Propuesta de una Política de Ciberseguridad para las Fuerzas Armadas

Pérez Martínez, Wilmer Ramiro y Ramos Pilco, Marco Antonio

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Estrategia Militar Terrestre

Trabajo de titulación, previo a la obtención del título de Magíster en Estrategia Militar Terrestre

Msc. Vargas Borbua, Robert Bolívar

07 de septiembre del 2020

URKUND

Urkund AnalysisResult

Analysed Document: (D63825267)	TESIS_CIBERSEGURIDAD_PEREZ.docx
Submitted:	2/13/2020 3:20:00 AM
Submitted By:	
Submitted email	jbolanos@difusion.com.mx
Similarty	0%
Analysis address:	jbolanos.GDC@analysis.urkund.com

Sources included in the report:

Firma:

.....

Crnl. E.M Vargas Borbua, Robert Bolivar

DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación: **"Propuesta de una Política de Ciberseguridad para las Fuerzas Armadas"**, fue realizado por los señores: **Tcrn. E.M Pérez Martínez, Wilmer Ramiro y Tcrn. E.M Ramos Pilco, Marco Antonio** el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 07 de septiembre del 2020

Firma:

.....

Crnl. E.M Vargas Borbua, Robert Bolivar

DIRECTOR

C.C.: 1001410263

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Nosotros, **Tcrn. E.M Pérez Martínez, Wilmer Ramiro** con cédula de ciudadanía Nº 0501764468 **y Tcrn. E.M Ramos Pilco, Marco Antonio,** con cédula de ciudadanía Nº 0602305773, declaramos que el contenido, ideas y criterios del trabajo de titulación: **"Propuesta de una Política de Ciberseguridad para las Fuerzas Armadas"** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 07 de septiembre del 2020

Firmas

Tcrn. E.M. Pérez Martínez, Wilmer Ramiro

CI.: 0501764468

Tcrn. E.M Ramos Pilco, Marco Antonio

CI.: 0602305773

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSTGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, **Tcrn. E.M Pérez Martínez, Wilmer Ramiro**, y **Tcrn. E.M Ramos Pilco, Marco Antonio** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Propuesta de una Política de Ciberseguridad para las Fuerzas Armadas"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 07 de septiembre del 2020

Firmas

Tcrn. E.M Pérez Martinez, Wilmer Ramiro

CI. 0501764468

Tcrn. E.M. Ramos Pilco Marco Antonio

CI. 0602305773

Dedicatoria

Los señores: Tcrn. E.M Pérez Martínez, Wilmer Patricio y Tcrn. E.M Ramos Pilco, Marco Antonio, como miembros de Fuerzas Armadas y consientes de la importancia de este proyecto de investigación, el mismo que nos permite alcanzar un peldaño más en nuestra carrera profesional queremos dedicar este trabajo a nuestros Padres presentes y ausentes, esposas e hijos que son el pilar fundamental en nuestras vidas, son el motor que nos empujan a seguir luchando para alcanzar nuestras metas propuestas.

A nuestro Ejército ecuatoriano que nos ha dado la oportunidad de superarnos, a los Docentes, Instructores y profesores, que con sus conocimientos supieron orientarnos en este arduo camino.

A todos ellos, nuestro eterno agradecimiento.

Sangolquí, 07 de septiembre del 2020

Agradecimiento

A la Universidad de Fuerzas Armadas ESPE, en especial al Departamento de Seguridad y Defensa, a sus oficiales en servicio activo y pasivo por darnos la oportunidad de ser parte del más grande y prestigioso instituto y poder aportar a nuestras Fuerzas Armadas.

A nuestro Director de Tesis, por ser la guía permanente en este proceso, de enseñanza aprendizaje.

Sangolquí, 07 de septiembre del 2020

Índice

Índice de Tablas

Índice de Figuras

Resumen

El uso obligatorio de las tecnologías de la información y las comunicaciones, dan como resultado una serie de riesgos que afectan los derechos de las personas, las infraestructuras críticas de la información y los intereses vitales de todos los cibernautas, lo que ha generado amenazas que inclusive las Fuerzas Armadas del Ecuador no están exentas, esto conduce a un mayor problema al no contar con políticas de ciberseguridad que permitan resguardar y proteger la seguridad digital.

Frente a las ciberamenazas y a la falta de políticas de ciberseguridad, el presente trabajo de titulación se centrará en formular una política de seguridad digital realizando un análisis de diferentes estándares internacionales, así como el análisis legal que está incorporado a nivel nacional en las diferentes instituciones, permitiendo de esta manera promover la coordinación entre instituciones gestionando los riesgos del ciberespacio.

Finalmente se propondrá políticas de ciberseguridad para proteger la información digital de las Fuerzas Armadas, acogiendo las normas y propuestas de las instituciones responsables de la seguridad informática en el país, como es el MINTEL (Ministerio de Telecomunicaciones), lo que permitirá el cumplimiento y accionar adecuado de las actividades acorde al nivel de madurez de nuestra institución en el campo jurídico, en el área técnica, área organizacional, en búsqueda de una cooperación con las diferentes instituciones encargadas de la seguridad de datos.

Palabras clave:

- **CIBERSEGURIDAD**
- **CIBERAMENAZAS**
- **CIBERESPACIO**

Abstract

Mandatory use of information and communication technologies, result in a series of risk to affect people's rights, critical infrastructure and the vital interest to all cybernaut to generate threats even of Armed Forces of Ecuador are exempt, this conducts to a huge problem not counting with politics of cybersecurity that allow guard and protect digital security to our institution.

In front of cyberthreats and lack of cybersecurity politics this work of degree is focus in formulate a politic of digital security making an analysis of different international standards, as well as, legal analysis that is incorporating to a national level different institutions, to this form allow to promote coordination and collaboration between institutions and manage risks of cyberspace.

Finally, will be proposed politics of cybersecurity to protect digital information of the Armed Forces, welcoming proposals and norms to responsible institutions of computing security in the country, like as MINTEL (Ministerium of Telecommunications), that allow compliance and right actuate to all activities according to our institution in the legal field, in the technique area, organizational area in the searching of cooperation with institutions in charge of data security.

Key words:

- **CYBERSECURITY**
- **CYBERMENACE**
- **CYBERSPACE**

Capítulo I

Problema

El mundo globalizado a obligado el uso de las tecnologías de la información y las comunicaciones, dando como resultado una serie de riesgos que afectan los derechos de las personas, las infraestructuras críticas de la información y los intereses vitales de nuestro país, nacional e internacional.

Estos riesgos pueden provenir de múltiples fuentes y resultar en fenómenos cuyas consecuencias pueden afectar de manera grave a la seguridad pública, los derechos fundamentales, e inclusive comprometer la seguridad externa del país mediante actividades de espionaje y ciberataques llevados a cabo por otros países, grupos organizados o incluso, por sujetos individuales.

En tal consecuencia el ciberespacio es una fuente cada vez más considerable de riesgos y amenazas, situación a la que las Fuerzas Armadas ecuatorianas no están exentas. Los delincuentes y espías buscan instituciones dentro de los Estados con bajos estándares de seguridad en el ciberespacio, para instalar redes y bases de operaciones para sus organizaciones, que pueden ser físicas o virtuales. Esto no sólo daña la imagen de nuestra institución, sino que puede tener efectos sociales y económicos.

Al respecto, las Fuerzas Armadas debe ser un actor proactivo frente a la materia de seguridad cibernética, que permita generar una política de ciberseguridad donde se concibe una perspectiva de maximización y armonización de las garantías fundamentales de las personas que integran nuestra institución, como el debido proceso, la libertad de expresión, el acceso a la información y a la protección de la vida privada, entre otras. Dado que el ciberespacio es un ambiente donde las personas cuentan con los mismos derechos que en el mundo físico, una política de

ciberseguridad no incidirá negativamente en el goce o ejercicio de éstas. Siguiendo esta línea se debe considerar la “Resolución A/HRC/20/L.13” promulgada por el Consejo de Derechos Humanos de las Naciones Unidas, la cual protege los derechos de los individuos en espacios virtuales como el Internet (Asamblea General - OHCHR, 2012).

Planteamiento del Problema

Grandes cantidades de datos son transmitidos desde el interior como el exterior de un país y entre estos datos, se encuentran aquellos que representan un gran riesgo de seguridad a la nación y sus conciudadanos, especialmente en el funcionamiento de las infraestructuras críticas que son vitales para el desarrollo del país y su supervivencia como nación.

Las amenazas escondidas o camufladas entre estos datos no son fáciles de detectar con medios convencionales, la determinación de comportamientos inusuales tampoco puede hacerse de manera rápida y certera. La detección y en consecuencia el tiempo de reacción para impedir o minimizar el impacto del cibercrimen es crítico y cada vez se hace más corto si se quiere mantener la integridad, confidencialidad y disponibilidad de la información que está ligada a un entorno físico real (Vaca, 2017).

No existe una política de ciberseguridad para las Fuerzas Armadas ecuatorianas, que permita resguardar la seguridad de los usuarios del ciberespacio, proteger la seguridad digital de nuestra institución, promover la colaboración y coordinación entre instituciones y gestionar los riesgos del ciberespacio.

Formulación del Problema

En vista de que los sistemas y métodos de seguridad cibernéticos pueden ser definidos en la institución Militar, partiendo de estrategias y políticas desarrolladas en los objetivos institucionales y en varios niveles de abstracción, con una estructura

coherente para gestionar de manera sistemática los riegos y amenazas cibernéticas, se presenta a manera de interrogante el siguiente problema de investigación:

¿En qué medida incide una política de ciberseguridad en la protección de la información digital de las Fuerzas Armadas, específicamente en la Fuerza Terrestre?

Antecedentes

Países líderes en tecnología han tenido diversos ataques cibernéticos en todos los campo y el Ecuador no ha sido la excepción, se han dado ataques a páginas del gobierno y en semanas anteriores se confirmó el ataque a una área de defensa de la Fuerza Aérea, donde se pone en manifiesto la importancia de disponer de estrategias y de organismos que se encarguen de controlar los diferentes tipos de amenazas en el campo de ciberseguridad y ciberdefensa, ya que en nuestro país se observa una gran cantidad de situaciones que ponen en discrepancia el accionar de la seguridad informática por las siguientes razones:

La Secretaria General de la Administración Pública según acuerdo ministerial número 119, publicado en registro oficial número 139 del 1 de agosto de 2007, dentro de sus atribuciones y responsabilidades está “Preparar proyectos de leyes y reglamentos para la regulación, control, evaluación y seguimiento de los proyectos informáticos; así como para el acceso a la información” (Presidencia de la República, 2008).

Desde agosto de 2007 durante los años siguientes no se realizó ninguna gestión por parte de la Secretaría General de la Administración Pública misma pasó a llamarse Secretaría Nacional de Administración pública. La SNAP, juntamente con el Ministerio de Telecomunicaciones y la Secretaría Nacional de Inteligencia, conformaron la Comisión para la Seguridad Informática.

Dicha comisión tiene dentro de sus atribuciones “establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional”, como tal estableció el Esquema Gubernamental de Seguridad de la Información que debía ser implementado en su totalidad en febrero de 2015 en todas las instituciones públicas (Acuerdo Ministerial 166, 2013).

Sin embargo, en los Acuerdos Ministeriales 119 y 166 mencionados no se establecen responsabilidades directas de acción para lo que es la Ciberseguridad y la Ciberdefensa, solo se estableció que en base a la IS0 27000 las instituciones del estado deben regirse a las mencionadas políticas de seguridad que da la norma.

