son tres sistemas, las Centrales y Redes de Energía, las Tecnologías de Información y Comunicación y el Sistema de Finanzas.

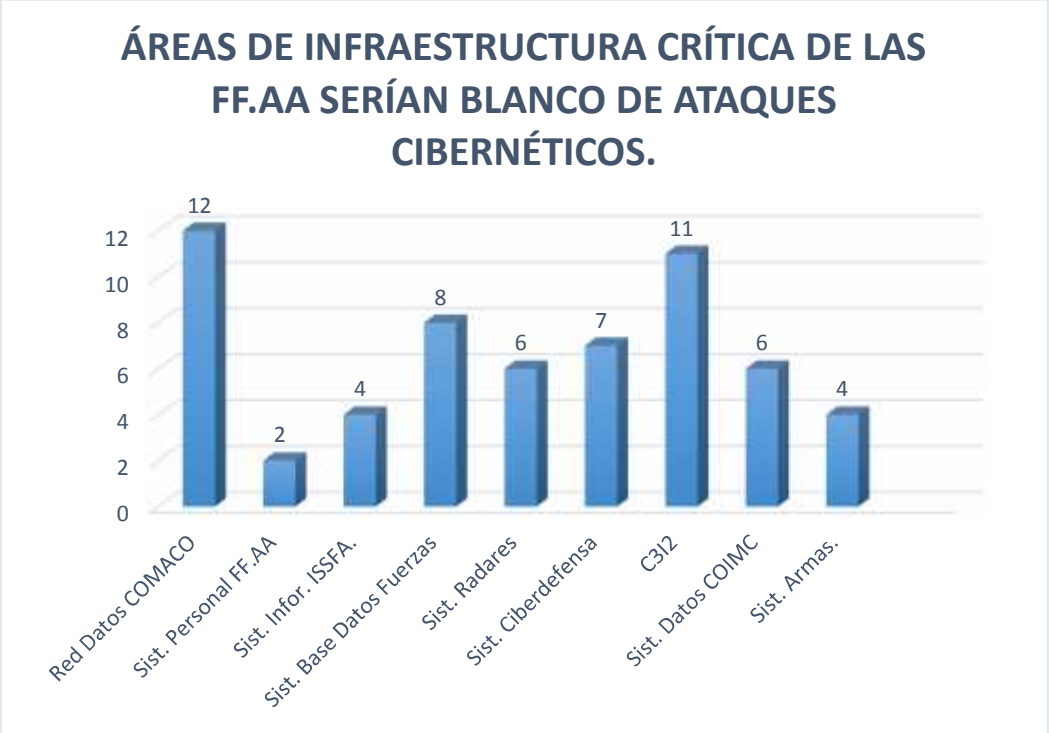


Figura 3. Áreas Infraestructura Critica de FF.AA posibles blancos

Las áreas de infraestructura crítica de las Fuerzas Armadas que serían blanco de un ciberataque son los siguientes: la Red de Datos del Comando Conjunto con 12 nominaciones, C3I2 con 11 nominaciones, el Sistema de base de datos de las Fuerzas Terrestre, Aérea y Naval con 8 nominaciones, luego el Sistema de Ciberdefensa con 7 nominaciones, el Sistema de radares y el Sistema del Comando de Inteligencia Militar Conjunto tienen 6 nominaciones, el Sistema informático del ISSFA y el Sistema de armas tienen 4 nominaciones y por último el Sistema de personal de las Fuerzas Armadas.

Los tres principales sistemas de la infraestructura crítica de las Fuerzas Armadas que según los expertos que serían blanco de un ciberataque son: la Red

de Datos del Comando Conjunto, C3I2 y los Sistemas de datos de las Fuerzas, aunque hay una variedad de criterios en relación a esta pregunta.

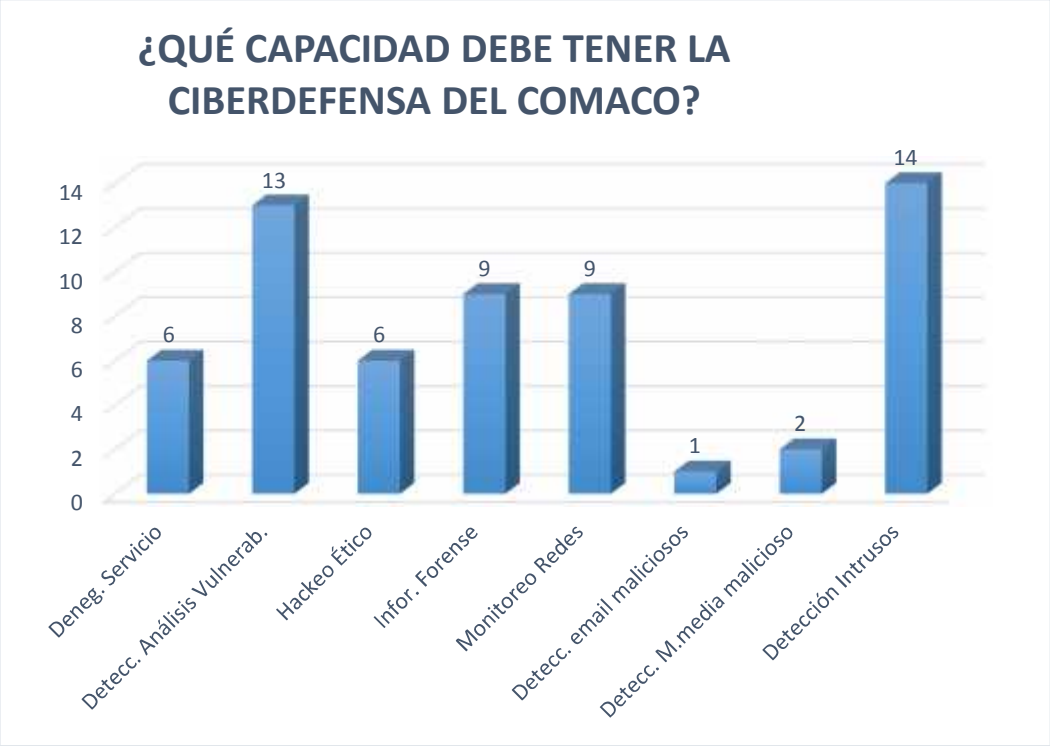


Figura 4. Capacidad Ciberdefensa del COMACO

Las capacidades que deben tener la Ciberdefensa en Ecuador de acuerdo a los expertos son las siguientes: detección de intrusos con 14 nominaciones, detección y análisis de vulnerabilidades con 13 nominaciones, luego informática forense y monitoreo de redes ambos con 9 nominaciones, luego la denegación de servicio y el Hackeo ético con 6 nominaciones, la detección multimedia malicioso con 2 nominaciones y por último la detección de email maliciosos con 1 nominación.

Las principales capacidades que debe tener la Ciberdefensa en Ecuador son la detección de intrusos y la detección - análisis de vulnerabilidades.

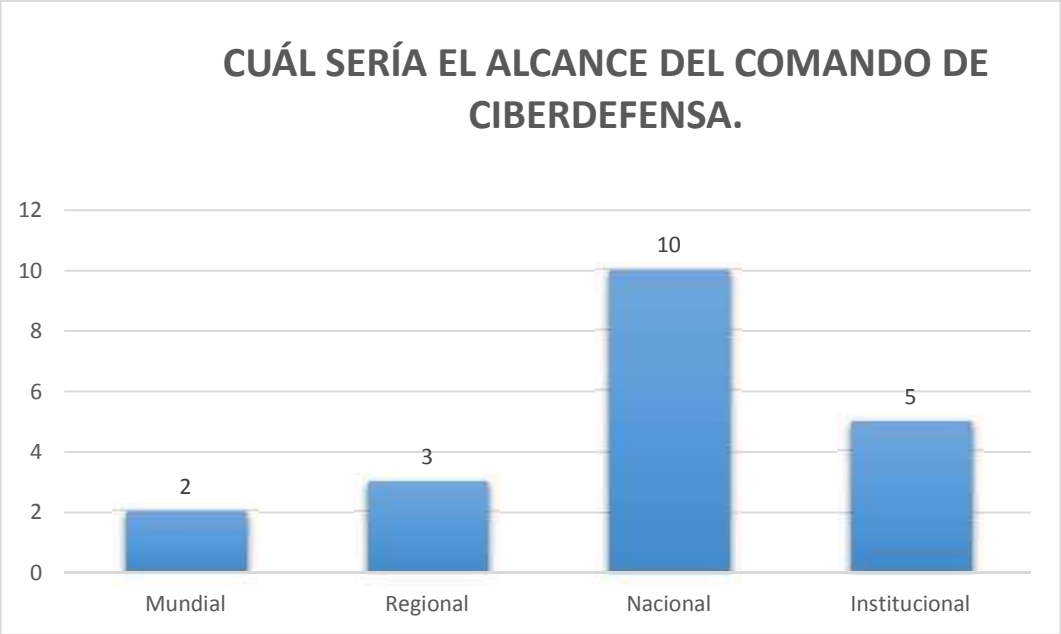


Figura 5. Alcance del Comando de Ciberdefensa

El alcance del Comando de Ciberdefensa 10 personas que son la mayoría dicen que debería ser a nivel nacional, 5 personas dice que debería ser a nivel institucional, 3 personas dicen que debería ser a nivel regional y 2 personas dicen que el alcance debería ser a nivel mundial.

La mayoría de personas explicaron que debería ser a nivel nacional considerando que el Comando de Ciberdefensa al pertenecer a las Fuerzas Armadas lo relaciona con la defensa de la soberanía nacional y en tal virtud nominaron que su alcance debería ser a nivel nacional, otras personas relacionaron el alcance nacional con la colaboración de otros países a nivel regional y mundial.

