Estrategia Nacional de Ciberseguridad

Chiza López, Diego Fernando e Izurieta Cabrera, Hugo Ricardo

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

PhD. Cárdenas Delgado, Sonia Elizabeth

20 de Julio de 2020

HOJA DE RESULTADOS DE LA HERRAMIENTA URKUND

URKUND

Document Information

Analyzed document	Rev_Estrategia Nacional de Ciberseguridad.docx (D77228014)
Submitted	7/27/2020 7:13:00 PM
Submitted by	Cardenas Delgado Sonia Elizabeth
Submitter email	secardenas@espe.edu.ec
Similarity	1%
Analysis address	secardenas.espe@analysis.urkund.com

Firmado electrónicamente por:

CARDENAS
DELGADO
SONIA
ELIZABETH

……

Cárdenas Delgado, Sonia Elizabeth

DIRECTORA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, Estrategia Nacional de Ciberseguridad fue realizado por los señores Chiza López, Diego Fernando e Izurieta Cabrera, Hugo Ricardo, 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, 03 de septiembre de 2020

Firmado electrónicamente por:
SONIA ELIZABETH CARDENAS DELGADO

Cárdenas Delgado, Sonia Elizabeth

Directora

C.C.: 1713261160

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

Responsabilidad de Autoría

Nosotros, **Chiza López, Diego Fernando e Izurieta Cabrera, Hugo Ricardo**, con cédulas de ciudadanía Nº 1001830676 y 1802177616 respectivamente, declaramos que el contenido, ideas y criterios del trabajo de titulación: **Estrategia Nacional de Ciberseguridad** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí 20 de Julio de 2020

Chiza López Diego Fernando
C.C.: 1001830676

Izurieta Cabrera Hugo Ricardo
C.C.: 1802177616

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, **Chiza López, Diego Fernando e Izurieta Cabrera, Hugo Ricardo**, autorizamos a la Universidad de Fuerzas Armadas ESPE publicar el trabajo de titulación: **Estrategia Nacional de Ciberseguridad** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí 20 de Julio de 2020

.....
Chiza López Diego Fernando
C.C.: 1001830676

.....
Izurieta Cabrera Hugo Ricardo
C.C.: 1802177616

DEDICATORIA

Este trabajo de investigación lo dedico a las personas más importantes en mi vida, mi querida esposa Adry quien siempre se ha constituido en mi fortaleza ante cualquier adversidad, y a mis queridos hijos Juan Diego y Manuela, que con su ingenuidad de niños siempre me han apoyado.

Diego Chiza

A mi familia, mi amada esposa Yashmin, compañera de viaje y mi inspiración, sin ti nada sería posible. A mis preciosos hijos que los llevo en mi corazón. A mis padres, fuente de valores y sacrificio. Gracias por tanto y por todo.

Hugo Izurieta

AGRADECIMIENTO

Primero agradezco a Dios, quien con su infinita misericordia me ha concedido la dicha de la salud poder llevar a cabo este trabajo de investigación, a la Academia de Guerra que ha contribuido con todo su personal e infraestructura para dotarme de los conocimientos necesarios para desempeñarme de la mejor manera en la institución, y finalmente a mi querido ejército que se constituye en la mejor institución de nuestro país.

Diego Chiza

Mi agradecimiento a Dios, arquitecto de nuestros destinos, quien ha permitido llevar este trabajo investigativo a feliz término, a nuestra institución militar, cimiento firme de nuestra formación castrense, cuna de hombres y mujeres con espíritus indomables, a nuestra directora de tesis PhD. Sonia Cárdenas, por su disponibilidad y presteza en el aporte de este trabajo de investigación, a mi amigo y compañero Diego por sus largas jornadas de trabajo compartidas y su amistad siempre sincera.

Hugo Izurieta

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

RESUMEN

El siglo veintiuno se presenta con muchos avances tecnológicos para la humanidad, los cuales por un lado facilitan el desarrollo de las actividades pero por otro presentan un gran desafío en cuanto a la seguridad, utilizamos la tecnología prácticamente en todos los ámbitos de nuestro que hacer, pero no estamos conscientes de los peligros que su utilización representa, esta realidad proyectado en la dimensión nacional significa que como país estamos expuestos a muchos peligros derivados del uso de la tecnología, en el presente trabajo de investigación hemos iniciado con un diagnóstico de la situación actual del Ecuador en el área de la ciberseguridad, estableciendo ámbitos de acción en los cuales se necesita una directriz del estado que permita articular y coordinar los esfuerzos de diferentes organismos nacionales, complementados con el apoyo de organismos internacionales, todo esto ha sido plasmado en la propuesta realizada como Estrategia Nacional de Ciberseguridad, en la que presentamos las líneas de estratégicas de acción, las cuales posteriormente se materializan los objetivos a alcanzarse a través de cada una de las estrategias propuestas, por lo que este trabajo se constituye en un aporte desde la óptica netamente académica, conscientes de las limitantes principalmente económicas para que pudiera implementarse en el mediano plazo.

PALABRAS CLAVE:

- **ESTRATEGIA NACIONAL**
- **CIBERSEGURIDAD**
- **INFRAESTRUCTURA CRÍTICA**

ABSTRACT

The twenty-first century is presented with many technological advances for humanity, which on the one hand facilitate the development of activities but on the other hand present a great challenge in terms of security, we use technology in virtually all areas of our work, but we are not aware of the dangers that their use represents, this reality projected in the national dimension means that as a country we are exposed to many dangers arising from the use of technology, in this research work we have begun with a diagnosis of the current situation of Ecuador in the field of cyber security, Establishing areas of action in which a State directive is needed to articulate and coordinate the efforts of different national organizations, complemented by the support of international organizations, all this has been reflected in the proposal made as the National Cybersecurity Strategy, in which we present the lines of strategic action, which subsequently materialize the objectives to be achieved through each of the proposed strategies, so this work is a contribution from the purely academic, aware of the limitations mainly economic so that it could be implemented in the medium term.

KEY WORDS

- NATIONAL STRATEGY
- CIBERSECURITY
- CRITICAL INFRAESTRUCTURE

CAPÍTULO I: GENERALIDADES

Planteamiento del Problema

El acelerado desarrollo de las sociedades ha desembocado en una dependencia total de los sistemas de información, hoy en día prácticamente todas las actividades del ser humano involucran en mayor o menor grado la intervención y utilización de tecnologías de la información, lo que ha impulsado el crecimiento de los países a nivel mundial en términos económicos, evidenciando eficiencia, crecimiento de mercado y sobre todo iniciativas para mejor la economía, sin embargo, los usuarios no son conscientes de los riesgos que conlleva una población con mayor capacidad de conexión digital, en la que de sufrir interrupción en los servicios en los que se basa el funcionamiento de las sociedades modernas, los resultados serían inciertos e inimaginables, pudiendo ocasionar pérdidas no solo económicas sino incluso de vidas humanas.

Como ejemplo, podemos citar a Estonia como una potencia del mundo, digitalmente hablando, con altos niveles de gobierno electrónico, en el año 2007 sufrió uno de los primeros ciberataques por parte de un grupo de piratas informáticos presumiblemente provenientes de Rusia. Dicho ataque dejó fuera de servicios las páginas web del Gobierno llevando al país casi a su paralización total, para superar la crisis de comunicaciones utilizaron nuevamente el fax y el teléfono.

En mayo de 2017, se reportó el ataque de mayor impacto producido hasta esa fecha llamado *WannaCry*. Este ataque se produjo debido a fallas producidas en el sistema operativo Windows de Microsoft, lo que permitió vulnerar y detener operaciones de fábricas, sistemas de transporte y sistemas de telecomunicaciones. Además, el ataque consistió en secuestrar información gubernamental, empresarial y de personas importantes a cambio de dinero. Se estima que el problema alcanzó a 150 países afectando a miles de computadoras alrededor del

mundo. En el Reino Unido, de acuerdo con la Oficina Nacional de Auditoría de ese país, en su investigación sobre el ciber ataque WannaCry del 27 de octubre de 2017, se concluyó que como resultado de este ataque se volvió inoperable el equipo médico de un considerable número de entidades conexas al Servicio Nacional de Salud inglés. Afectando el sistema de salud y la seguridad pública.

En junio de 2017, otro software malicioso llamado NotPetya, se extendió alrededor del mundo en cuestión de minutos, causando un verdadero caos en los sistemas conectados de internet en más de 6 decenas de países alrededor del mundo, incluido el aparato gubernamental, la banca privada, empresas y demás. De las estimaciones realizadas por LLoyds Bank, se estableció que el costo de este ataque podría llegar a costar igual que los daños ocasionados por la tormenta Sandy, por citar un ejemplo, la compañía naviera Moller-Maersk una de las más grandes del mundo, tuvo que detener sus operaciones en la mayoría de sus 76 terminales portuarias interrumpiendo el comercio marítimo por semanas. Las pérdidas a consecuencia de este acto terrorista informático fueron incalculables.

En América Latina, los reportes públicos sobre ataques cibernéticos sofisticados no son frecuentes en comparación con el resto del mundo, sin embargo, de los pocos reportados tenemos el ejemplo de México, donde a mediados de 2018 algunos Bancos reportaron haber sido blanco de grupos de ciberdelincuentes, que ejecutaron ataques de tipo Amenaza Persistente Avanzada (APT, por sus siglas en inglés) los cuales habrían sido ejecutados o al menos respaldados por actores estatales (Bloomberg, 2018). Acorde al reporte expuesto por la OEA en septiembre de 2018, relacionado al sistema de ciberseguridad en el sector bancario para América Latina y el Caribe, 9 de cada 10 entidades bancarias fueron víctimas de ataques cibernéticos en el último

año, los ataques tuvieron una efectividad del 37% y un 39% de estos ataques no fueron reportados.

En el Ecuador, las estadísticas referentes a violaciones a la ciberseguridad en su mayoría han sido sobre el sistema financiero, según el reporte Ciberseguridad escenarios y recomendaciones 2014 que emitió el Ministerio Coordinador de Seguridad, en ese año hubo un incremento de un 37% de afectación a la banca virtual, 14% a las tarjetas de crédito y 46% en cajeros electrónicos, de igual manera la prensa también ha sufrido ataques, especialmente en sus sitios web que utilizan el dominio .ec, dichos ataques dejaron momentáneamente fuera del aire sus páginas web, también han sido atacados sitios web del gobierno presuntamente por el grupo denominado Anonymous (Vargas & Recalde, Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa, 2017).

El Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe, es claro al concluir que la mayoría de los países en la región les falta implementar herramientas tendientes a combatir las amenazas del ciberespacio, solo seis países han diseñado una Estrategia de Ciberseguridad entre ellos México, Colombia, Panamá, Paraguay, Chile y Costa Rica. En este informe se recomienda hacer lo que fuere indispensable para proteger la infraestructura clave para el siglo XXI. Según cálculos del Centro de estudios estratégicos Internacionales y la empresa McAfee en su estudio Net Losses: Estimating the Global Cost of Cybercrime realizado en el año 2014, el cibercrimen le cuesta al mundo aproximadamente $570.000 millones de dólares anualmente en términos macroeconómicos representa un 0,5% de su PIB. Lo que se traduce en restar en cuatro veces el monto anual de las donaciones de la comunidad internacional para el desarrollo. Con esos recursos se podría cuadruplicar el número de investigadores científicos en la

región y muchos más aportes en beneficio del desarrollo y la seguridad tan venida a menos en estos tiempos.

En el Ecuador las nuevas tecnologías se adoptan con esmero y en forma acelerada por el retraso frente a las economías de la región, en el caso gubernamental se está aprovechando cada vez más los medios digitales para ofrecer servicios a la ciudadanía, sin embargo la falta de decisión política y la limitación de recursos no permiten promover una conciencia plena de prevención y mitigación de los riesgos provenientes de la actividad ilícita con los medios digitales, el Modelo de Madurez de Capacidad de Seguridad Cibernética desarrollado por la OEA, establece que el Ecuador, así como muchos países en la región es vulnerable a sufrir ataques cibernéticos potencialmente devastadores, al no contar con estrategias en el ámbito de ciberseguridad, planes que protejan la infraestructura critica o un organismo que asuma el comando y control de seguridad cibernética, lo que debilita la posición de los entes de control como las fiscalías que no tienen los instrumentos legales para investigar los delitos cibernéticos sobre una legislación débil al respecto.

Formulación del Problema

¿Cómo enfrentaría el Estado ecuatoriano las amenazas provenientes del ciberespacio que atenten contra su ciberseguridad, aplicando estándares internacionales acordes a la realidad nacional?

Interrogantes de Investigación

- ¿Cuál es la situación actual de la ciberseguridad en el Ecuador?
- ¿Existe en el Ecuador legislación sobre el ciberespacio, enmarcada en una estructura funcional que limite su uso indebido, y permita el seguimiento y

control a las instituciones del estado?

- ¿Dispone el estado ecuatoriano de una cultura de ciberseguridad, programas de formación especializada, campañas de concientización y procesos enseñanza aprendizaje en todos los sectores y niveles de la sociedad?
- ¿Mantiene el Ecuador convenios internacionales que permitan el intercambio de información, capacitación y transferencia tecnológica para la implementación de medidas de seguridad en el ciberespacio?
- ¿Dispone el estado de políticas y estrategias de ciberseguridad para la prevención, detección, protección y recuperación ante incidentes en el ciberespacio?

Delimitación del Objeto de la Investigación

El presente trabajo de investigación se fundamentará en todo lo relacionado a ciberseguridad en el territorio nacional. Según la recomendación UIT-T X.1205 de abril de 2008 de la Unión Internacional de Telecomunicaciones, la Ciberseguridad la conforman varios elementos que van desde conceptos de seguridad, políticas, estrategias, directrices, métodos de gestión de riesgos, nuevas tecnologías, practicas saludables, acciones gubernamentales, usuarios de las TIC´s entre otros. Para ello se apoya en una escala estandarizada, protocolos de seguridad, reglamentación, métodos y leyes provenientes a minimizar los riesgos que conlleva mantener una infraestructura informática.

El presente trabajo de investigación será desarrollado a nivel nacional, tomando como referencia los principales sectores de la sociedad: Banca, debido a que en el país son el mayor objetivo de los ataques informáticos. Las universidades, donde se encuentran los profesionales

de las áreas del conocimiento involucradas en la ciberseguridad (electrónica, sistemas, mecatrónica, mecánica). Organismos de seguridad y defensa como las Fuerzas Armadas y la Policía Judicial, entes responsables de proteger el ciberespacio, por ser parte del teatro de operaciones y su injerencia es primordial para la defensa del territorio nacional, en el caso interno la policía debe judicializar los delitos informáticos. Expertos del sector privado, que ofrecen servicios especializados de ciberseguridad. Organizaciones que administran infraestructura crítica del estado, por ser una de las áreas más sensibles a ser protegidas mediante la ciberseguridad.

Se tomará como base para el estudio, los incidentes de ciberseguridad ocurridos a partir del año 2015 en los diferentes sectores de la sociedad ecuatoriana, considerando una evaluación y supervisión constantes de los esfuerzos y acciones realizadas de manera independiente en el país, a fin de garantizar la calidad de la seguridad frente a la naturaleza cambiante de las amenazas.

Objetivos

Objetivo General

Proponer Estrategias Nacionales que permitan enfrentar y neutralizar las amenazas a la ciberseguridad del estado provenientes del ciberespacio aplicando estándares internacionales acordes a la realidad nacional.

Objetivos Específicos

- Diagnosticar cuál es la situación actual de la ciberseguridad en el Ecuador.
- Determinar si en la legislación ecuatoriana se encuentra tipificado y sujeto a sanción las acciones ilícitas en el ciberespacio, y si permite el seguimiento y control de la ciberseguridad en las instituciones del estado.

- Analizar la existencia de convenios internacionales y su ámbito de aplicación en el Ecuador con relación a la ciberseguridad.
- Aplicar técnicas de recopilación de datos para conocer el nivel de conocimiento que tiene la sociedad ecuatoriana acerca de ciberseguridad
- Proponer las políticas y estrategias de ciberseguridad para la prevención, detección, protección y recuperación ante incidentes en el ciberespacio.

Justificación

Los beneficios del uso del ciberespacio y sus permanentes innovaciones son numerosos. La incorporación de nuevas capacidades en áreas como la seguridad y defensa, las comunicaciones, la investigación científica, procesos industriales, la gestión del conocimiento, la gobernanza son evidentes y cuantificables. Además, la generalización del acceso a las redes por parte de la población aumenta sus oportunidades de progreso y desarrollo lo que se verá reflejado en un indiscutible impacto social en la comunidad.

En la actualidad los Estados deben enfrentar constantes daños a su infraestructura tecnológica y de información, lo que genera grandes pérdidas en los gobiernos, administración pública o en las empresas consideradas como estratégicas, pues son las que mayormente proveen los recursos para la administración de los estados, por lo que precisa atención inmediata de los diferentes actores estatales.

En el campo de la defensa el tema revierte mayor importancia, la capacidad de desarrollo de los pueblos está dado por la capacidad que dispongan sus gobiernos para implementar más y mejores métodos de seguridad, razón por la cual los Estados necesitan contar con instituciones con la capacidad tecnológica para combatir estas amenazas, una de ellas y sobre la cual recae la

mayor responsabilidad es sin duda las Fuerzas Armadas, quien es responsable por el desarrollo del Poder Militar del Estado.