En tal consecuencia a nivel del Estado Ecuatoriano se está trabajando en temas de la seguridad de la información en forma aislada y no coordinada, la Secretaria Nacional de Inteligencia tiene un ente de Ciberinteligencia, la Policía Nacional creo una Unidad de Cibercriminal y todo esto se ha realizado sin un ente que lidere los esfuerzos.

Justificación

Es necesario formular una política de ciberseguridad en Fuerzas Armadas que desde una perspectiva de política institucional incorpore en sus procesos críticos niveles de seguridad en el ciberespacio según estándares nacionales e internacionales, permitiendo de esta manera resguardar la seguridad de los usuarios del ciberespacio, proteger la seguridad digital de nuestra institución, promover la colaboración y coordinación entre instituciones y gestionar los riesgos del ciberespacio.

A nivel nacional, el desafío para nuestras Fuerzas Armadas es contar con una política de ciberseguridad que oriente las acciones de nuestra institución armada en materia de ciberseguridad, junto con implementar y poner en marcha las medidas que sean necesarias para proteger la seguridad de los usuarios del ciberespacio,

considerando estrategias educativas orientadas al autocuidado y prevención en ambiente digital.

Importancia

De lo descrito se determina que la importancia de una política de ciberseguridad para las Fuerzas Armadas es necesaria para:

- Resguardar la seguridad de las personas en el ciberespacio
- Proteger la seguridad de la institución armada
- Promover la colaboración y coordinación entre instituciones
- Gestionar los riesgos del ciberespacio

Una política de ciberseguridad para las Fuerzas Armadas entrega orientaciones y líneas de acción de aplicación general para la implementación y evaluación de diversas actividades tendientes a minimizar estos riesgos y amenazas del ciberespacio en nuestra institución, las cuales se deberán implementar en procura de mantener y preservar la seguridad institucional.

Esta política permitirá el cumplimiento y accionar adecuado de las actividades dentro de nuestra institución en el campo jurídico, en el área técnica, área organizacional, junto con la creación de capacidades y cooperación con las diferentes instituciones encargadas de la seguridad de datos.

Objetivos

Objetivo General

Proponer una política de ciberseguridad para proteger la información digital de Fuerza Armadas, mediante la colaboración y coordinación con las instituciones responsables de la seguridad informática en el país.

Objetivos Específicos

a. Describir las vulnerabilidades, amenazas, delitos informáticos y definiciones más importantes en el campo de la ciberseguridad.

b. Analizar las políticas de ciberseguridad de los diferentes países y el marco legal de nuestro país referente a la ciberseguridad.

c. Establecer las políticas de ciberseguridad para Fuerzas Armadas, utilizando un modelo de madurez de capacidad de ciberseguridad y los ejes propuestos por el MINTEL (Ministerio de Telecomunicaciones).

Capítulo II

Marco teórico

Antecedentes Investigativos

Una vez determinada la falta de una política de Ciberseguridad en las Fuerzas Armadas de nuestro país, se realizó un acercamiento al Departamento de Ciberseguridad del CC.FF. AA para recibir los lineamientos necesarios que permita iniciar con nuestra investigación.

A través de este departamento se obtuvo la información de Políticas de Ciberseguridad de varios países entre los que tenemos: Argentina, Uruguay, Chile, Colombia y Paraguay donde podemos evidenciar la importancia que estos Estados dan a la seguridad informática, haciendo conciencia que todo país debe estar al día en materia de seguridad más aun una institución como la nuestra que es responsable de la seguridad, porque cualquier error o ataque exitoso puede vulnerar el bienestar y los derechos de los ciudadanos, afectar intereses particulares y comunes, afectar información calificada que ponga en peligro el cumplimiento exitoso de las operaciones militares.

Mediante esta investigación se considera el desarrollo de una política de ciberseguridad para proteger la información calificada de Fuerzas Armadas.

Fundamentación Teórica

Durante el desarrollo de nuestra investigación se ha considerado como base para una fundamentación teórica, fuentes de información como textos relacionados a la Ciberdefensa, información digital a través de la herramienta del Internet, experiencias de profesionales en este campo.

Políticas de Ciberseguridad

Introducción

Es un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad, son lineamientos que protegen a los usuarios privados y públicos contra posibles acciones de violación de fuentes de datos, junto con la protección de la privacidad de los ciudadanos.

La Ciberseguridad ha adquirido una relevancia cada vez mayor en las agendas de los gobiernos y de las instituciones tanto públicas como privadas, pasando de ser un tema de exclusiva incumbencia de los técnicos del área de la informática, a un foco de política pública en donde intervienen académicos, empresas, periodistas, políticos y miembros de la sociedad civil. Los ataques informáticos de gran escala, cada vez más sofisticados y frecuentes, han transformado a la Ciberseguridad en un tema de interés para la opinión pública, prioritario para el mantenimiento del modelo de negocios de las empresas que dependen de la red y de relevancia estratégica para los gobiernos (Viollier & Martínez , 2013).

Importancia de una Política de Ciberseguridad

Consideramos que una política de Ciberseguridad en un estado o en una institución es fundamental por las siguientes razones.

Es necesario resguardar la seguridad de las personas

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

Para proteger la seguridad de un país o de una institución

Es necesario promover el resguardo de las redes y sistemas informáticos del sector público y privado, especialmente aquellas que son esenciales para el adecuado funcionamiento del país, velando por la continuidad operacional de los servicios básicos.

Promover la colaboración y coordinación entre instituciones

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

Para gestionar los riesgos del ciberespacio

Es necesario considerar el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de las capacidades para la prevención y la recuperación ante incidentes de Ciberseguridad que se presenten, configurando un ciberespacio estable y resiliente.

La Ciberseguridad

Introducción a la Ciberseguridad

En la actualidad el desarrollo tecnológico alcanzado por la humanidad ha acortado distancias, tiempos de comunicaciones y velocidad de trasmisión de datos alrededor del mundo, convirtiéndose en un factor primordial para el desarrollo de las naciones, afectando las costumbres y tradiciones de las sociedades e incluso la doctrina de las Fuerzas Armadas.

La Ciberdefensa y Ciberseguridad se han convertido en áreas claves de los estudios estratégicos. Desde el análisis de Vargas, su desarrollo actual coincide con el advenimiento de la sociedad de la información, las redes entre computadoras y el fenómeno “Internet”, cuya expansión ha configurado la quinta dimensión de la guerra moderna y ha afectado sensiblemente la vida cotidiana de los diversos actores en el mundo global. De hecho, su estudio se convierte en una tarea obligada para la conducción político-estratégica de la defensa de las naciones. En el Ecuador, dichas temáticas (ampliamente discutidas) se han focalizado en una dimensión pragmática (Vargas, 2017).

De acuerdo con Castro hoy en día la soberanía de los Estados a nivel mundial ha sido quebrantada a través de los medios tecnológicos, afectando la infraestructura crítica que en algunos casos ha logrado niveles alarmantes de daños a través de ataques cibernéticos que podrían paralizar su sistema financiero, sistema eléctrico, sistema de comunicaciones, sistemas de armamento de las Fuerzas Armadas, sistemas hidrocarburíferas, 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 (Catro, 2015).

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 (Vargas, 2017).

Amenazas y Vulnerabilidades Existentes en el Ciberespacio

La Seguridad Nacional se puede ver comprometida por elementos de muy diversa índole según su naturaleza geopolítica, tecnológica, económica o social, entre otras. Esta Estrategia distingue entre amenazas, que comprometen o pueden socavar la Seguridad Nacional, y desafíos que, sin tener de por sí entidad de amenaza, incrementan la vulnerabilidad, provocan situaciones de inestabilidad o pueden propiciar el surgimiento de otras amenazas, agravarlas o acelerar su materialización. En el mundo actual, tanto las amenazas como los desafíos suelen estar interconectados y sus efectos traspasan fronteras. (Departamento de Seguridad Nacional, 2017).

Análisis de amenazas.

Para realizar un análisis de amenazas, se define a todo elemento o acción capaz de atentar contra la seguridad de la información donde uno o más eventos que proporcionan información puede sufrir una degradación de su seguridad en cualquiera de sus dimensiones: confidencialidad (acceso, difusión, observación, copiado, robo),

integridad (modificación, sustitución, reordenamiento, distorsión) o disponibilidad (destrucción, daño, contaminación, dejar fuera de servicio).

Dentro de las amenazas existentes en el ciberespacio podemos mencionar los siguientes:

Conflictos armados. Esta se mantiene como una de las amenazas más significativas para la Seguridad Nacional, especialmente en el actual contexto de tensión geopolítica, competición y fragmentación del orden internacional. El aumento de las capacidades de proyección militar, terrestre, aérea y naval, de diversos Estados, así como de capacidades en otros dominios como el ciberespacio o el espacio aéreo y ultraterrestre, es una de las tendencias asociadas a dicho contexto (Amenazas y Desafíos para la Seguridad Nacional, 2017).

Crimen organizado. Es una amenaza de naturaleza transnacional, flexible y opaca. Se trata de un fenómeno con una enorme capacidad desestabilizadora, que contribuye a debilitar el Estado y mina la buena gobernanza económica. Entre sus manifestaciones más graves se pueden mencionar los tipos delictivos relacionados con la trata de seres humanos o con los tráficos ilícitos de diversa índole, además del blanqueo de capitales y el uso de paraísos fiscales, esta amenaza amplía sus horizontes a través del empleo de la tecnología, recurso creciente para desarrollar actividades delictivas. (Amenazas y Desafíos para la Seguridad Nacional, 2017).

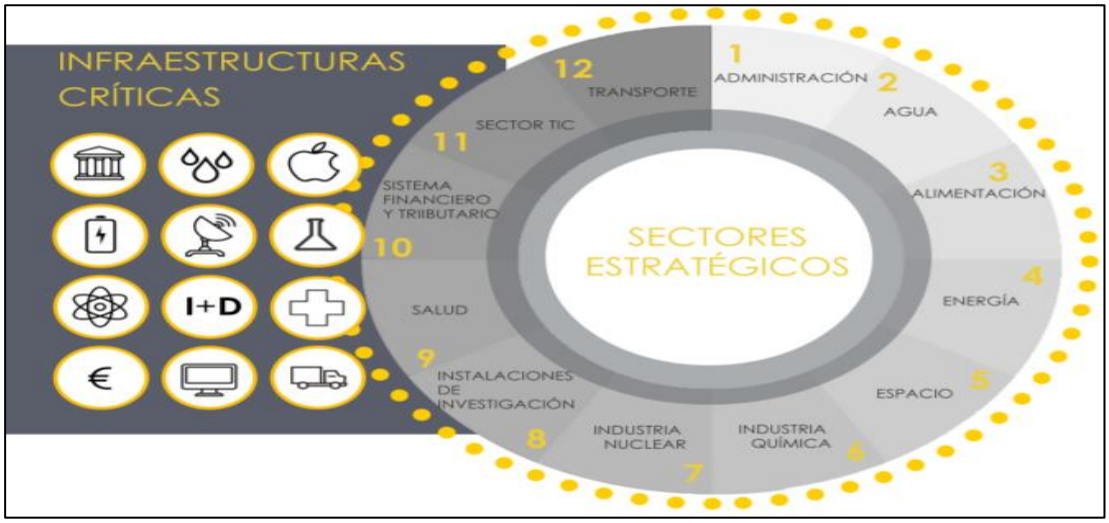
Espionaje. Es una amenaza de primer orden para la seguridad, que se ha adaptado rápidamente a las posibilidades que ofrece la tecnología moderna. En este sentido el ciberespacio juega hoy un papel más relevante a nivel de espionaje y es utilizado por Estados, grupos o individuos que usan sofisticados

programas que proporcionan acceso a ingentes volúmenes de información y datos sensibles. Ante esta fenómeno resulta necesaria la mejora de las capacidades tecnológicas y de inteligencia para aplicar una respuesta eficaz (Amenazas y Desafíos para la Seguridad Nacional, 2017).