Figura 6. Principales limitaciones

Las principales limitaciones del Comando de Ciberdefensa de acuerdo a los resultados de la tabulación son los siguientes: Capacitación con 16 nominaciones, luego la infraestructura física y la concienciación de los mandos y nivel político, ambos con 12 nominaciones, el presupuesto con 10 nominaciones, el software con licencia, 4 nominaciones y otras limitaciones como la rotación de personal que mencionaron algunos expertos con 3 nominaciones.

Según los expertos entonces las tres principales limitaciones de la Ciberdefensa son: la capacitación, la infraestructura física y la concienciación de los mandos y políticos.

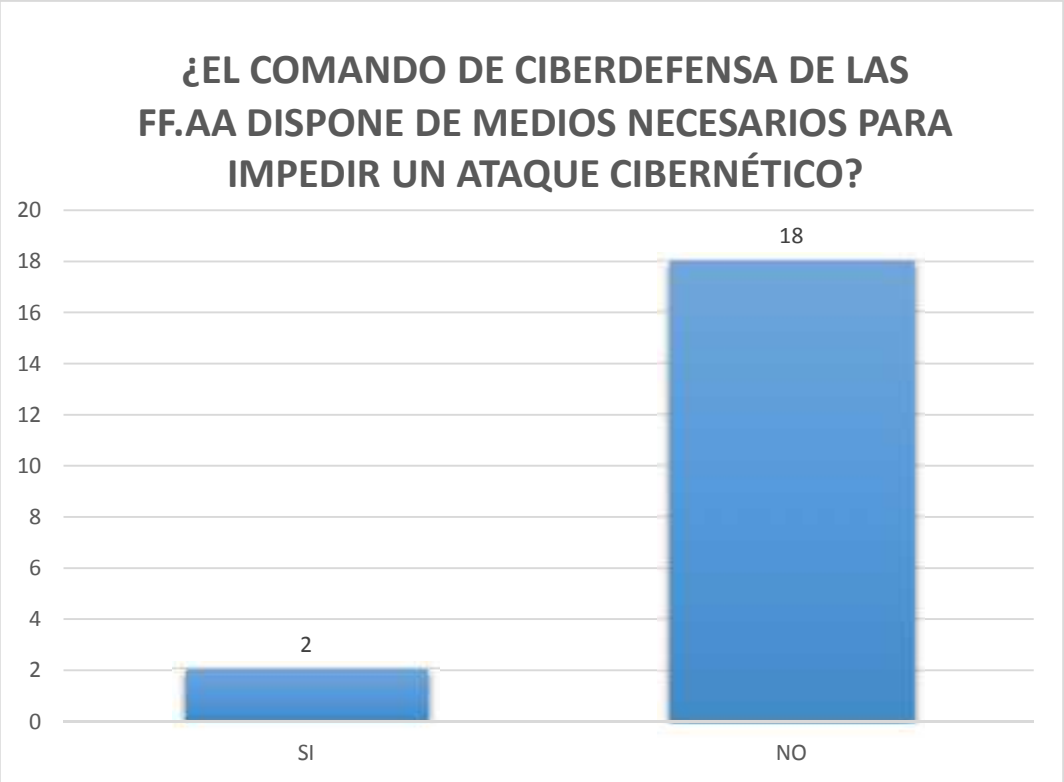


Fig. 7. ¿Capacidad de impedir un ataque cibernético?

Ante la pregunta que si el Comando de Ciberdefensa de las Fuerzas Armadas dispone de medios necesarios para impedir un ataque cibernético es contundente al contestar 18 personas que no dispone de medios para impedir un ataque y apenas dos personas que no están ligadas a la profesión militar contestaron que si tenía medios para impedir un ataque cibernético.

La decisión de crear un Comando de Ciberdefensa es reciente por lo tanto esta capacidad no está todavía bien consolidada por lo que la mayoría de las personas cercanas a las Fuerzas Armadas están conscientes que no están en capacidad de impedir un ataque cibernético.

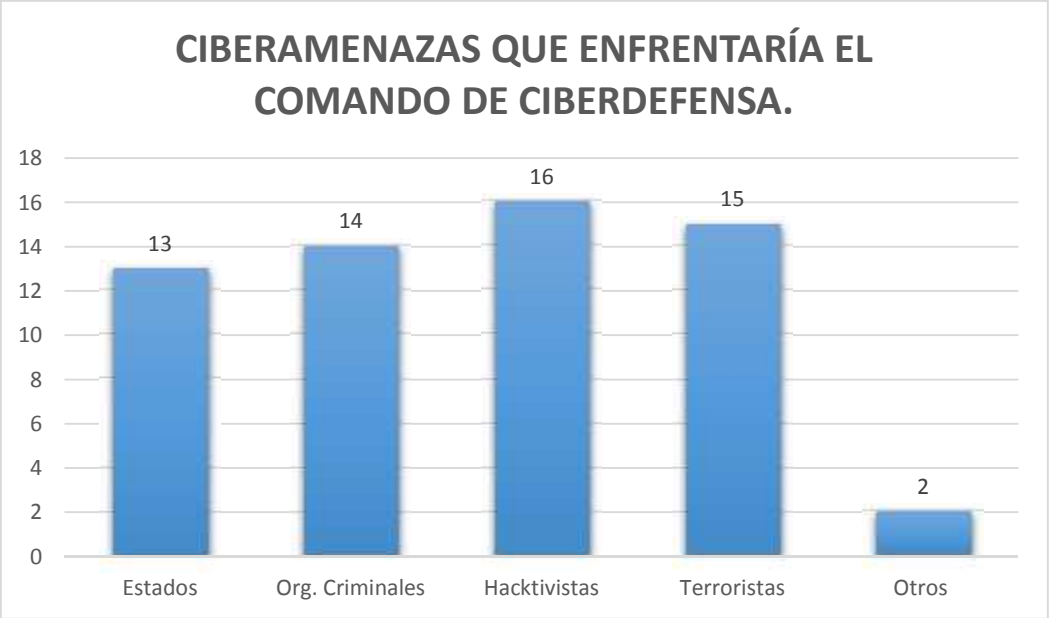


Fig. 8. Ciberamenazas

Las ciberamenazas que enfrentaría el Comando de Ciberdefensa de acuerdo al grupo de expertos son: los hacktivistas con 16 nominaciones, los terroristas con 15 nominaciones, las organizaciones criminales con 14 nominaciones, los Estados con 13 nominaciones y otros con 2 nominaciones.

Las tres principales ciberamenazas que enfrentaría el Comando de Ciberdefensa son entonces de acuerdo a las entrevistas los hacktivistas, los terroristas y las organizaciones criminales.

¿QUÉ POLITÍCAS DE ESTADO AFECTARÍAN LA CIBERDEFENSA?

Por ser una pregunta abierta existieron numerosas respuestas que no pueden ser tabuladas, sin embargo anotaremos las principales políticas que mencionaron los entrevistados.

Tabla 2

Políticas que afectan la Ciberdefensa

ORD	POLÍTICAS QUE AFECTARIAN LA CIBERDEFENSA
01	Reducción de presupuesto
02	Falta de apoyo gubernamental
03	Falta de un marco legal apropiado
04	Creación de organismos paralelos

CONTINÚA ➡

05	Estado acceda a información de los ciudadanos
06	Falta de políticas de Ciberdefensa y Ciberseguridad nacionales.
07	Falta de inversión en sistemas de Ciberseguridad.
08	Políticas de acceso libre a sistemas informáticos críticos.
09	No disponer de convenios internacionales.

Las políticas que afectarían a la Ciberdefensa de acuerdo al grupo son variadas, las que más afectarían está la del presupuesto que depende de las políticas gubernamentales de acuerdo a la importancia que crea que la Ciberdefensa deba estar, la falta de políticas relacionadas a este campo y también resulta importante la falta de colaboración con otros Estados que están muy avanzados al no disponer de convenios internacionales.

¿QUÉ POLÍTICAS DE ESTADO BENEFICIARÍAN LA CIBERDEFENSA?

Esta pregunta igualmente es abierta y por lo tanto existieron numerosas respuestas de las cuales se menciona las más importantes.

Tabla 3

Políticas que benefician a la Ciberdefensa

ORD	POLITICAS QUE BENEFICIARÍAN LA CIBERDEFENSA
01	Apoyo económico
02	Creación legislación adecuada
03	Proteger la información estratégica del Estado.
04	Capacitación en todos los niveles
05	Crear marco legal adecuado
06	Creación de Ciberdefensa en el nivel político estratégico
07	Disponer de convenios internacionales
08	Control del espectro electromagnético.
09	Alianzas estratégicas con Estados que tengan sistemas de Ciberseguridad.
10	Crear una institución que centralice todo lo relacionado con la Ciberdefensa.
11	Protección de la infraestructura critica del Estado.
12	Seguridad de la información.
13	Educación de seguridad informática.
14	Ley de protección de datos.
15	Ley de seguridad de la información

Las políticas que beneficiarían a la Ciberdefensa existen algunas que han mencionado las principales el apoyo económico, una adecuada legislación,

capacitación en todos los niveles, la implementación de políticas claras de Estado relacionadas a la Ciberdefensa y Ciberseguridad, convenios o alianzas estratégicas con países que tengan avanzados sistemas de Ciberseguridad, crear un marco legal adecuado, entre otras. En vista que la creación del Comando de Ciberdefensa es reciente existe un largo camino para que se vayan concretando varios proyectos que vayan en beneficio de la Ciberdefensa para la protección de la infraestructura crítica informática del país.

¿CUÁLES CONSIDERA QUE SON LOS HECHOS MAS SIGNIFICATIVOS QUE DETERMINA LA NECESIDAD DE CREAR UNA UNIDAD DE CIBERDEFNSA?