El presente trabajo contribuye con una propuesta de gestión y mejora de uno de los complejos escenarios que actualmente deben afrontar los actores políticos y principalmente los Estados en el campo de la Seguridad y Defensa; específicamente la Ciberseguridad y sus ámbitos de acción como la protección y recuperación de los sistemas de infraestructura crítica ante agresiones que utilizan el ciberespacio como entorno y móvil para interferir en las actividades de los ciudadanos, sus actividades y de las instituciones.

Este trabajo investigativo toma especial relevancia porque busca aportar en forma práctica en la organización e implementación de directrices necesarias para que el estado ecuatoriano cuente con una estructura encargada de la organización, planificación, ejecución y supervisión de todas las actividades relacionadas al campo de la ciberseguridad, los sistemas y las tecnologías de la información para mantener la seguridad en los procesos que desarrollan las instituciones tanto del estado como privadas, con especial interés a la infraestructura crítica y áreas que son vitales para el desarrollo del país. En el campo de seguridad y defensa se busca mantener el mando y control de las operaciones militares que desarrollan FF. AA y que están consagradas en la Constitución; en el campo social y económico se busca proteger el sistema financiero, el comercio, la productividad, el manejo de datos personales entre otros que se constituyen blancos permanentes para los delincuentes informáticos, más aún cuando estos se relacionan con el crimen organizado.

De acuerdo con la bibliografía estudiada, en nuestro país no se han propuesto políticas definidas referentes a seguridad en el ciberespacio, cada institución del estado ha asumido distintas iniciativas basadas en la complejidad de su infraestructura, su interconectividad, las aplicaciones y tecnologías asociadas a su giro de negocio particular. En definitiva, lo realizado para mejorar la ciberseguridad, ha sido en su gran mayoría iniciativas puntuales de instituciones públicas o políticas de manera limitada por lo que han resultado poco efectivos.

Este escenario de configuración estatal revela las falencias y amenazas a las que estamos expuestos los ciudadanos y las instituciones públicas y privadas; por lo que este proyecto de investigación es de especial relevancia ya que se propondrán estrategias en ciberseguridad tendientes a la implementación de nuevas estructuras organizativas y fortalecimiento de las ya existentes de carácter técnico, con el objeto de hacer frente a los desafíos que el uso del ciberespacio tiene para la seguridad nacional.

Sin duda alguna es una propuesta de actualidad y de originalidad evidente, ya que, a nivel nacional, en el área de ciberseguridad no existen estudios que aporten en la implementación de estrategias tendientes a mejorar esta inseguridad informática que vivimos día a día.

Este trabajo es factible debido a que los autores tienen los conocimientos necesarios para desarrollar el estudio en cuestión, también, se dispone de los recursos informáticos necesarios y el acceso a bibliografía especializada. Es factible obtener referencias de políticas y estrategias implementadas por otros países en el ámbito de la ciberseguridad. Se realizarán encuestas y entrevistas para recopilar información de personal especializado. Los datos obtenidos serán Procesados mediante técnicas estadísticas cuantificables. Los resultados facilitaran proponer alternativas y estrategias para que el estado ecuatoriano mejore y estandarice el control y la administración del ciberespacio de acuerdo con su capacidad de desarrollo.

CAPÍTULO II: MARCO TEÓRICO

Fundamentación Teórica

Antecedentes de la investigación

Ante el creciente número de amenazas provenientes del ciberespacio, surge la imperiosa necesidad en los estados de orientar mecanismos tendientes a proteger su infraestructura, por lo que en el mundo se han venido desarrollando Estrategias Nacionales de Ciberseguridad, tendencias que han tardado en llegar a América Latina, sólo seis países han estructurado una Estrategia de Ciberseguridad, México fue el último en presentar su Estrategia, el 13 de noviembre de 2017 (OEA-BID, 2017), Colombia lo realizo entre el 2011 y 2016, Panamá en el 2013, Paraguay en 2017 y Costa Rica en 2017.

En el Ecuador no se han priorizado lineamientos ni políticas en el campo de seguridad de la información que trabajen y construyan una estrategia nacional de ciberseguridad que detenga el aumento de estas amenazas informáticas que afectan significativamente la seguridad del estado; se evidencia falta de coordinación, iniciativas aisladas como la implementación del Comando de Ciberdefensa dentro de las Fuerzas Armadas, cuya misión de proteger y defender la infraestructura crítica e información estratégica del Estado aún no se puede verificar; también se puede mencionar la disposición a las instituciones públicas de la obligatoriedad de crear el Esquema Gubernamental de Seguridad de la Información (EGSI). Medidas que han demostrado ser insuficientes, por lo que se vuelve necesario el desarrollado de una estrategia nacional de ciberseguridad que permita guiar, controlar y gestionar el ciberespacio.

Fundamentación General

Los continuos ataques a la red de infraestructura crítica, que se han evidenciado en los últimos años y que han afectado en el plano de la seguridad nacional de los Estados Unidos, han sido el detonante para que el presidente Barack Obama promulgue un decreto para la mejora de la Ciberseguridad de Infraestructura Critica, encargando al Instituto Nacional de Estándares y Tecnología NIST (National Institute of Standards and Technology por sus siglas en inglés) la implementación de una planificación que vaya a mitigar los riesgos asociados a este tipo de entornos, con el apoyo del Gobierno, la industria y los usuarios. Como resultado de este esfuerzo se puso en consideración el documento llamado Marco para la mejora de la ciberseguridad en Infraestructuras críticas (Framework for Improving Critical Infrastructure Cybersecurity), conocido como NIST Cybersecurity Framework, promulgado en febrero de 2014.

Esta no fue la primera iniciativa puesta en ejecución, puesto que la OTAN a través del Centro de Excelencia de Ciberdefensa Cooperativa – CCDCOE desarrolló, hace algún tiempo atrás, una importante doctrina orientada a proteger el sistema de estructuras críticas que posee el estado para la defensa nacional. El documento al que nos referimos se lo conoce como Manual del Marco de Trabajo de Ciberseguridad Nacional, publicado en 2012. Así también podemos mencionar el ISO/IEC con su estándar ISO/IEC 27032:2012 Técnicas de Seguridad de la Información – Guía de ciberseguridad, base para la materialización de la guía para el manejo en el campo de la ciberseguridad.

Actualmente uno de los trabajos más completos para desarrollar una estrategia de ciberseguridad exitosa, es la guía elaborada por la Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO) y el Centro de Excelencia de Ciberdefensa

Cooperativa de la OTAN (CCDCOE OTAN), en la que se materializa el esfuerzo, la pericia y la experiencia y el conocimiento de los actores más destacados en materia de implementar estrategias y políticas en ciberseguridad, sustentadas en los siguientes estándares:

- Control para la información y tecnologías relacionadas, Control Objectives for Information and Related Technology (COBIT)
- 20 Controles de Seguridad Crítica, Top 20 Critical Security Controls (CSC)
- ANSI/ISA-62443-2-1 (99.02.01)-2009,
- ANSI/ISA-62443-3-3 (99.03.03)-2013,
- ISO/IEC 27001:2013,
- NIST SP 800-53 Rev. 4:

Fundamentación Específica

Acceso a internet en el Ecuador

La conectividad que el Ecuador pose hacia el mundo es privilegiada, en cuanto a infraestructura se refiere, ya que cuenta con tres cables submarinos: PANAM, SAM1, PCSS y aunque el país tiene una alta cobertura de fibra óptica (94% a nivel cantonal), aún existen 13 cantones que carecen de este servicio básico, a nivel parroquial la cobertura del servicio de internet llega al 91%, sin embargo la efectividad de este servicio por viviendas llega apenas al 37%, existiendo una diferencia considerable entre cobertura y penetración del servicio de Internet (Ministerio de Telecomunicaciones MINTEL, 2018). En las últimas estadísticas disponibles, la población que refiere edades de más de 5 años se ha beneficiado del servicio de internet en el último año, eso corresponde al 58% de la población, de los cuales un 66% corresponde al área urbana y el 39.6% del área rural (Instituto Nacional de Estadistica y Censo INEC, 2017). Según la

(Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL, 2018) al año 2018 existían en el país 10,4 millones de cuentas de internet contratadas, de es 1,8 millones de cuentas de internet fija y 8,6 millones de cuentas de internet móvil.

Libro Blanco de la Sociedad de la información y el conocimiento.

El Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) puso en consideración el: Libro Blanco de la Sociedad de la Información y del Conocimiento 2018 (LBSIC), que, a decir del Ing. Guillermo León Santacruz, titular de esa cartera de estado, se constituye un proyecto inmediato del MINTEL, encuadrado en el Plan Nacional de Desarrollo 2017-2021 Toda una Vida, que incentiva la estructuración de una Sociedad de la Información y del Conocimiento a través de la implementación de políticas y estrategias que promuevan un cambio significativo en el uso de las tecnologías digitales, para lo cual se han determinado cinco ejes: Infraestructura y Conectividad, Gobierno Electrónico, Inclusión y Habilidades Digitales, Seguridad de la Información y Protección de Datos Personales, Economía Digital y Tecnologías Emergentes; promoviendo directrices en busca de acortar la brecha digital en la sociedad, creando condiciones óptimas para su acceso masivo privilegiando a los más necesitados.

En términos generales el LBSIC busca expandir una estrategia que fortalezca el desarrollo de la Sociedad de la Información y del Conocimiento en Ecuador, el resultado que se espera es incentivar el crecimiento económico, buscar la tan anhelada equidad e inclusión social y el buen manejo de la administración pública.

Dicho documento pretende alcanzar los siguientes objetivos:

- Presentar una radiografía del actual manejo de la Sociedad de la Información y del Conocimiento en Ecuador.

- Orientar el empleo de las herramientas que fortalezcan los lineamientos de la Política Pública en materia de telecomunicaciones y de información.
- Impulsar la colaboración permanente entre estado y usuarios para la articulación de los ejes que servirán para la construcción de una sociedad con oportunidades de acceder a la información y al conocimiento tecnológico.

Este Plan contempla tres Ejes Programáticos y nueve Objetivos Nacionales de Desarrollo, basados en la sustentabilidad ambiental y desarrollo territorial.

En lo referente a desarrollo de las Tecnologías de la información el Plan establece las siguientes políticas:

- Lineamientos de Acceso Equitativo a Infraestructura y Conocimiento.
- Aumento de las TIC´s y el servicio público de telecomunicaciones, considerando como prioridad la zona rural, la frontera, Amazonia y la región insular.
- El acceso a la información permitirá en corto plazo tener a la ciudadanía educada e informada fortaleciendo y masificando el acceso a la información.
- En el Objetivo 7 se habla de mejorar el Gobierno electrónico al 2021 con la premisa Mas sociedad, mejor Estado.
- Incentivar a la sociedad participativa, con un Estado al servicio de la ciudadanía.
- Mejorar la burocracia en la tramitología de las entidades públicas, promoviendo la efectividad, traducida en efectividad económica, política y social.

Plan Nacional de Gobierno Electrónico 2018-2021

El Gobierno Electrónico en Ecuador tiene como premisa fundamental modernizar las relaciones y crear un vínculo entre el gobierno a los ciudadanos, empleando las TIC en todo su potencial, considerando a los grupos sensibles como la punta de lanza del proyecto, facilitando de esta manera el acceso a los servicios públicos a cualquier hora y lugar utilizando sus teléfonos celulares y/o, computadoras según fuere el caso. El Gobierno Electrónico facilitará a los sectores

productivos un menor esfuerzo burocrático con las instituciones públicas y privadas, políticas que se verán reflejadas en efectividad y disminución de recursos y aumento de oportunidades.

En esta dinámica es importante los acuerdos que se deben efectivizar con las demás funciones del Estado al igual que con los gobiernos seccionales por la independencia de cada uno de ellos, pero cuando hablamos de masificar este beneficio a todos los sectores del país, su participación es fundamental para llevar a cabo esta iniciativa por parte del estado, incorporando así a los ciudadanos en las decisiones y en la participación de la política pública del gobierno, priorizando siempre a los grupos sensibles que han sido de alguna manera relegados o marginados por la condición socio – económica.

A decir del Gobierno electrónico, el Plan concibe la situación actual del Ecuador en tres programas: Gobierno Abierto, Gobierno Cercano y Gobierno Eficaz y Eficiente, cada uno promueve estrategias e iniciativas que facilitarán a los diferentes sectores, en forma armónica alcanzar los objetivos que se ha propuesto el MINTEL.

Con Gobierno Abierto, el objetivo es fijar las directrices para que las instituciones públicas ayudados por el sistema tecnológico, brinden la oportunidad al ciudadano de interactuar con las instituciones estatales, que el acceso a la información que administra el Estado sea oportuno sencillo y mantenga estándares de privacidad que den confianza al usuario.

Gobierno Cercano, busca la conexión entre gobierno y ciudadanía por medio de los servicios electrónicos.

Gobierno Eficaz y Eficiente tiene como objetivo promover la labor de las instituciones públicas, sobre la base de resultados y evidencias, brindando servicios oportunos de buena calidad a los ciudadanos a bajos costos, para lo cual se emplearán herramientas como la nube, el software libre, la gestión del conocimiento el teletrabajo, intercambio de información entre otros.

Sistemas de Gestión de la Seguridad de la Información (SGSI)

La ISO 27001[1], define como información a todo el conjunto organizado de datos que constituye un valor importante para la entidad que la posee, independientemente de cómo se la administre o transmita, de su procedencia o de la fecha de elaboración. La confidencialidad se define como la condición por la cual la información no puede estar disponible a entidades no autorizadas, la integridad debe ser entendida como la conservación de la veracidad y oportunidad de la información, quiere decir, que esta no sea alterada sin la debida autorización, y la disponibilidad como la condición de que la información pueda empleada por personal que estén autorizados, previo trámite de requerimiento.

Se considera importante mantener la seguridad de la información con la implementación de herramientas que lleven a un flujo sistemático y documentado de toda la información que se procesa en una organización, adoptando un enfoque de gestión de riesgos, que pretende garantizar la seguridad de esta.

Dada la alta dependencia de los sistemas de información, juntamente con los procesos más los sistemas que la maniobran, se los cataloga como activos valiosos para las organizaciones, mantener su confidencialidad, integridad y disponibilidad es esencial para su funcionamiento y lograr los objetivos de las organizaciones.

[1] ISO 27001 Estándar para la seguridad de la información (*Information technology - Security techniques - Information security management systems - Requirements*) aprobado y publicado como estándar internacional en octubre de 2005 por la International Organization for Standardization(ISO).

Un SGSI busca establecer políticas y procedimientos orientados a los objetivos de la organización con el propósito de alcanzar un nivel de exposición que este bajo los niveles de riesgos ya asumidos.

Gestión de Seguridad de la Información NTE INEN-ISO/IEC 27000

La Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000 TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, es una traducción literal de la Norma Internacional ISO/IEC 27000:2016, el servicio Ecuatoriano de Normalización INEN es el responsable de la traducción y el Comité Técnico de Normalización de Tecnologías de la Información es responsable de su adopción.

Al poner en ejecución la normativa que rige que rige el SGSI, las estructuras constituidas están en condiciones de promover un marco que permita gestionar la seguridad de sus activos de información, también pueden preparar, promover e implementar un esquema para tramitar que lleve a velar por la seguridad de sus activos de información y acondicionar una evaluación autosuficiente de su SGSI.

Esquema Gubernamental de Seguridad de la Información (EGSI)

El acelerado avance tecnológico y la necesidad de contar con un marco regulatorio que proteja la importante información que manejan las entidades gubernamentales , agilitan para que el estado ecuatoriano en el año 2013 adopte las medidas necesarias para conservar la seguridad en la información que se produce y resguarda en los organismos pertenecientes a la Administración Pública Central, Institucional dependientes de la Función Ejecutiva, dispuso mediante acuerdo ministerial 166, el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información, estableciéndolo como

Esquema Gubernamental (EGSI), mismo que será el cual podrá ser inspeccionado en forma continua en periodos establecidos de acuerdo a lo estipulado por la Secretaría Nacional de la Administración Pública.

Equipos de respuesta a incidentes de seguridad informática.

Una de las definiciones que mejor describe un incidente de seguridad informática se le atribuye a las acciones o hechos que perjudiquen la connotación de confidencialidad, integridad o disponibilidad de la información de una organización. Este proceso de administración coordinada de los incidentes de seguridad que pueden presentarse a nivel nacional es controlado a través de las estructuras denominadas CSIRT Equipos de Respuesta ante Incidentes de seguridad computacional, acrónimo del inglés Computer Security Incident Response Team.

Un CSIRT es un equipo para minimizar y controlar los daños ante un ciberataque, que además asesora, responde y recupera la normalidad en las operaciones, así como previene que ocurran futuros incidentes, para lo cual los equipos intervienen como coordinadores en todas aéreas, individuos o procesos que intervienen en el hecho.

En los CSIRT sus miembros constituyen equipos con roles definidos y tareas específicas que pueden agruparse para tratar algún problema de seguridad, dependiendo el tipo que se establezca de la frecuencia, y nivel de peligrosidad de los incidentes de seguridad entre otros factores.