Infraestructura crítica. Son aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas (Figura 1). Las infraestructuras estratégicas incluyen las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información y de la comunicación sobre las que descansa el funcionamiento de los servicios esenciales. Los servicios esenciales son necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento del sector público.

Figura 1

Infraestructuras críticas



Nota. El gráfico representa los sectores estratégicos que considera el Ecuador. Tomado de *Amenazas y desafíos para la seguridad nacional,* Departamento de Seguridad Nacional 2017.

En el último período se han observado diversas amenazas en el ciberespacio, manifestadas en ciberataques, las cuales de acuerdo con su objetivo pueden agruparse en: ciberespionaje, ciberterrorismo y/o cibercrimen (Sancho, 2010) Asimismo, de acuerdo con Fojón y Sanz quienes realizan las ciberamenazas pueden clasificarse de acuerdo a su “autoría e impacto en las siguientes categorías: Ataques patrocinados por Estados; Terrorismo extremismo político e ideológico; Ataques del crimen organizado; Ataques de perfil bajo” (realizados por personas con conocimiento especializado en TIC por motivos personales) (Fojón & Sanz, 2010). La manera en que estas organizaciones, grupos o personas pueden desarrollar un ciberataque es variada, entre las que destacan:

El virus Stuxnet

Atacó a computadoras que controlaban los reactores nucleares de Irán, el cual ha sido denominado como “una de las piezas de software malicioso más sofisticadas que existen” (Sancho, 2010).

Los ataques DDoS (Distributed Denial of Service)

Los ataques fueron entre fines de los 90´s e inicios del siglo XXI, “funcionan enviando una avalancha de gigabytes de tráfico a una determinada red, generando cuellos de botella en firewalls, enrutadores y en las mismas conexiones, hasta que estos colapsan. Cualquier acceso al servicio es entonces denegado y nadie puede acceder a la página. Otra forma de hacerlo es enviando miles de peticiones de servicio por segundo. Cuando el servidor receptor intenta procesarlo todo se bloquea rápidamente y se cierra, y la página queda fuera de combate”, el movimiento social Anonymus ha realizado ataques con esta técnica y también han sido objeto de ataque con la misma (Sancho, 2010).

Botnets “(Robots de la red)

Son redes de ordenadores zombis que se emplean para realizar ataques, envíos masivos de correos basura y espionaje contra empresas, infectando ordenadores sin que sus propietarios lo sepan. Cada máquina reclutada por el virus se pone en contacto sigilosamente con el cibercriminal a la espera de sus órdenes. Éstos son usados frecuentemente para fraudes de empresas, bancarios y publicitarios (Sancho, 2010).

Zeus

Es un virus de tipo botnet (troyano) que se propaga por los navegadores, tanto Explorer como Firefox. Por medio de la recopilación de datos del usuario y sus contraseñas, suplanta su identidad y roba datos financieros y/o envía spam. Dentro de los ataques de perfil bajo las amenazas más comunes en el ámbito informático, se hacen presentes por fraudes, robos o virus, y pueden ser resumidos en las siguientes amenazas (Sancho, 2010).

Malware

Son códigos diseñados por ciberdelincuentes cuyo objetivo es el de variar el funcionamiento de cualquier sistema informático, sobre todo sin que el usuario infectado se dé cuenta. Tienen la capacidad de corromper los archivos que haya guardado en el disco duro o incluso destruir determinados archivos (Oceano IT, 2014).

Spyware

Se trata de un software espía que tiene la capacidad de recopilar información de un ordenador y transmitirla sin el conocimiento de la persona afectada, poniendo en peligro la seguridad del ordenador afectado (claves, cuentas de correo, cuentas bancarias, *etc*. (Oceano IT, 2014).

Ransomware

Tanto para ordenadores como para teléfonos móviles, es una de las amenazas que más está creciendo últimamente. Un programa bloquea cualquiera de estos dos dispositivos con un mensaje en el que se pide un rescate para que el usuario pueda volver a recuperar el control. Se le exige un rescate en Bitcoin para que no pueda ser rastreada la persona o personas que han lanzado esta amenaza (Oceano IT, 2014).

Phishing

Es otra de las grandes amenazas actuales y llega mediante correo electrónico. Mediante ingeniería social o con webs que simulan a la perfección ser webs auténticas se consigue adquirir información confidencial de forma fraudulenta (Oceano IT, 2014).

Troyanos

En este caso, se trata de un programa que cuando se ejecuta, proporciona al atacante la capacidad de controlar el equipo infectado de forma remota y en muchas ocasiones sin el conocimiento del usuario (Oceano IT, 2014).

Gusanos

Pueden replicarse bajo mil y una formas diferentes en nuestro sistema, y hacer que desde nuestro ordenador se envíe un gran número de copias de sí mismo a muchos otros equipos mediante el correo electrónico a nuestros contactos y éstos a los suyos, convirtiéndose en una seria amenaza (Oceano IT, 2014).

Backdoor o puerta trasera

En ocasiones, algunos programadores maliciosos dejan una puerta trasera para así poder evitar los sistemas de seguridad de acceso para poder acceder al sistema con total comodidad y sin conocimiento de los usuarios (Oceano IT, 2014).

Análisis de vulnerabilidades

Para comprender las vulnerabilidades existentes en el ciberespacio es necesario considerar lo relativo a las ciberamenazas las mismas que son crecientes en la actualidad, los Estados persiguen la expansión de sus intereses geopolíticos a través de acciones de carácter ofensivo y subversivo, como de organizaciones terroristas, grupos de crimen organizado y actores individuales. Estos grupos aprovechan el carácter anónimo que el ciberespacio ofrece para conseguir sus fines a un mínimo coste y asumiendo un riesgo menor dada la dificultad de atribución. El robo de datos e información, los ataques ransomware y de denegación de servicios, el hackeo de dispositivos móviles y sistemas industriales y los ciberataques contra las infraestructuras críticas son ejemplos de ciberamenazas (Departamento de Seguridad Nacional, 2017).

La utilización del ciberespacio como medio para la realización de actividades ilícitas, acciones de desinformación, propaganda o financiación terrorista y actividades de crimen organizado, entre otras, impacta en la Seguridad Nacional, amplificando la complejidad y la incertidumbre, y también pone en riesgo la propia privacidad de los ciudadanos (Figura 2).

Figura 2

Vulnerabilidades del ciberespacio

Nota. El gráfico representa las vulnerabilidades del ciberespacio. Tomado de *Amenazas y desafíos para la seguridad nacional,* Departamento de Seguridad Nacional 2017.

Las vulnerabilidades se consideran como una debilidad en la seguridad de un entorno que puede llegar a permitir o facilitar la actuación de una amenaza; las vulnerabilidades pueden ser de naturaleza técnica, procedimental u operacional. Habitualmente, en el ámbito TIC, la vulnerabilidad suele ir asociada a un defecto en el software o en la configuración del mismo que puede permitir que se materialice una amenaza. En este sentido podemos describir los entornos tecnológicos que pueden constituirse elementos del ciberespacio y donde se pueden generar vulnerabilidades los cuales son descritos en la Figura 3.

Figura 3

Elementos del ciberespacio

Nota. El gráfico representa como está conformado el ciberespacio. Tomado de Machin, 2016.

Delitos informáticos cometidos en el ciberespacio

El constante desarrollo tecnológico que tiene la sociedad supone una evolución en las formas de delinquir, dando lugar, a nuevos métodos de delitos tradicionales como también a través de medios digitales. Dado esta evolución se ha creado muchos sistemas interactivos online y de tratamientos en tiempo real. Estos sistemas se han visto la necesidad de implementar contraseñas identificativas de usuarios para controlar y restringir el acceso a los datos. (Acurio, 2005).

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto.

Según Davara, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (Acurio, 2005).

Según Miguel Estrada, cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo (Acurio, 2005).

Según María José Viega, toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma (Acurio, 2005).

Según Julio Téllez, las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y las actitudes ilícitas en que tienen las computadoras como instrumento o fin. (Acurio, 2005).

Partiendo de esta compleja situación y tomando como referencia el “Convenio de Ciberdelincuencia del Consejo de Europa”, se puede definir los delitos informáticos como: “los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos”.

Las características principales de los delitos informáticos son:

- Sólo una determinada cantidad de personas pueden llegar a cometerlos.
- El sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional (Acurio, 2005).
- Provocan pérdidas económicas.
- Son muchos los casos y pocas las denuncias.

- Presentan grandes dificultades para su comprobación, por su carácter técnico.
- Tienden a proliferar, por lo que se requiere su urgente regulación legal (Acurio, 2005)
- Delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas (Acurio, 2005).
- Actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.” (Acurio, 2005)
- Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución” (Acurio, 2005).

La investigación de los delitos informáticos cometidos en el ciberespacio, es un problema excesivamente complejo, ahora es posible que un país sea vulnerado por un enemigo o por la ciberdelincuencia en sus redes e infraestructuras informáticas desde cualquier parte del planeta, como veremos en los siguientes párrafos.

- La infraestructura crítica en el 2017 fue el área primordial para los ataques cibernéticos y se considera que no solo abarca la red eléctrica, sino que también incluye los sectores de defensa y salud, procesos de fabricación cruciales, producción de alimentos, agua y transporte, un acontecimiento claro es el de enero de 2017 donde las amenazas a infraestructuras críticas fueron noticia cuando un informe de Reuters aseguró que el corte de energía eléctrica en Ucrania "fue un ataque cibernético" (BBC Mundo, 2018).
- Otra área que ha sufrido ataques cibernéticos es la democracia esto se pudo notar en La inclusión de la tecnología en los procesos electorales era cuestión de tiempo, especialmente considerando las razones por las que algunos países (como Argentina, Brasil, Alemania o Estados Unidos) decidieron implementar en alguna medida el voto electrónico donde el problema empieza cuando no se complementan,

sino que se reemplazan comprometiendo por completo al sistema de voto al ser posible quebrar completamente el carácter secreto de los votos (Acurio, 2005).

- Los hackers han conseguido robar propiedad intelectual o información clave de empresas u organismos estatales, muchas veces los afectados ni siquiera se enteran de que han sido víctimas de una sustracción, porque es posible penetrar una red y asumir el rol de administrador autorizado sin activar alarmas, toda infiltración se puede oscurecer o borrar.
- Los dispositivos que se conectan a Internet son fabricados por múltiples empresas, por lo que se pierde el control sobre lo que realmente contienen, otro tanto sucede con la elaboración de los programas informáticos, en su creación intervienen varias personas y compañías, por lo que los “errores” de programación permiten a los hackers penetrar los softwares y crear formas de engañar los sistemas.
- El Internet tiene un diseño que no estaba pensado para todos los usos que ahora se aplican en los sistemas TIC, como en el gobierno, educación y comercio electrónico, todas las capacidades que tienen ahora los celulares, los servicios públicos, gestión de infraestructuras de manera remota, donde los dispositivos inteligentes tienen la aptitud de espiar con imagen y sonido a sus usuarios por lo que esto permite adquirir una progresiva complejidad y esto nos vuelve más vulnerables, además las aplicaciones tienen muy diversas variables, lo que imposibilita controlar todas sus funciones.