Esta pregunta es abierta y son varias las respuestas que dieron los expertos sobre la necesidad de crear una unidad de Ciberdefensa, de las cuales se menciona las más importantes.

Tabla 4

Hechos significativos para la necesidad de crear una unidad de Ciberdefensa.

ORD	HECHOS MAS SIGNIFICATIVOS
01	Incremento de amenazas cibernéticas
02	No hay unidad responsable para enfrentar estas amenazas cibernéticas.
03	Ciberespionaje
04	Avance tecnológico en todos los campos
05	Cambio de escenarios
06	Dependencia de la tecnología
07	Hechos a nivel mundial sobre espionaje y ciberataques.
08	Vulnerabilidad de la información.
09	Intrusión en sistemas de seguridad del Estado.
10	Uso extensivo de Bot nets.
11	Necesidad de mantener las comunicaciones durante situaciones de emergencia o catastróficas.
12	Hackeos
13	Detección de intrusos en la web
14	Defensa del Estado de derecho
15	Mantener la paz interna
16	Estado mundial de Ciberseguridad
17	Casos de espionaje entre países.
18	Enfrentar ciberamenazas a nivel de seguridad nacional.
19	Ataques cibernéticos a empresas.
20	Hackeo de cuentas del Presidente y del Estado.

¿Qué motivó a que se cree una unidad de Ciberdefensa? De acuerdo al grupo de expertos que fueron entrevistados existen muchos motivos por los que se vio la necesidad de crear este tipo de unidad, los hechos que han venido ocurriendo a nivel mundial sobre el espionaje y los ciberataques a nivel mundial que son de dominio público, el incremento cada día de amenazas cibernéticas como el Hackeo de cuentas del Presidente y del Estado, el ataque cibernético a varias empresas del país, el hecho que cada vez tenemos más dependencia de la tecnología, la intrusión en varias páginas web del Estado y de las Fuerzas Armadas y el hecho principal que no existe una unidad de Ciberdefensa en el país que pueda defender la infraestructura informática del país. La política del gobierno ha visto la necesidad de crear un Comando de Ciberdefensa a cargo de las Fuerzas Armadas.

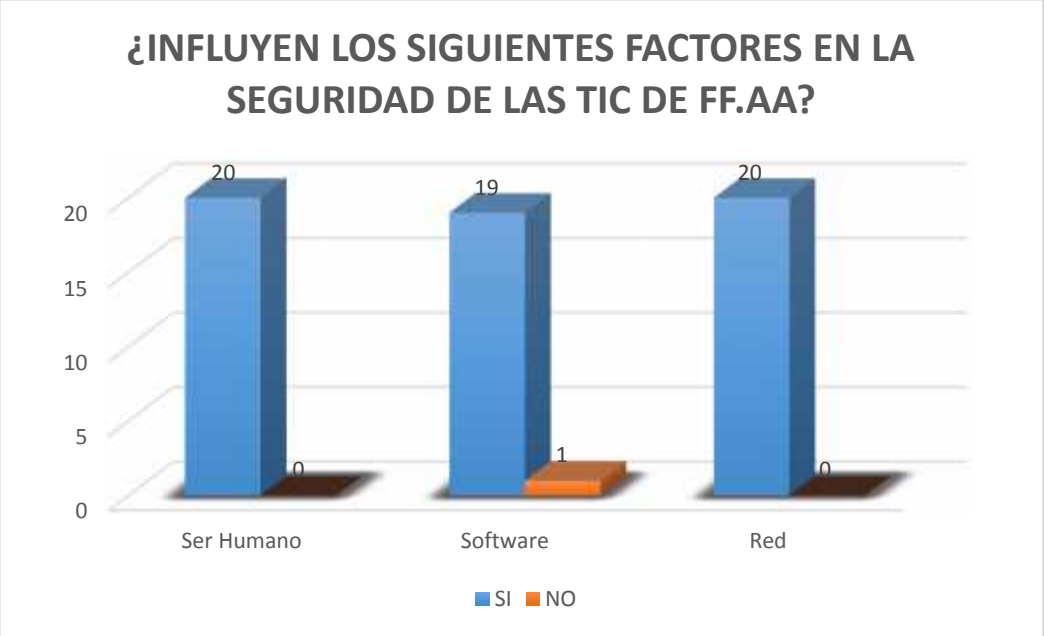


Fig. 9. Factores que influyen en la seguridad de las TIC de las FF.AA.

La pregunta si el ser humano, el software y la red influyen en la seguridad de las tecnologías de la información y comunicación los resultados fueron los siguientes: de 20 expertos los 20 dicen que si influye el ser humano, acerca del software de 20 personas, 19 contestan que sí influye y solamente una persona contestó que no influye, de 20 personas, las 20 contestaron que sí influye la red en la seguridad de las TIC de las Fuerzas Armadas.

Los factores ser humano, software y la red definitivamente sí influyen en la seguridad de las Tecnologías de la Información y de Comunicación de las Fuerzas Armadas.

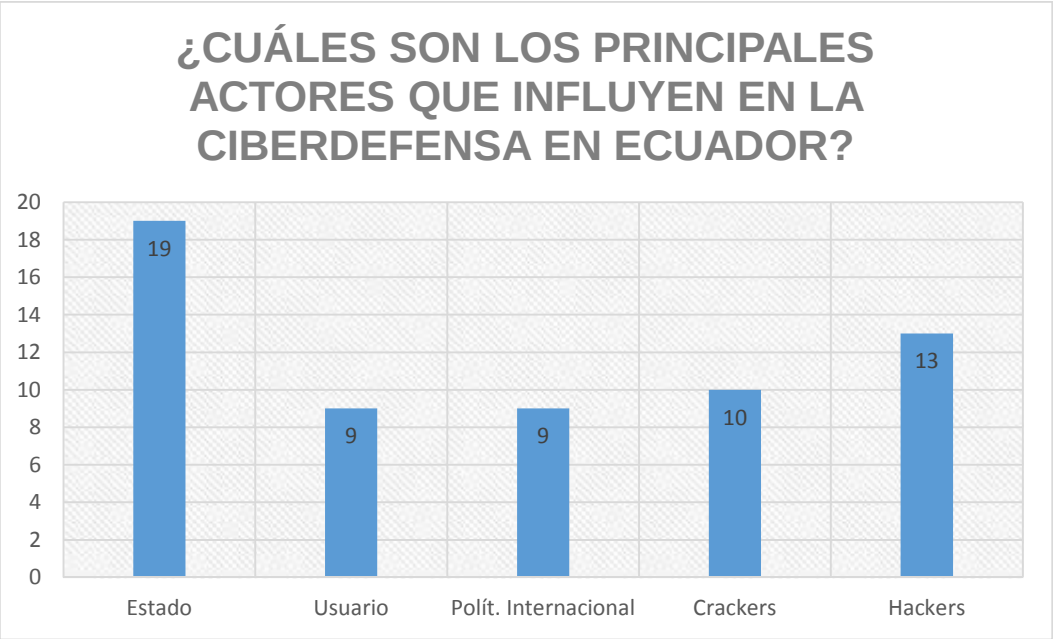


Fig. 10. Actores que influyen en la Ciberdefensa en Ecuador.

En esta pregunta los expertos debían escoger tres actores principales que influyen en la Ciberdefensa en Ecuador, los resultados de la tabulación son los siguientes: El Estado fue nombrada con 19 nominaciones, luego los hackers con 13 nominaciones, los crackers con 10 nominaciones, el usuario y la política internacional fueron nominados ambos actores con 9 nominaciones.

Los tres principales actores que influyen en la Ciberdefensa en Ecuador son: el Estado, los hackers y los crackers.

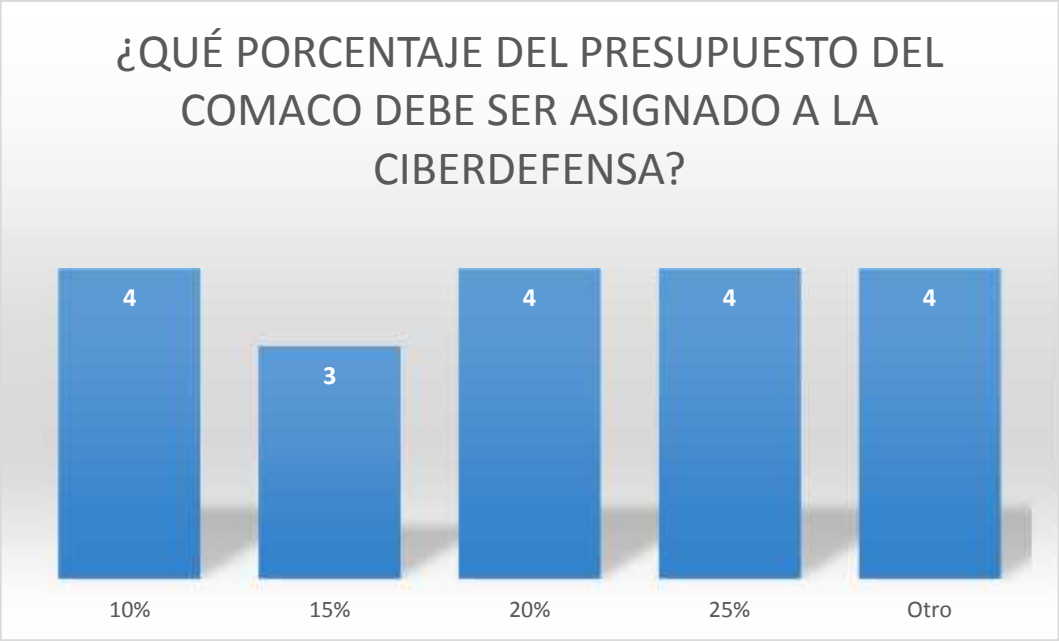


Fig. 11. Porcentaje del presupuesto de la Ciberdefensa.