Por otro lado, estos equipos pueden ser internos, es decir constituidos como parte de la organización, o ser externos, organizaciones privadas que proveen servicios a otras organizaciones sea por necesidad o en forma frecuente, entre ellos tenemos los que pertenecen a las instituciones públicas, al sector educativo o proveedores de los servicios de ciberseguridad a quienes se les asigna la misión de solventar los incidentes a nivel local o nacional si fuere el caso.

Entre sus bondades un CSIRT tiene la facilidad de detectar actividades de sospechosa procedencia, así como de investigar e indagar a los artífices de un ciberataque, permitiendo neutralizar a los cibercriminales y perseguirlos legalmente.

La estructura de un CSIRT depende de lo que hará y cómo pretende lograr sus objetivos, los servicios que ofrecerá, el tamaño de la organización, la distribución geográfica de la organización, entre otros, pudiendo ser a través de un equipo local, centralizado o distribuido.

EcuCert

Un Equipo de Respuesta ante Emergencias Informáticas o como se lo conoce en inglés Computer Emergency Response Team CERT, lo constituye un equipo de profesionales de cibserseguridad encargados de implementar medidas preventivas y reactivas a fin proteger los sistemas informáticos de cualquier incidente de seguridad, para lo cual deberá monitorear permanentemente el estado de las redes y los ordenadores protegidos, entre sus obligaciones estará el emitir alertas relativas a amenazas y vulnerabilidades y proveer información para mejorar la seguridad de estos sistemas.

Para el caso de Ecuador, el Ministerio de Telecomunicaciones a través de la Agencia de Regulación y Control ARCOTEL dispone del Centro de Respuesta a Incidentes Informáticos ECUADOR denominado EcuCert, cuya misión consiste en contribuir con la seguridad de las redes de telecomunicaciones del país; entre su oferta de servicios consta la concientización y capacitación, para lo cual se mantiene en contacto con otros equipos de este tipo dentro y fuera del país.

Delitos informáticos en la legislación ecuatoriana COIP

En el Ecuador los delitos informáticos son sancionados a través del Código Orgánico Integral Penal (COIP), específicamente en sus artículos desde el 178 hasta el 234. (Código Orgánico Integral Penal, 2014, págs. 93-95)

A continuación, un resumen de los artículos del COIP que guardan relación con estos delitos informáticos.

- El Artículo 178 que básicamente trata sobre la violación a la intimidad, mismo que en el Código Penal derogado lo consideraba como una contravención de tercera clase, mientras que en el COIP se considera una importancia tal, al punto que la sanción es penalizada con cárcel de uno a tres años, se cataloga a la violación a la intimidad como una acción que afecta la libertad del comercio electrónico en el Ecuador.
- El Artículo 186 habla sobre la estafa, delito que ha causado grandes pérdidas en el sector financiero, el gubernamental, empresarial y personas naturales. La afectación es a través de ocultamiento de hechos falsos, en beneficio patrimonial u ocultando hechos verdaderos en beneficio personal o de terceros, sancionado con penas que van entre cinco a siete años. También en este artículo se habla de personas que defrauden a través del uso de dispositivos electrónicos especialmente al sistema bancario.
- El Artículo 190 contempla la figura de apropiación fraudulenta empleando medios electrónicos; se refiere a la utilización en forma fraudulenta del sistema informático, redes electrónicas o de telecomunicaciones para a apropiación de bienes o transferencias no consentidas que afecten a terceros, la pena es igual que la del artículo 178.

- De igual manera desde los artículos 191 al 195 las sanciones van con penas privativas de libertad de uno a tres años y se refieren a todos los delitos referentes al mal uso de terminales móviles, comercialización de bases de datos, cambio de etiquetas en terminales y otros.
- El Artículo 229 habla sobre la revelación de información en beneficio propio o de terceros, realizadas a través de un sistema electrónico donde se evidencie la violación a la intimidad y fueron cometidos por servidores públicos con una sanción de uno a cinco años de prisión.
- El Artículo 230 establece todos los delitos referentes a interceptación, escucha, grabación, clonación, comercialización de información y otros. Es muy importante la interpretación de este artículo del COIP por que establece una gama de delitos que se relacionan con la privacidad y el sigilo de la información que han afectado tanto a instituciones públicas y privadas como a personas naturales, que generalmente se han relacionado a los casos de corrupción que hemos visto durante estos últimos 10 años en el Ecuador. Este articulo impulsa el fortalecimiento del comercio electrónico, ya que de alguna manera asegura las cuentas bancarias o tarjetas de crédito de los usuarios.

Comité Interamericano Contra el Terrorismo (CICTE)

Este organismo emitió la declaración sobre el FORTALECIMIENTO DE LA SEGURIDAD CIBERNÉTICA EN LAS AMÉRICAS, realizada en marzo de 2012 en Washington D.C, Estados Unidos. En la cual los países miembros se comprometieron entre otras cosas a las siguientes:

- La necesidad de fortalecer los medios que conforman los CSIRT, mismos que son los responsables establecer las alertas, vigilancia sobre incidentes cibernéticos.
- La política de que los Estados Miembros formen parte activa de la Red de Seguridad Hemisférica de los CSIRT y de Autoridades en Seguridad Cibernética para que la información compartida entre los Estados Miembros sea aprovechada en beneficio de proteger la infraestructura critica que poseen. Y prevenir incidentes relacionados a la ciberseguridad.

- La política de incrementar las medidas de seguridad de las instituciones gubernamentales y sectores estratégicos que poseen infraestructura critica relacionados especialmente a centros tecnológicos.
- Continuar implementando estrategias nacionales de seguridad cibernética integrales y comprometer a los actores tanto gubernamentales como privados en su implementación y desarrollo.

Libro Blanco de la Defensa Nacional 2018.

La Política de la Defensa Nacional del Ecuador emitida a través de su Libro Blanco 2018 considera los ciberataques como una amenaza de nueva procedencia, relacionados al libre acceso a medios tecnológicos, y que el avance en la automatización de los procesos, servicios y productos de las instituciones, sean estas públicas o privadas, incrementan su vulnerabilidad por ende del estado. Es el argumento por el cual los estados promueven la implementación de políticas y estrategias en ciberseguridad, ciberdefensa y defensa aeroespacial, para incrementar el potencial de las capacidades de Fuerzas Armadas en el en los nuevos escenarios con amenazas diferentes a las tradicionales.

Fuerzas Armadas claramente han definido como riesgo a:

> Los ciberataques y vulneración de la infraestructura crítica del Estado, que se basan en la explotación de las debilidades de las redes informáticas, ejecutadas a través de mecanismos tecnológicos de ciberterrorismo, ciberdelito, cibercrimen, ciber espionaje, e infiltración de los sistemas informáticos, convirtiéndose en un potente instrumento de agresión contra la infraestructura del Estado, lo cual podría comprometer la seguridad nacional".
>
> (Ministerio Defensa Nacional, 2018, pág. 53)

Con este antecedente, se ha formulado el posible escenario para FF. AA en el año 2030, en el que se espera que el sector Defensa impulse políticas de ciberdefensa que comprometa a las instituciones que por su naturaleza entren en el marco de la seguridad cibernética nacional y mantengan capacidad de respuesta ante la amenaza a la infraestructura critica del estado.

Finalmente, el Libro Blanco manifiesta que en el ámbito del desarrollo de la industria de la defensa pretende esta pretende ser potenciada por la generada nacionalmente manifiesta que ésta permite proveer de productos y servicios estratégicos especializados, que influyan en forma directa y tangible en las capacidades de las Fuerzas Armadas, con lo que incrementara su capacidad operativa en lo referente a ciberseguridad/ciberdefensa, la gestión de riesgos, las relaciones internacionales y el apoyo al desarrollo nacional.

Comando de ciberdefensa COCIBER

El Comando de Ciberdefensa (COCIBER) nace ante la necesidad de maniobrar las capacidades de defensa, exploración y respuesta que mantiene Fuerzas Armadas en el ciberespacio, orientado a proteger la infraestructura crítica y la información del estado con el fin de salvaguardar los intereses nacionales.

Se espera que hasta el 2021, se convierta en la organización que lidere el campo de la defensa, exploración y respuesta en el dominio cibernético, sobre la infraestructura crítica del país, con talento humano capacitado, equipamiento, software y tecnología de punta, actuando dentro del marco del sistema de ciberdefensa.

Protección de Infraestructura crítica del Estado.

El término Infraestructura Crítica es empleado para describir a los sistemas físicos y virtuales que dispone un estado y constituyen fuentes primarias sea de servicios o de financiamiento de los cuales se atiende a su ciudadana y que su funcionamiento no admite soluciones alternativas.

La Protección de las Infraestructuras Críticas o Estratégicas surge como necesidad por que se encuentra expuesta a un sin número de riesgos y amenazas sean de carácter natural o

antrópicos, razón por la cual los estados a través de sus órganos de control de protección tienen que diseñar protocolos y articular mecanismos de protección que garanticen el normal funcionamiento y brinden el servicio más eficiente a la colectividad.

Para cumplir con este objetivo de estado, los diferentes gobiernos abordan esta problemática desde diferentes enfoques, concomitantes con la realidad de cada uno de ellos, sin embargo, vale resaltar que esas perspectivas se resumen en los siguientes puntos: creación de un marco normativo estricto; impulsar las relaciones público-privadas. El objetivo principal en la protección de la infraestructura crítica es fomentar el desarrollo, mejorar significativamente los estándares de seguridad, ser previsivo con medidas oportunas de detección de amenazas tanto físicas como las provenientes del ciber espacio para garantizar un nivel de protección en que el Estado brinde esa seguridad a la inversión tanto nacional como extranjera.

Base Legal.

Constitución Política de la República del Ecuador.

El artículo 3 de la Constitución de la República del Ecuador es fundamental porque empieza recalcando la vigencia de los derechos humanos, libertades fundamentales de los ciudadanos y la seguridad social.

En el artículo 17 de la Constitución de la República del Ecuador garantiza el ejercicio eficaz y el goce de los derechos humanos sin discriminación alguna, haciendo referencia a más de la Constitución vigente a los pactos, declaratorios, convenios y más instrumentos internacionales de los cuales el Ecuador es signatario.

En el artículo 66 de la Constitución abordamos la educación, catalogándola como un derecho irrenunciable de las personas y tanto el estado, la sociedad como la familia deben velar

por el acceso a este bien básico. La educación se la califica como área prioritaria de inversión pública, la misma que garantizará el desarrollo de un estado buscando siempre la equidad social, mientras que el estado implementará todos los mecanismos necesarios para alcanzar este objetivo.

En el artículo 80 ya se establece la obligación del estado en fomentar la ciencia y tecnología en todos los niveles educativos, su objetivo es mejorar significativamente los estándares de calidad, lo que se traducirá en resultados positivos en productividad y competitividad con un manejo ordenado y sustentable en el tiempo de los recursos naturales que posee el estado y sobre todo suplir las necesidades básicas de la población, priorizando siempre los grupos menos favorecidos. También se establece las libertades a las actividades de orden científico y tecnológicas, mismas que se llevaran a cabo en universidades, escuelas politécnicas, institutos de educación superior, centros de investigación que brinden el sustento legal necesario para una actividad como esta.

En los artículos 83, 147, 261 se establece la corresponsabilidad de la ciudadanía en el mantenimiento de la paz y el orden social, así como la obligación del primer mandatario en direccionar la política de defensa nacional.

La Ley de Seguridad Pública y del Estado.

Esta ley es muy importante para el manejo de la seguridad en el estado ecuatoriano ya que a través de la regulación de la seguridad integral garantiza el orden público, la convivencia, la paz, el buen vivir etc., en donde el Estado empleando sus órganos de control deben trabajar en la prevención de todo tipo de riesgos y amenazas sean estas naturales o antrópicas. Para el cumplimento de esta ley el Estado deberá diseñar e implementar políticas, planes, acciones y

estrategias que garanticen la soberanía, integridad territorial y coadyuven a alcanzar el bienestar colectivo, el desarrollo integral y el pleno ejercicio de los derechos humanos.

Ley Orgánica de la Defensa Nacional.

En esta citada ley se define la misión constitucional de Fuerzas Armadas relacionada a la conservación de la soberanía nacional; la defensa de la integridad territorial y garantizar los derechos y libertades de los ciudadanos, pero además estar presente y colaborar con las instituciones del estado en el desarrollo del país, sus actividades económicas permitidas están relacionadas exclusivamente a materia de defensa y seguridad nacional, las competencias asignadas al Comando Conjunto de las Fuerzas Armadas están relacionadas con la planificación del empleo de las fuerzas, el mantenimiento de la seguridad nacional y la calificación de los recursos estratégicos relacionados con la seguridad nacional.

Ley de Comercio Electrónico

En la Ley de Comercio Electrónico para nuestro análisis nos referiremos al título V que trata sobre las infracciones informáticas, en su artículo 57 explica que se consideran como infracciones informáticas las de carácter administrativo y las que consten en el código penal la pena va desde un año hasta cinco con multas, esto cuando se haya violado las seguridades electrónicas o informáticas.

Código Orgánico Integral Penal.

En el COIP vamos a encontrar los delitos contra el derecho a la intimidad personal y familiar, donde se abordan temas que van en desmedro de la confidencialidad de la información personal, del mal uso de medios electrónicos para sacar provecho personal o para beneficio de terceros, información contenida en soportes informáticos de entidades públicas o privadas que

se den mal uso para beneficio personal o de terceros, hechos tipificados en esta ley y que van con sanciones de privación de la libertad de uno a tres años.

Ley de Protección de Datos Personales.

Actualmente el Ecuador esta desprotegido por la falta de una ley que proteja los datos personales. El proyecto de ley se encuentra en la Asamblea Constituyente para su debate y aprobación, sin embargo, es necesario realizar algunas puntuaciones sobre este proyecto de ley:

- Surge ante la falta de un mecanismo jurídico direccionado a proteger la información privada de los ciudadanos ante la proliferación de las amenazas derivadas del mal uso de los sistemas de información y del ciber espacio.
- Son muchos países en el mundo que al momento cuentan con una legislación en esta materia que ha servido no solo para regular la protección de datos personales sino para incrementar la productividad de las empresas en forma segura. El desarrollo de estas políticas ha sido de tal, que han servido de base en la implementación de políticas eficientes de gobierno electrónico, otorgándoles una connotación transnacional conjugando el lenguaje jurídico al desarrollo tecnológico.
- En el Ecuador la protección de datos personales no está estructurada en forma coherente, hay mucha dispersión de ideas y actores, denota un escaso enfoque a combatir las amenazas futuras producto del desarrollo tecnológico y de las necesidades mismas del usuario.

Ley de Transparencia Acceso a la Información Pública.

En esta ley se establece que todas las personas tienen acceso a la información pública y que además el Estado está en la obligación de garantizar este derecho. La información que manejan las instituciones, entidades, organizaciones o personas jurídicas de derecho público o

privado que tengan relación o participación con el Estado, las ONG's los institutos de educación superior que reciban beneficios del estado son sujetos al principio de publicidad, por ende, la información es publica, excepto las que constan en esta ley.

Libro Blanco de la Sociedad de la Información.

El Libro Blanco de la Sociedad de la Información y del Conocimiento (LBSIC), corresponde a una iniciativa del Ministerio de Telecomunicaciones y de la Sociedad de la Información, enmarcado en área sus competencias, que recoge las necesidades de la ciudadanía, enmarcada en el Plan Nacional de Desarrollo 2017-2021 Toda una Vida.

El objetivo principal trazado en este documento es dar a conocer los lineamientos que aportaran al fortalecimiento de la Sociedad de la Información y del Conocimiento en Ecuador, con lo cual se impulsará el crecimiento económico, la equidad e inclusión y la eficiencia de la administración pública.

En el contexto mundial la UIT (Unión Internacional de Telecomunicaciones) de la cual el Ecuador forma parte tomaron la definición de la Sociedad de la Información en base al desarrollo de las telecomunicaciones y el papel primordial que desempeñan en el desarrollo social, económico, cultural y militar de las sociedades; además tomaron conciencia de la mundialización de las telecomunicaciones y como estas deben desarrollarse en forma armónica con las políticas, las reglamentaciones, los servicios que los estados promulgan.

Para lo cual en la Asamblea General de las Naciones Unidas realizo la Cumbre Mundial sobre la Sociedad de la Información (CMSI) misma que se efectuó en dos fases, la primera en Ginebra en el 2003 y la segunda en Túnez en el 2005.

La primera tuvo como objetivo de materializar una declaración de voluntades en la cual se especifique medidas concretas que den el cimiento necesario de la Sociedad de la Información,

esta tomó el nombre de Declaración de Principios y el Plan de Acción, aprobada en diciembre del 2003; con una participación de representantes de 175 países.

La segunda en se realizó en Túnez en 2005 y su objetivo fue reconocer la importancia que ha tomado la revolución las TIC's y su incidencia en el desarrollo mundial, con la participación de representantes de 174 países del mundo.

A nivel regional en el 2005 en Rio de Janeiro (Brasil) se realizó la Primera Conferencia Ministerial Regional de América Latina y el Caribe, como resultado se diseñó un Plan de Acción que fue el instrumento que abrió la brecha de una visión regional y un compromiso político de los estados miembros para incentivar el acceso de estas importantes herramientas como sustento del desarrollo de la región.