Definiciones más importantes en el campo de la ciberseguridad

Ciberseguridad

La Unión Internacional de Telecomunicaciones (UIT), aprobó una definición de ciberseguridad tal como se expresa en la Recomendación UIT–T X.1205, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos,

acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno" (UIT-T X.1205, 2008).

La palabra seguridad proviene del latín *securitas* que a su vez se deriva de *securas (*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. (ConceptoDefinicion, 2016).

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, la evolución de los procesadores digitales luego de pasar por el ámbito militar y los centros de investigación científica hizo accesibles a los individuos de las empresas y los hogares las computadoras personales. Dispositivos que al vincularse en red producen un sistema interconectado a escala planetaria. Estos recursos combinados generan el "NUEVO MUNDO", 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 (EcuRed, 2012).

Ciberespacio: Es el espacio real y existente, invisible a los ojos, por el que transita el 90% de la información que emplea el mundo, transformada en los simples objetos de conocimiento u órdenes de ejecución de actividades, haciendo uso de la inteligencia artificial. Algunos entienden que es un espacio virtual mundial, que interconecta sistemas de información, dispositivos móviles y sistemas de control de procesos de todo tipo, industrial, empresarial, suministro de agua, energía eléctrica, gas, sistemas bancarios, y todos los servicios de los que hace uso la sociedad en su vida diaria con proyección de futuro. Esta soporta por comunicaciones en Internet, redes de telefonía móvil, el sistema satelital y telecomunicaciones y sistemas clásicos de comunicación física (Stel, 2014).

Ciberamenaza

Es el grado de certeza que poseen los Estados o particulares, de que sus infraestructuras críticas o sistemas vitales empleados para el desarrollo de la vida en sociedad, presentes en el ciberespacio, pueden ser atacados por organizaciones estatales encubiertas o no, por organizaciones particulares privadas o por individuos interesados en hacer daño (Stel, 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 (Conpes 3701, 2011).

Ciberguerra

Es el conflicto bélico que utiliza el ciberespacio como escenario principal, en lugar de los campos de batalla convencional. También se podría definir como el conjunto de acciones que se realizan para producir alteraciones en la información y los sistemas del enemigo, a la vez que se protege la información y los sistemas del atacante (Cubeiro, 2016).

Ciberataque

Según la publicación conjunta del Departamento de Defensa de los Estados Unidos de América, engloba toda acción llevada a cabo a través de las redes informáticas para interrumpir, denegar o destruir la información o las propias redes y ordenadores que la manejan (Cubeiro, 2016).

Ciberataque es la producción de daños físicos, en claro paralelismo con el concepto de “ataque armado”. “Un ciberataque es una operación tanto ofensiva como defensiva, en la que razonablemente puede esperar que cause daño o la muerte de personas o la destrucción de objetivos” (Schmitt, 2013).

Ciberinteligencia

La inteligencia es el producto obtenido de la recolección, evaluación, análisis, integración e interpretación de toda la información disponible, potencialmente significativa y que permita su transformación en conocimiento, de forma que resulte útil al decisor a la hora de tomar sus decisiones con el menor nivel de incertidumbre posible, siguiendo el ciclo de Inteligencia. En cuanto la Ciberinteligencia se refiere a las

actividades de inteligencia en los procesos de la ciberseguridad que se ocupan de analizar (Intenciones-oportunidades de los ciberactores y prevenir, identificar, localizar y atribuir ataques o amenazas a través del ciberespacio (Asint360, 2016).

Hacker

Etimológicamente, la palabra hacker deriva del vocablo inglés “hack” (cortar, golpear), a mediados de los 60, el término comenzó a formar parte de la cultura informática al ser utilizado para definir un perfil de conocimiento y capacidad con las computadoras que tenían determinadas personas. Llegando a concluir que un hacker es una persona que por sus avanzados conocimientos en el área de informática tiene un desempeño extraordinario en el tema y es capaz de realizar muchas actividades desafiantes e ilícitas desde un ordenador (Castro, 2015).

Sistemas de variables

Políticas de seguridad

Ciberseguridad

Hipótesis

Una política de ciberseguridad en las Fuerzas Armadas promueve un ciberespacio libre, abierto, seguro con capacidad de enfrentar adversidades que se presenten.

Tabla 1

Operacionalización de las variables.

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	INSTRUMENTO
		• Diagnóstico	• Aproximación del problema • Descripción de las amenazas	Guía de observación Cuestionario
		• Necesidad de una Política	• Resguardar la seguridad de las personas en el ciberespacio • Proteger la seguridad de la información digital • Proteger la seguridad de	Entrevista Cuestionario

1.Políticas de seguridad informática	Es un plan de acción para afrontar riesgos de seguridad, o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad.	• Ejes de la Política.	Fuerzas Armadas • Gestionar los riesgos del ciberespacio • Infraestructura de la información • Prevención y sanción • Sensibilización, formación y difusión • Cooperación y relaciones internacionales • Institucionalidad de la ciberseguridad	Guía de observación Entrevista Cuestionario

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	INSTRUMENTO
2. Ciberseguridad	Conjunto de acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propia y negarlo a terceros	• Incidentes de ciberseguridad relacionados con la información	• Espionajes • Fraudes • Robos de identidad	Guía de Observación Cuestionario
		• Incidentes de ciberseguridad relacionados con la infraestructura	• Infección por malware • Ataques contra redes	Guía de Observación Cuestionario

Capitulo III

Políticas de Ciberseguridad de los Diferentes Países y el Marco Legal de Nuestro País referente a la Ciberseguridad

Políticas de Ciberseguridad de los Países a Nivel Latinoamérica

Considerando la importancia que tiene una política de ciberseguridad para un Estado o para cualquier institución especialmente aquellas que tienen como misión la seguridad tanto interna como externa, los países a nivel mundial y en forma puntual en Latinoamérica dentro de sus políticas de estado han considerado la elaboración y puesta en práctica de una política de ciberseguridad para la convivencia pacífica y el normal desarrollo de sus pueblos.

A nivel de Latinoamérica podemos mencionar países como Colombia que es un referente en materia de ciberseguridad porque han sido supremamente juiciosos en la formulación de lineamientos de políticas que se encuentran plasmadas en dos documentos del “Consejo Nacional de Política Económica y Social (CONPES)” (Departamento Nacional de Planificación, 2011).

El primer documento CONPES, “Lineamientos de política para ciberseguridad y ciberdefensa”, de 2011, se concentró en contrarrestar las amenazas cibernéticas bajo los objetivos de la defensa del país y desde la lucha contra el cibercrimen. “La construcción de capacidad se hace al interior del sector defensa con tres instancias: a nivel del Ministerio de Defensa Nacional con el equipo de respuesta a emergencias cibernéticas de Colombia, el Centro Cibernético Policial de la Policía Nacional, y el Comando Conjunto Cibernético” (Departamento Nacional de Planificación, 2011).

El nuevo documento CONPES, “Política Nacional de Seguridad Digital”, de 2016, incluye la gestión del riesgo como elemento clave para avanzar hacia la seguridad digital”. “En el logro de un entorno seguro en Internet en el ciberespacio, hay

una cantidad de actores comprometidos; entre esos están por supuesto las entidades estatales, la empresa privada, la comunidad y los operadores de infraestructuras críticas" (Departamento Nacional de Planificación, 2011).

Chile de igual forma establece una Política Nacional de Ciberseguridad primer instrumento de política pública del Estado que orientará la acción del país en la materia, con el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente, ante esto el Ministerio de Defensa Chileno considera la Política Nacional de Ciberseguridad como un insumo imprescindible en el proceso de desarrollo de capacidades y políticas propias en la materia para el sector de la Defensa Nacional, que se materializarán en la próxima Política de Ciberdefensa y los contenidos del Libro de la Defensa que se encuentran en elaboración (National Cybersecurity Policy (NCSP), 2017).

Uruguay y específicamente sus Fuerzas Armadas como respuesta a las amenazas cibernética ha implementado El Centro de Respuesta a Incidentes de Seguridad Cibernética (DCSIRT) cuya función principal es la implementación de la Política de Gestión en Seguridad de la Información en el Ministerio de Defensa Nacional, fomentar el compromiso de buen uso del equipamiento e infraestructura informática, la política de gestión de riesgo y un plan de concienciación en Gestión de Seguridad de la información (Ministerio de Defensa Nacional, 2015).

La política de ciberseguridad brasileña se ha desarrollado en un contexto de creciente preocupación con el incremento en el número de ataques cibernéticos y por la capacidad del país de hacer frente a ellos, así como por la oportunidad de no quedar detrás de las principales potencias mundiales en el enfrentamiento de las amenazas cibernéticas. Brasil está en la lista de los países más golpeados por el cibercrimen tanto por origen de actividades criminales, como por el número de víctimas de esas actividades (Nathan, 2015).

Análisis de las políticas de ciberseguridad de los países que disponen de estas normas a nivel latinoamericano

Se analizarán las respuestas de los países latinoamericanos, que han adoptado estrategias relevantes de ciberseguridad en la región.

Las respuestas que analizaremos son Estatales, es decir que nos enfocaremos en ver cuáles son las instituciones estatales que se encargan de la ciberseguridad del país, de qué manera se gestionan los incidentes informáticos y si cuentan con políticas para desarrollar las acciones necesarias en la seguridad cibernética dentro del entorno digital.

CHILE

Para analizar y exponer las respuestas de Chile frente a las ciberamenazas, usaré el texto “BASES PARA UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD” determinando el campo de interés, lo ejes en los cuales agrupan las medidas de las políticas de seguridad, las instituciones que participan en la ciberseguridad y otras alternativas de solución a la seguridad informática.

Campos de interés

- En mención al análisis se determina que la política de ciberseguridad para Chile es necesaria para: i) resguardar la seguridad de las personas en el ciberespacio; ii) proteger la seguridad del país; iii) promover la colaboración y coordinación entre instituciones; iv) gestionar los riesgos del ciberespacio (Subsecretaría de Defensa Nacional del Ministerio de Defensa Nacional, 2015).
- La Política Nacional de Ciberseguridad en Chile agrupan las diversas medidas que, de acuerdo con estándares internacionales, se implementan en el marco de políticas de ciberseguridad:

- Infraestructura de la información.
- Prevención y sanción.
- Sensibilización, formación y difusión.
- Cooperación y relaciones internacionales.
- Institucionalidad de la ciberseguridad (Subsecretaría de Defensa Nacional del Ministerio de Defensa Nacional, 2015).

Instituciones Responsables

Los organismos encargados de la seguridad cibernética en Chile son el MISP y Secretaría Ejecutiva MDN.

COLOMBIA

Para analizar y exponer las respuestas de Colombia frente a las ciberamenazas, usaré el documento del CONPES “POLÍTICA NACIONAL DE SEGURIDAD DIGITAL 3854”, observando el campo de interés, lo principios en los cuales agrupan las medidas de las políticas de seguridad, las instituciones que participan en la ciberseguridad y otras alternativas de solución a la seguridad informática (Departamento Nacional de Planificación, 2011).

Campos de interés

Los campos de interés sobre los cuales trata de intervenir Colombia son los siguientes:

- Se establece un marco institucional, creando una máxima instancia de coordinación y control a la seguridad del gobierno además de establecer figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional (Departamento Nacional de Planificación, 2011).
- Se crearán las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas

mediante mecanismos de participación activa y permanente, adecuando el marco legal y regulatorio de la materia y brindando la capacitación para comportamientos responsables en el entorno digital (Departamento Nacional de Planificación, 2011).