La pregunta sobre qué porcentaje del presupuesto del Comando Conjunto de las Fuerzas Armadas debe ser asignado a la Ciberdefensa, el grupo de expertos contestaron lo siguiente: el 10% contestaron 4 personas, el 15% contestaron 3 personas, el 20% contestaron 4 personas, el 25% contestaron 4 personas y otro porcentaje contestaron 4 personas.

El grupo de expertos no tiene definido un porcentaje del presupuesto que debería ser asignado a la Ciberdefensa, se repartieron entre los porcentajes descritos y otras personas contestaron que debería ser de acuerdo a sus necesidades sin enmarcarse en un porcentaje.

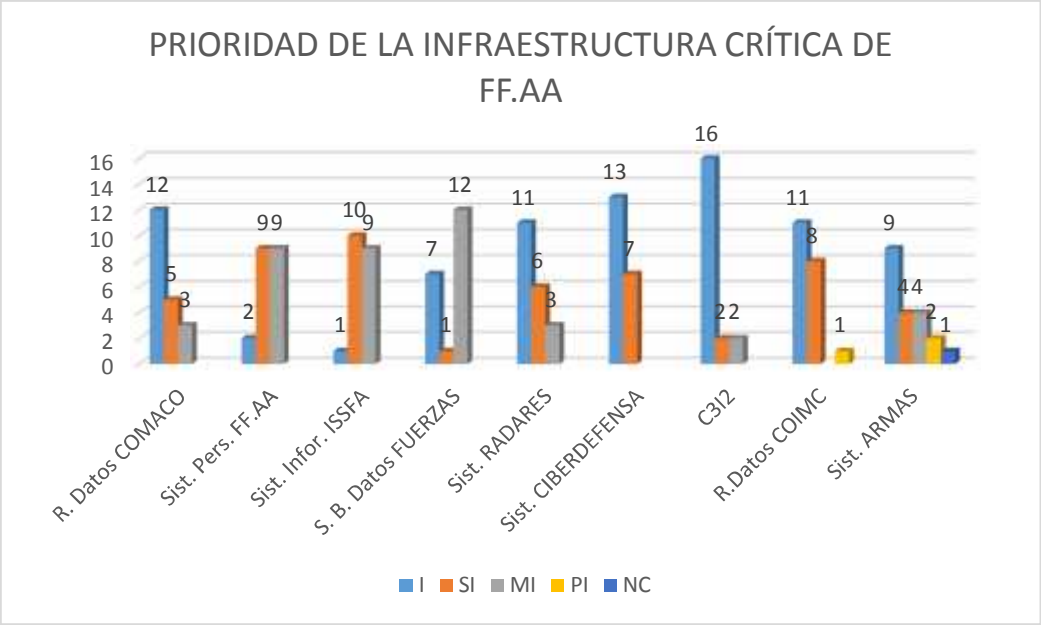


Fig. 12. Prioridad infraestructura critica de FF.AA.

Esta pregunta contenía una tabla en la que el grupo de expertos debía clasificar la prioridad o la importancia de la infraestructura critica de las Fuerzas Armadas con los siguientes resultados:

Red de datos del Comando Conjunto, 12 personas dicen que es indispensable, 5 personas dicen que es sumamente importante y 3 personas dicen que es medianamente importante.

El sistema de personal de las Fuerzas Armadas, 2 personas dicen que es indispensable, 9 personas dicen que es sumamente importante y 9 personas dicen que es medianamente importante.

El sistema informático del ISSFA, 1 persona dijeron que es indispensable, 10 personas dicen que sumamente importante y 10 personas dicen que es medianamente importante.

El sistema de base de datos de las Fuerzas, 7 personas dicen que es indispensable, 1 persona dice que es sumamente importante y 12 personas dicen que es medianamente importante.

El sistema de radares, 11 personas dicen que es indispensable, 6 personas dicen que es sumamente importante y 3 personas dicen que es medianamente importante.

El sistema de Ciberdefensa, 13 personas dicen que es indispensable y 7 personas dicen que es sumamente importante.

El sistema C3I2, 16 personas dicen que es indispensable, 2 personas dicen que es sumamente importante y 2 personas dicen que es medianamente importante.

La red de datos del Comando de inteligencia militar conjunta, 11 personas dicen que es indispensable, 8 personas dicen que es sumamente importante y 1 persona dice que es poco importante.

El sistema de armas, 9 personas dicen que es indispensable, 4 personas dicen que es sumamente importante, 4 personas dicen que es medianamente importante y 1 persona dice que es nada importante.

De todos los sistemas de acuerdo a las entrevistas a este grupo de expertos en primer lugar de prioridad está el sistema C3I2, el sistema de Ciberdefensa y el sistema de red de datos del Comando Conjunto de las Fuerzas Armadas.

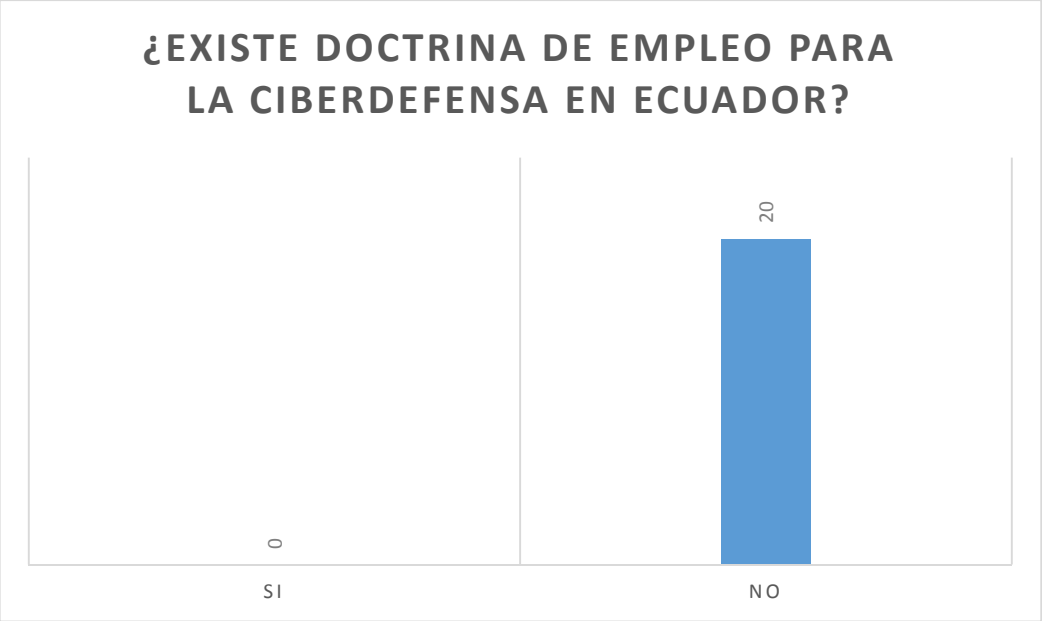


Fig. 13. Doctrina de empleo de la Ciberdefensa en Ecuador.

La pregunta sobre si en Ecuador existe doctrina de empleo para Ciberdefensa la contestación fue unánime las 20 personas entrevistadas contestaron que no hay doctrina en Ecuador para el empleo de la Ciberdefensa.

El Comando de Ciberdefensa es creado recientemente por lo tanto no dispone todavía de doctrina para el empleo de sus medios.

¿CUÁL ES LA INFRAESTRUCTURA BÁSICA QUE DEBE TENER LA CIBERDEFENSA?

Esta pregunta es abierta, el grupo de expertos mencionaron numerosas y variadas respuestas de las cuales mencionamos a continuación las más importantes.

Tabla 5

Infraestructura básica de la Ciberdefensa.

ORD	INFRAESTRUCTURA BÁSICA DE LA CIBERDEFENSA
01	Seguridad física, seguridad lógica (claves), seguridad de acceso a la información.
02	Centro de monitoreo y centro de análisis.
03	Grupo de respuesta, grupo de explotación y grupo de respuesta.
04	Infraestructura física para 130 personas y equipos.
05	Equipo de análisis de vulnerabilidades, equipo para detectar amenazas, data center robusto.
06	Hardware, software con licenciamiento en áreas de defensa (explotación, respuesta y forense.
07	Crear la capacidad para la protección de infraestructura crítica y realizar operaciones básicas ofensivas en el ciberespacio.
08	Redes de nueva generación (redundancia, Escalada, Alta disponibilidad, Seguridad) Planes de continuidad (planes de recuperación de desastres).
09	Estructura orgánica: hardware relacionado, software de monitoreo, hacking y forense.
10	Los servidores necesarios con el software y herramientas.
11	Personal con altos niveles de ética, profesionalidad, responsabilidad y habilidades.
12	Hardware y software para seguridad y monitoreo de las redes de las FF.AA
13	Centro de monitoreo de Sistemas críticos, Laboratorio de análisis forense, laboratorio de malware, sandbox.
14	Data center, sensores de monitoreo, segmentos de red aislada.
15	Debe contar con un centro de respuestas a incidentes militares, laboratorios de guerra cibernética, laboratorio forense, laboratorio de pruebas.
16	Monitoreo de red, SIM (manejo de información de seguridad), herramientas para análisis forense y evaluación de seguridad.

Las respuestas de las personas entrevistadas son variadas de acuerdo a su experiencia y a los estudios de varios modelos de otros países, lo que la mayoría menciona es que debe tener un centro de monitoreo y un centro de análisis,

hardware, software, hacking y forense; debe tener un centro de respuestas a incidentes militares, laboratorios de guerra cibernética, laboratorio forense, de acuerdo a modelos de otros países debe tener un grupo de respuesta, grupo de explotación y grupo de respuesta, pero sobretodo debe tener personal con altos niveles de ética, profesionalidad, responsabilidad y habilidades.