En el Ecuador el punto más relevante para el diseño de una política en esta materia, se registra en 1995. Esta iniciativa estuvo liderada por el Consejo Nacional de Telecomunicaciones (CONATEL), por ser el organismo rector en telecomunicaciones. Una vez creado el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), en el año 2009, la Sociedad de la Información se vio fortalecida, uno de sus hitos más importantes fue la Estrategia Digital, que impulsó los pilares de: Alistamiento Digital, Banda Ancha y Gobierno Digital. En el 2013 con la implementación de Gobierno Electrónico en la Administración Pública Central, la Sociedad de la Información se vio fortalecida. Adicional destacamos otros hitos entre los cuales tenemos:

- Ley Orgánica de Telecomunicaciones en febrero del 2015
- Ley General de los Servicios Postales en octubre del 2015
- Ley Orgánica de Gestión de la Identidad y Datos Civiles en febrero del 2016
- Plan Nacional de Telecomunicaciones y tecnologías de Información del Ecuador 2016-2017.

Hipótesis

La Estrategia Nacional de Ciberseguridad permitirá disponer de un marco regulatorio basado en estándares internacionales que permita enfrentar y neutralizar las amenazas provenientes del ciberespacio que atentan contra la seguridad del estado.

Sistema de Variables.

Variable Independiente

Estrategia Nacional de ciberseguridad.

Variable Dependiente

Marco regulatorio para la gestión del sistema de ciberseguridad nacional que posibilite neutralizar las amenazas del ciberespacio.

Descripción de las Variables

Conceptualización de las Variables

Anexo “A” CONCEPTUALIZACIÓN DE LAS VARIABLES

Operacionalización de las Variables

Anexo “A” CONCEPTUALIZACIÓN DE LAS VARIABLES

CAPÍTULO III: MARCO METODOLÓGICO

Enfoque de la Investigación.

Considerando que la propuesta de construcción de una política pública requiere de una investigación muy completa del fenómeno social, este tema en particular empleó una investigación científica mixta, en la que el tratamiento de la información cuali-cuanti (cualitativa-cuantitativa), presenta resultados confiables y válidos, con sustento en el contexto teórico y metodológico.

Para el efecto sobre la base de la propuesta de (Sautu, 2003, pág. 250), se determinó que debe contener cada una de las variables que dan lugar a las estrategias metodológicas, partiendo de la concepción cuantitativa en la que se evidencia una mayor revisión de los conceptos teóricos que dieron lugar a las variables y sus relaciones.

En torno a las variables cualitativas se realizó un mayor énfasis en los aspectos epistemológicos del tema, esto es diseñar a lo largo de la investigación planteamientos axiológicos y éticos, que son una guía para enunciar los objetivos de investigación: identidad social y estigma. (Dalle, 2005, pág. 56)

Esta investigación evidencia la aplicación de un diseño No experimental, puesto que no existe la manipulación deliberada de variables, y sesgos en la interpretación de los resultados, manteniendo la objetividad de manera estandarizada, ya que se otorgó las mismas condiciones a todos los participantes.

Sobre la base del estudio presentado, fue pertinente el empleo de la investigación aplicada, especialmente al área técnica, donde el análisis del caso se particularizó a la construcción inicial del diagnóstico específico de la ciberdefensa y ciberseguridad del Estado.

La presente propuesta constituye un proyecto factible, porque en el lineamiento político estratégico está presente dentro de sus objetivos la Seguridad y defensa, lo cual nos permite establecer una línea de acción para presentar una estrategia de Ciberseguridad.

Tipos de Investigación.

En base al objeto de estudio y sus características, así como las particularidades del tema, se empleó la investigación aplicada e investigación exploratoria, considerando para el efecto la información obtenida de las fuentes primarias y secundarias, que se constituyeron en el personal especialista y técnico de ciertas instituciones públicas y privadas del Estado.

A través del estudio de este caso orientado a la ciberdefensa, se presentaron los puntos de vista y particularidades del tema dentro del ámbito regional y local, cuya indagación se articula a las necesidades del proyecto puesto que al no existir estudios específicos relacionados al tema de investigación en cuanto al entorno nacional; ser recurrió al empleo de fuentes bibliografías y conceptos dentro el contexto internacional que contribuyen al campo de estudio en entornos diferentes.

Esta investigación aplicó instrumentos de medición a las variables, donde se obtuvieron datos estadísticos que una vez analizados fueron puestos en evidencia, empleando para el efecto la investigación descriptiva.

El estudio se transforma en explicativo al obtener los datos y relacionarlos con el objeto de estudio y el problema a fin de obtener una solución mediante una propuesta de aplicación.

Población

Para la presente investigación se consideró cinco personas de las instituciones siguientes: Comando de Ciberdefensa de las FF.AA, organismo cuya misión es operar las capacidades de

defensa, exploración y respuesta en el ámbito cibernético a fin de proteger la infraestructura critica como la informática calificada como estratégica por parte del estado, en la Subdirección de Delitos Informáticos de la Policía Judicial a cargo de la investigación e inteligencia antidelincuencial de los cibercrímenes, en el Grupo de Seguridad Técnica Presidencial, unidad encargada de la seguridad de las primeras autoridades del país, en la Empresa pública de hidrocarburos del Ecuador (EP PETROECUADOR) y en la Corporación Nacional de Electricidad (CENEL) instituciones a cargo de gestionar dos de las infraestructuras críticas del país, en dos de los principales centros de educación superior como la Universidad de Fuerzas Armadas – ESPE y en la Escuela Politécnica Nacional, en dos instituciones bancarias cuya matriz se encuentra en la ciudad de Quito como son el Banco Pichincha y el Banco General Rumiñahui, en la Fiscalía General del Estado (Dirección de investigaciones Delitos Informáticos) institución que en coordinación con la Policía Judicial está a cargo de la investigación de delitos, y además con expertos en ciberseguridad provenientes del sector privado. Por consiguiente, la población está formada por 55 personas que laboran en las instituciones antes mencionadas.

Muestra

Tal como considera CLACSO en su metodología de la investigación, "El universo de estudio y las unidades de análisis comienzan a delimitarse cuando se construyen los objetivos de investigación. Sin embargo, estos adquieren mayor especificidad en la definición de la estrategia metodológica. En esta etapa del diseño, la selección de la muestra o los casos ocupa un lugar muy importante. Se trata de elegir un conjunto de unidades del universo de estudio de acuerdo con determinados criterios que el investigador considera relevantes en función de su objetivo de investigación" (Dalle, 2005)

Para esta investigación se empleó la técnica de muestreo no probabilístico intencional ya que permitió seleccionar casos característicos de una población limitando la muestra específicamente a estos casos. Además, que la población fue muy variable por consiguiente la muestra también lo fue.

Tabla 1.

Detalle de elementos tomados para muestra

INSTITUCION	PERSONAL ENCUESTADO
FUERZAS ARMADAS (COCIBER-EXPERTOS)	10
POLICIA NACIONAL (PJ DELITOS INFORMÁTICOS)	05
GRUPO DE SEGURIDAD TECNICA PRESIDENCIAL	05
INFRAESTRUCTURA CRÍTICA (CENEL)	05
INFRAESTRUCTURA CRÍTICA (PETROECUADOR)	05
UNIVERSIDADES (ESPE-EPN)	05
BANCA (PICHINCHA, BGR)	05
FISCALIA GENERAL DEL ESTADO	05
EXPERTOS SECTOR SEGURIDAD	05
EXPERTOS PARTICULARES	05
TOTAL	55

Nota. Esta tabla muestra de dónde se tomaron las muestras para realizar la presente investigación.

Métodos de Investigación

Para nuestra investigación se empleó el Método Hipotético Deductivo, ya que su procedimiento lógico y ordenado lo convierten una práctica científica que parte con varios pasos esenciales que son: observación del fenómeno a estudiar, creación de una hipótesis para explicar

el fenómeno, deducción de consecuencias o proposiciones y finalmente la verificación o comprobación de la verdad de los enunciados deducidos.

En este mismo orden de ideas, se partió de razonamientos individuales que en lo posterior se trasladó a conocimientos generales, al medir las variables del objeto de estudio se realizó una investigación cuantitativa, donde los resultados fueron sometidos a un tratamiento de información para obtener las respuestas sobre la investigación.

En términos generales en este método las hipótesis son consideradas los puntos de partida para las nuevas deducciones, tal como lo afirma Rodríguez Andrés "Se parte de una hipótesis inferida de principios o leyes o sugerida por los datos empíricos, y aplicando las reglas de la deducción, se arriba a predicciones que se someten a verificación empírica, y si hay correspondencia con los hechos, se comprueba la veracidad o no de la hipótesis de partida. Incluso, cuando de la hipótesis se arriba a predicciones empíricas contradictorias, las conclusiones que se derivan son muy importantes, pues ello demuestra la inconsistencia lógica de la hipótesis de partida y se hace necesario reformularla" (Rodríguez, 2017)

Técnicas de Recolección de Datos.

La recolección de datos se realizó sobre las fuentes primarias y secundarias del objeto de estudio, para las fuentes primarias se aplicó una encuesta y entrevistas y para las fuentes secundarias se aplicó un tipo de revisión bibliográfica.

Para el caso de la encuesta, esta se realizó con el fin de obtener el diagnóstico previo de la situación actual de la ciberdefensa en el Estado ecuatoriano, así como también entrevistas que son concebidas como herramientas metodológicas para recolectar datos cualitativos, cuyo fin es emplearlas cuando el problema de estudio no se lo puede observar o tiene cierta complejidad de hacerlo. (Hernández, 2010)

En lo correspondiente a la revisión bibliográfica, el acopio de la información se lo hizo en base a las fuentes primarias o documentos destacados en el ámbito de la ciberdefensa como son las normas constitucionales, COIP, Ley Orgánica de las Comunicaciones, Políticas Públicas de Defensa y de la Sociedad de la Información, entre otras. Así como también instrumentos internacionales que describen el apoyo y cooperación de Organismos internacionales como la OEA, UNASUR, CAN, etc.

Instrumentos de Recolección de Datos.

Sobre la base de los métodos y técnicas de producción de datos, según las diferentes estrategias metodológicas en la presente investigación recurrimos a las encuestas, dentro de la metodología cualitativa. Los instrumentos que se aplicaron para las fuentes fueron los siguientes: entrevista y guía de encuesta, las mismas que se aplicaron en forma física por los investigadores; también se aplicaron fichas bibliográficas que generaron cada miembro del equipo de estudio para la recolección de información.

Técnicas para el Análisis e Interpretación de Datos

Una vez finalizado el proceso de recolección de datos, inicia el proceso de análisis, no obstante, considerando que el análisis de datos en esta parte del estudio está enfocado a la combinación de estrategias cuantitativas y cualitativas, se desarrollará una estrategia secuencial ya que tal como afirma el Consejo Latinoamericano de Ciencias Sociales, “permite profundizar, complementar y comparar resultados aumentando la validez del estudio. Cualquiera sea el diseño seleccionado, el investigador debe dar cuenta de la estrategia que utilizará para analizar los datos. Esta constituyó una falencia recurrente en muchas de las propuestas” (CLACSO, 2005)

En este orden de ideas, para el análisis de la información se aplicó un análisis descriptivo para los resultados de las variables, donde se describió la distribución de las puntuaciones y frecuencias de los datos analizados en relación con las preguntas del cuestionario cerrado aplicado para el estudio.

La tabulación fue realizada en base a las preguntas, por lo que se obtuvieron los resultados en cada una. Abstrayendo los porcentajes del total, con conclusiones parciales. Para finalmente representarlos mediante gráficos tipo circular, puesto son los que brindan una mejor apreciación al lector.

La interpretación de los datos se los realizó en porcentajes verificados de las frecuencias con lo cual se puso énfasis en la interpretación cuantitativa de los resultados y no en los resultados matemáticos de estos. Ver Anexo “B” TABULACIÓN DE DATOS.

CAPÍTULO IV: DESARROLLO DE LA INVESTIGACIÓN

Diagnosticar, Cuál es la Situación Actual de la Ciberseguridad en el Ecuador

Introducción

El presente objetivo se encuentra alineado al diagnóstico de la situación actual de la ciberseguridad en el Ecuador, puesto que a través del tratamiento de la política pública en los distintos niveles con poder de decisión más los acondicionamientos estructurales necesarios para el uso del ciberespacio como quinto elemento geopolítico demuestran la relevancia que Estado ecuatoriano proporciona a la seguridad de su población y los recursos. En este sentido el análisis de la situación actual de la ciberseguridad permitió establecer la línea base a partir de la cual presentar una propuesta nacional que permita reducir la incidencia de las amenazas al Estado.

Conocimiento del hecho.

Actualmente el Estado ecuatoriano para enfrentar las menazas en el área de la defensa considera una estructura gubernamental establecida en el decreto ejecutivo 439 la cual estará dirigida por el Consejo Sectorial de Seguridad, y estará compuesta por los titulares de los ministerios de: Defensa Nacional, Interior, Justicia Derechos Humanos y Cultos, el secretario de Gestión de Riesgos y el Director del Centro de Inteligencia Estratégica. Uno de los objetivos de esta estructura es el de coordinar esfuerzos y así poder evaluar el cumplimiento de objetivos y metas de la agenda compartida, poniendo en marcha programas con visión interinstitucional de varios sectores.

Siguiendo con el análisis de la normativa Constitucional, en el Art. 3, numeral 8 se garantiza entre otros el derecho a la seguridad integral, así como en el Art.16. el derecho de todos

los ciudadanos en forma individual o colectiva al acceso a las nuevas tecnologías de información y comunicaciones.

Adicionalmente, en el art. 262 de la constitución, los GAD´s asumen la competencia exclusiva de emitir las políticas de investigación, desarrollo e innovación en su respectivo territorio alineadas a la Planificación Nacional, lo cual debe ser complementado con la integración regional, de acuerdo con el art. 423 numeral 2.

El Plan Nacional de Desarrollo Toda una vida para el período 2017–2021 se constituye como el lineamiento obligatorio dentro de la Planificación Pública del Estado ecuatoriano, articula los proyectos de largo plazo en los cuales interviene la sociedad, configurando una economía a su servicio para propender al cumplimiento de los objetivos nacionales, considerando primordialmente la sustentabilidad ambiental y el desarrollo territorial equitativo.

Uno de los instrumentos que tiene una gran relevancia es La ley Orgánica de la Defensa Nacional, que fue creada en base a los retos que impone la modernidad y desarrollo nacional, y permite organizar el sistema de defensa nacional al asignar atribuciones a los organismos que lo conforman y así poder cumplir con los preceptos constitucionales en el ámbito de la defensa nacional.

El Ministerio de Defensa Nacional como componente Político Estratégico de la Defensa, emitió sus políticas de Defensa a través del Libro Blanco mediante decreto ejecutivo Nº 633, en el que se articulan las estrategias y lineamientos que seguirá las Fuerzas Armadas para alcanzar sus objetivos frente a las amenazas identificadas para la seguridad y Defensa del Estado, cumpliendo los preceptos constitucionales en apoyo al Estado a través de sus diferentes organizaciones.

En lo referente al contexto internacional, El Ministerio de Defensa Nacional cumpliendo lo dispuesto en la Ley de Seguridad Pública y del Estado, juntamente con el Ministerio de Relaciones Exteriores tiene la responsabilidad de articular los convenios y acuerdos internacionales en cuanto a la Defensa refiere. Para el presente periodo se han visto fortalecidas las relaciones con países Europeos, Asiáticos, y Latinoamericanos, que mantienen una lógica de cooperación reembolsable y no reembolsable, cabe destacar que para el presente trabajo de investigación los convenios existentes que más se relacionan con la ciberseguridad y defensa son los que se mantienen con el Reino Unido de Gran Bretaña, México y Brasil.

Acorde a lo expuesto en las entrevistas a expertos, y en base a la investigación se determina que el Ecuador no posee una política pública orientada específicamente al ámbito de la Ciberseguridad, existiendo únicamente directivas e instructivos internos de las instituciones que se alinean a los procesos técnicos de sus usuarios más no a la implementación de un sistema que articule todos los sectores de la sociedad y que permita incrementar la seguridad del ciberespacio.

Análisis

Tal como se mencionó anteriormente según el art. 16 numeral 16 de la constitución, el Estado ecuatoriano garantizará a sus habitantes el derecho universal de acceso a las tecnologías de información y comunicación, así como también articular las decisiones político estratégicas en los consejos sectoriales de seguridad, sin embargo el tema particular de la Ciberseguridad vincula al sector Defensa como al Sector de las Telecomunicaciones, sin que exista aún una clara definición de la responsabilidad de la conducción en este tema en particular, donde se evidencia la ausencia de políticas públicas así como estrategias para proporcionar cibserseguridad tanto durante el uso como en la administración de bienes y recursos.

Conclusiones parciales

Ecuador garantiza en su norma constitucional la seguridad integral, protección de sus recursos y la planificación del desarrollo nacional, a esta ley suprema se suma la Planificación Nacional propuesta en el Plan Nacional de Desarrollo Toda una Vida, quien conjuntamente con la Secretaría Nacional de Planificación, son los encargados de delinear tanto los planes, y estos en relación con los programas y sus proyectos que beneficien al Ecuador, especialmente en áreas estratégicas considerando los nuevos escenarios, amenazas y riesgos, por lo que queda abierta la posibilidad para proponer y plasmar una estrategia en al ámbito de la ciberseguridad.

