Polo del Conocimiento

Pol. Con. (Edición núm. 56) Vol. 6, No 3
Marzo 2021, pp. 1229-1250
ISSN: 2550 - 682X
DOI: 10.23857/pc.v6i3.2431

Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano

Analysis of public cyber security policies. Ecuadorian case study

Análise de políticas públicas de segurança cibernética. Estudo de caso equatoriano

Alan Eduardo Leyva-Méndez [I]
alanleyvamendez@gmail.com
https://orcid.org/0000-0002-1647-1953

Correspondencia: alanleyvamendez@gmail.com

Ciencias técnicas y aplicadas
Artículo de revisión

***Recibido:** 26 de febrero de 2021 ***Aceptado:** 02 de marzo de 2021 * **Publicado:** 12 de marzo de 2021

I. Magister en Sistemas de Información Mención en Gestión de Seguridad de la Información, Ingeniero en Sistemas Informáticos, Docente Investigador de la Carrera de Tecnologías de la Información en la Facultad de Ingenierías de la Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador.

Resumen

La seguridad cibernética se ha convertido en un aspecto clave de los estudios estratégicos para el establecimiento de políticas públicas en las naciones y, el Estado ecuatoriano no escapa a ello. El desarrollo de dichas políticas coincide con el crecimiento de la sociedad de la información, las redes entre servidores informáticos y el fenómeno del ciberespacio el cual, reflejado en la cotidianidad por el internet, se ha establecido como una nueva dimensión para la guerra moderna y afecta sensiblemente la vida de toda la sociedad y, más aún en los tiempos pandémicos que vivimos. En tal sentido, se plantea un estudio del caso de la República del Ecuador en función a las políticas públicas que rigen a la nación en el espectro de la seguridad cibernética, con la objeto de cumplir con el propósito de analizar la situación estratégica que delinea la política del Estado ecuatoriano, basándose en una metodología de investigación documental por medio del método de estudio de caso, fundamentado en el enfoque cualitativo, sostenido por la revisión documental y la recopilación de fuentes para el desarrollo del tema y posteriormente discutir las reflexiones suscitadas del tema.

Palabras claves: Política pública; seguridad cibernética; ciberdefensa; ciberataque.

Abstract

Cybersecurity has become a key aspect of strategic studies for the establishment of public policies in nations and the Ecuadorian State does not escape it. The development of these policies coincides with the growth of the information society, the networks between computer servers and the phenomenon of cyberspace which, reflected in daily life on the internet, has established itself as a new dimension for modern warfare and affects sensibly the life of the whole society and, even more so in the pandemic times that we live. In this sense, a study of the case of the Republic of Ecuador is proposed based on the public policies that govern the nation in the spectrum of cybersecurity, in order to comply with the purpose of analyzing the strategic situation that outlines the policy of the Ecuadorian State, based on a documentary research methodology through the case study method, based on the qualitative approach, sustained by the documentary review and the collection of sources for the development of the subject and later discuss the reflections raised on the subject .

Keywords: Public policy; cyber security; cyber defense; cyber attack.

Resumo

A segurança cibernética tornou-se um aspecto fundamental dos estudos estratégicos para o estabelecimento de políticas públicas nas nações, e o Estado equatoriano não escapa dela. O desenvolvimento destas políticas coincide com o crescimento da sociedade da informação, das redes entre servidores informáticos e do fenómeno do ciberespaço que, reflectido no quotidiano da Internet, se consagrou como uma nova dimensão para a guerra moderna e afecta sensivelmente a vida dos toda a sociedade e, ainda mais nos tempos de pandemia que vivemos. Nesse sentido, propõe-se um estudo do caso da República do Equador com base nas políticas públicas que regem a nação no espectro da cibersegurança, a fim de cumprir com o propósito de analisar a situação estratégica que delineia a política do Equador. Apresentar, com base na metodologia de pesquisa documental através do método do estudo de caso, com base na abordagem qualitativa, sustentada na revisão documental e na recolha de fontes para o desenvolvimento da temática e posteriormente discutir as reflexões suscitadas sobre a temática.

Palavras-chave: Políticas públicas; segurança cibernética; defesa cibernética; ataque cibernético.