- Se fortalece la defensa y seguridad digital a nivel nacional y transnacional con enfoque de gestión de riesgos.
- Se impulsa con un enfoque estratégico la cooperación, colaboración y asistencia en materia de seguridad digital nacional e internacional.

Políticas de Seguridad

A través de este documento la política de seguridad digital encamina su accionar incluyendo la gestión de riesgos como elemento más importante, esto lo hace a través de la siguiente propuesta: implementar un conjunto de principios en todos los niveles del Gobierno y de las organizaciones públicas; y adoptar una estrategia nacional para la gestión de riesgos de seguridad digital (Departamento Nacional de Planificación, 2011).

Principios generales:

- Conocimiento, capacidades y empoderamiento.
- Responsabilidad.
- Derechos humanos y valores fundamentales.
- Cooperación.

Principios operativos

- Evaluación de riesgos y ciclo de tratamiento.
- Medidas de seguridad.
- Innovación.
- Preparación y continuidad (Departamento Nacional de Planeación, 2011).

Dimensiones Estratégicas

- Gobernanza de la seguridad digital.
- Marco legal regulatorio de la seguridad digital.
- Gestión sistemática y cíclica de seguridad digital.
- Cultura ciudadana para la seguridad digital.
- Capacidad para la gestión de riesgo de seguridad digital (Departamento Nacional de Planificación, 2011).

Instituciones Responsables

Los organismos encargados de la seguridad cibernética en Colombia son los siguientes:

- Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ministerio de Defensa Nacional.
- Dirección Nacional de Inteligencia.
- Departamento Nacional de Planeación (Departamento Nacional de Planificación, 2011).

PARAGUAY

Para analizar y exponer las respuestas de Paraguay frente a las ciberamenazas, usaré el documento “Plan Nacional de Ciberseguridad República del Paraguay”, observando el campo de interés, lo principios en los cuales agrupan las medidas de las políticas de seguridad, las instituciones que participan en la ciberseguridad y otras alternativas de solución a la seguridad informática (Ministerio de Tecnologías de la Información y Comunicación, 2018).

Campos de interés

El campo de interés en Paraguay fija medidas de ciberseguridad en áreas prioritarias, apoyando el progreso y la innovación de las Tics en el país, este Plan Nacional se concentra en seis ejes de acción: Sensibilización y Cultura; Investigación,

Desarrollo e Innovación; Protección de Infraestructuras Críticas; Capacidad de Respuesta ante Incidentes Cibernéticos; Capacidad de Investigación y Persecución de la Ciberdelincuencia; y Administración Pública y Coordinación (MITIC, 2018).

Políticas de Seguridad

La política pública de ciberseguridad en Paraguay se orienta en los principios orientadores para la formulación e implementación de cualquier de cualquier política pública de ciberseguridad los cuales son:

- Proporcionalidad: las medidas deben ser adecuadas, necesarias, y proporcionales, respetando los derechos fundamentales.
- Coordinación de Esfuerzos y Uso Eficiente de Recursos Escasos: se debe adoptar la gestión de riesgo en la implementación de políticas de ciberseguridad, a fin de priorizar y justificar las acciones elegidas.

Responsabilidad Compartida: todos los agentes públicos y privados con responsabilidad en esta materia, incluyendo también a la sociedad civil, la academia y los ciudadanos, han de sentirse involucrados en la implementación de este Plan Nacional (MITIC, 2018).

Desarrollo e Innovación: se reconoce la importancia de la innovación para el desarrollo de una economía digital.

- Cooperación Internacional: el carácter transnacional de las amenazas hace que sea esencial promover la cooperación regional y global.
- Monitoreo y Evaluación: Se incorporará el monitoreo en las políticas públicas de ciberseguridad, con el fin de retroalimentar la gestión de las mismas y corregirlas eventualmente (MITIC, 2018).

Instituciones Responsables

- Secretaría Nacional de Tecnologías de la Información y Comunicación SENATICs.
- Equipo de Respuesta a Emergencias Cibernéticas – CERT-PY.
- Secretaría de Emergencia Nacional – SEN.
- Ministerio de Relaciones Exteriores – MRE.
- Ministerio de Justicia – MJ.
- Ministerio de Defensa Nacional – MDN.
- Ministerio del Interior – MI.
- Policía Nacional – PN.
- Ministerio de Hacienda – MH.
- Ministerio de Industria y Comercio – MIC.
- Ministerio de Obras Públicas y Comunicaciones – MOPC.
- Ministerio de Educación y Cultura – MEC.
- Ministerio Público – MP.
- Comisión Nacional de Telecomunicaciones – CONATEL.
- Consejo Nacional de Ciencia y Tecnología – CONACYT (MITIC, 2018).

Analizar el marco legal de nuestro país referente a la ciberseguridad

El presente trabajo analiza la construcción de políticas de ciberseguridad para Fuerzas Armadas a través de un análisis que permita definir un Marco de Seguridad Cibernética empleando para su tratamiento los siguientes preceptos teóricos:

El desarrollo de las tecnologías de la información y las telecomunicaciones multiplican las relaciones e interacciones sociales para la comunicación, intercambio de datos o desarrollo de negocios. Enmarcado dentro de esa tendencia, muchas infraestructuras críticas de la estructura militar ocupan el ciberespacio en sus procesos.

Este desarrollo conlleva riesgos asociados que al usar el ciberespacio afecta los derechos de las personas, las infraestructuras críticas de la información y los intereses vitales de Fuerzas Armadas a nivel nacional e internacional. Los riesgos pueden provenir de múltiples fuentes y resultar en fenómenos cuyas consecuencias pueden afectar de manera grave la seguridad interna e inclusive comprometer la seguridad externa de esta institución mediante actividades de espionaje y ciberataques llevados a cabo por grupos organizados o personas.

Según datos de European Network and Information Security Agency (ENISA), al año 2013 más de 35 países contaban con una Estrategia Nacional de Ciberseguridad (ENCS) y países como Holanda y Estonia ya llevan más de una versión. Otros países como por ejemplo el Reino Unido, cada año realiza un proceso de evaluación de esta estrategia, lo que ayuda al desarrollo y perfeccionamiento de la misma. Esto ha posibilitado que la comunidad internacional especializada presente importantes avances técnicos, doctrinarios y normativos, en los distintos foros existentes, tanto desde una perspectiva de seguridad internacional como seguridad interna de cada país (ENISA, 2014).

Nuestro país no es ajeno a la búsqueda de estrategias de políticas de ciberseguridad, de esta manera la Secretaría Nacional de Inteligencia, conjuntamente con otras instituciones como la SNAP, el Ministerio de Telecomunicaciones conformaron en el 2011 la Comisión para la Seguridad Informática.

Dicha comisión tiene dentro de sus atribuciones “establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional”, como tal estableció el Esquema Gubernamental de

Seguridad de la Información que debió ser implementado en su totalidad en febrero de 2015 en todas las instituciones públicas (Acuerdo Ministerial N.- 166, 2015).

Sin embargo, en los Acuerdos Ministeriales 119 y 166 mencionados no se establecen responsabilidades directas de acción para lo que es la Ciberseguridad, solo se estableció que en base a la IS0 27000 las instituciones del estado deben regirse a las mencionadas políticas de seguridad que da la norma.

Por su parte a nivel del Estado ecuatoriano se está trabajando en temas de la seguridad de la información en forma aislada y no coordinada, la Secretaria Nacional de Inteligencia tiene un ente de Ciberinteligencia, Fuerzas Armadas dispone de un área de ciberseguridad, la Policía Nacional creo una Unidad de Cibercriminal y todo esto se ha realizado sin políticas que lideren los esfuerzos de estas instituciones.

De lo descrito es necesario establecer responsabilidades directas de acción y definir Políticas institucionales en los temas concernientes a estos parámetros de defensa informática.

A continuación, describiremos el marco legal existente y que tiene relación con el tema de investigación, de acuerdo con el siguiente detalle.

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 (Contitución de la República del Ecuador 2008, 2008).

“Las Fuerzas Armadas tienen como misión fundamental la defensa de la soberanía y la integridad territorial” (Contitución de la República del Ecuador 2008, 2008).

La Constitución de la República contribuye a la misión fundamental que es la defensa de la soberanía, al estudiar sobre la implementación de una nueva capacidad

estratégica con la creación de un ente que controle la seguridad informática a nivel nacional permitiendo proteger la infraestructura crítica de las diferentes instituciones del estado.

Código Orgánico Integral Penal (COIP)

El Código Orgánico Integral Penal (COIP) entró en vigencia a partir del mes de agosto de 2014 incluyen artículos relacionados con los delitos contra la seguridad de los activos de los sistemas de información y comunicación que son sancionados con prisión siendo los siguientes:

- “Artículo 178: Violación a la intimidad: La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grave, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años” (Asamblea Nacional del Ecuador, 2014).
- Artículo 192: “Intercambio, comercialización o compra de información de equipos terminales móviles: La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años”). (Asamblea Nacional del Ecuador, 2014).
- Artículo 193: “Reemplazo de identificación de terminales móviles: La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será

sancionada con pena privativa de libertad de uno a tres años"). (Asamblea Nacional del Ecuador, 2014).

- Artículo 195: "Infraestructura ilícita: La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años" (Asamblea Nacional del Ecuador, 2014).
- Artículo 212: "Suplantación de identidad: La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años" (Asamblea Nacional del Ecuador, 2014).
- 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. (Asamblea Nacional del Ecuador, 2014)
- 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. (Congreso Nacional, 2004).

Capitulo IV

Propuesta de Políticas de Ciberseguridad para las Fuerzas Armadas

La propuesta que se plantea a continuación se acoge por un lado a las regulaciones estatales dictadas por el MINTEL (Ministerio de Telecomunicaciones de la Sociedad de la Información), a través del libro blanco de la sociedad de la información y del conocimiento en lo concerniente a los cinco ejes de acción, y por otro lado se emplea el modelo de madurez de capacidades de seguridad cibernética en cada una de sus etapas de formación, lo que me permitirá el manejo adecuado de la información en determinados momentos donde la institución interactúa en el ciberespacio.

Haciendo referencia al párrafo anterior, a continuación, se va a realizar una breve descripción de cada una de estas herramientas que hemos utilizado y desde las cuales se desprenden las políticas que proponemos.

Ejes propuestos por el MINTEL (Ministerio de Telecomunicaciones de la Sociedad de la Información)

El Ministerio de Telecomunicaciones a través del Libro Blanco de la Sociedad de la Información y del Conocimiento, busca el fortalecimiento de la sociedad de la información y del conocimiento mediante el desarrollo y explotación de las comunicaciones y de las Tecnologías de la Información y Comunicación (TIC), que permite a los Estados alcanzar un desarrollo en todos los aspectos con el propósito de dar una mejor calidad de vida a los ciudadanos (MINTEL-LB, 2018).

Esta entidad tiene como su principal Objetivo “Dar a conocer la estrategia que contribuirá al desarrollo de la Sociedad de la Información y del Conocimiento en el Ecuador, a fin de impulsar el crecimiento económico, la equidad e inclusión y la eficiencia de la administración pública” (MINTEL-LB, 2018), y para poder cumplir con este objetivo se propone los siguientes ejes:

- Infraestructura y conectividad.
- Gobierno Electrónico.
- Inclusión y habilidades digitales.
- Seguridad de la información y protección de datos personales.
- Economía digital y tecnologías emergentes). (MINTEL-LB, 2018).