El empleo del ciberespacio es una temática de gran relevancia para la seguridad, especialmente debido a que dicho empleo se fundamenta en la globalización de las tecnologías de la información y comunicaciones (TIC) como se afirma en el Libro Blanco de la Defensa las Fuerzas Armadas deberán elaborar la estrategia adecuada a fin de dotar a las Fuerzas Armadas de la capacidad necesaria para poder intervenir en el ciberespacio y hacer frente a los actores que desde ahí pudieran atacar la infraestructura crítica del país. (Ministerio Defensa Nacional, 2018)

En este sentido, es necesario la planificación intersectorial e Interagencial para aplacar el déficit de políticas, estrategias y lineamientos con el fin de contrarrestar las amenazas que a través del manejo de las TIC´S, así como del uso criminal del ciberespacio afecten a la seguridad del Estado ecuatoriano en general.

Determinar el Grado de Cultura y Especialización en Ciberseguridad, que Existe en el Ecuador en las Diferentes Áreas de la Sociedad.

Introducción

El Estado ecuatoriano considerando la nueva dinámica geopolítica y entornos de la seguridad mundial, el surgimiento de actores multidimensionales, amenazas hibridas y riesgos globales, ha incrementado sus estrategias especialmente para mejorar la utilización del ciberespacio, incrementando entre otros programas la implementación de gobierno electrónico, aumentando la disponibilidad de comunicaciones, a la vez que su explotación a través de técnicas como el big data, y plataformas digitales.

Sin embargo, la propuesta que mantiene el currículo nacional tanto de educación general básica, como superior y el bachillerato general unificado es muy débil frente al escenario global, regional y nacional en el ámbito de la ciberseguridad.

En este sentido es necesario analizar cuáles serían las mejores propuestas para aprovechar las ventajas para el proceso de enseñanza – aprendizaje en la era de la información, en la que podría considerarse una opción el dotar de conocimientos de seguridad para el uso seguro de las tecnologías de la información desde el nivel primario, básica superior y bachillerato con el fin de proponer una alternativa de estudios orientados a satisfacer las necesidades y demandas en el tercer y cuarto nivel que corresponden a las carreras universitarias y en la que se evidencia el fortalecimiento profesional en el campo de la ciberdefensa.

Conocimiento del hecho.

Dentro del contexto nacional el incremento acelerado de los medios tecnológicos para los quehaceres rutinarios de los ciudadanos, así como los avances tecnológicos presentados por

las compañías públicas y privadas para mejorar el servicio a la comunidad son evidentes. Sin embargo, en el área educativa y de cultura, se presenta un gran desafío para el estado, debido a la existencia de grandes brechas de habilidades en relación con la capacitación obtenida por los usuarios y los mismos trabajadores informáticos que requieren de grandes habilidades digitales. En el Estado ecuatoriano son muy escasas las personas calificadas para ocupar estas posiciones. A nivel mundial la tendencia se mantiene, así por ejemplo los datos del gobierno chino enfatizan la carencia al menos de 7,5 millones de especialistas en TIC, mientras que, en Europa, las estimaciones apuntan a 500.000 puestos para los profesionales de las TIC que no están llenos en 2020. (Africa Code Week, 2018)

En el Ecuador, la planificación de la educación general básica y del bachillerato general unificado presenta propuestas muy elementales en la que se involucra a los niños y jóvenes en proyectos orientados al uso de los medios tecnológicos con fines didácticos únicamente (Ministerio de Educación, 2016, pág. 11).

El Ministerio de Educación creó el Sistema Integral de Tecnologías para la Escuela y la Comunidad (SíTEC), con el objetivo de proveer el equipamiento necesario como pizarras, proyectores, computadores, para los establecimientos de educación básica como secundaria, y así mejorar los programas educativos para facilitar la adopción del uso de las tecnologías.

En la universidad donde se imparte el nivel más alto de conocimiento, no obstante, no existe una oferta adecuada la cual cumpla con parámetros que le permitan adquirir habilidades y destrezas con un nivel calificado, por lo que por el momento se requiere especializarse en el exterior, hasta que se concreten ofertas educativas en el país.

En el año 2018 de acuerdo con la información provista por el Instituto Ecuatoriano de Estadística y Censos (INEC), cerca de la tercera parte de la población (35.1%) ha usado Internet el

último año. No obstante su acceso en el área rural todavía es exiguo en comparación al área urbana (17.8% en relación con el 43,9%). En cuanto al uso de internet su uso es mayoritario en los jóvenes cuyas edades están comprendidas entre los 16 y los 24 años lo que representa un 64,9%, tendencia que se ha mantenido durante los últimos cinco años. (Navarrete, Ginger, & Mendieta, 2018)

A diferencia de otras realidades, existen organismos no gubernamentales como Africa Code Week el cual involucra a un millón de jóvenes y equipa a 200,000 docentes de ciencias con recursos para enseñar TIC. En 2016, la campaña involucró a más de 400,000 estudiantes de 30 países con un 50% de participación de niñas en los Talleres de codificación. La Unión de Agricultores de Vietnam (VNFU) está capacitando a 30,000 agricultores en el uso de Internet, herramientas básicas de productividad y aplicaciones agrícolas. Argentina está capacitando a 100,000 programadores, 10,000 profesionales y 1,000 empresarios durante cuatro años.

Análisis

Los Estados y Organizaciones no gubernamentales se encuentran de manera permanente preocupados por presentar alternativas para mejorar sus capacidades y cultura de ciberseguridad, con el fin de mitigar las amenazas y riesgos que se encuentran en el ciberespacio. Sin embargo, Ecuador, aún no presenta una iniciativa integral en el área de la ciberseguridad, la misma ausencia de esta se evidencia en el contenido del currículo nacional de las instituciones de educación de nivel básico, medio y superior.

Tabla 2

Currículo por área de conocimiento

Área de conocimiento	Asignaturas para EGB	Asignaturas para BGU
Interdisciplinar	----------	Emprendimiento y gestión

*Nota***:** Esta tabla tiene como base información del Ministerio de Educación 2016.

Así como de instituciones Estatales públicas y privadas que urgen de una capacitación y adiestramiento de habilidades técnicas y de administración, puesto que a nivel local no existen o no se alinean a la realidad que la situación lo exige.

Conclusiones parciales.

La ciberseguridad y ciberdefensa es un tema de gran importancia en el contexto mundial, en la que los Estados, organizaciones no gubernamentales y actores multidimensionales se preparan de manera permanente para enfrentarse a los retos y desafíos que la utilización del ciberespacio y el dominio del Big Data los exige.

En este contexto se han creado leyes, normativas y disposiciones multisectoriales con el fin de normar el uso, empleo y administración de las redes tecnológicas que contribuyen al desarrollo de sus usuarios. Sin embargo, a nivel local existe un grave problema, por cuanto no se tienen claras las definiciones políticas y administrativas en torno a este tema. Por lo que es muy necesario y urgente proponer una estrategia que incentive a la comunidad académica, y a la sociedad en general que utiliza las TIC´S, a los miembros encargados de la Defensa, a fin de normar el uso y poder mantener un efectivo control de las plataformas tecnológica para contribuir al desarrollo nacional y optimizar los medios para proteger al Estado, la población y sus recursos estratégicos de las amenazas y riesgos multidimensionales existentes.

Determinar si en la Legislación Ecuatoriana se Encuentra Tipificado y Sujeto a Sanción las Acciones Ilícitas en el Ciberespacio y si Permite el Seguimiento y Control de la Ciberseguridad en las Instituciones del Estado.

Introducción

Como se puede inferir a través de este objetivo, se obtendrá información sobre la normativa legal vigente en cuanto a ciberseguridad, en lo que respecta a las sanciones sobre acciones ilícitas que se pueden realizar por parte de los diferentes actores multidimensionales a mediante el uso y administración de las plataformas digitales en el Estado ecuatoriano. Una vez revisada esta legislación se analizará la necesidad de implementar la estrategia más adecuada que minimice los efectos del crimen y delito informático sobre las personas y recursos estratégicos del Estado.

Conocimiento del hecho.

Tomando en consideración el avance tecnológico global, es muy importante observar cuales son las tendencias sobre el uso y administración de los recursos informáticos dentro de la normativa legal, debido a que quienes lo usan ilegalmente han crecido de forma exponencial logrando evadir las leyes y normas de seguridad, defensa, el accionar de fiscales y normas jurídicas de los Estados.

Es así como sorprende como dentro del informe de los mayores riesgos del mundo para el año 2019 se presentan a los ciberataques de robo de identidad personal con un 64%, los ataques que interrumpen la operación y la infraestructura con un 80%; y, robo de datos y dinero con un 82% (Informe Global de Riesgos, 2019).

En Ecuador la incidencia de los ataques cibernéticos se encuentra a la orden del día, tal como se demuestra en el mapa de ciberamenazas en tiempo real en el que figuramos en el puesto 53, no obstante en la madrugada del 11 de abril de 2019 Ecuador pasó a ocupar el puesto 25 según Kaspersky[2]

En este sentido es importante evidenciar que la Organización Mundial de Comercio, desde 1980, en su art. 61 establece los derechos de autor cuando se presentan casos de falsificación, y se menciona los procedimientos y sanciones penales. Del mismo modo el Convenio de Berna, La Convención de Estocolmo sobre la propiedad intelectual, la Convención de la Organización de Cooperación y Desarrollo Económico (OCDE) para la Protección y producción de Fonogramas de 1971, iniciaron el proceso para aplicar leyes penales contra el uso indebido de programas de computación.

La OCDE, ya en 1986 presentó a través de un informe las normas legislativas vigentes y las propuestas para contrarrestar el uso indebido de los medios informáticos mediante el establecimiento de sanciones, tal como posteriormente también lo haría las Naciones Unidas en cuando definió los Tipos de delitos informáticos en el año 1992.

En Wuzburgo fue presentada otra propuesta por parte de la Asociación de Derecho Penal en contra de los delitos informáticos y la subsidiariedad en caso de no tener el control desde el derecho consuetudinario.

Ya en 1997 en Madrid-España se realizaron las Segundas Jornadas Internacionales sobre el Delito Cibernético, donde se presentaron temas sobre el uso del internet, y el marco legal de la

[2] Empresa proveedora de servicios de seguridad de Tecnologías de Información considerado como uno de los más importantes del mundo

informática, las aplicaciones en la administración de las tecnologías informáticas y cibernéticas, su uso para el lavado de dinero, el contrabando y principalmente el narcotráfico.

En este sentido los países europeos con el propósito de disminuir el uso de los medios electrónicos para el cometimiento de delitos, establecieron un convenio específico sobre la Ciberdelincuencia, más conocido como El Convenio de Budapest del 23 de noviembre de 2001.

En lo correspondiente a los países del occidente, hasta la presente fecha existen consensos distintos, por lo que cada uno de los Estados dispone de su legislación propia, la que es emulada por otros países de acuerdo con sus capacidades y vulnerabilidades.

Claro ejemplo es el de los Estados Unidos que a partir de 1994 adoptó el Acta de Abuso Computacional, directamente relacionado al manejo de virus informáticos, contaminar programas o bases de datos, alterar, modificar o interrumpir la operación normal de los medios y herramientas tecnológicas, los sistemas o redes informáticas, donde ya se penaliza el delito con sanciones pecuniarias de $10000 por cada persona afectada y de $50000 en caso de acceder de manera imprudente a una base de datos.

En los países de la región se puede verificar como se han expedido cuerpos legales al respecto, así por ejemplo en Venezuela en el 2001 se emitió la ley contra los delitos informáticos, en Chile, la ley contra el delito de hacking, en República Dominicana la Ley contra los crímenes y delitos de alta tecnología, en El Salvador se emitió la Ley Especial Contra los Delitos Informáticos, y en Colombia la Ley de Protección de Datos personales.

En el Ecuador, la legislación vigente se pone de manifiesto en el Código Integral Penal (COIP), donde se tipifica y sanciona varias infracciones relacionadas al uso inadecuado de terminales móviles, revelación ilegal de información contenida en bases de datos, interceptación ilegal de comunicaciones, Transferencia electrónica de activos patrimonial, ataques contra la

integridad de sistemas informáticos. Ataques contra la confidencialidad de información pública reservada, ataques contra el acceso no autorizado a un sistema informático.

Análisis

De manera general observamos que dentro del contexto mundial, los Estados han sido coherentes al momento de elaborar sus políticas públicas de ciberseguridad y defensa, en la que fortalecen sus estrategias para enfrentar acciones que atenten al Estado y a sus recursos.

En este sentido los Estados han creado y contribuido a la formación de organizaciones gubernamentales, así como ONG´S que tienen por finalidad gestionar la política pública y privada en el ámbito de la ciberseguridad para disminuir el cometimiento de cibercrimen y sus delitos conexos que atentan a las personas y a los Estados.

A nivel Europeo, norte americano y América Latina, los Estados han plasmado sus políticas públicas en contra del mal uso de los medios tecnológicos, por lo que bajo su legislación han criminalizado las acciones ilícitas que se realicen en el ciberespacio, en la que han tenido muy buenos resultados.

No así en el caso ecuatoriano, que aún no dispone de un modelo de gobernanza en ciberseguridad y defensa que integre y materialice en una sólida estructura institucional su funcionamiento, así como sus alcances para enfrentar las ciberamenazas y ciberataques mediante una legislación propia que permita mantener un constante control y seguimiento dentro de la estructura del Estado.

Sin embargo, hasta que se presente esta propuesta, el COIP, mantiene dentro de la legislación nacional varios artículos que sancionan los delitos e infracciones en el ámbito de la seguridad de la información, no obstante estas aún no tienen el sustento necesario como para enfrentarse al mal uso del internet, los ciberataques, las crisis causadas por la información falsa

(fake new) generada y distribuida mediante la utilización de las redes sociales con fines violentos lo cual puede tener consecuencias impredecibles.

Conclusiones parciales

Se ha evidenciado el incremento de las oportunidades tecnológicas emergentes que requieren de la interconectividad física y tecnológica de manera acelerada generando un aumento en los ataques cibernéticos contra los Estados y las personas, tal como se presentó en el mapa interactivo de Kaspersky dando a conocer su verdadero poder en el que el ciberespacio que se constituye el quinto elemento geopolítico como objetivo central para su dominio y expansión.

El constante fallo en las operaciones empresariales, el corte de los flujos de suministro, las paras abruptas de los sistemas de control informático, los daños en infraestructura y las interacciones con los clientes, son preocupaciones que los tomadores de decisiones políticos tienen de manera permanente, para lo cual deberán establecer lineamientos inmediatos para enfrentar a este grave problema mundial.

Dentro de la política pública y legislación ecuatoriana existe una debilidad, ya que no se tiene un tratamiento adecuado a los delitos informáticos, y al mal uso de las plataformas digitales que afectan a las personas y los recursos, sin embargo existen pocos artículos del COIP que de manera disuasiva tratan el tema. Por lo que se hace evidente la necesidad de promulgar una estrategia que fortalezca el control del Ciberespacio, cuyos actores traten el tema de manera Interagencial, con presupuesto y bajo un solo conductor que enfrente a esta amenaza multidimensional y sobre todo que criminalice esta actividad bajo una legislación reflexiva y coherente.

Analizar la Existencia de Convenios Internacionales y su Ámbito de Aplicación en el Ecuador con Relación a la Ciberseguridad.

Introducción

Dentro del contexto mundial, las acciones tomadas por los diferentes Estados sobre el tema ciberseguridad se articulan a la lógica de sus capacidades estratégicas, sus recursos disponibles, el presupuesto disponible, su infraestructura crítica, sus procedimientos de gestión gubernamental y la necesidad de establecer un modelo de gobernanza para la defensa y seguridad, donde el apoyo internacional a través de acuerdos, convenios y cooperación reembolsable y no reembolsables son necesarios.

No obstante, para el Ecuador la construcción de una Política de ciberseguridad es un tema pendiente, puesto que aún no se dispone de un organismo rector en el área, el cual defina las acciones estratégicas y planes de acción que deberán adoptar de manera coordinada las instituciones públicas y privadas, desde los más altos niveles de decisión hasta los usuarios para hacer frente a este escenario que potencializa el uso del ciberespacio de manera acelerada.

Conocimiento del hecho.

Dentro del contexto mundial vemos que los Estados para definir una política propia de ciberseguridad inicialmente conceptualizan el problema, determinan sus capacidades estratégicas conjuntas públicas y privadas bajo estándares internacionales y se articulan a la lógica de mundialización del problema. Hablar de ciberataques y ciberdefensa por ejemplo es alinearse al ISO/IEC 27032_2013[3], como norma internacional, así como también tomar como referencia la

[3] Estándar internacional para ciberseguridad

Guía de la ciberseguridad para los países en desarrollo (ITU, 2007 /ITU,2011) como modelos para el establecimiento de estrategias de ciberseguridad con alcance nacional, constituyéndose evidencias de la importancia del relacionamiento internacional básico que deben propender los Estados.

En este mismo orden de ideas, la estandarización bajo normas internacionales permite articular las políticas y estrategias de los Estados, ya sea de manera bilateral y multilateral, por lo que es necesario hablar de una norma aceptada mundialmente como es la Organización Internacional de Normalización (ISO) que articula su sistema de gestión de seguridad de la información (SGSI)[4].