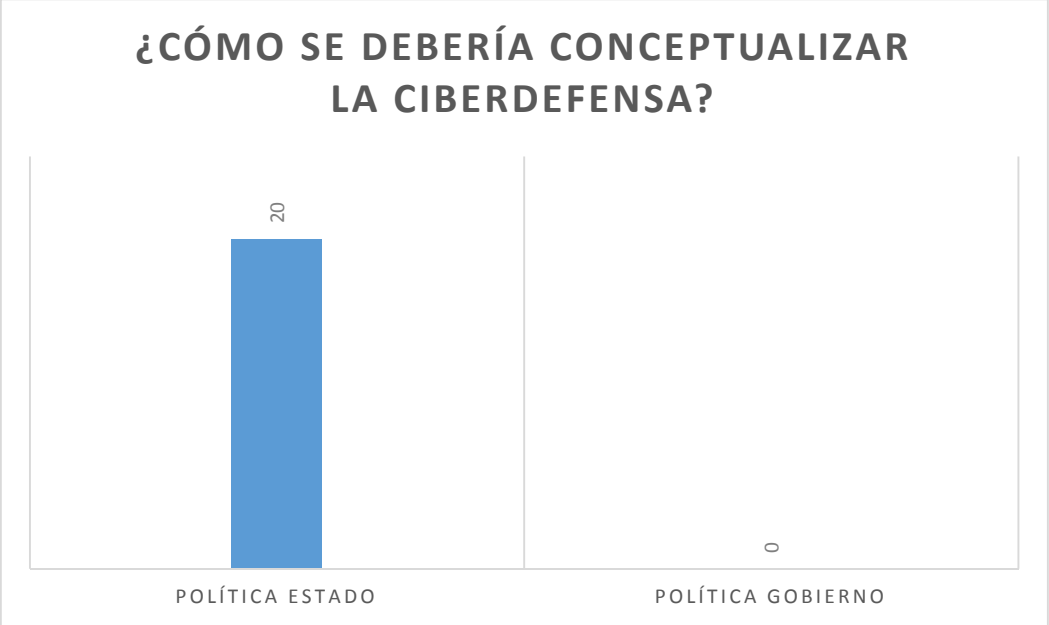


Fig. 14. Conceptualizar la Ciberdefensa.

La pregunta de cómo se debería conceptualizar a la Ciberdefensa tuvo dos alternativas, como Política de Estado o como Política de gobierno, todas las personas entrevistadas contestaron que debería ser Política de Estado.

Actualmente como se encuentra la situación mundial y regional, la Ciberdefensa debe ser considerada como una política de Estado y no solamente del gobierno de turno por la importancia estratégica que tiene la protección de la infraestructura digital critica del Estado.

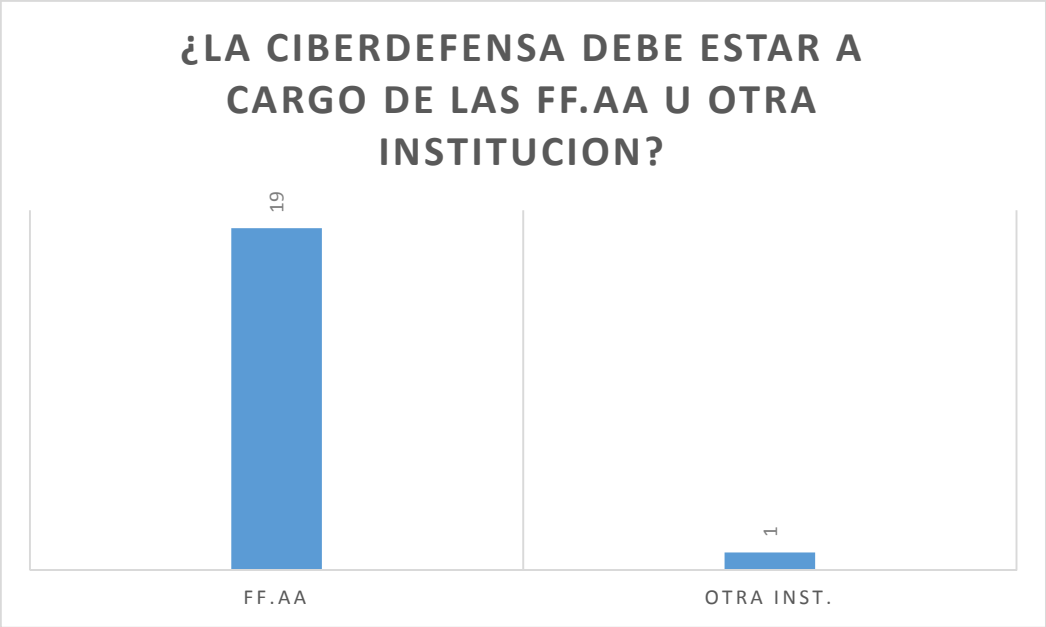


Fig. 15. Ciberdefensa a cargo de FF.AA u otra institución.

La pregunta sobre si la Ciberdefensa debe estar a cargo de las Fuerzas Armadas u otra institución, 19 personas contestaron que debe estar a cargo de las FF.AA y solamente una persona dice que debería estar a cargo de otra institución.

Está claro que para la mayoría que las Fuerzas Armadas debe estar a cargo de las Fuerzas Armadas, algunos expertos mencionaron que al ser las Fuerzas Armadas estarían en condiciones de realizar acciones ofensivas mientras que otra institución que no sea las FF.AA no tendría la legalidad que estas operaciones requiere, a pesar que a nivel mundial se observa que no hay responsabilidades de ningún país en aceptar que realizaron ataques cibernéticos a otro Estado, más bien la legalidad sería por la defensa de la soberanía nacional.

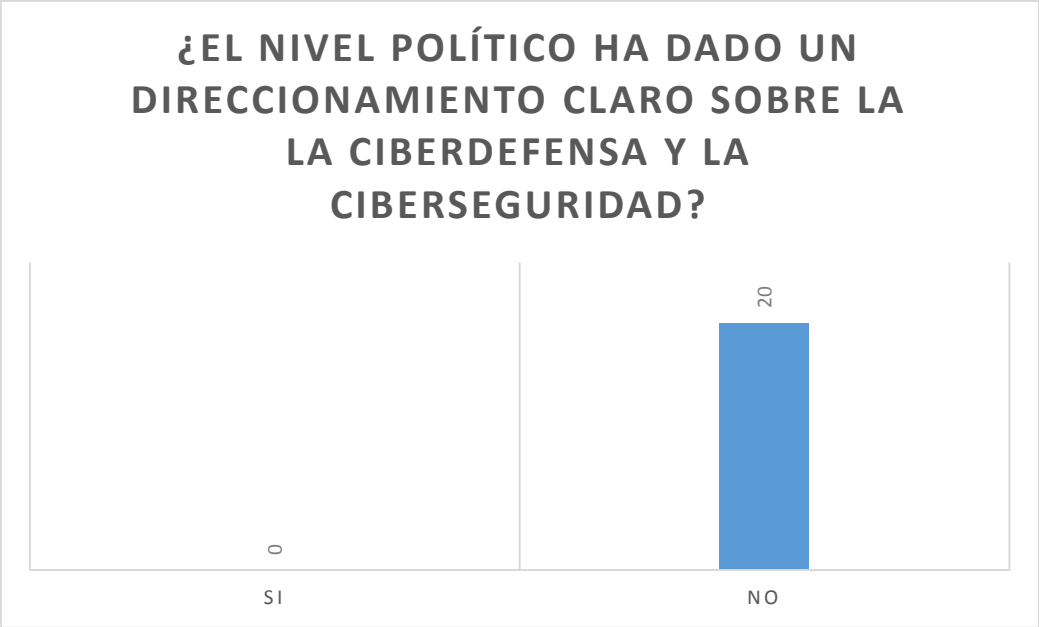


Fig. 16. Direccionamiento político de la Ciberdefensa y la Ciberseguridad.

Esta pregunta sobre si existe un direccionamiento político en cuanto a la Ciberdefensa y Ciberseguridad todos los entrevistados sin excepción contestaron que no hay un direccionamiento político claro respecto a esta nuevo campo, por ser una área nueva no existe ni legislación ni políticas claras sobre estas actividades que se vienen constituyendo un problema por cuanto el uso de la tecnología se ha incrementado rápidamente y las regulaciones son muy lentas en este campo.

¿QUÉ INSTITUCION DEBE ESTAR ENCARGADA DE LA CIBERSEGURIDAD?

Por ser una pregunta abierta tuvo varias contestaciones de diferente índole, de las cuales se menciona las siguientes:

Tabla 6

Institución encargada de la Ciberseguridad.

ORD	INSTITUCION ENCARGADA DE LA CIBERSEGURIDAD
01	El Comando Conjunto de las Fuerzas Armadas.
02	El Ministerio del Interior.
03	FF.AA en coordinación con la Policía Nacional.
04	Concejo de Seguridad Pública del Estado (COSEPE).
05	Ministerio Coordinar de Seguridad (MICS).

CONTINÚA ➡

06	Una Subsecretaria a nivel Estado.
07	Concejo Nacional de Ciberseguridad
08	El Estado, FF.AA y Policía Nacional.
09	El Ministerio de Telecomunicaciones.
10	Un organismo civil.
11	Una institución con independencia política, administrativa con canal de comunicación directa con el gobierno.