Introducción

Según Sancho (2017), “todo sistema político requiere considerar tres factores básicos: seguridad como condición, institucionalidad como medio y desarrollo como objetivo”. Considerando esto, la seguridad en el ciberespacio representa una condición ineludible para las relaciones dentro de un Estado. La utilización de las tecnologías de información y comunicación en el accionar de todas las actividades de los Estados y de la sociedad en general, supone que la dependencia de las redes de internet y del ciberespacio constituya la entrada a que se produzcan las ciberamenazas y/o los ciberataques, entendiéndose que para este nuevo panorama de acción no existen limitantes y, dichas amenazas afectan la seguridad de las naciones y de sus ciudadanos, paralizando la infraestructura crítica del Estado generando considerables pérdidas económicas.

Con ello, se tiene que, en los países desarrollados, la seguridad cibernética se caracteriza por poseer un enfoque integral, que considera aspectos económicos, sociales, educativos, jurídicos, técnicos, diplomáticos, militares y relacionados con la inteligencia. Tanto así, que las consideraciones de soberanía en la formulación de políticas públicas van direccionadas a las ramas militares, policiales, entes privados y redes de inteligencia de los gobiernos (Organización para la Cooperación y el Desarrollo Económico, 2012)

Por tanto, la seguridad cibernética se ha convertido en un aspecto fundamental para la seguridad nacional y, la República del Ecuador, como país en vías de desarrollo presenta vulnerabilidad ante las ciberamenazas, ya que se aprecia que los delitos cibernéticos se han convertido en agentes más sofisticados, tornando complejas las actividades de ciberespionaje militar, industrial y político. El Estado ecuatoriano, busca como optimizar los recursos económicos, humanos, teóricos y financieros disponibles en el campo de la seguridad cibernética; ya que la dependencia de las tecnologías de información y comunicaciones (TICs) extranjeras representan un riesgo a nivel de ciberseguridad, tanto a nivel financiero, como político y estratégico.

Es por ello que, de acuerdo con Delgado, (2014) se asume que "en los últimos años se ha evidenciado un esfuerzo importante por parte del Estado Ecuatoriano por adaptarse a las nuevas amenazas que supone el entorno digital. El Ministerio Nacional de Defensa, señala que considera al espacio cibernético como "vital" para la seguridad del Estado y sus ciudadanos, por lo que busca accionar en el desarrollo de capacidades operativas y políticas específicas".

En tal sentido, la importancia de la transformación digital de la sociedad se ha puesto como objetivo prioritario en la agenda de la mayoría de los Gobiernos y, específicamente en el Ecuador. Las políticas públicas del Estado se deben orientar en función a una Estrategia Nacional de Seguridad Cibernética, en donde se busque garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección, defensa, análisis, investigación, recuperación y respuesta a ciberataques y, de acuerdo con González (2018) se reconoce al ciberespacio como "un nuevo ámbito de relación que ha proporcionado el desarrollo de las nuevas tecnologías de la información y las comunicaciones, diluyendo fronteras, permitiendo una globalización sin precedentes, propiciando nuevas oportunidades, pero que conlleva serios riesgos y amenazas".

En el Ecuador, las nuevas tecnologías se patrocinan con esmero y en forma acelerada por el retraso frente a las economías de la región, en el escenario gubernamental se están explotando 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. En contexto, la Organización de Estados Americanos, establece que el Ecuador, así como muchos países de la región latinoamericana, es susceptible a ataques cibernéticos potencialmente devastadores, al no contar con estrategias concretas en el ámbito de seguridad cibernética, planes que protejan la

infraestructura crítica o un organismo bien desarrollado que asuma el comando y control de la 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.

Por lo anteriormente descrito, es fundamental tomar esta temática desde el punto de vista de las políticas públicas que se han formulado en torno a la ciberseguridad en la República del Ecuador, con el propósito de analizar las políticas públicas basadas en las estrategias de seguridad cibernética que rigen en el Estado ecuatoriano.

En tal sentido se plantea la investigación documental, basado en el análisis de fuentes primarias de documentos impresos y electrónicos referidos a las políticas públicas que establecen el análisis del caso de estudio en las estrategias en seguridad cibernética que sigue el Estado ecuatoriano.

Desarrollo

A continuación, se muestran fundamentos importantes para la temática a abordar, como lo es: la política pública; aspectos importantes sobre: ciberespacio, ciberdefensa y ciberseguridad; algunos aspectos a tomar en cuenta para las estrategias nacionales en seguridad cibernética y políticas públicas y ciberseguridad.