En su estructura, Ecuador dispone de los organismos responsables en el ámbito de las Telecomunicaciones y la Defensa, los cuales han sabido articular las normas nacionales en y alinearse a las normas internacionales, con el fin de mantener una lógica de cooperación cuando se lo requiera. Al interior del país es el Ministerio Telecomunicaciones el encargado de verificar el correcto uso del espectro electromagnético mediante la asignación de frecuencias fuera de la banda militar, y de ser el caso gestiona ante organismos internacionales como la Unión Internacional de Telecomunicaciones UIT la asignación de posiciones orbitales geoestacionarias o satelitales para el Ecuador (Ley Orgánica de Telecomunicaciones; Art. 107).

Acorde a lo expresado, el Estado ecuatoriano dispone de la Secretaria de Planificación y Desarrollo como la organización a cargo de formular la política pública de manera ordenada y coherente, de conformidad con la norma constitucional, y con el Plan Nacional de Desarrollo el cual par el período presidencial 2017 a 2021 se denomina Toda una Vida. Sin embargo la existencia de convenios y acuerdos internacionales en materia técnica sobre la aplicación de

[4] SGSI Sistema de gestión de seguridad de la información contenida en la ISO/IEC27000.

estándares relacionados a la ciberseguridad son muy limitados, constituyéndose en un problema que debe ser articulado de manera inmediata, ya que sus alcances están limitados únicamente al sector privado, lo que debilita el control hacia los sectores estratégicos del Estado, que a pesar de tener una cultura de seguridad no le limita a los ataques cibernéticos que a la fecha de estudio[5] se han visto vulnerados de manera permanente

Análisis

Frente a la problemática actual, gran parte de los Estados a nivel mundial poseen políticas y estrategias para el control, administración y regulación del ciberespacio, con el fin de minimizar los riesgos del uso ilícito de las redes y recursos informáticos contra los activos de información de la población y de la infraestructura crítica de los Estados.

Para enfrentar a estas amenazas en el área de la ciberseguridad, Ecuador cuenta con instrumentos propios vinculados tanto a la Defensa como a las Telecomunicaciones donde se definen los intereses del Estado y su articulación a la lógica de cooperación con sus pares a nivel internacional.

Sin embargo es imprescindible fomentar el apoyo mutuo en este ámbito con el fin de fortalecer una estrategia de ciberseguridad y ciberdefensa que proporcione los elementos necesarios para fortalecer las capacidades de gestión, control y administración de los recursos informáticos que le permitan actuar de manera permanente frente a incidencia de las amenazas multidimensionales en el campo de la ciberseguridad.

[5] Ataques cibernéticos a causa de la entrega de Julián Assange a la justicia Británica. Abril 2019

Conclusiones parciales

La estandarización de procesos y normas en base a estándares internacionales ha contribuido en la gestión de la ciberseguridad, permitiendo reducir la incidencia del uso inapropiado de los recursos informáticos, estableciéndose incluso procesos tendientes a la judicialización como medida de control en el ámbito de la seguridad y defensa de los bienes y recursos de los Estados.

El Estado ecuatoriano para mantener una estructura adecuada a la actual era de la información, ha iniciado una profunda reorganización institucional, sin embargo, hasta el momento no ha considerado el fortalecimiento de sus capacidades estratégicas de ciberseguridad, existiendo la necesidad de establecer mecanismos para la cooperación internacional y articulación de los esfuerzos de instituciones públicas y privadas nacionales para enfrentar a la amenaza multidimensional creciente en este ámbito.

Casi no existen convenios o acuerdos de cooperación internacional en cuanto a ciberseguridad se refiere pese a que en otras áreas existen convenios con países como Estados como Brasil, Colombia, México, Reino Unido de Gran Bretaña, Estados Unidos de América y España, por lo tanto existe el interés de las partes que puedan satisfacer los requerimientos de complementariedad y subsidiariedad que le permitan enfrentar de manera bilateral o multilateral al problema. Por lo que es necesario establecer de manera definitiva una alternativa que permita alinear las inmensas necesidades de ciberseguridad con las capacidades estratégicas, y los exiguos recursos del Estado.

Proponer las Políticas y Estrategias de Ciberseguridad para la Prevención, detección, protección y recuperación ante incidentes en el ciberespacio.

Introducción

Los ataques cibernéticos pasaron de ser una motivación intelectual, económica, política y social a ser un método más de cooptación de estructuras criminales al interior de organismos estatales y no gubernamentales con el fin de obtener información con el ánimo de acceder a recursos materiales y económicos, empleando para el efecto al ciberespacio, Tal situación ha pasado a ser preocupación de las agendas de los Estados, en la que se incluyen estrategias locales e internacionales para enfrentar a esta amenaza multidimensional.

El Estado ecuatoriano a través de sus ministerios correspondientes en las áreas de la defensa y de las telecomunicaciones, así como de la legislación nacional han tomado ciertos criterios de complementariedad y subsidiariedad para enfrentar los incidentes cibernéticos ejecutados a partir del mes de abril de 2019 manifestados a favor de Julián Assange y Wikileaks, empleando los recursos y capacidades estratégicas propias del Estado, que si bien es cierto se cree tener un blindaje para proteger su infraestructura y evitar el riesgo de ataques, no cuenta con la tecnología, ni el personal preparados para la mitigación inmediata de los riesgos de esta índole, tal como se evidencia en las encuestas y entrevistas a expertos.

De esta manera surge la necesidad de establecer mecanismos y directrices inmediatas con el fin de obtener una política pública coherente frente a los avances tecnológicos que contribuya a garantizar la seguridad de la información a través de limitar incidentes originados por diversos actores: hackers, activistas políticos, ciberdelincuentes, ciberterrorismos, entre otros.

Conocimiento del hecho

Asumiendo el hecho que la utilización ilegal de los recursos tecnológicos es frecuente hoy en día y que este fenómeno no ha surgido de manera inmediata, vemos que los Estados han potencializado sus políticas y estrategias en base a las experiencias propias como el caso de Julián Assange y Wikileaks y de terceros, como los ciberataques ejecutados por fuerzas regulares rusas contra el Estado de Georgia, en el año 2008, donde se produjeron ataques cibernéticos en tres fases: ataques de pequeña escala, ataques bien coordinados y organizados y ataques de menor escala, estos últimos empleados en el post conflicto.

Es evidente que esta forma de guerra no convencional afecta a todos los miembros y organizaciones propias del Estado, causando pérdidas de confianza, capacidad política, económica, social, militar y financiera del gobierno tanto a nivel interno como en el contexto internacional.

Estas dinámicas de conflictividad sugieren un aprovechamiento de los Estados para enfrentar al problema mediante el establecimiento de programas que concentren a toda la nación, con el fin de alcanzar los objetivos estratégicos conjuntos desarrollando nuevas estrategias, con tecnología e infraestructura de punta, capacitación, entrenamiento y soporte técnico local e internacional que contribuyan a las necesidades propias como es de suma urgencia en el caso ecuatoriano.

Es preciso además, considerar que, la incidencia de este problema de índole internacional ha sido aprovechado por muchos Estados desarrollados los cuales se adhieren a la política implementada especialmente por organismos multilaterales como la OEA, ONU y UE, donde sus decisiones político-estratégicas han permitido enfrentar a las amenazas cibernéticas con óptimos resultados.

Frente a esta dinámica de coerción y criminalidad establecida por actores físicos y virtuales en el ciberespacio es evidente el empleo de nuevas políticas y estrategias por parte del Estado ecuatoriano, con el fin de disponer de una política pública Interagencial para enfrentar las amenazas y disminuir su incidencia local e internacional, preservando el interés primario de la Constitución que es la vida de las personas, bajo un estricto orden democrático, sostenible y seguro.

Análisis

En el ciberespacio, se desarrollan actualmente millones de ataques cibernéticos con graves consecuencias sobre personas y recursos estratégicos de los Estados. Las amenazas y riesgos a las estructuras legales ya no solo son vistas a través de las computadoras e información digital, sino que van de la mano juntamente con actores físicos y virtuales que utilizan la electrónica, la nanotecnología y el espectro electromagnético como su punta de lanza para adueñarse del control del ciberespacio.

Bajo esta opción ilegal de la toma de control del poder, algunos Estados consideran el empleo del ciber poder, mediante políticas, estrategias y lineamientos que fortalecen el poder nacional el cual abarca el poder político, poder de la información, poder militar y poder económico, que a decir de María Cristina Rosas (2012) son elementos primordiales en el desarrollo de políticas nacionales de los Estados. (Rosas, 2012)

Sobre la base de la situación que vive actualmente el Estado ecuatoriano, y ante la falta de una política pública que determine claramente los objetivos, lineamientos y estrategias en el campo de la ciberseguridad, es necesario proteger de manera inmediata a la población y sus recursos delineado para tal efecto una estructura funcional apropiada la cual tenga participación

especializada de diferentes instituciones (Inter agencial) así como del sector privado del Estado ecuatoriano.

Conclusiones parciales

El fortalecimiento acelerado de las telecomunicaciones, así como el empleo generalizado de las TIC´S, incentiva para que los actores identificados que configuran las amenazas multidimensionales en el ciberespacio actúen de manera silenciosa disminuyendo los riesgos que los involucren dificultando su control y eliminación.

Bajo esta nueva dinámica ilegal de poder, los Estados desarrollados han creado estrategias tanto locales como regionales con el fin de enfrentar a estas amenazas. Estrategias que han sido socializadas y puestas a prueba, logrando resultados adecuados para sus necesidades.

Sin embargo, Ecuador se encuentra definiendo una nueva lógica de seguridad y defensa cuyo contexto se traduce a la nueva política de ciberseguridad y ciberdefensa, la misma que va a ser implementada con apoyo de las instituciones responsables., En la actualidad debido a la transversalidad de las tecnologías de la información, la ciberseguridad debe ser conceptualizada bajo el paradigma desde el diseño de los entornos, abarcando todas las áreas involucradas con un enfoque participativo de todos, adoptando la seguridad por defecto.

CAPÍTULO V: PRESENTACIÓN DE LA PROPUESTA

Título de la Propuesta:

Estrategia Nacional de Ciberseguridad 2020

Antecedentes de la Propuesta

El objetivo propuesto para esta investigación se refiere a la construcción de la política pública, con base en la normativa legal vigente en el Ecuador, que considera al ciberespacio como un medio necesario e importante en el desarrollo y evolución de lo Estado.

De este modo, la elaboración de una estrategia nacional de ciberseguridad fortalecerá la capacidad del Estado para identificar, gestionar, responder y mitigar los riesgos de ciberseguridad con el objeto de proteger la infraestructura crítica y sus activos de información, gestionando los riesgos y amenazas, entendidas desde una perspectiva integral, con la participación y colaboración de entes públicos y privados, centros de educación y la sociedad en general, a fin de asegurar la confidencialidad, integridad y disponibilidad de la información que permita la continuidad del estado.

Desarrollo de la Propuesta

La estrategia nacional de ciberseguridad producto de este estudio, tiene la finalidad de fortalecer la protección de la soberanía del Ecuador en este nuevo dominio, procurando incrementar nuestra resiliencia en caso de un ciberataque. Un ciberataque a los habitantes, la infraestructura crítica o a los intereses del Ecuador tiene la capacidad de dañarlo gravemente, por lo tanto, el Estado podrá hacer uso de medios digitales o físicos en su defensa, si así lo estimare necesario.

El Ecuador comprende que las amenazas existentes en el campo cibernético afectan a la seguridad del Estado, bajo este contexto la ciberseguridad en el Ecuador debe ser tratada de manera integral, involucrando a entidades tanto del sector público como privado y la ciudadanía en general. Esta política aporta al esfuerzo del Estado de brindar seguridad en el ciberespacio a todos los ecuatorianos desde el ámbito de su competencia.

Esta estrategia conlleva el cumplimiento de acciones en el área de la ciberseguridad, siendo su complejidad el motivo para plantear su horizonte de ejecución al corto y mediano plazo. En coherencia con los documentos de la planificación nacional para la Seguridad Integral y la Defensa Nacional, se mantiene el año 2030 como el horizonte temporal referente para llegar a su implementación.

Líneas de acción de la ciberseguridad

La ciberseguridad se ha convertido en tema de interés nacional e internacional, con el incremento de amenazas cibernéticas y el inevitable uso de tecnologías de la información en todos los ámbitos tanto público como privado. Como nos encontramos viviendo la llamada era de la información, la identidad de los ciudadanos es un activo digital y con ello se abre en el ciberespacio una nueva dimensión para el cometimiento de actividades ilícitas, que podrían producir consecuencias físicas, es decir que, una acción llevada a cabo en el mundo virtual puede llevar a graves consecuencias en el mundo real, con la capacidad de atentar incluso a la estructura, estabilidad, institucionalidad y gobernabilidad del Estado, alteración de la paz colectiva, amenazas a la soberanía y al ciudadano, atentando contra la seguridad que el propio Estado está obligado a brindar como condición a la sociedad para su normal desenvolvimiento.

A continuación, se detallan las siguientes líneas de acción:

- Capacidad del Estado para enfrentar las ciberamenazas

Se refiere a la capacidad de prevención, monitoreo, respuesta y recuperación.

- Seguridad de la información de la administración pública

  Se refiere a seguridad de la información que manejan las entidades del sector público.

- Seguridad de la infraestructura crítica

  Se refiere a la infraestructura crítica digital del país tanto público como privado.

- Cibercriminalidad

  Se refiere a delitos cometidos en el ciberespacio a través de medios digitales.

- Ciberdefensa

  Se refiere al aspecto de la ciberseguridad inherente a la defensa de la soberanía en el ciberespacio.

- Capacidad del sector privado ante ciberamenazas

  Se refiere a la capacidad de prevención, monitoreo, respuesta y recuperación que tiene el sector privado y su vinculación con el sector público para fortalecer y desarrollar esas capacidades.

- Sociedad y cultura de ciberseguridad

  Se refiere al rol que tiene la sociedad para la ciberseguridad y la necesidad de generar consciencia sobre la ciberseguridad.

- Investigación, desarrollo e innovación

  Se refiere a las capacidades del país para I+D+i en el ámbito cibernético.

Objetivos específicos de la propuesta

Objetivo 1: Fortalecer la ciberseguridad a nivel nacional.

E 1.1. Diseñar e implementar un marco nacional interinstitucional para proteger la información, sistemas y servicios del Estado de las diferentes ciberamenazas.

- Creando un Comité Interinstitucional de Ciberseguridad que coordine integre y socialice toda la información referente a la protección de las instituciones Públicas y privadas del Estado ecuatoriano ante posibles ciberamenazas.
- Participando de manera activa con los delegados de la Presidencia de la República, Vicepresidencia de la República, Ministerios de Gobierno, Telecomunicaciones, Defensa, Relaciones Exteriores, Centro de Inteligencia Estratégica, y Fiscalía General del Estado, así como también representantes de la academia, sociedad civil y público en general.

E 1.2. Actualización de la normativa jurídica nacional y desarrollo de normas técnicas necesarias para la ciberseguridad nacional.

- Delegando a la Fiscalía General del Estado y sus órganos competentes en coordinación con las Instituciones Públicas y privadas del Estado la actualización de la normativa nacional jurídica y técnica en el ámbito de la ciberseguridad.

E 1.3. Determinar el impacto de la interrupción de los servicios digitales públicos e identificar la infraestructura crítica nacional.

- Definiendo las infraestructuras que pueden ser consideradas como críticas en base a una normativa y metodología institucional, en coordinación del Comité Interinstitucional de ciberseguridad cuáles son.

E 1.4. Fortalecer la capacidad de respuesta ante incidentes.

- Determinando los estándares y niveles de seguridad de la información de acuerdo con sus particularidades y establecer los parámetros mínimos necesarios para proteger a los usuarios públicos y privados de los ataques informáticos.

Objetivo 2: Fortalecer la seguridad ciudadana y del Estado en el ámbito digital a nivel nacional.

E 2.1. Recopilar información estadística actualizada referente a las amenazas y riesgos a la seguridad ciudadana y del Estado.

- Integrando un equipo político y técnico que determine las competencias y atribuciones de los actores públicos y privados, mediante un diagnóstico nacional integral con la finalidad de sectorizar e impartir disposiciones para minimizar los riesgos y amenazas a la ciudadanía.
- Fomentando la participación de representantes de los sectores público y privados especialmente de los encargados de la defensa interna y externa del estado, así como el ente rector de las Telecomunicaciones.

E 2.2. Implementar en los GAD´S y juntas parroquiales normas y procedimientos que contribuyan a la administración de los recursos informáticos y digitales.

- Creando departamentos adscritos a los infocentros a nivel nacional donde se concientice el uso y la importancia de la ciberseguridad.

E 2.3. Localizar posibles actores que atenten a la seguridad de las personas y del Estado, especialmente en el ámbito de la ciberseguridad.

- Promoviendo la cultura informática y uso legal de los recursos tecnológicos involucrando a los principales actores de la sociedad en coordinación con las autoridades de los GAD´S.

Objetivo 3: Fortalecer la ciberdefensa para contribuir con la ciberseguridad nacional e incrementar la resiliencia del país, protegiendo la infraestructura crítica digital priorizada del Estado.

E 3.1. Proteger la infraestructura crítica digital de Fuerzas Armadas y la priorizada del Estado para garantizar el normal funcionamiento del país.