Infraestructura y conectividad

Las últimas tendencias a nivel mundial debido al desarrollo de plataformas de acceso libre como Netflix, WhatsApp, Facebook entre otras, han obligado a las diferentes operadoras a invertir ingentes cantidades de dinero para actualizar sus equipos y de esta forma acoplar su tecnología (MINTEL-LB, 2018).

En Ecuador es necesario incrementar la infraestructura de las telecomunicaciones, para poder ampliar la cobertura de los servicios a nivel nacional (con especial atención en aquellos sectores de difícil acceso, logrando con ello eliminar todo obstáculo que retarde el desarrollo y el despliegue la infraestructura (Figura 4).

Gobierno Electrónico

La finalidad de este eje es lograr que el Gobierno se acerque cada vez más a sus ciudadanos mediante la utilización de las Tecnologías de la Información y Comunicación (TIC), poniendo énfasis en los grupos de atención prioritaria para que ellos puedan acceder a todos los servicios públicos utilizando los medios tecnológicos y de esta forma simplificar y disminuir la tramitología. (MINTEL-LB, 2018).

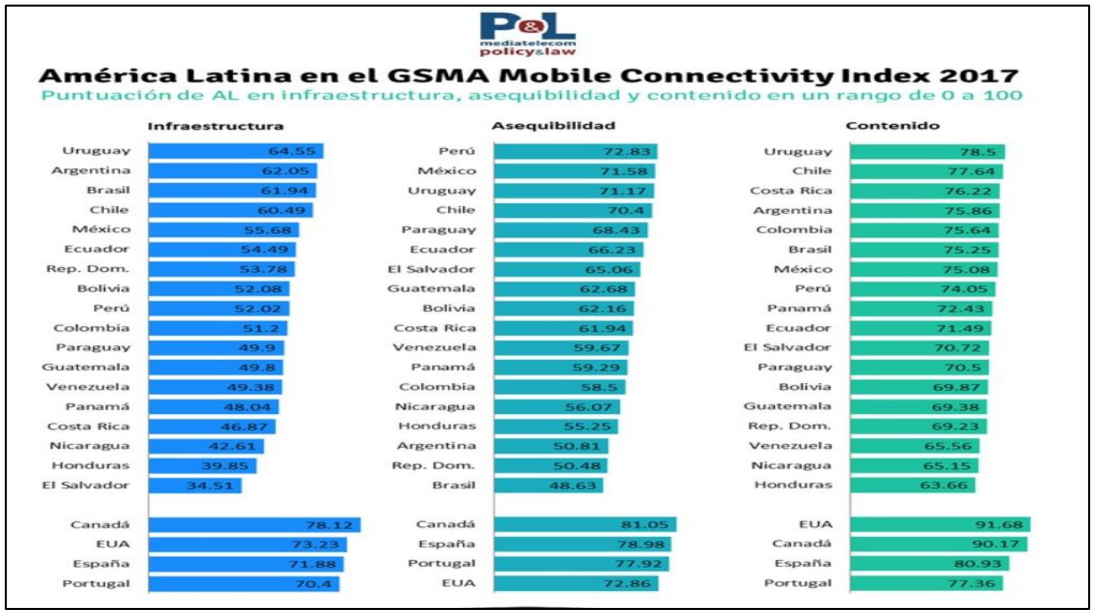
De acuerdo con la Secretaría Nacional de la Administración Pública (SNAP), existen 385 trámites 100% en línea, entregados por 38 instituciones; cabe destacar:

- La declaración de impuestos en línea, del Servicio de Rentas Internas (SRI).
- El sistema de comprobantes electrónicos, del SRI.

- a postulación a becas y ayudas económicas, de la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación.
- La obtención de certificados, de diversas instituciones.
- La certificación de firma electrónica, del Banco Central del Ecuador (BCE).
- La realización de trámites relacionados con la matriculación vehicular, del SRI
- El registro de proveedores y entidades contratantes, del Servicio Nacional de Contratación Pública (SERCOP). (MINTEL_PLAN, 2016).

Figura 4

Conectividad índex 2017



Nota. El gráfico representa en un rango de 0 a 100 la disponibilidad de cada país en infraestructura, asequibilidad y conectividad, Meditecom 2017.

Inclusión y habilidades digitales

Para el Ecuador este eje es de suma importancia, puesto que uno de los objetivos es permitir que sus ciudadanos puedan acceder a las ventajas que brindan las herramientas tecnológicas, de esta forma se contribuye a la democratización de las

herramientas TIC, no sólo en términos de acceso sino también en términos del uso que se les puede dar a las mismas, (MINTEL-LB, 2018).

El Estado pretende disminuir los porcentajes de personas que hasta la fecha no han tenido la oportunidad de tener acceso a una computadora, internet o un teléfono celular, buscando las estrategias necesarias mediante el desarrollo de habilidades digitales en el sistema educativo en el que se incluyen en los diferentes currículo de educación materias en ciencias y computación, también se pretende desarrollar habilidades digitales para los diferentes empleos y para impulsar nuevos negocios y emprendimientos digitales. Con esto se tiene como resultado un incremento en la utilización de las TIC (MINTEL-LB, 2018).

Seguridad de la información y protección de datos personales

El Índice Global de Ciberseguridad (GCI), emitido por la Unión Internacional de Telecomunicaciones (UIT), publicado en el 2017, ubicó al Ecuador en el puesto 66 de 193 países a nivel mundial, y lo posicionó en el sexto lugar entre los países de América Latina y el Caribe. (MINTEL-LB, 2018).

El GCI gira en torno a la Agenda de Ciberseguridad Global de la UIT (GCA) y sus cinco pilares: jurídico, técnico, organizativo, creación de capacidades y cooperación, siendo categorizado como intermedio en los tres primeros. Por esta razón, la encuesta del GCI consideró que Ecuador tiene un nivel intermedio de compromiso con la seguridad cibernética (MINTEL-LB, 2018).

Por otro lado, es importante mencionar que en la región 10 países cuentan con estrategias nacionales de ciberseguridad, gracias a la cooperación internacional recibida de parte de la Organización de Estados Americanos (OEA); por lo que resulta significativo que Ecuador dirija sus esfuerzos para construir su estrategia de ciberseguridad (MINTEL-LB, 2018).

Economía digital y tecnologías emergentes

En cuanto a Economía Digital se plantea su desarrollo a través de la Transformación Digital de las empresas, la evolución del Comercio Electrónico, el impulso de la innovación y emprendimientos de base tecnológica; así como, de la dinamización de la industria TIC y del aprovechamiento de las Tecnologías Emergentes (MINTEL-LB, 2018).

En referencia a las Tecnologías Emergentes, conforme las tendencias a nivel de la región, en la Agenda Digital eLAC2020 se recomienda a los países aprovechar su potencial para el desarrollo sostenible, proponiendo trabajar en los siguientes objetivos:

- Promover el diseño de políticas públicas apoyadas en la innovación basada en datos.
- Impulsar en las políticas públicas y diseño de servicios digitales el uso convergente de diferentes tipos de tecnologías emergentes.
- Promover servicios financieros digitales (MINTEL-LB, 2018).

Modelo de Madurez de capacidad de Seguridad Cibernética (CMM)

El Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM, por sus siglas en inglés) es una propuesta del Centro Global de Seguridad Cibernética de la Universidad de Oxford [XII] y fue incorporado por la OEA y por el BID en el estudio referido para hacer más accesible la comprensión de estos riesgos. (BID, 2016).

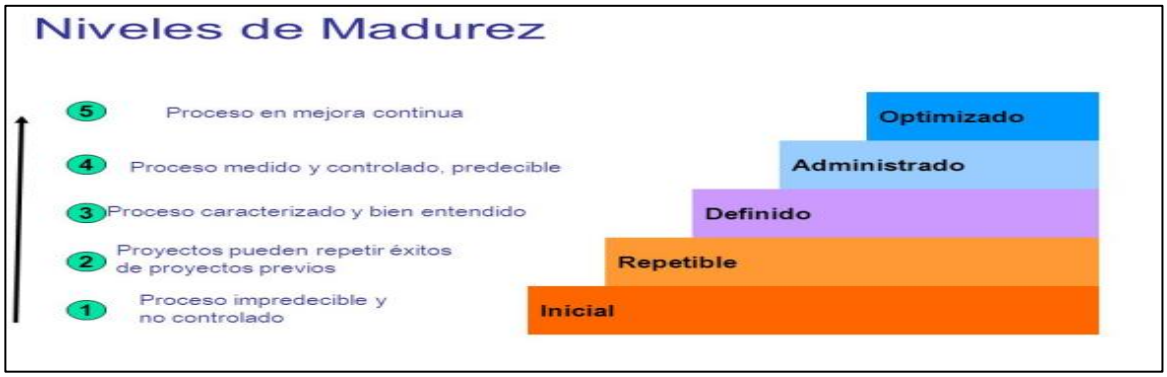
El CMM es un modelo único de desarrollo y cambio organizacional. Mientras una organización dada, progresa de un nivel al siguiente, su cultura es transformada a través de mejoras evolutivas de sus procesos. Cada nivel de maduración se caracteriza por la implementación e institucionalización de diversos grupos de prácticas (áreas de procesos) que contribuyen a la capacidad de desarrollo obtenida en aquel nivel. (BID, 2016).

Es necesario entonces poder determinar el grado de madurez de los procesos actuales e identificar los puntos claves en donde se deberán enfocar la atención de mejoras para sí lograr por una parte alcanzar la calidad del software y por otra la mejora de los procesos.

Llegando a concluir que un modelo de madurez de capacidades de seguridad cibernética es una estrategia de mejora, una señalización de deficiencias de una organización y una guía para poder avanzar hacia una cultura de calidad. Estableciendo para ello cinco niveles de madurez, niveles que son progresivos y no autónomos como se muestra en la Figura 5.

Figura 5

Niveles de madurez



Nota. El gráfico representa los niveles de madurez en forma ascendente (BID, 2016).

Cada dimensión ofrece una serie de factores e indicadores de capacidad cibernética para que una organización comprenda la etapa de madurez en la que se encuentra. Se han identificado etapas de madurez y éstas varían desde una etapa inicial, donde una organización puede que apenas haya comenzado a considerar la seguridad cibernética, hasta un escenario dinámico, donde una organización es capaz de adaptarse rápidamente a los cambios en el panorama de la seguridad cibernética en

lo relativo a las amenazas, las vulnerabilidades, los riesgos, la estrategia económica o el cambio de las necesidades organizacionales. (Rea & Sánches, 2017).

Un modelo de madurez, por lo tanto, proporciona un punto referencia con el que una organización puede evaluar el nivel actual de capacidad de sus prácticas, procesos y métodos, y establecer objetivos y prioridades para la mejora. Además, cuando un modelo es ampliamente utilizado en una industria en particular (y los resultados de la evaluación son compartidos), las organizaciones pueden comparar su desempeño con otras organizaciones. (Rea & Sánches, 2017).

Para medir la progresión, los modelos de madurez en seguridad típicamente tienen "niveles" a lo largo de una escala (algunos utilizan una escala de niveles de indicadores de madurez). Cada nivel de madurez está definido por un conjunto de atributos. Si una organización alcanza estos atributos, ha logrado tanto ese nivel como las capacidades que representa el nivel. (Rea & Sánches, 2017).