Política Pública

Según Cortés (2015), "las políticas públicas son el conjunto de objetivos, decisiones y acciones que lleva a cabo un gobierno para solucionar los problemas que en un momento determinado los ciudadanos y el propio gobierno consideran prioritarios (p. 11). Por lo cual, desde este punto de vista, las políticas públicas se pueden entender como un proceso que se inicia cuando un gobierno o un directivo público detecta la existencia de un problema que, por su importancia, merece su atención y termina con la evaluación de los resultados que han tenido las acciones emprendidas para eliminar, mitigar o variar ese problema (Bañon & Carrillo, 1997).

Luego, Guerrero (2007), detalla que las políticas públicas ponen de manifiesto la naturaleza y la composición interna del sistema jerárquico de autoridades y dan cuenta del régimen de competencias y responsabilidades en el ejercicio del poder institucionalizado, que constituyen el referente crucial que fundamenta su razón de ser gubernamental en la acción estatal y la acción pública, es decir, los gobiernos (vías las políticas) hacen que la interacción orgánica entre el Estado y la sociedad se exprese y cumpla un propósito definido; estas deben ser comprendidas como el

vector que sintetiza el conjunto de proposiciones, decisiones y operaciones dinámicas e interdependientes entre actores políticos, sociales e institucionales, a través de las cuales se busca imprimir un rumbo a la sociedad (p. 27).

Por tanto, Guerrero (2007), infiere en que para entender la Política Publica se debe presentar la Tipología de Políticas Públicas de acuerdo a tres corrientes de tendencia estructuralista, a saber:

1. Hegemónicas, que reflejan los intereses del proyecto político hegemónico.
2. Transaccionales, producto de negociación entre sectores de poder.
3. Dominación, que buscan preservar un orden establecido.

Especifica Cortés (2015), que en la perspectiva de incorporar en el análisis las tensiones y conflictos que se originan y desarrollan en los procesos de estructuración y trazado de políticas públicas, estas pueden clasificarse de acuerdo con dos grandes criterios, su inscripción en el régimen político y su finalidad (p. 12). Por su inscripción en el régimen político, pueden ser:

- **Estructurales:** ya que dan cuenta de la razón de ser del estado y del ejercicio de gobierno, y que, por su naturaleza, son continuas, no descentralizables, ni delegables; asimismo, expresan claramente la función gubernativa del estado (por ejemplo, la política monetaria, fiscal o de defensa nacional).
- **Sectoriales:** dan cuenta de la manera en que está dividido orgánica y funcionalmente el aparato estatal; no necesariamente son continuas, pueden ser descentralizadas o delegables en otros niveles e instancias de la administración pública o de la sociedad (por ejemplo, la política social, industrial, etc).
- **Territoriales:** por lo que dan cuenta de la distribución de competencias y responsabilidades entre niveles de gobierno. Hacen relación a la razón de ser del Estado y el gobierno en los escenarios de mayor relación con los ciudadanos, involucra los elementos mínimos requeridos para la vida en comunidad (por ejemplo, las políticas de servicios públicos, políticas de seguridad y orden público).

Por su finalidad, pueden ser:

- **Inerciales**, por su naturaleza, buscan mantener el rumbo de la acción del Estado y de la sociedad en la consecución de un propósito (por ejemplo, la lucha contra la inflación, las políticas de justicia y bienestar social).

Pol. Con. (Edición núm. 56) Vol. 6, No 3, marzo 2021, pp. 1229-1250, ISSN: 2550 - 682X

- **Promocionales**, por su naturaleza, buscan recomponer la correlación de fuerzas (sectorial o territorial) presentes en la gestión de determinadas acciones del Estado o de la sociedad (por ejemplo, las políticas de distribución del ingreso, la política de la paz).
- **Compensatorias**, se encaminan hacia la restitución de los equilibrios sectoriales o de la dinámica del crecimiento.
- **Contingentes**, busca enfrentar, con carácter estructural, problemas o situaciones inesperadas que, por su magnitud, general desestabilización o producen conmoción social.

Aspectos importantes sobre: ciberespacio, ciberdefensa y ciberseguridad

En la actualidad se puede observar que cuanto mayor es el índice de desarrollo de una sociedad, mayor dependencia se tiene de los sistemas de información y de las comunicaciones (Leiva, 2015), por lo que el mismo autor, menciona que cualquier intrusión, manipulación, sabotaje o interrupción de estos sistemas y de la Infraestructura Crítica de la Información - ICI pueden llegar a ser afectadas millones de personas. Asimismo, refiere que en los conflictos tradicionales existen fronteras y límites, mientras que en el ciberespacio no es así.