- Actualizando la normativa para la definición de infraestructuras críticas e infraestructuras críticas digitales del Estado.
- Elaborando en conjunto con el Comité Interinstitucional de Ciberseguridad el catálogo de infraestructuras críticas e infraestructuras críticas digitales del Estado
- Desarrollando la metodología para identificación y priorización de infraestructura crítica digital del Estado, en función de los sectores estratégicos establecidos en la Constitución

E 3.2. Fortalecer la capacidad de protección en el ciberespacio de la infraestructura crítica de Fuerzas Armadas y la priorizada del Estado.

- Actualizando la normativa en vigencia que permita el empleo de los recursos humanos y tecnológicos considerando el dominio del ciberespacio.
- Fortaleciendo el talento humano de las Fuerzas Armadas desarrollando la carrera militar de ciberdefensa.
- Incluyendo de manera transversal el quinto dominio de las operaciones en los cursos de formación y perfeccionamiento.
- Motivando la participación de personal especializado en la ciberdefensa.

E 3.3. Incrementar la investigación e innovación para el desarrollo de la capacidad de ciberdefensa.

- Priorizando líneas de investigación científica y tecnológica en el ámbito de la ciberseguridad identificadas en base a las necesidades.
- Incentivando en las universidades públicas y privadas el desarrollo del talento humano en áreas de ciberseguridad y ciberdefensa.
- Incentivando el desarrollo de líneas de investigación científica y tecnológica en ciberseguridad en universidades y centros académicos del país.
- Fortaleciendo la capacidad de respuesta ante incidentes por medio del CSIRT (Cyber Security Incident Response Team) en las Instituciones públicas y privadas del Estado.
- Implementando un Centro de Operaciones de ciberseguridad SOC (Security Operations Center por sus siglas en inglés) en cada Institución Pública del Estado.
- Potencializando el talento humano a través del desarrollo e implementación de carreras y plazas de trabajo enfocadas a la investigación científica y tecnológica en ciberdefensa.

E 3.4. Apoyar a los demás sectores del Estado en la protección de la infraestructura crítica nacional en caso de grave conmoción o crisis.

- Estableciendo los protocolos de colaboración con otras instituciones ante un incidente o un ataque en el ciberespacio.
- Incentivando la creación de estructuras de colaboración efectivas para la ciberseguridad y ciberdefensa.
- Estableciendo procesos y protocolos para compartir información relevante para la ciberseguridad nacional.

E 3.5. Fortalecer los lazos de cooperación internacional en materia de ciberdefensa.

- Desarrollando un plan de cooperación internacional en base a las necesidades identificadas para el fortalecimiento de la capacidad de ciberdefensa.
- Compartiendo información sobre amenazas y riesgos en el ámbito de la ciberseguridad con los países de la región
- Fortaleciendo la participación del Estado ecuatoriano en las reuniones bilaterales y mecanismos de integración con Colombia y Perú.

Objetivo 4: Construir una red público – privada para potenciar las capacidades nacionales para la ciberseguridad.

E 4.1. Fortalecer el sector público privado del Estado ecuatoriano en la implementación de protocolos y planes de contingencia en el ciberespacio desde un enfoque colectivo.

- Fomentando la participación de representantes de los sectores público y privados especialmente de la Presidencia de la República, Ministerio de Relaciones Exteriores y Movilidad Humana, Ministerio de Telecomunicaciones, Ministerio del Interior, Centro de Inteligencia Estratégica y GAD´S.

E 4.2. Promover el fortalecimiento del centro de operaciones gubernamental para el intercambio de la información sensible del Estado.

- Conformando un equipo técnico Interagencial que desarrolle la propuesta para materializar una red segura gubernamental en base a la normativa nacional.
- Estableciendo protocolos claros para el manejo de los recursos tecnológicos en base a la normativa legal y en vigencia.

E 4.3 Incentivar el ingreso de talento humano contratado, altamente calificado, en el ámbito de ciberseguridad

- Fortaleciendo el recurso humano y material del centro de operaciones gubernamental, con el fin de disponer de un medio eficiente para las instituciones públicas del Estado ecuatoriano.

Objetivo 5: Incrementar la concientización en materia de ciberseguridad.

E 5.1 Difusión de las directrices existentes sobre seguridad del manejo de la información.

- Socializando la información en medios oficiales y plataformas tecnológicas accesibles a la población y mediante campañas en los centros educativos públicos y privados a nivel nacional.
- Precautelando y restringiendo el uso de los recursos tecnológicos y plataformas virtuales públicas de manera objetiva.

E 5.2 Fomentar el intercambio de buenas prácticas nacionales e internacionales para incrementar la seguridad de la información del Estado.

- Participando de manera activa en foros, conferencias y espacios académicos públicos y privados a nivel nacional e internacional con el fin de acceder, a las más técnicas para el desarrollo de capacidades de ciberseguridad.
- Actualizando de manera permanente la información relevante en el ámbito de la ciberseguridad a través de los sectores públicos y privados, especialmente desde la Presidencia de la República, Ministerio de Relaciones Exteriores y Movilidad Humana, Ministerio de Telecomunicaciones, Ministerio del Interior, Centro de Inteligencia Estratégica y GAD´S.
- Capacitando al talento humano en temas administrativos, técnicos y de gestión en el ámbito de la ciberseguridad, tanto en el país como en el exterior.

E 5.3 Diseñar programas y campañas para fomentar la cultura de seguridad cibernética en el sector público privado

- Fortaleciendo y desarrollando centros de investigación para la investigación científica y tecnológica en el ámbito de la ciberseguridad.
- Generando vínculos con universidades y centros de investigación como apoyo a las actividades de la ciberdefensa.
- Creando alianzas público-privadas para la colaboración y el intercambio de experiencias e ideas en el ámbito de ciberseguridad.

Acciones inmediatas

Tabla 3.

Acciones inmediatas

ETAPA	ACTIVIDADES	RESPONSABLES	INICIO	FINALIZACIÓN
APROBACIÓN DEL PROYECTO DE TESIS	Presentación y Defensa del Proyecto	UFA "ESPE"		29/11/2019
PREPARACIÓN Y DIAGNÓSTICO	Conformación del equipo político y técnico	MINTEL	02/12/2019	03/01/2020
	Diagnóstico inicial y elaboración de hoja de ruta	MREMH		
	Identificación del problema y levantamiento de escenarios	MREMH		
	Mapeo de actores clave	MINTEL		
	Matriz de competencias	PRESIDENCIA		
	Diagnostico Nacional Integrado (público y privado)	PRESIDENCIA		
	Recopilación de información de ciberseguridad	CIES		
	Análisis comparativo de mejores prácticas	MREMH		
FORMULACIÓN DE LINEAMIENTOS, DEFINICIÓN DE POLÍTICAS	Desarrollo de seminario taller con temáticas referentes a cooperación internacional y bilateral del Estado ecuatoriano	MINTEL, MDI, MIDENA, CIES, MREMH,PRESIDENCIA	03/01/2020	06/03/2020
	Desarrollo de think tanks sobre ciberseguridad	MINTEL, MDI, MIDENA, CIES, MREMH,PRESIDENCIA		
	Participación: mesas de trabajo	MINTEL, MDI, MIDENA, CIES, MREMH,PRESIDENCIA		
	Priorización de amenazas y riesgos en el ciberespacio	PRESIDENCIA		
	Formulación de políticas, lineamientos, metas, indicadores, programas y proyectos.	PRESIDENCIA		
	Elaboración de documento de política	MINTEL		
APROBACIÓN Y AVAL DE POLÍTICA SECTORIAL E INCORPORACIÓN EN EL SISTEMA	Ajustes y validación de la propuesta a nivel del equipo técnico.	MIDENA	06/03/2020	05/06/2020
	Presentación de la propuesta para revisión y aprobación por el Gabinete Sectorial de Seguridad	GSS		
	Socialización de la Estrategia Nacional de Ciberseguridad	PRESIDENCIA		
	Presentación y aprobación de la política en el COSEPE	MIDENA		

Nota. Esta tabla muestra las etapas, actividades, responsables y tiempos de ejecución de la presente investigación.

Para el cumplimiento de las estrategias de ciberseguridad se deben definir parámetros administrativos, económicos y técnicos que son motivo de un análisis detallado, que salen de la propuesta, sin embargo, se pone a consideración, los siguientes:

a. Operadores de infraestructuras críticas. -

Se requiere definir:

- Catalogación y gestión de riesgo.
- Protocolos de Intercambio de Información.
- Plan de Respuesta ante Incidentes y Emergencias Cibernéticas en las Infraestructuras Críticas.
- Cronograma de Ejercicios y Simulacros.
- Directrices claras de Ciberseguridad a la Administración Pública.
- Perfiles adecuados de puntos focales y responsabilidades bien definidas.

b. Sector financiero. -

Involucramiento de los siguientes actores:

- Banco Central
- Superintendencia de Economía Popular y Solidaria
- Superintendencia de Compañías, Valores y Seguros
- Representantes del sector privado.

c. Educación y cultura. -

- Protocolos de Ciberseguridad para la educación de niveles básicos, básica superior, bachillerato, universidad hasta el tercer nivel.

- Desarrollo curricular de formación en Ciberseguridad en la educación universitaria y profesional (no solo a nivel técnico informático, si no en política pública, leyes, estrategia y Seguridad Nacional).
- Programas de investigación en Ciberseguridad.
- Programas de capacitación en Ciberseguridad para funcionarios públicos.
- Campaña nacional de concientización en Ciberseguridad.
- Programa de Protección de la Niñez en Línea.
- Identificación de programas existentes a nivel local.

d. Sector de tecnologías de la información y comunicaciones

- Se requiere Articulación de la Ciberseguridad con la agenda digital del país.
- Involucramiento de prestadores de servicios de comunicaciones.

e. Administración pública. -

- Involucramiento con las demás entidades gubernamentales, incluso la administración pública de los municipios.
- Procedimientos y trámites para la aprobación de la Estrategia Nacional de Ciberseguridad.

f. Sistema de justicia y marco legal. -

- Vinculación de la Estrategia Nacional de Ciberseguridad con otros planes de seguridad y desarrollo.
- Elaboración de legislación contra ciberdelincuencia y ratificación del Convenio de Budapest.
- Fortalecimiento de las capacidades de la Policía Nacional, Ministerio Público y Poder Judicial.
- Involucramiento de Poderes Judicial y Legislativo en la formulación de la Estrategia Nacional de Ciberseguridad.

g. Sociedad civil. -

- Establecimiento de principios orientadores.
- Establecimiento de un protocolo de divulgación responsable de vulnerabilidades.
- Protección de datos personales

Métodos y Criterios de Validación de la Propuesta

Como parte del proceso de validación se empleó la matriz FODA, como instrumento de carácter analítico, que puede ser aplicado a cualquier situación.

Tabla 4 .

Matriz FODA

FACTORES INTERNOS			
FORTALEZAS (PRINCIPALES)		**DEBILIDADES (PRINCIPALES)**	
F1	La Estrategia de Ciberseguridad es un proyecto prioritario para el Estado ecuatoriano, por lo que se suman instituciones públicas y privadas para su elaboración.	D1	Poco personal calificado y entrenado para obtener, analizar y presentar información relevante en el campo de la ciberseguridad.
F2	La política pública multisectorial orientada a la gestión del espacio y las comunicaciones se encuentra plasmada en la norma constitucional y en el Plan Nacional de Desarrollo 2017-2021	D2	Desconocimiento de la normativa en vigencia.
F3	Se articulan las necesidades entre el Ministerio de Telecomunicaciones, MREMH y Ministerio de Defensa Nacional para promulgar acuerdos y seguir una hoja de ruta a fin de construir la Política de Ciberseguridad del Estado ecuatoriano.	D3	Poco interés en plasmar acuerdos y convenios internacionales, por desconocimiento de los procedimientos de política exterior
F4	Conocimiento del tema y apoyo institucional de información de primera mano en el nivel político estratégico.	D4	No existe un adecuado direccionamiento estratégico.
FACTORES EXTERNOS			
OPORTUNIDADES (PRINCIPALES)		**AMENAZAS(PRINCIPALES)**	
O1	Las instituciones públicas del Estado que ofrecen productos y servicios en base a una infraestructura tecnológica disponen de centros	A1	Que la Asamblea Nacional no de paso a la firma de los nuevos acuerdos y convenios de cooperación internacional en el ámbito de la ciberdefensa

	CSIRT, que coadyuvan al cumplimiento de su misión constitucional		
O2	El Estado ecuatoriano a través del MREMH, promulga los requerimientos y necesidades de política exterior en el ámbito de la ciberseguridad.	A2	Que otras instituciones del Estado no permitan la aplicación por pugna de poder y de intereses.
O3	Acceso a la información privilegiada en el contexto internacional en el ámbito de la ciberseguridad	A3	Que la parte política minimice el riesgo en el ámbito de la ciberseguridad, limitando los convenios y acuerdos de cooperación en el contexto internacional
O4	Estrecha colaboración de entidades públicas dentro del Consejo Sectorial de Seguridad	A4	Resistencia al cambio por parte de las entidades públicas.

Nota: Esta tabla muestra las fortalezas y debilidades tanto de los factores internos como externos de la investigación sobre ciberseguridad.

Tabla 5.

Correlación significativa

	O1	**O2**	**O3**	**O4**	**A1**	**A2**	**A3**	**A4**
F1	+	+	+	+	+	+	+	+
F2	+	+	+	+	+	+	+	+
F3	+	+	+	+	+	+	+	+
F4	+	+	+	+				
D1	+	+	+		+			
D2	+	+	+		+	+		+
D3	+	+	+	+	+	+	+	+
D4	+	+		+	+	+	+	+

Nota: Esta tabla muestra con base a la muestra que se puede observar en la Tabla 1. La correlación significativa.

Tabla 6.

Puntuación en base al grado de correlación

	O1	O2	O3	O4	A1	A2	A3	A4
F1	4	4	3	3	3	2	2	2
F2	4	3	2	2	3	2	2	2
F3	4	3	3	3	3	2	1	2
F4	4	3	2	2	0	1	1	1
D1	4	2	3	0	2	0	0	0
D2	2	2	2	0	2	2	0	0
D3	1	1	1	0	3	2	1	1
D4	2	2	0	1	1	0	0	0

Nota: Esta tabla muestra la puntuación en base al grado de correlación

Tabla 7.

Valoración global

	O1	O2	O3	O4		A1	A2	A3	A4		
F1	4	4	3	3	**14**	3	2	2	2	**9**	**23**
F2	4	3	2	2	**11**	3	2	2	2	**9**	**20**
F3	4	3	3	3	**13**	3	2	1	2	**8**	**21**
F4	4	3	2	2	**11**	0	1	1	1	**3**	**14**

	16	**13**	**10**	**10**	**49**	**9**	**7**	**6**	**7**	**29**	**F78**

D1	4	2	3	0	**9**	2	0	0	0	**2**	**11**
D2	2	2	2	0	**6**	2	2	0	0	**4**	**10**
D3	1	1	1	0	**3**	3	2	1	1	**7**	**10**
D4	2	2	0	1	**5**	1	0	0	0	**1**	**6**
	9	**7**	**6**	**1**	**23**	**8**	**4**	**1**	**1**	**14**	**D37**
	25	**20**	**16**	**11**	**O72**	**17**	**11**	**7**	**8**	**A43**	**115**

Nota: Esta tabla muestra la valoración global obtenida con las encuestas.

Tabla 8.

Interpretación cuantitativa de la matriz FODA

FACTOR	PUNTUACIÓN	PORCENTAJE
Debilidades	37	16,08 %
Amenazas	43	18,69 %
Oportunidades	72	31,30 %
Fortalezas	78	33,91 %
Total	230	100,00 %

Nota: Esta tabla muestra los resultados cuantitativos obtenidos mediante el estudio de Fortalezas y Debilidades (FODA).

Dentro del análisis de la matriz FODA se ha identificado los siguientes resultados:

- Las fortalezas identificadas son mayores a las amenazas, y a las oportunidades.
- Las oportunidades mayores a las debilidades.
- Es necesario potenciar las fortalezas minimizando las amenazas

- Superar las debilidades nos permite aprovechar las oportunidades y protegernos de los efectos de las amenazas y proteger y fortalecer las potencialidades internas para minimizar las debilidades.

Tabla 9.

Estrategias FODA

	FORTALEZAS	**DEBILIDADES**
OPORTUNIDADES	**F-O** **ESTRATEGIA (MAXI – MAXI)** **UTILIZAN LAS FORTALEZAS PARA MAXIMIZAR LAS OPORTUNIDADES.** Fortalecer las capacidades estratégicas de las Instituciones gubernamentales para garantizar el derecho de las personas y la seguridad del Estado	**D-O** **ESTRATEGIA (MINI – MAXI)** **APROVECHA LAS OPORTUNIDADES PARA MINIMIZAR LAS DEBILIDADES** Gestionar los recursos tangibles e intangibles del Estado en materia de ciberseguridad sobre la base de la capacitación, entrenamiento y perfeccionamiento de las autoridades, técnicos y sociedad en general
AMENAZAS	**F-A** **ESTRATEGIA (MAXI – MINI)** **UTILIZAN LAS FORTALEZAS PARA MINIMIZAR LAS AMENAZAS.** Difundir la Política pública de ciberseguridad como eje prioritario de la seguridad y defensa del Estado ecuatoriano, considerando la Inter agencialidad y participación de todos los componentes del Estado	**D-A** **ESTRATEGIA (MINI – MINI)** **PARA MINIMIZAR LAS DEBILIDADES EVITANDO LAS AMENAZAS**. Impulsar el fortalecimiento crítico del talento humano público y privado en los institutos, universidades y escuelas politécnicas del Estado ecuatoriano en el ámbito de la ciberseguridad, TIC´S y sistemas computacionales.