La Ciberseguridad es un campo muy amplio tan importante para un país que incluso la Ciberdefensa está inmersa en la Ciberseguridad, por lo tanto debe ser manejado por una institución del Estado que permita coordinar todas las acciones relacionadas a la seguridad a nivel nacional, que tenga comunicación directa con el gobierno y que se le dé la importancia que se merece, actualmente el Ministerio Coordinador de Seguridad es quien lleva y coordina todas las acciones relacionadas a la seguridad con varios ministerios como el Ministerio del Interior, el Ministerio de defensa y ha tenido éxito con el manejo del ECU 911, la pregunta es si con toda la responsabilidad que tiene se le va a incrementar la Ciberdefensa o debe ser una institución completamente a parte pero en coordinación directa con varias instituciones que ya tienen algo relacionado con los CERT de varias instituciones como la Superintendencia de telecomunicaciones, o de la Universidad Técnica Particular de Loja que tiene organizadas sus centros de respuesta informática de tal manera de organizar una red en beneficio de la Ciberseguridad.

Fig. 17. Diseño de Estrategias, Acc. Ofensivas y Acc. Defensivas.

Esta pregunta está relacionada con la actitud estratégica del país la cual es defensiva y su orientación es proactiva, es decir, se fundamenta en la prevención y alerta temprana en tal virtud el empleo de la fuerza militar es el recurso de última instancia, pero al tratarse de la Ciberdefensa ¿se puede diseñar estrategias? todas las personas entrevistadas contestaron que SÍ, ¿se puede diseñar acciones ofensivas? 17 personas contestaron que SÍ y 3 personas contestaron que NO, ¿se puede diseñar acciones defensivas? Todas las personas entrevistadas contestaron que SÍ.

La mayoría de los entrevistados están de acuerdo en que se pueden diseñar estrategias, acciones ofensivas y acciones defensivas en el campo de la Ciberdefensa, sin que con estas acciones se crea que se está atacando a otro Estado, sino es parte de la defensa que la Ciberdefensa debe proporcionar al defender la infraestructura tecnológica del país.

4.2. CONCLUSIONES DE LOS INSTRUMENTOS DE NVESTIGACION.-

A través de los instrumentos lograron contestar las diferentes preguntas que requiere la investigación por parte de un grupo de expertos en el tema de la Ciberdefensa a fin de determinar la tendencia más probable así como las principales variables para continuar con la construcción de los escenarios.

Los hechos mundiales actuales y la experiencia de los entrevistados nos indican que los sistemas militares más sensibles de ataques cibernéticos son aquellos relacionados con el mando y control como son la información clasificada de las Fuerzas Terrestre, Naval y Aérea; el mando y control del Comando Conjunto que los militares lo denominamos como C3I2, es decir, Comando, Control, Comunicaciones, Informática e Inteligencia; y los servidores que almacenan información clasificada.

Las áreas de la infraestructura crítica del Estado que podrían ser blancos de ataques cibernéticos están las centrales y redes de energía en las que están incluidas la electricidad, petróleo, gas, refinerías; las tecnologías de las comunicaciones y de la información; y el sistema de finanzas.

El Comando de Ciberdefensa para cumplir con su misión debe estar en capacidad de detectar intrusos a los diferentes sistemas informáticos, además debe estar en capacidad de detectar y analizar las vulnerabilidades de su sistema propio de la Ciberdefensa, debe estar en capacidad de monitorear las redes y disponer de informática forense y sobre todo debe estar en capacidad de evitar un ataque cibernético a la infraestructura digital critica del Estado y de las Fuerzas Armadas por parte de los hacktivistas, terroristas, organizaciones criminales y por parte de los Estados con la ayuda del Estado con la emisión de políticas que beneficiarían a la Ciberdefensa como el apoyo económico, una legislación adecuada, el control del espacio electromagnético, firmar alianzas estratégicas con países que se encuentran más avanzados en este tema, realizar una capacitación en todos los niveles, concienciación en los niveles políticos sobre la importancia de la Ciberdefensa para la defensa de los intereses nacionales.

Por tratarse de una capacidad que recién se está creando tiene diferentes limitaciones como en su infraestructura física, la capacitación de su personal, el presupuesto, el hardware y software, la falta de concienciación de los mandos militares y políticos que poco a poco con la generación de varios proyectos se irán superando estas limitaciones.

La organización de la Ciberdefensa debe tener una infraestructura básica que debe estar constituido con equipos de alta tecnología, debe tener un centro de monitoreo, un centro de análisis, hardware y software en áreas de explotación,

respuesta y forense, tener la capacidad de proteger la infraestructura crítica y realizar operaciones básicas ofensivas en el ciberespacio, debe contar con un centro de respuestas a incidentes militares, laboratorios de guerra cibernética, laboratorio forense, laboratorio de pruebas, equipo para detectar amenazas, un data center robusto, en su infraestructura física debe tener un espacio para 130 personas y su personal con altos niveles de ética, profesionalidad, responsabilidad, habilidades y muy comprometidos con su institución en el cumplimiento de su misión.

Analizado los resultados de las entrevistas a este grupo de expertos en el tema se concluye que las principales variables son las siguientes:

- Capacitación.
- Presupuesto.
- Marco Legal.
- Infraestructura y tecnología.
- Políticas de Estado.
- Talento Humano.
- Convenios internacionales.

CAPITULO 5

5. CONSTRUCCION DE ESCENARIOS

5.1. Paso 1. Identificación de las fuerzas principales. (definición de las principales variables que modelan la realidad – sectores).

Tabla 7

Fuerzas principales y definición.

FUERZAS PRINCIPALES	DEFINICION
Capacitación	Proceso de enseñanza-aprendizaje, mediante el cual se desarrolla las habilidades y destrezas de los miembros de Ciberdefensa, que les permitan un mejor desempeño en sus labores habituales.
Presupuesto	Recursos económicos que se estima será necesario para el fortalecimiento de la Ciberdefensa.
Marco legal	Proporciona las bases sobre las cuales las instituciones construyen y determinan el alcance y naturaleza de su participación, es el orden normativo e institucional de la conducta humana en sociedad inspirada en postulados de justicia.
Infraestructura física y Tecnológica	Conjunto de elementos o servicios que están considerados como necesarios para que una organización pueda funcionar o para que una actividad se desarrolle efectivamente. Conjunto de dispositivos físicos y aplicaciones de software que requiere para operar.
Políticas de Estado	Es aquella que hace a los intereses del pueblo, independientemente del gobierno (de turno), es la determinación política para hacer frente a los riesgos y amenazas cibernéticos.
Talento Humano	capacidad de la persona que entiende y comprende de manera inteligente la forma de resolver en determinada ocupación, asumiendo sus habilidades, destrezas, experiencias y aptitudes propias de las personas talentosas
Convenios Internacionales	Compromisos de mutuo acuerdo entre los Estados.

5.2. Paso 2. Establecimiento de los Estados alternativos de cada Sector. (factores).

Tabla 8

Estados alternativos de cada sector.

FUERZAS	ID.	VALOR	DEFINICIÓN
CAPACITACIÓN	C 1	EXCELENTE	Personal con títulos de 4to nivel, capacitados en las TICs y que manejan tecnología de última generación.
	C 2	MUY BUENA	Personal con títulos de 3er nivel capacitados en las TICs en óptimas condiciones de mantenerse actualizados.
	C 3	BUENA	Personal con títulos de acuerdo a su jerarquía, manejan las TICs debido a su experiencia, no han sido capacitados en Ciberdefensa.
	C 4	REGULAR	Personal con títulos de Tecnólogo, conocen las TICs superficialmente, no han sido capacitados.
	C 5	DEFICIENTE	Personal no tiene título de Bachiller, no conocen las TICs, no están capacitados

FUERZAS	ID.	VALOR	DEFINICIÓN
PRESUPUESTO	P 1	MUY FAVORABLE	Estado asigna recursos económicos de acuerdo al requerimiento.
	P 2	FAVORABLE	Estado asigna recursos económicos suficientes para cumplir la misión.
	P 3	MEDIANAMENTE FAVORABLE	Estado asigna recursos económicos con recortes de lo presupuestado.
	P 4	DESFAVORABLE	Estado no asigna recursos económicos suficientes para cumplir la misión.
	P 5	ADVERSA	Estado no asigna recursos económicos

FUERZAS	ID.	VALOR	DEFINICIÓN
MARCO LEGAL	L 1	MUY FAVORABLE	Legislación específica y completa en materia de Ciberseguridad
	L 2	FAVORABLE	Legislación distribuida en varias leyes que regula las actividades aunque no en forma completa.
	L 3	MEDIANAMENTE FAVORABLE	Legislación que contiene regulaciones muy generales que no son suficientes en materia de Ciberdefensa.
	L 4	DESFAVORABLE	Legislación muy escasa que no sanciona actividades ilegales en internet.
	L 5	ADVERSA	Ausencia de legislación específica y completa en materia de Ciberseguridad

FUERZAS	ID.	VALOR	DEFINICIÓN
INFRAESTRUCTURA FISICA Y TECNOLOGICA	I 1	EXCELENTE	Capacidad de detección, prevención, contención y respuesta ante ciberataques, hardware y software de última generación, instalaciones físicas amplias y confortables.
	I 2	OPTIMA	Capacidad de detección, prevención, contención y respuesta ante ciberataques, hardware y software actualizado, instalaciones físicas cómodas.
	I 3	NORMAL	Capacidad de detección, prevención, contención y respuesta ante ciberataques, hardware y software con licencia, instalaciones físicas adecuadas.
	I 4	BAJA	Sin capacidad de detección, prevención, contención y respuesta ante ciberataques, hardware y software desactualizadas, instalaciones físicas incómodas.
	I 5	MINIMA	Sin capacidad de detección, prevención, contención y respuesta ante ciberataques, hardware y software obsoletas, instalaciones físicas inadecuadas.