Inicial o Nivel 1

En este nivel se encuentran las instituciones que no tienen procesos definidos, no disponen de un ambiente estable para el desarrollo y mantenimiento de software. Aunque se utilicen técnicas correctas de ingeniería de software, los esfuerzos se ven minados por falta de planificación (Niurka & Hernández, 2007).

Repetible o Nivel 2

En este nivel se pretende repetir el éxito de los resultados alcanzados, la principal diferencia con el anterior nivel es que el proyecto es gestionado y controlado durante el desarrollo de este. El desarrollo no es opaco y se puede saber el estado del proyecto en todo momento (Niurka & Hernández, 2007).

Definido o Nivel 3

Este nivel significa que la forma de desarrollar proyectos (gestión e ingeniería) está por definir quiere decir que está establecida, documentada y que existen métricas (obtención de datos objetivos) para la consecución de objetivos concretos, se considera un nivel óptimo puesto que proporciona muchos beneficios y no ven la necesidad de ir más allá porque tienen cubiertas la mayoría de sus necesidades (Niurka & Hernández, 2007).

Cuantitativamente Gestionado/Administrado o Nivel 4

Se caracteriza porque las organizaciones disponen de un conjunto de métricas significativas de calidad y productividad, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El software resultante es de alta calidad (Niurka & Hernández, 2007).

Optimizado o Nivel 5

Los procesos de los proyectos y de la organización están orientados a la mejora de las actividades. Mejoras incrementales e innovadoras de los procesos que mediante métricas son identificadas, evaluadas y puestas en práctica (Niurka & Hernández, 2007).

Matriz de políticas de ciberseguridad aplicando los ejes de acción propuestos por el MINTEL y el modelo de madurez de capacidad de seguridad cibernética (CMM)

El MINTEL ha propuesto los ejes de desarrollo para la seguridad de la información digital y a través de la matriz que se propone podemos plantear diferentes políticas acordes a la conformación de las diferentes instituciones.

En las Fuerzas Armadas existen varios documentos como directivas, instructivos, normativas, manuales en los que se dispone el control y seguridad de la información, por lo que a través de esta matriz se busca administrar adecuadamente

estos documentos, acorde a la conformación, desarrollo, modificación de las diferentes áreas, unidades y demás instalaciones que evolucionan en el desempeño institucional militar.

En la matriz planteamos políticas para cada etapa de evolución institucional la cual está relacionada con los ejes propuestos por el MINTEL, la implementación de las mismas permitirá a nuestra organización fomentar un ambiente estable, permitiendo involucrar estrategias que manejen la nueva tecnología, causa principal de la inseguridad digital que acarrea diferentes desafíos, mismos son enfrentados y solucionados por las políticas enunciadas en la Tabla 2.

Tabla 2

Matriz de políticas de Ciberseguridad

EJES DE ACCIÓN (MINTEL)	**NIVEL CMM**	**POLÍTICAS**
EJE 1: Infraestructura y Conectividad	Inicial	- Asegurar la implantación de la normativa sobre Protección de las Infraestructuras Críticas con el fin de conseguir una seguridad que abarque tanto el ámbito físico como el tecnológico. Para ello, se evaluará la inclusión de las medidas de ciberseguridad oportunas en los distintos planes que se establezcan.
	Repetible	- Asegurar la plena implantación del Esquema de Seguridad y articular los procedimientos necesarios

		para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados.
	Definido	- Desarrollar y mantener actualizadas las instrucciones de prevención y detección, incluyendo procedimientos de respuesta frente a situaciones de crisis y planes de contingencia específicos ante incidentes de ciberseguridad, asegurando su integración en el Sistema de Seguridad institucional. (Gobierno de España, 2013) - Acceder a los sistemas de información, contando con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información institucional. Los niveles de seguridad de acceso deberán controlarse por un administrador único. - Delimitar responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes. - Acceder a Internet por medio del sistema de seguridad con cortafuegos incorporado, restringiendo accesos no pertinentes a través de la

		Red establecida para ello. No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.
	Cuantitativo gestionado	- Fomentar el desarrollo de productos y servicios en materia de ciberseguridad por medio de instrumentos, entre otros, como el Plan de Investigación Científica y Técnicas de evaluación y de Innovación e iniciativas
	Optimizado	- Reforzar la implantación y seguridad de la infraestructura común y segura en la institución, potenciando su uso y sus capacidades de seguridad y resiliencia. (Gobierno de España, 2013) - Optimizar el modelo de interconexión de los organismos de las Administraciones a las redes de voz y datos, maximizando su eficacia, disponibilidad y seguridad. (Gobierno de España, 2013)
	Inicial	- Impulsar el establecimiento de canales de información, detección y respuesta. (Gobierno de España, 2013)

EJE 2: Gobierno Electrónico		- Desarrollar un Marco de Conocimientos de Ciberseguridad en los ámbitos técnico, operativo y jurídico. (Gobierno de España, 2013)
	Repetible	- Asegurar la cooperación de las áreas con responsabilidades en ciberseguridad, en especial entre las Tics de las Fuerzas y el departamento de Ciberdefensa del Comando Conjunto de las Fuerzas Armadas. La organización institucional y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos, articulando los instrumentos adecuados a tal efecto (Gobierno de España, 2013) - Garantizar la coordinación, la cooperación y el intercambio de información entre las Fuerzas, las instituciones militares autónomas, las áreas locales, y los organismos competentes de la Universidad de Fuerzas Armadas para asegurar la permanente concienciación, formación y capacidad de respuesta a través del Sistema de Intercambio de Información y Comunicación de Incidentes. (Gobierno de España, 2013)

	Definido	- Impulsar la cooperación entre las diferentes instituciones que maneja información para la seguridad de un estado, promoviendo el intercambio de información sobre vulnerabilidades, ciberamenazas y sus posibles consecuencias, especialmente en lo relativo a la protección de los sistemas de interés nacional (Gobierno de España, 2013)
	Cuantitativo gestionado	- Impulsar modelos y técnicas de análisis de ciberamenazas y medidas de protección de productos, servicios y sistemas, así como su especificación, evaluación y certificación.
	Optimizado	- Promover la cooperación con diferentes instituciones y los servicios de la ciberseguridad, con el fin de mejorar conjuntamente las capacidades de detección, prevención, respuesta y recuperación frente a los riesgos de seguridad del ciberespacio, impulsando la participación activa de los proveedores de servicios, así como el desarrollo y adopción de códigos de conducta y buenas prácticas.

EJE 3: Inclusión y habilidades digitales	Inicial	- Implantación de Certificación de habilidades digitales para emprendimiento institucional militar en tecnologías de información.
	Repetible	- Potenciar la creación, difusión y aplicación de las Mejores Prácticas en materia de Ciberseguridad en el ámbito de la Administración informática de una Institución (Gobierno de España, 2013)
	Definido	- Extender y ampliar los programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con Universidades y centros especializados (Gobierno de España, 2013)
	Cuantitativo gestionado	- Desarrollar y ejecutar un Programa de Ejercicios de Simulación de Incidentes de Ciberseguridad, para evaluar y perfeccionar las acciones llevadas a cabo en este ámbito (Gobierno de España, 2013) - Impulsar las actividades de certificación de ciberseguridad de acuerdo con las normas y estándares de reconocimiento internacional, incluyendo estos criterios en los procesos de desarrollo y adquisición de productos o sistemas.
	Optimizado	- Potenciar las capacidades militares y de inteligencia para ejercer una acción oportuna, legítima y

		proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la seguridad institucional (Gobierno de España, 2013) - Ampliar y mejorar las capacidades de detección y análisis de ciberamenazas que permitan la identificación de procedimientos y orígenes de ataque, y la elaboración de la inteligencia necesaria para una defensa y protección más eficaz de las redes nacionales (Gobierno de España, 2013) - Ampliar y mejorar las capacidades de los organismos con competencias en la investigación y persecución del ciberterrorismo y la ciberdelincuencia, así como asegurar la coordinación de estas capacidades con las actividades en el campo de la ciberseguridad, a través del intercambio de información e inteligencia por los canales de comunicación adecuados (Gobierno de España, 2013)
EJE 4: Seguridad de la información	Inicial	- Desarrollar nuevos servicios horizontales seguros, de acuerdo con directrices de la Dirección de Tecnologías de la Información y de las Comunicaciones de la institución, organismo

y protección de datos personales		responsable de la coordinación, dirección y racionalización del uso de las TIC en la Fuerza Terrestre. - Promover la armonización legislativa y la cooperación jurídica en la lucha contra la ciberdelincuencia y el ciberterrorismo, apoyando la negociación y adopción de convenios internacionales en la materia (Gobierno de España, 2013)
	Repetible	- Integrar en el marco legal institucional las soluciones a los problemas que surjan relacionados con la ciberseguridad para la determinación de los tipos penales y el trabajo de los departamentos competentes (Gobierno de España, 2013)
	Definido	- Asegurar a los profesionales del Derecho el acceso a la información y a los recursos que les proporcionen el nivel necesario de conocimientos en el ámbito judicial para la mejor aplicación del marco legal y técnico asociado (Gobierno de España, 2013)
	Cuantitativo gestionado	- Ampliar y mejorar permanentemente las capacidades de Ciberseguridad de las Fuerzas Armadas que permitan una adecuada protección de sus Redes y Sistemas de Información y Telecomunicaciones, así como de otros sistemas

		que afecten a la seguridad institucional. Se potenciará su cooperación con los diferentes órganos con capacidad de respuesta ante incidentes cibernéticos en aspectos de común interés (Gobierno de España, 2013)
	Optimizado	- Impulsar las actividades de sensibilización para asegurar que los usuarios y toda la institución, reconozca que tienen acceso a información relativa a vulnerabilidades, ciberamenazas e información sobre cómo proteger mejor su entorno tecnológico (Gobierno de España, 2013) - Ampliar y fortalecer las capacidades de detección y respuesta ante ciberataques dirigidos contra objetivos de carácter institucional, organizacional, incluyendo a usuarios e instituciones militares (Gobierno de España, 2013)
EJE 5: Economía digital y tecnologías emergentes	Inicial	- Impulsar el desarrollo de estándares en ciberseguridad a través de los organismos y entidades de normalización y certificación nacionales e internacionales, y promover su adopción (Gobierno de España, 2013)
	Repetible	- Propiciar el desarrollo de programas de Concienciación en Ciberseguridad, en colaboración

		con personal de comunicación, a través de los organismos con competencias en la materia, la necesaria coordinación y racionalización de esfuerzos (Gobierno de España, 2013)
	Definido	- Fomentar los mecanismos para apoyar a la institución y usuarios en el uso seguro de las TIC, reforzando los conocimientos en materia de seguridad, promoviendo la adopción de herramientas, la difusión de normativa y el uso de buenas prácticas (Gobierno de España, 2013) - Asesorar y dar soporte al desarrollo de módulos educativos de sensibilización en ciberseguridad, dirigidos a todos los niveles de la enseñanza (Gobierno de España, 2013)
	Cuantitativo gestionado	- Control y evaluación de incidentes, impulsando la participación de tics, en los Programas de Ejercicios de simulación de incidentes de Ciberseguridad (Gobierno de España, 2013) - Desarrollar modelos de simulación que permitan analizar las dependencias entre las diferentes Infraestructuras Críticas y los riesgos acumulados por éstas (Gobierno de España, 2013)

	Optimizado	- Ampliar y mejorar las capacidades de los equipos de respuesta de incidentes, potenciando la colaboración y coordinación con el Centro para la Protección de Infraestructuras Críticas, con los diferentes órganos con capacidad de respuesta ante incidentes y con las unidades operativas de las Fuerzas (Gobierno de España, 2013)

Conclusiones

- La información digital se ha convertido hoy en día en la parte fundamental de todo Estado ya que las instituciones tanto públicas como privadas han digitalizado casi en su totalidad la documentación estratégica y han automatizado sus procesos, en tal consecuencia las Fuerzas Armadas ecuatorianas no estás exentas de ser parte del ciberespacio por ende es una fuente cada vez más considerable de riesgos y amenazas, es de esta manera que la propuesta **que se encuentra descrita en la matriz de políticas de seguridad informática permiten** fomentar un ambiente estable, involucrando destrezas que manejen los desafíos que presenta la integración a nuevas tecnologías.
- Durante nuestra investigación se ha puesto en práctica en la II D.E "LIBERTAD" algunas de las políticas propuestas, combinando los siguientes medios:
  - En eje de infraestructura y conectividad se empleó documentos como el ESQUEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DIGITAL DE LA F.T. (EGSID) – V.1 mismo precautela la seguridad de información de la II DE.
  - En el eje Seguridad de la información y protección de datos personales se empleó dispositivos como el CYBEROAM dando seguridad a la red informática.
  - En el eje Economía digital y tecnologías emergentes se dictaron charlas de seguridad informática, en las que se capacita a los usuarios el uso adecuado del antivirus institucional Avira, también se activó el firewall, los navegadores se encuentran desactivados la opción de auto guardar las

contraseñas y la instalación innecesaria de programas o aplicaciones que pueden ser dañinos, con estas normas en cierta medida se concientiza a los usuarios en empleo de los medios informáticos.