Por su lado, Valdez (2019), menciona que el ciberespacio, es una palabra inventada por el escritor William Gibson en su obra "Le Neuromancien" en el año 1984, quien describe el espacio virtual en el que circulan los datos electrónicos de las PC de todo el mundo. El autor señala que de acuerdo a The UK Cyber Security Strategy, el ciberespacio es un dominio interactivo formado por redes digitales que se utiliza para almacenar, modificar y comunicar información. Incluye Internet, pero también los otros sistemas de información que respaldan los negocios, infraestructura y servicios. En tal sentido, Leiva (2015) indica que el ciberespacio es un ambiente único, sin fronteras geográficas, anónimo, asimétrico y puede ser considerado fácilmente clandestino.

En este sentido, sale a flote la palabra ciberdefensa, en el que Acosta et al. (2009), la definen como la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques y Leiva (2015), la considera como un ámbito de la seguridad nacional en el que los gobiernos deben definir una estrategia, que deben ejecutarse en coordinación con los sectores público y privado, ser compatible con los derechos y libertades individuales y ser coordinada con otras acciones para detectar las distintas amenazas, establecer sistemas de respuesta y recuperación ante eventualidades y además se debe fomentar la cooperación internacional como punto clave para lograr tratados internacionales y la colaboración.

Así también, el término de ciberseguridad está presente para la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados Valdez (2019). Por lo que, para Leiva (2015), la ciberseguridad se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información, es decir, es donde los controles de ciberseguridad son eficaces y el ciberespacio es considerado confiable, flexible y seguro para la ICI, y expresa que cuando esos controles están ausentes, incompletos, o mal diseñados, el ciberespacio es considerado como tierra de nadie. En definitiva, para Leiva (2015), la ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

Algunos aspectos a tomar en cuenta para las estrategias nacionales en seguridad cibernética

De acuerdo con la posición de Leiva (2015), en las últimas décadas, las nuevas tecnologías, los servicios electrónicos y de redes de comunicación se han integrado cada vez más a nuestra vida diaria. Por lo cual Luiijf et al. (2013), señalan que una Estrategia Nacional de Ciberseguridad se puede definir como un plan de acción nacional sobre la base de una visión nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio; por tanto, se puede decir que una Estrategia Nacional de Ciberseguridad (ENCS) es un instrumento para mejorar la seguridad y la resistencia de la ICI y la sustentabilidad de los servicios nacionales de información (Leiva, 2015) y que tiene unos objetivos a perseguir, como son:

- Alinear acciones para trabajar de manera armoniosa,
- Coordinar la cooperación de los sectores público y privado, y
- Transmitir directivas, responsabilidades y establecer relaciones entre todas las partes involucradas.

De esta manera, se debe tener en consideración los principales aspectos en los que se enfocan la mayoría de los países que tienen implementadas sus ENCS, y que deben tenerse en cuenta en la elaboración de las estrategias o políticas públicas para la ciberseguridad de una nación y así poder afrontar los riesgos del ciberespacio:

1. Protección de: ICI, economía, seguridad nacional y bienestar social

2. Enfoque de la estrategia y/o política pública referida a: concientización, conocimiento, educación y capacidades cibernéticas militares
3. Participación del sector público en la estrategia y política pública en cuanto a: liderazgo y marco jurídico
4. Participación del sector privado referente a la: participación en la estrategia y política
5. Cooperación internacional, contando con la: cooperación en su grupo (geopolítico) y cooperación con otros países
6. Comparación de ENCS desde diferentes puntos de vista, entre los cuales se encuentran: los documentos publicados, los bloques geopolíticos, el marco legal y los convenios o tratados multilaterales
7. Políticas Nacionales de Ciberseguridad efectivas

Políticas Públicas y Ciberseguridad

La ciberseguridad cada vez tiene más importancia en el campo jurídico. La difusión y acceso a las Tecnologías de la Información y la Comunicación (TIC) incrementó el uso del ciberespacio a nivel mundial. La ciberseguridad en la actualidad (2019) debería ser implementada por todos los países ya que ninguno está exento de un ataque cibernético (Moncayo, 2019). En este orden de ideas, Moncayo (2019) cita que la ciberseguridad según Finnemore y Hollis (2016) es:

"la protección de las TIC contra el acceso no autorizado que lleva a la pérdida de al menos uno de los siguientes aspectos: confidencialidad (acceso a datos confidenciales sin autorización); integridad (cambio de datos para generar información fabricada o resultados); autenticidad (ocultando o falsificando la fuente de datos); y / o disponibilidad (bloquear o impedir el acceso a las TIC). Estas actividades cibernéticas hostiles ocurren cuando los adversarios, desde piratas informáticos, activistas hasta criminales y estados organizados, aprenden, obtienen acceso y explotan vulnerabilidades, es decir, debilidades que hacen que las TIC sean susceptibles de infiltración por parte de actores no autorizados" (p. 19).