Nota: Esta tabla muestra las oportunidades y amenazas que se pueden presentar en esta investigación.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La llegada de Internet estableció un nuevo esquema de comunicación a nivel global. La forma tradicional de comunicar, promocionar y difundir información de las organizaciones, empresas e instituciones dio un giro completo y se enfocó en este nuevo medio al cual lo consideró su mejor aliado.

El internet como herramienta global surgió para ser fortalecida, no se pensó en un riesgo de ataque o el robo de datos o información, era algo improbable, básicamente debido al pensamiento de que, al estar conectados, no había nada físico y se asumía como tácito que lo virtual no era susceptible de ser sustraído (robado), porque no había evidencia física de ello. Sin embargo, con el tiempo se fue comprendiendo la información que empezó a fluir por el internet y que era susceptible de ser interceptada, manipulada, modificada y eliminada.

De a poco, los Estados fueron implementando mecanismos de seguridad básica., surgiendo como primer gran paso los cortafuegos (firewall), sea hardware, software o ambos, mismos que se consideraron como el esquema de seguridad más adecuado para la protección de la información, la conectividad e infraestructura. Esto permitía tener el control de ingreso a las

redes locales desde el exterior, así como monitorear el tráfico interno hacia el exterior y proveer restricciones o autorizaciones.

A medida que las aplicaciones desarrolladas de la forma tradicional, sea para ejecutarse de forma local o en modo cliente servidor, empezaron a migrarse para ser usadas vía web, los requerimientos de seguridad fueron aumentando. Sin embargo, la seguridad no fue considerada inicialmente como un imperativo y se dio prioridad a la disponibilidad de los aplicativos en la web. Esto dio pasó a que muchos aplicativos tuvieran vulnerabilidades de diseño, programación o implementación, las cuales fueron aprovechadas inicialmente por usuarios con conocimientos avanzados a quienes se les denomina hackers, pero poco a poco se han hecho más asequibles para quien no posee mayor conocimiento que su pasión por el código.

La masificación de las aplicaciones y funcionalidades ejecutándose en internet, permite tener acceso a información en tiempo real y desde cualquier lugar del mundo, ha sido objeto de constante revisión y análisis en busca de vulnerabilidades y debilidades para explotarlas y así poder acceder a información no autorizada.

Hoy en día mejorar la seguridad es una preocupación primordial, por lo que han proliferado las soluciones para hacerlo a través de protocolos; el desarrollo de aplicaciones que permiten ocultar las direcciones IP; el cifrado de la información; sin contar que una de las primeras acciones fue el crear accesos restringidos a través de redes virtuales privadas (VPN), ya que se debe tener claro que Internet no es algo físico, pese a que abarca computadores, servidores, routers y demás infraestructura de red.

Actualmente, la seguridad dejó de ser el último elemento para considerar y está siendo parte de todo proceso de desarrollo y pruebas, previo a la puesta en producción de una aplicación. Pese a ello, los tiempos que puede demandar corregir vulnerabilidades o debilidades en las

aplicaciones son extensos, al tener que solucionar algo que por diseño no fue considerado, esto comercialmente obliga a que una vez implementada la aplicación se vayan generando actualizaciones de seguridad para corregir los errores, las cuales se van incorporando a medida que pasa el tiempo, siendo este tiempo el que puede ser aprovechado para explotar los agujeros de seguridad y obtener información valiosa o provocar fallos masivos en sistemas o aplicaciones.

Con el decremento en el precio de los dispositivos móviles estos se han popularizado adoptándose los dispositivos inteligentes en forma masiva, lo que ha generado un nuevo entorno para la obtención de información. La escaza preparación que se tiene de medidas de seguridad al usar la tecnología sin información personal o información crítica reservada y la necesidad de mantenerse conectado y estar a la altura de la tecnología, es el ambiente ideal para que, a través de miles y miles de aplicaciones, la información privada de las personas y confidencial de las instituciones pueda estar al alcance de unos cuantos clics y sin necesitar mayor esfuerzo que el desconocimiento.

La proliferación de los dispositivos móviles ha provocado que a nivel mundial, alrededor del 52% de tráfico web sea a través de smartphones, y su mayor utilidad sea para mensajería instantánea y redes sociales con un 74%. Adicionalmente, el 60% del tráfico es para compras online; y, un 59% del uso de la red es para la lectura de noticias.

Las estadísticas no hacen más que cuantificar el acceso no autorizado a la información privada de las personas. Unas tres cuartas partes del tráfico está enfocado a redes sociales y mensajería, siendo las aplicaciones que se usan para el efecto, objetivo de hackers o peor aún, aplicaciones maliciosas para acceder a información privada como cuentas bancarias, tarjetas de crédito de los usuarios y remitirlas a grandes centros de almacenamiento y procesamiento de datos (big data).

Nuevamente esto va atado a la educación, ya que por la premura de estar conectados o usar la mejor aplicación para la interacción en mensajería o redes sociales, los usuarios descargan aplicaciones y al momento de instalarlas, no leen detenidamente los acuerdos de uso, donde en la mayor parte de los casos (no en todos) se solicita autorización para recopilar información del usuario y compartirla o almacenarla para otros fines. Estos son los compromisos en general ignorados generalmente omitidos por las personas y luego, cuando se presenta algún inconveniente, es apenas conocida en detalle con la consiguiente insatisfacción de no haber tomado las precauciones del caso.

Recomendaciones

A medida que los avances en materia de conectividad han ido facilitando las comunicaciones mediante el uso de dispositivos inteligentes como teléfonos móviles, asistentes personales, computadores, en el plano personal, lo mismo ha sucedido en el ámbito industrial donde gran parte de la infraestructura denominada crítica por ser la encargada de proveer servicios necesarios para el funcionamiento adecuado de la nación, es controlada y administrada por sistemas de control, muchos de los cuales pueden ser accedidos a través de la red. Con ello, la seguridad toma un giro radical y pasa de ser algo enfocado al ámbito empresarial o individual, pasando a ser un tema de seguridad y defensa de los Estados.

Alrededor del mundo se tiene conocimiento de ataques e incidentes sobre sistemas críticos en muchos países, ya que los gobiernos cada vez dependen más de la tecnología digital, conectividad e internet. Esto crea la oportunidad para que existan no solo países sino también organizaciones que la aprovechen como oportunidad para generar ataques cibernéticos a otros estados, lo que les ha convertido en una especie de paraísos cibernéticos, ya que impulsan o apoyan la conformación de verdaderos ejércitos de hackers que están dedicados a efectuar

ataques para obtener información, como el caso del ataque a Google en 2010; o, afectar la infraestructura crítica de una nación como es el caso sucedido en 2015 el ataque conocido como BlackEnergy sobre la red de distribución eléctrica de Ucrania, el cual ocasionó que más de 225.000 personas se quedaran sin servicio.

El Centro de Estudios Estratégicos de Washington D. C., con base en datos estadísticos de ataques informáticos realizados sobre empresas de defensa, agencias gubernamentales, empresas de alta tecnología que representen pérdidas millonarias, de millones de dólares, entre otros, da cuenta que en hasta la actualidad son más de 120 los ataques han causado daños significativos a ese país.

En el Ecuador la situación de ciberseguridad no es diferente sin poder ser cuantificada económicamente pero si teniendo conciencia de su problemática, por lo que desde marzo de 2019, Ecuador inicio el desarrollo de una Estrategia Nacional de Ciberseguridad, con el financiamiento del Banco Interamericano de Desarrollo, y tiene como objetivo presentar cuatro productos: determinar la situación actual de la ciberseguridad en el país, articular un Plan de mejoras; y la Guía para la implementación de un (SOC) Centro de Operaciones de Ciberseguridad; y, una Metodología para el desarrollo de la Estrategia Nacional de Ciberseguridad, todo esto adaptado a la realidad ecuatoriana. (Ministerio de Telecomunicaciones MINTEL, 2018)

Considerando lo sucedido en abril del 2019, cuando se realizó el retiro del asilo político de Julian Assange, el fundador de Wikileaks quien estuvo asilado desde el 2012 en la Embajada de Ecuador ante el Reino Unido, se produjeron ataques sobre sitios web de varios gobiernos autónomos descentralizados y organismos del gobierno actividad atribuida a presuntos defensores y activistas del hacker australiano, sin que haya habido una reacción coordinada por parte de las autoridades o alguna institución ecuatoriana.

Los diferentes medios de prensa informaron en abril 15 de 2019, que producto del retiro del asilo a Assange, habían sido detectados más de 40 millones de ataques cibernéticos a diferentes infraestructuras del Ecuador, hecho informado por el Viceministro de TIC's.

Este hecho puso en evidencia la extrema necesidad de tener una política de ciberseguridad en el país, ya que cada entidad asume la seguridad de sus sistemas como a bien tenga. Y para una confirmación del problema, en agosto de 2019, uno de los principales bancos del sector financiero del Ecuador sufrió una caída de sus sistemas informáticos, atribuido a un ataque informático, lo que obviamente causó incertidumbre y preocupación de la ciudadanía en todo el sistema financiero.

A raíz de los ataques recibidos en abril de 2019, el Ministerio de Telecomunicaciones del Ecuador, solicitó la ayuda de países amigos, lo que hizo que Israel sea uno de los primeros en ofrecer su ayuda para mitigar el problema, dejando entrever la falta de una política de seguridad que obligue tanto a las instituciones públicas como a las privadas, a cumplir requisitos mínimos que garanticen la seguridad de la información de sus sistemas informáticos.

Previo a los eventos y ataques del mes de abril de 2019, el Ministerio de Telecomunicaciones y Sociedad de la Información, publicó una nota donde hace referencia a que Ecuador ocupa el sexto lugar entre 19 países de América Latina en lo que refiere a ciberseguridad. En concordancia con ello, diario El Comercio de Quito, publicó el 23 de septiembre un artículo donde indica que de acuerdo con el Índice Global de Ciberseguridad (GCI), el Ecuador se ubica en el séptimo lugar en América Latina, es decir se considera con un nivel medio de compromisos acatados. En dicho artículo también se hace referencia a que la mayoría de las entidades públicas aún mantienen su información en sus propias estructuras, y no en el centro de datos del gobierno. (Diario El Comercio, 2019)

La falta de una política de ciberseguridad ha provocado que cada entidad del sector público, empresa privada o entidad de cualquier tipo que tengas sistemas de información conectados a Internet, ha provocado que en repetidas ocasiones sus servicios se vean afectados. Esto conlleva una desconfianza de la ciudadanía que prefiere hacer sus transacciones de manera tradicional en lugar de usar servicios en línea que muchas entidades ofrecen; además de que, por cultura, en el Ecuador, la gente mayor parte de la gente adulta, excepto los Millennials, es escéptica en cuanto a la seguridad debido a que las noticias sobre fraudes cibernéticos abundan, y los casos presentados se vuelven virales rápidamente en las diferentes redes sociales.

Contribuyen a toda la problemática la falta de campañas de concientización, a través de programas de capacitación en seguridad de la información, actividad que debe ser dirigida tanto a nivel individual como empresarial o institucional, se concluye fácilmente que el país, pese a los rankings que dicen que estamos relativamente bien, debe establecer una política de ciberseguridad, en la cual estén involucrados los estamentos gubernamentales como el Ministerio del ramo, poder legislativo, judicial y las entidades de seguridad y defensa; y por la sociedad civil, organizaciones sociales y gremios empresariales.

Finalmente, es necesario plantear una pregunta que requiere una respuesta urgente: ¿Ecuador se encuentra preparado en materia de seguridad informática para hacer frente a las amenazas y riesgos en el ciberespacio y proteger a sus ciudadanos y su infraestructura crítica?

Independientemente de la respuesta el trabajo presentado contribuirá a la planificación de la política pública de ciberseguridad de nuestro Estado ecuatoriano.

Para lograr este objetivo, se pone a consideración de manera general las líneas estratégicas multisectoriales, las cuales fueron detalladas en base a la naturaleza y pertinencia de los sectores de seguridad, defensa y telecomunicaciones, entre otros.

BIBLIOGRAFÍA

Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL. (2018). *Boletín Estadístico - IV Trimestre 2018 - Ecuador.* Quito: ARCTOEL.

Bloomberg. (29 de May de 2018). *Bloomberg cybersecurity.* Obtenido de Mexico Foiled a $110 Million Bank Heist, Then Kept It a Secret: https://www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret

Center for Strategic and International Studies; McAfee. (5 de June de 2014). *CSIS.* Obtenido de Net Losses: Estimating Global Cost of Cybercrime: https://www.csis.org/analysis/net-losses-estimating-global-cost-cybercrime

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal.* Quito: Asamble Nacional.

Comité interministerial. (2017). *Estrategia Nacional de Ciberseguridad.* Mexico: Gobierno Nacional.

Comité Interministerial sobre Ciberseguridad. (2017). *Politica Nacional de Ciberseguridad 2017-2021.* Santiago : Ministerio del Interior.

Dalle, P. (2005). *Manual de metodología. Construcción del marco teórico, formulación de los objetivos y elección de la metodología.* Buenos Aires: CLACSO, Consejo Latinoamericano de Ciencias Sociales .

El Universo. (10 de Agosto de 2014). *Diario el Universo.* Obtenido de Ciberataques en el Ecuador: https://www.eluniverso.com/2009/05/13/1/1431/82615AC354164A25ABE48FCDE222C48E.html

Hathaway, M. (2018). *Gestión del Riesgo Cibernético Nacional.* Washington: Organización de estados americanos OEA.

Hernández, R. (2010). *Metodología dela Investigación.* México: Mc Graw Hill Educación.

HM Government. (2016). *Estrategia de Ciberseguridad Nacional 2016-2021.* Londres: HM Government.

Instituto Ciberseguridad Española. (2013). *Estrategia de Ciberseguridad Nacional.* Madrid: Presidencial del Gobierno.

Instituto Nacional de Estadistica y Censo INEC. (2017). *Tecnologías de la Información y Comunicación ENEMDU-TIC 2017.* Quito: INEC.

International Telecomunications Union. (2008). *SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD, Aspectos generales de la ciberseguridad.* New York: ITU.

Lloyds of London;. (17 de July de 2017). *Lloyds bank.* Obtenido de Extreme cyber-attack could cost as much as Superstorm Sandy: https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report

Ministerio de Educación. (2016). *Educación General Básica SUPERIOR.* Quito: MINEDUC.

Ministerio de Telecomunicaciones MINTEL. (2018). *Libro Blanco de la Sociedad de la Informción y el Conocimiento 2018.* Quito: MINTEL.

Ministerio Defensa Nacional. (2018). *Politica de Defensa Nacional, Libro Blanco 2018.* Quito: MDN.

Ministerio del Interior. (2011). *Lineamiento de Política para ciberseguridad y Ciberdefensa.* Bogota: Departamento Nacional de Planeación.

MINTEL. (2018). *Plan Nacional de Gobierno Electrónico 2018-2021.* Quito: MINTEL.

National Audit Office. (27 de October de 2017). *Investigation: WannaCry cyber attack and the NHS.* Obtenido de National Audit Office: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

Navarrete, Ginger, & Mendieta, R. (2018). *LAS TIC Y LA EDUCACIÓN ECUATORIANA EN TIEMPOS DE INTERNET.* GUAYAQUIL: ESPIRALES.

OEA-BID. (2017). *Informe Ciberseguridad 2016.* Washington: OEA.

OEA-CICTE. (2012). *Declaración Fortalecimiento de la seguridad cibernética en las américas.* Washington D.C.: OEA.

Rodríguez, A. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Escuela de Administración de Negocios*, 1-26.

Rosas, M. C. (2012). *¿Seguridad amplia o militarización? Rumbo a una agenda de seguridad nacional para México.* México: Olof Palme A.C.

Secretaria Nacional de Planificación y Desarrollo SENPLADES. (2017). *Plan Nacional del Buen Vivir Toda una Vida 2017-2021.* Quito: SENPLADES.

UIT, COMSEC, CTO, OTAN(CCDCOE). (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad.* Ginebra: Creative Commons Attribution 3.0.

Vargas, R., & Recalde, L. . (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *Urvio*, 5.

Vargas, R., & Recalde, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *Urvio No. 20*, 5.

ANEXOS

ANEXO "A". *(Click para visualizar la información)*

Dentro de la Carpeta "Anexo A", se encuentran los siguientes documentos:

- Figura 1. Nivel de seguridad den el Ecuador
- Figura 2. Acciones del estado ecuatoriano
- Figura 3. Medidas de seguridad implementadas
- Figura 4. Lugar donde capacitarse
- Figura 5. Necesidad para controlar ciberespacio
- Figura 6. Preparación de las instituciones
- Figura 7. Conocimiento problemas ciberseguridad
- Figura 8. Nivel de conocimiento
- Figura 9. Conocimiento de convenios internacionales
- Figura 10. Ámbitos de cooperación internacional