FUERZAS	ID.	VALOR	DEFINICIÓN
POLITICAS DE ESTADO	E 1	MUY FAVORABLE	Existen políticas que enfrentan los riesgos y amenazas cibernéticas.
	E 2	FAVORABLE	Existen políticas que fomentan la educación y concienciación de la Ciberseguridad.
	E 3	MEDIANAMENTE FAVORABLE	Existen políticas muy generales que en algo regula los riegos y amenazas cibernéticas.
	E 4	DESFAVORABLE	Existen políticas muy tibias que no tienen objetivos claros.
	E 5	ADVERSA	Ausencia de políticas sobre la Ciberseguridad.

FUERZAS	ID.	VALOR	DEFINICIÓN
TALENTO HUMANO	V1	EXCELENTE	Personal muy capacitado con altos niveles de ética, profesionalidad, responsabilidad, habilidades y comprometido.
	V2	MUY BUENA	Personal comprometido muy capacitado con habilidades, aptitudes, destrezas, con experiencia y responsabilidad
	T 3	BUENA	Personal capacitado con habilidades, aptitudes, destrezas, responsable, pero sin experiencia.
	T 4	REGULAR	Personal sin capacitación, sin aptitudes, destrezas ni experiencia.
	T 5	DEFICIENTE	Personal no capacitado, no comprometido, sin aptitudes, destrezas ni experiencia.

FUERZAS	ID.	VALOR	DEFINICIÓN
CONVENIOS INTERNACIONALES	V 1	MUY FAVORABLE	Ciberdefensa fortalecida con la ejecución de convenios a nivel Unasur, Regional y Mundial con el objetivo de mejorar la seguridad de nuestro ciberespacio.
	V 2	FAVORABLE	Convenios bilaterales y multilaterales con otras naciones en el ámbito de la Ciberdefensa para mejorar los canales de información, detección y/o respuesta coordinada ante incidentes cibernéticos.
	V 3	MEDIANAMENTE FAVORABLE	Participación en foros multilaterales e internacionales donde se aborde la Ciberdefensa.
	V 4	DESFAVORABLE	No participa en foros internacionales ni multilaterales.
	V 5	ADVERSA	No dispone de convenios internacionales y está aislada de la comunidad internacional.

5.3. Paso 3. Construcción de la Matriz Sectores/Factores.

Tabla 9

Matriz Sectores/Factores.

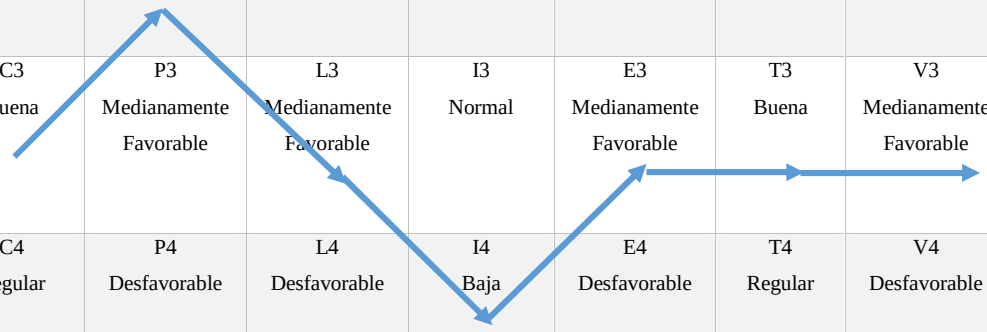
C	P	L	I	E	T	V
Capacitación	Presupuesto	Marco Legal	Infra física y Tecnológica	Políticas Estado	Talento Humano	Convenios Internacional.
C1 Excelente	P1 Muy Favorable	L1 Muy Favorable	I1 Excelente	E1 Muy Favorable	T1 Excelente	V1 Muy Favorable
C2 Muy Buena	P2 Favorable	L2 Favorable	I2 Óptima	E2 Favorable	T2 Muy Buena	V2 Favorable
C3 Buena	P3 Medianamente Favorable	L3 Medianamente Favorable	I3 Normal	E3 Medianamente Favorable	T3 Buena	V3 Medianamente Favorable
C4 Regular	P4 Desfavorable	L4 Desfavorable	I4 Baja	E4 Desfavorable	T4 Regular	V4 Desfavorable
C5 Deficiente	P5 Adversa	L5 Adversa	I5 Mínima	E5 Adversa	T5 Deficiente	V5 Adversa

5.4. Paso 4. Calibración de la Matriz.

Tabla 10

Calibración de la Matriz.

C	P	L	I	E	T	V
Capacitación	Presupuesto	Marco Legal	Infra física y Tecnológica	Políticas Estado	Talento Humano	Convenios Internacional.
C1 Excelente	P1 Muy Favorable	L1 Muy Favorable	I1 Excelente	E1 Muy Favorable	T1 Excelente	V1 Muy Favorable
C2 Muy Buena	P2 Favorable	L2 Favorable	I2 Óptima	E2 Favorable	T2 Muy Buena	V2 Favorable
C3 Buena	P3 Medianamente Favorable	L3 Medianamente Favorable	I3 Normal	E3 Medianamente Favorable	T3 Buena	V3 Medianamente Favorable
C4 Regular	P4 Desfavorable	L4 Desfavorable	I4 Baja	E4 Desfavorable	T4 Regular	V4 Desfavorable
C5 Deficiente	P5 Adversa	L5 Adversa	I5 Mínima	E5 Adversa	T5 Deficiente	V5 Adversa



To (2015): C3; P2; L3; I4; E3; T3; V3

5.5. Paso 5. Construcción de Escenarios.

Tabla 11

Construcción de Escenarios.

C	P	L	I	E	T	V
Capacitación	Presupuesto	Marco Legal	Infra física y Tecnológica	Políticas Estado	Talento Humano	Convenios Internacional.
C1 Excelente	P1 Muy Favorable	L1 Muy Favorable	I1 Excelente	E1 Muy Favorable	T1 Excelente	V1 Muy Favorable
C2 Muy Buena	P2 Favorable	L2 Favorable	I2 Óptima	E2 Favorable	T2 Muy Buena	V2 Favorable
C3 Buena	P3 Medianamente Favorable	L3 Medianamente Favorable	I3 Normal	E3 Medianamente Favorable	T3 Buena	V3 Medianamente Favorable
C4 Regular	P4 Desfavorable	L4 Desfavorable	I4 Baja	E4 Desfavorable	T4 Regular	V4 Desfavorable
C5 Deficiente	P5 Adversa	L5 Adversa	I5 Mínima	E5 Adversa	T5 Deficiente	V5 Adversa

OPTIMISTA		C1	P1	L1	I1	E1	T1	V1
MAS PROBABLE		**C3**	**P2**	**L3**	**I2**	**E3**	**T3**	**V2**
PESIMISTA		**C3**	**P3**	**L3**	**I4**	**E3**	**T3**	**V4**

5.6. Paso 6. Narración del Escenario más Probable.

El Comando de Ciberdefensa de Fuerzas Armadas del Ecuador para el año 2017 en el área de capacitación dispone de personal de oficiales y voluntarios con títulos académicos de acuerdo a su jerarquía, que manejan las técnicas de información y comunicación, en condiciones de mantenerse capacitados en el área de Ciberdefensa, con los recursos económicos suficientes que serán asignados por el gobierno para el cumplimiento de su misión, referente al marco legal hay regulaciones muy generales que no son suficientes, el Comando de Ciberdefensa tendría una capacidad de detección, prevención, contención y respuesta ante ciberataques con hardware y software actualizados ubicados en instalaciones cómodas que permiten realizar el trabajo en forma eficiente, a pesar que existen políticas de Estado muy generales que en algo regula los riesgos y amenazas cibernéticas, en el campo de talento humano que conforme el Comando de Ciberdefensa estará capacitado con habilidades, aptitudes, destrezas, con responsabilidad pero sin experiencia, se firman convenios bilaterales y multilaterales con otras naciones en el ámbito de la Ciberdefensa para mejorar los canales de información, detección y/o respuesta coordinada ante incidentes cibernéticos.

5.7. Paso 7. Identificación de Oportunidades y Amenazas.

Oportunidades:

Se detectan tres oportunidades, una en P2, el presupuesto que está asignado para el Comando de Ciberdefensa está comprometido, el Estado ha designado los recursos económicos suficientes para cumplir con la misión de proteger la infraestructura crítica de las Fuerzas Armadas.

Estrategia:

Presentar proyectos para proteger la infraestructura critica del Estado y hacer conocer las consecuencias que podría sufrir el Estado y la importancia que tiene la Ciberdefensa para su defensa para que se asigne recursos económicos a fin de ampliar la protección no solo de la infraestructura critica de las Fuerzas Armadas sino la infraestructura critica del Estado en coordinación con otras instituciones del país relacionadas con la seguridad.

Oportunidad:

Se detecta en I2 sobre la infraestructura física y tecnológica en la que el Comando de Ciberdefensa tendría la capacidad de detección, prevención, contención y respuesta ante ciberataques, hardware y software actualizado, operando en instalaciones físicas cómodas.

Estrategia:

Demostrar y difundir las capacidades del Comando de Ciberdefensa al poder político con el fin de lograr el apoyo económico y político para el fortalecimiento de la Ciberdefensa.

Oportunidad:

Se detecta en V2 relacionado a los convenios bilaterales y multilaterales con otras naciones en el ámbito de la Ciberdefensa para mejorar los canales de información, detección y/o respuesta coordinada ante incidentes cibernéticos, se debe aprovechar la política regional de integración en especial de UNASUR para intercambiar experiencias y actuar en coordinación con otros países que tiene mayor experiencia que el nuestro.