En este contexto, la definición de ciberseguridad que presenta Moncayo (2019) es la precisa para poder entender el objetivo de la ciberseguridad, ya que menciona los aspectos que las TIC deben asegurar en el resguardo de sus datos, como lo son: la confidencialidad, la integridad, la autenticidad y la disponibilidad.

Por otro lado, señala Vargas, Recalde y Reyes (2017), que es importante tener en cuenta a la ciberdefensa, que está orientada a las acciones de un Estado para proteger y controlar las amenazas, peligros o riesgos de naturaleza cibernética, con el fin de permitir el uso del ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía y la integridad territorial; sin soslayar que en los nuevos escenarios que plantea el ciberespacio, pueden incidir en el momento de trazar rutas estratégicas plausibles para el cumplimiento de las diversas misiones militares de ciberdefensa (p. 36).

Así pues, toda esta sociedad que se encuentra interconecta o en la red necesita de una protección eficiente y eficaz, por lo cual mientras una sociedad se va desarrollando y acoplando cada vez más a todo aquello que ofrecen las TIC, más van incluyendo en sus prácticas una forma de protegerse en dicho medio (Moncayo, 2019).

Por su parte, Subirats et. al (2008), indican que el gobierno nacional es quien debe ocuparse por la mejora de la ciberseguridad en un país, por medio de la formulación de políticas públicas que se encarga de regular los problemas de ciberseguridad. Así, una política pública es la acción gubernamental organizada para solucionar un problema público, una vez que ha sido implementado en la agenda de un gobierno. Por tanto, la política pública, es considerada como la solución de un sistema político-administrativo que es empleado en la realidad social (p. 33).

En síntesis, una implementación de una política pública en el contexto de la seguridad cibernética, un Estado puede enfrentar los problemas que en el día a día sin la adecuada protección los puede estar experimentando.

Metodología

En este punto, el trabajo se aboca en primer lugar a la investigación documental, como fuente primaria para el desarrollo del documento, las cuales fueron tomadas de documentos impresos y electrónicos. De esta manera se cumple con lo señalado por Palella y Martins (2012), sobre el diseño de la investigación documental o bibliográfica:

"Se fundamenta en la revisión sistemática, rigurosa y profunda de material documental de cualquier clase. Se procura el análisis de los fenómenos o el establecimiento de la relación entre dos o más variables. Cuando opta por este tipo de estudio, el investigador utiliza documentos; los recolecta, selecciona, analiza y presenta resultados coherentes. El diseño bibliográfico utiliza los

procedimientos lógicos y mentales propios de toda investigación: análisis, síntesis, deducción, inducción, entre otros" (p. 87).

En segundo lugar, se tomó un el método de estudio de caso, la cual es una herramienta valiosa de investigación, de acuerdo a Martínez (2006), es útil en la generación de resultados que posibilitan el fortalecimiento, crecimiento y desarrollo de las teorías existentes o el surgimiento de nuevos paradigmas científicos, lo que contribuye al desarrollo de un área determinada. En este sentido, el caso de estudio es el análisis de las políticas públicas en el tema de la seguridad cibernética en Ecuador.

Análisis y discusión de resultados

A continuación, se presentan los resultados del caso ecuatoriano, reflejado más recientemente en dos trabajos de investigación, a saber:

- Vargas, Recalde y Reyes, (2017) sobre Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa, y
- Moncayo (2019) quien estudió las Herramientas jurídicas para garantizar la ciberseguridad del Estado. Análisis comparado de Colombia, Chile y Ecuador.