- Para el eje Gobierno Electrónico se remite cada semana a la DTIC´S, el reporte de ataques informáticos, con el fin de que esta dirección registre, analice y haga el seguimiento necesario para verificar e identificar al atacante. Posterior a esto se procede a realizar o tomar las medidas correctivas y así evitar futuros ingresos a la red de personas mal intencionadas.
- Con esta implementación de medios podemos concluir que alcanzar una ciberseguridad optima es muy difícil sin el apoyo y concientización de los usuarios y administradores informáticos responsables de la seguridad, esto debido a la naturaleza y dimensiones del ciberespacio, es por esta razón que un adecuado uso de las políticas permitirá cumplir objetivos que alcancen una ciberseguridad efectiva, bloqueando los ciberataques implementados por los diferentes delincuentes cibernautas.

- Al validar la matriz de políticas de ciberseguridad aplicando los Ejes de acción propuestos por el MINTEL y el Modelo de Madurez de capacidad de Seguridad Cibernética (CMM), en el Batallón de Operaciones Especiales en Selva N° 54 “CAPT. CALLES” podemos concluir que cumplimos con los siguientes ejes:
  - Eje de Infraestructura y Conectividad por cuanto existen documentos y normativas impuestas por el escalón superior que permite mantener la seguridad de la información, entre los documentos que hacemos referencia tenemos el Esquema de Gestión de Seguridad de la Información Digital de la F.T (EGSID) – V.1, en el que hacemos referencia el LITERAL “C”

Esquema de gestión de seguridad de la información digital; NUMERAL “4” Seguridad de la información en las unidades de la F.T; LITERAL “b” la unidad deberá disponer de por lo menos un técnico o encargado en seguridad de la información a fin de que implante y revise el cumplimiento del esquema, políticas, normas, estándares y guías, que garanticen las acciones preventivas y correctivas para salvaguardar la infraestructura tecnológica y la información.

- Dentro del Esquema de Gestión de Seguridad de la Información Digital de la F.T (EGSID) para la seguridad de la infraestructura y conectividad se dispone a los usuarios de equipos informáticos que para el uso e instalación de todo tipo de software se deberá disponer de la autorización del Oficial de Seguridad de la Información el mismo que será orientado exclusivamente a actividades inherentes a la institución.
- En el Eje de Gobierno Electrónico podemos hacer referencia que en la unidad se cumple por cuento las Fuerzas Armadas han implementado diferentes aplicativos como es el Sistema Integrado (SIFTE), el Sistema de Gestión Documental y Archivo de la Fuerza Terrestre (CHASQUI), Sistema de Inventarios Logístico del Ejército (SILOGE), entre otros con el propósito de facilitar la administración de los recursos humanos y logísticos de nuestra institución.
- En el eje Inclusión y habilidades digitales en el Batallón se ha implementado el UTM CYBEROAM con el propósito de realizar monitoreo permanente, lo que permite detectar varios incidentes de seguridad, como se demuestra en la Tabla 3.
-

Tabla 3

Reporte de CYBEROAM, BOES 54

DIRECCION IP	10.24.2.135-10.24.2.158-10.24.2.124-10.24.2.12-10.24.2.2-10.24.2.119-10.24.2.135-10.24.2.135 10.24.2.133-10.24.2.103
USUARIO	OFICINAS Y BODEGAS DE UNIDAD
LOCALIDAD	OFICINAS Y BODEGA
EQUIPO	PC Y WIFI
TIPO DE INCIDENTE	PAQUETES INVALIDOS
NORMAS INCUMPLIDAS	PROCEDIMIENTOS PARA EL USO DE LOS SERVICIOS WEB LITERAL (1) INSTRUCCIONES GENERALES CAPITULO (J) NUMERAL (15) USAR LOS SERVICIOS PARA PROPAGAR VIRUS, GUSANOS, TROYANOS OCUALQUIER OTRO PROGRAMA QUE IMPIDA EL CORRECTO FUNCIONAMIENTO DE LAS COMPUTADORAS"
NORMATIVA VIGENTE	INSTRUCTIVO FT-DTIC-2019-001-c-INS DE FECHA 06 DE MARZO DE 2019

Nota. La tabla representa un reporte del CYBEROAM de una unidad militar del Ejército ecuatoriano donde se evidencia la norma incumplida, CYBEROAM.

Bibliografía

Acuerdo Ministerial 166. (25 de septiembre de 2013). Obtenido de https://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%83%C2%B3n.pdf

Acuerdo Ministerial N.- 166. (2015). Obtenido de https://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%c3%83%c2%b3n.pdf

Acurio, S. (2005). *Delitos Informáticos.* Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Asamblea General - OHCHR. (29 de junio de 2012). Obtenido de https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf

Asamblea Nacional del Ecuador. (Febrero de 2014). Obtenido de https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Asint360. (Marzo de 2016). *Asint360.com*. Obtenido de http://www.asint360.com/que-es-la-ciberinteligencia-la-inteligencia-en-materia-de-ciberseguridad/

BID. (2016). Obtenido de https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Castro, E. (2015). *Repositorio ESPE*. Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/11583/1/T-ESPE-049543.pdf

Catro, E. J. (2015). *Estudio prospectivo de la ciberdefensa en las Fuerzas Armadas del Ecuador*. Obtenido de http://repositorio.espe.edu.ec/handle/21000/11583

ConceptoDefinicion. (17 de Octubre de 2016). Obtenido de https://conceptodefinicion.de/seguridad/

Congreso Nacional. (Mayo de 2004). Obtenido de https://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/09/LOTAIP.pdf

Conpes 3701. (Julio de 2011). *LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA.* Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Contitución de la República del Ecuador 2008. (20 de Octubre de 2008). Obtenido de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Cubeiro, E. (2016). *Conceptos Fundamentales de Inteligencia.* Valencia: Tirant lo Blanch.

Departamento de Seguridad Nacional. (2017). *Estrategia de Seguridad Nacional 2017*. Obtenido de https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

Departamento Nacional de Planificación. (2011). Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

EcuRed. (2012). *EcuRed*. Obtenido de https://www.ecured.cu/Ciberespacio

ENISA. (2014). *Web oficial de la UE.* Obtenido de https://europa.eu/european-union/about-eu/agencies/enisa_es

Estrategia de Seguridad Nacional 2017 - DSN. (2017). Obtenido de https://www.dsn.gob.es/sites/dsn/files/ESN2017_capitulo_4.pdf

Gobierno de España. (2013). Obtenido de https://www.dsn.gob.es/es/file/146/download?token=Kl839vHG

Machín, N. (Octubre de 2016). *Redalyc*. Obtenido de https://www.redalyc.org/pdf/767/76747805002.pdf

Mediatelecom. (2017). Obtenido de http://mediatelecom.com.mx/category/instacharts/page/2/

Ministerio de Defensa Nacional. (2015). Obtenido de https://www.mdn.gub.uy/?p=3639#.XWV1--hKhPY

MINTEL_PLAN. (2016). Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/08/Libro_plan_tti_REGISTRO-OFICIAL_30_AGOSTO.pdf

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

MITIC. (2018). Obtenido de https://www.mitic.gov.py/materiales/publicaciones/plan-nacional-de-ciberseguridad-paraguay

Nathan, R. M. (Septiembre de 2015). *FOREIGN AFFAIRS.* Obtenido de https://www.foreignaffairs.com/articles/south-america/2015-09-17/brazils-cybercrime-problem

National Cybersecurity Policy (NCSP). (2017). *www.ciberseguridad.gob.c.* Obtenido de https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

Niurka, S. G., & Hernández, C. (2007). *monografias.com.* Obtenido de https://www.monografias.com/trabajos59/calidad-software/calidad-software2.shtml

Oceano IT. (2014). *Las amenazas informáticas más comunes en la actualidad*. Obtenido de https://www.oceano-it.es/news-individual/369/amenazas-informaticas-mas-comunes-en-la-actualidad

Presidencia de la República. (23 de ABRIL de 2008). Obtenido de https://www.controlhidrocarburos.gob.ec/wp-content/uploads/MARCO-LEGAL-2016/Registro-Oficial-322-Decreto-Ejecutivo-1014.pdf

Rea, A., & Sánches, I. (2017). Obtenido de https://pdfs.semanticscholar.org/2f18/34996ff44aa7af09078f64cbfc832095a9a9.pdf

Sancho, C. (2010). Obtenido de ANEPE - Academia Nacional de Estudios Políticos y Estratégicos: https://www.anepe.cl/ciberespacio-delitos-amenazas-a-la-seguridad-y-guerras/

Schmitt, M. (2013). Obtenido de http://www.collaboratory.de/images/4/4b/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf

Stel, E. (2014). *SEGURIDAD Y DEFENSA DEL CIBERESPACIO.* Buenos Aires: Dunken. Obtenido de https://books.google.com.ec/books?id=H1lhAwAAQBAJ&pg=PA137&lpg=PA137&dq=Ciberespacio:+Es+el+espacio+real+y+existente,+invisible+a+los+ojos,+por+el+que+transita+el+90%25+de+la+informaci%C3%B3n+que+emplea+el+mundo,+transformada+en+los+simples+objetos+de+con

Subsecretaría de Defensa Nacional del Ministerio de Defensa Nacional. (2015). Obtenido de https://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf

UIT-T X.1205. (04 de 2008). Obtenido de https://www.itu.int › rec › dologin_pub › id=T-REC-X.1205-200804-I!!P...

Vaca, A. (2017). *Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE*. Obtenido de http://repositorio.espe.edu.ec/handle/21000/13248

Vargas, R. (2017). *Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa*.

Viollier, P., & Martínez , M. (21 de Noviembre de 2013). *Los delitos informáticos bajo la lupa de la evidencia empírica*. Obtenido de https://www.derechosdigitales.org/6645/los-delitos-informaticos-bajo-la-lupa-de-la-evidencia-empirica-que-tan-necesaria-es-una-ley/