Estrategia:

Solicitar al Gobierno se firmen convenios bilaterales y multilaterales con otros países a nivel regional y mundial con el fin de mantener una coordinación directa en la defensa de posibles ciberataques a la infraestructura crítica del Estado.

Amenazas:

Se detecta una amenaza en C3 sobre la capacitación del personal, para ser parte del Comando de Ciberdefensa todos sus integrantes debería tener títulos de acuerdo a su jerarquía, manejar las tecnologías de información y comunicaciones, tienen cierta experiencia, pero no han sido capacitados en el campo de la Ciberdefensa, el factor de la capacitación es muy importante y si no están capacitados no se podrá cumplir con la misión.

Estrategia para reducir amenazas:

Incluir en la compra de los equipos como parte del presupuesto la respectiva capacitación del personal que va a conformar el Comando de Ciberdefensa,

invitar a expertos de otros países más avanzados en este tema para mantenerse constantemente capacitados.

Amenaza:

Se detecta otra amenaza en L3 que corresponde al marco legal, si nos comparamos con otros países estamos muy retrasados en cuanto a leyes que regulen el uso del internet y las redes sociales permitiendo que se cometan varias actividades ilícitas y que no pueden ser sancionadas.

Estrategia para reducir amenazas:

Generar la necesidad al Ministerio de Defensa Nacional para que se exija la creación de un paquete normativo que regule específicamente todas las actividades ilícitas en el internet y las redes sociales para complementar la misión del Comando de Ciberdefensa de proteger la infraestructura critica de las Fuerzas Armadas, mejorar la actual legislación que contiene regulaciones muy generales que no son suficientes en materia de Ciberdefensa y engranar el esfuerzo de todas las instituciones en beneficio del Estado.

Amenaza:

Se detecta otra amenaza en E3 lo que se refiere a Políticas de Estado en el campo de la Ciberdefensa, existen políticas muy generales que en algo regula los riesgos y amenazas cibernéticas que no es suficiente para el funcionamiento de la Ciberdefensa y Ciberseguridad en el país.

Estrategia para reducir amenazas:

Solicitar que a través del Ministerio de Defensa se solicite al Gobierno Nacional se motiven la generación de políticas de Estado orientadas al manejo de la Ciberseguridad y Ciberdefensa alineadas a las leyes en materia de Defensa y de protección de la infraestructura crítica de las Fuerzas Armadas y del Estado.

Amenaza:

Se detecta otra amenaza en T3 Talento Humano, se puede disponer de personal capacitado con habilidades, aptitudes, destrezas, responsables, pero sin experiencia por estar en un proceso de creación del Comando de Ciberdefensa.

Estrategia para reducir amenazas:

Como parte de la adquisición de varios equipos para instalar las capacidades de la Ciberdefensa se debe adquirir un simulador o servidores en donde puedan

capacitarse en todos las situaciones posibles para que vayan adquiriendo poco a poco la experiencia que se requieren y posteriormente pasar al escenario real a fin de estar entrenado para enfrentar cualquier amenaza cibernética.

5.8. Paso 8. Conclusiones y Recomendaciones.

La situación del Comando de Ciberdefensa al 2017 se predice un mejor escenario que en el año actual (2015) al haber sido asignado una suma importante por parte del gobierno nacional para su creación. Sin embargo existen amenazas que hay que tomar en cuenta muy seriamente para enfrentar, neutralizar o adaptarnos a sus efectos, así como se han detectado fortalezas que hay que impulsarlas para respaldar la buena estructuración que servirá para disponer de todas las capacidades necesarias que debe tener la Ciberdefensa y poder cumplir con su misión que es la de proteger la infraestructura critica de las Fuerzas Armadas y posteriormente del Estado.

Una de las debilidades latentes es la capacitación del personal que conformará el Comando de Ciberdefensa el cual es un factor importante para su funcionamiento, se debe apoyar en la designación de personal que tenga títulos académicos de acuerdo a su grado en relación al orgánico y reforzarla con la capacitación incluida en la compra de equipos con tecnología de punta y complementadas con la asistencia a seminarios nacionales e internacionales.

El marco legal es casi inexistente en el campo de la seguridad de la información, a pesar de haberse incluido en el Código Orgánico Integral Penal algunos artículos que sancionan delitos informáticos sin embargo se necesita una ley de protección de datos, una ley seguridad de la información, una ley específica y completa en el ámbito informático que evite o regule las actividades ilícitas que se realizan a través de internet, paginas sociales y otras, por lo que es necesario que el nivel político tome conciencia sobre este tema e implante un marco legal acorde a la actualidad en donde el uso del internet ha tenido un incremento muy considerable en la población del país.

Un tema que va de la mano y es similar se trata de las políticas del Estado en el campo de la Ciberseguridad y la Ciberdefensa que actualmente no existen o si existen no son suficientes para el buen funcionamiento y el cumplimiento de la

misión, es necesario que el Gobierno implante políticas claras y especificas en este ámbito.

El talento humano es otro factor importante en el campo de la Ciberdefensa si no está capacitado correctamente podría constituir en una amenaza, al igual que si el personal no tiene las habilidades, destrezas, aptitudes en el campo informático, la rotación del personal es una amenaza para el buen funcionamiento de la Ciberdefensa, se debe pensar en una estrategia para que el personal que conforme este Comando tenga un tratamiento especial en ese aspecto, además de acuerdo a las entrevistas se ha concluido que el personal que debe conformar este Comando debe ser personal con altos niveles de ética, profesionalidad, responsabilidad y habilidades especiales, lo fundamental es disponer del personal más calificado e innovador posible y con la capacidad de desarrollar propias herramientas para estar delante de los posibles adversarios, en tecnología y en procedimientos.

Hay varias oportunidades que se debería aprovechar para reforzar el funcionamiento del Comando de Ciberdefensa, el presupuesto que ha designado el gobierno nacional debe ser ejecutado hasta el año 2017 de acuerdo a los proyectos presentados, se debe elaborar más proyectos relacionados a la protección no solamente de las infraestructura critica de las Fuerzas Armadas sino del Estado para que hasta el año 2021 sea una realidad y así disponer del apoyo del gobierno para la asignación de los recursos económicos de acuerdo al requerimiento, concienciar al nivel político las consecuencias que podría tener el país sino se organiza una entidad que organice la Ciberdefensa y la Ciberseguridad que debe abarcar todas las instituciones de seguridad, financiera y digital en ejecución conjunta.

La infraestructura física y tecnológica que al ser adquiridas recientemente seguramente tendrá la tecnología de punta y por lo tanto dispondrá la capacidad de detección, prevención, contención y respuesta ante ciberataques.

Los convenios internacionales es una oportunidad que se debe reforzar en vista que en la actualidad todavía no existe convenios, inicialmente se lo debe realizar con el bloque de UNASUR se debe aprovechar la política regional de integración para mejorar los canales de información, detección y/o respuesta

coordinada ante incidentes cibernéticos, para intercambiar experiencias y actuar en coordinación con otros países que tiene mayor experiencia que el nuestro.

Para concluir es importante señalar que como parte de la investigación se tomó contacto con el Comando de Ciberdefensa en España quienes mencionaron que el factor económico no es fundamental sino instrumental, lo fundamental es disponer de personal más calificado e innovador posible con la capacidad de desarrollar las propias herramientas para estar delante de los posibles adversarios, no se trata de tener mucho, ni de gastar mucho, sino de lo que se tenga o lo que se gaste sea en personal y en material que sepan estar por delante del resto en tecnología y procedimentalmente.

REFERENCIAS BIBLIOGRAFICAS

Barcelona, F. d. (2002). *(Http://www.fib.upc.edu/retro-informatica/historia/internet.html, 2002)*. Obtenido de Historia del internet.

Gallardo, A. (marzo de 2009). Manual de métodos de prospectiva. *Centro de estudios e investigaciones militares*. Santiago, Chile.

Gallardo, A. (2009). *Prospectiva Estratégica Aplicada.* Quito.

Hernandez, F. &. (2002). *Fundamentos de la metodologia de la investigacion.* Mexico: Mc Graw Hill/Interamericana Editorres, S.A. de C.V. (México).

http://www.cad.com.mx/historia del internet.htm, s. (s.f.). *http://www.cad.com.mx/historia del internet.htm, s.f.* Obtenido de http://www.cad.com.mx/historia del internet.htm, s.f.

Martinez, R. (18 de mayo de 2007). *http://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html*. Obtenido de Los ciberataques a Estonia desde Rusia alarman a la OTAN y a la U.E.

Miranda, H. (04 de marzo de 2011). *http://mirandahelena-ib-tpl.blogspot.com/2011/04/origen y definicion del ciberespacio.html*.

Mojica, F. (2008). Forecasting y Prospectiva dos alternativas complementarias para adelantarnos al futuro. *Centro de Pensamiento Estratégico y Prospectiva*, 01.

Orozco, D. (07 de junio de 2011). *Definicion de Seguridad*. Obtenido de http://conceptodefinicion.de/seguridad/ .

PNSI. (2014). Quito.

PNSI. (2014 - 2017). *Soberania Tecnologica y Ciencia Aplicada a la Seguridad.* Quito.

Telegrafo. (10 de septiembre de 2014). *Ecuador tendra comando de Ciberdefensa*.

The New York Times, citado por El Mundo. (16 de enero de 2011). *http://www.elmundo.es/elmundo/2011/01/16/internacional/1295180388.html*. Obtenido de Israel y EE.UU crearon el virus que dañó el programa nuclear iraní.

www.eltelegrafo.com.ec. (11 de noviembre de 2014). FF.AA analizan crear un Comando Operacional Cibernetico. *El Telegrafo*.