En primer lugar, Vargas, Recalde y Reyes, (2017), reflejan en su estudio lo siguiente:

La problemática de ciberdefensa y ciberseguridad en el Ecuador

En Ecuador, el acceso al internet ha registrado un elevado incremento durante los últimos 5 años. Por ejemplo, los datos muestran que en el año 2012 la población ecuatoriana alcanzaba el 22,5% y que en el 2015 se alcanzó el 32,8%, según estadísticas del Instituto Nacional de Estadísticas y Censo (INEC, 2016). Estos valores son palpables, cuando observan que las organizaciones financieras y comerciales (ejemplo bancos, industrias, turismo, entre otros) han aumentado sus servicios en línea (ejemplo banca electrónica, transacciones electrónicas, entre otros). Incluso, en las entidades públicas han automatizado sus servicios (ejemplo pago predial, pago de impuestos, entre otros) y han aumentado la oferta de servicios y productos por Internet (ejemplo facturación electrónica, sitios de compras, entre otros).

Analizando el incremento mencionado, suponen que podría deberse a varios motivos, tales como:

- La creación del plan de gobierno electrónico 2014-2017 (COSEDE, 2014),

- El incremento de controles de calidad a las empresas que prestan servicios de internet por la extinta Supertel (Delgado, 2014),
- La creación de redes comunitarias en zonas rurales (Ministerio Coordinador de Seguridad 2014),
- Las políticas de Gobierno para la transformación productiva y el desarrollo del Ecuador, entre otros.

Los autores indican que es importante recalcar que para el año 2015, el Ecuador se ubicó en el puesto 82 de 148 economías que aprovechan las TIC para la transformación productiva, desarrollo económico y bienestar de su población, superando a Argentina (100), país que ha sido un referente en avances TIC en América Latina en los últimos años (El Telégrafo, 2014). Esta innegable adopción de tecnologías ha devenido en desarrollo y, a su vez, en problemas de ciberseguridad. Al menos en Ecuador, las estadísticas referentes a violaciones a la seguridad cibernética han sido en su mayoría dentro del sistema financiero. Un incremento en sus cifras ha convertido a la ciberseguridad en un tema preocupante, especialmente para la banca ecuatoriana.

Vargas, Recalde y Reyes, (2017) mencionan que, por ejemplo, en 2014 se registró un aumento de 37% de robos a la banca virtual, 14% en tarjetas de crédito y 46% en cajeros electrónicos (Ministerio Coordinador de Seguridad 2014). Pero no solo los problemas han sido en los sistemas de la banca. La prensa ecuatoriana también ha sido expuesta a varios ataques en sus sitios web que utilizan el "dominio.ec" (El Universo, 2009), de la misma manera, ataques a sitios web del gobierno atribuidos al grupo Anonymous (El Comercio, 2012), ataques al sistema informático electoral del Ecuador (Andes, 2013), supuestos ataques cibernéticos procedentes de Colombia, Estados Unidos, Rusia, China y Francia sobre cuentas o datos personales de ciudadanos ecuatorianos (El Comercio, 2016), así como ataques a Twitter y redes sociales de personajes públicos (La República, 2014); y portales web de opinión libre (El Universo, 2016), entre otros.

Estrategia propia de ciberseguridad y ciberdefensa

Los autores antes referidos, indican que el Gobierno ecuatoriano, en su esfuerzo por minimizar estos problemas, tomó algunas decisiones de tipo político-coyuntural. Por ejemplo, conformó un Centro de Operaciones Estratégico Tecnológico que operó desde las 12AM del 4 de noviembre hasta las 21PM del 5 de noviembre de 2013, con el fin de realizar un monitoreo de ataques

informáticos sobre los equipos de seguridad de varias instituciones públicas (Ministerio Coordinador de Seguridad, 2014). Asimismo, se ejecutaron proyectos como: la implementación del Ecucert para el tratamiento de los incidentes Informáticos, iniciado a partir del año 2012 y también se promulgaron políticas más sustentables, como el Acuerdo Ministerial No. 166, emitido por la Secretaría Nacional de la Administración Pública, que obliga a las instituciones públicas (dependientes de la función ejecutiva) a la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) a partir del año 2013 (Ecuador Universitario, 2012), en dos fases.

Además, dispone el uso obligatorio de las Normas Técnicas Ecuatorianas para la Gestión de Seguridad de la Información, las cuales contemplan un conjunto de directrices para viabilizar la implementación de la seguridad de la información en las entidades públicas. No obstante, han sido muy pocas las que han implementado en parte el esquema y sus medidas, que dan mediada confianza a los ciudadanos de la administración pública. Paralelamente a lo estipulado en el Plan Nacional de Seguridad Integral (PNSI) 2014-2017, la Secretaría de Inteligencia incorpora en su Plan Estratégico Institucional 2015-2017 el objetivo de "incrementar los mecanismos de ciberseguridad para los sistemas de comunicación estratégicos del estado y la integridad de la información" (Inteligencia, 2014). A la par de estos acontecimientos, el 12 de septiembre de 2014, por el Acuerdo Ministerial No. 281 se crea el Comando de Ciberdefensa dentro de las Fuerzas Armadas, con la misión de "proteger y defender la infraestructura crítica e información estratégica del Estado" (El Comercio, 2014), mediante operaciones de protección del espacio cibernético, acciones de prevención, disuasión, explotación y respuesta ante eventuales amenazas, riesgos e incidentes (Freire, 2016).

Sin embargo, hasta el momento no existe un claro registro de la infraestructura crítica y, peor aún, de una definición de la información estratégica. En el mismo año, se anuncia la inclusión de la ciberdefensa como parte del currículo académico de la formación militar, sin concretarse hasta el día de hoy (El Universo, 2014).

En esta ambigüedad, cada institución participante ha asumido diferentes aproximaciones o iniciativas basadas no solo en la complejidad de su infraestructura, la interconectividad, las aplicaciones y tecnologías asociadas, sino también en los recursos que se podrían manejar en favor de dichas instituciones. En suma, estos esfuerzos para mejorar la ciberseguridad, ya sean iniciativas puntuales de entidades públicas o políticas gubernamentales, han sido fragmentados, limitados y

poco efectivos, generando vulnerabilidades expuestas y tácitas. Por lo tanto, a pesar de contar con una normativa legal específica en la materia y con instancias públicas para el efecto, aún no se tienen consensos y criterios técnico-metodológicos en torno al marco de trabajo o estándares en los que se apliquen los roles de los participantes, las metas y los procedimientos en el uso de tecnologías.

Vargas, Recalde y Reyes, (2017), citan que un estudio previamente realizado por Delgado (2014), confirma que "a pesar de todos los esfuerzos, Ecuador no trabaja en ciberseguridad de manera sistemática con políticas definidas, no tienen un plan de acciones para todas las entidades del país y que todas las decisiones de qué hacer en ciberseguridad recaen en el administrador del sitio web". Esta afirmación llama la atención respecto de la necesidad de establecer lineamientos transversales, que permitan al Ecuador trabajar en forma coordinada entre sus diferentes niveles de decisión y en cada uno de sus sectores estratégicos, para hacer frente a este nuevo escenario. En suma, ha limitado la potencial institucionalización de una gobernanza nacional en ciberseguridad y ciberdefensa (p. 10).

En este contexto, el debate en torno a la ciberseguridad y ciberdefensa en el Ecuador debe ser enfocado desde los conceptos fundamentales: el Estado, su seguridad, su desarrollo y defensa. Es imprescindible desarrollar una estrategia nacional de seguridad que incluya al ciberespacio y que agregue valor e influya a todos los niveles de decisión; y estos, a su vez, se conecten, de forma matricial, con las normas o estándares que son aplicables, con los sectores estratégicos involucrados, con el método de implementación y con los objetivos de seguridad que se van a plantear.

Aplicar una estrategia implica su inscripción de partida en el marco legal rector del país, que es la Constitución Política de la República del Ecuador, por lo que, tampoco hay que olvidarse del cumplimiento de la Ley de Seguridad Pública y del Estado (2009), el Ministerio Coordinador de Seguridad del Estado, también promulga el Plan Nacional de Seguridad Integral (PNSI) 2014-2017. Este plan se enfoca en el ser humano y la naturaleza, garantizando los derechos humanos y las libertades de los ecuatorianos y, sobre todo, la soberanía y la seguridad nacional, orientación en la cual ya se incluye al ciberespacio.

Los autores mencionan que el PNSI apunta a la consolidación de un gobierno eficaz y transparente a través de plataformas tecnológicas, y el desarrollo de capacidades para proteger a sus ciudadanos y sus intereses vitales de ataques virtuales, planteando así el ciberespacio, como nuevo esquema de

seguridad frente a las amenazas asimétricas y globales (transnacionales e intermésticas). Esta misma Ley, crea el Sistema de Seguridad Pública y del Estado y estipula la conformación del Consejo de Seguridad Pública y del Estado (COSEPE) para asuntos de Seguridad Nacional.

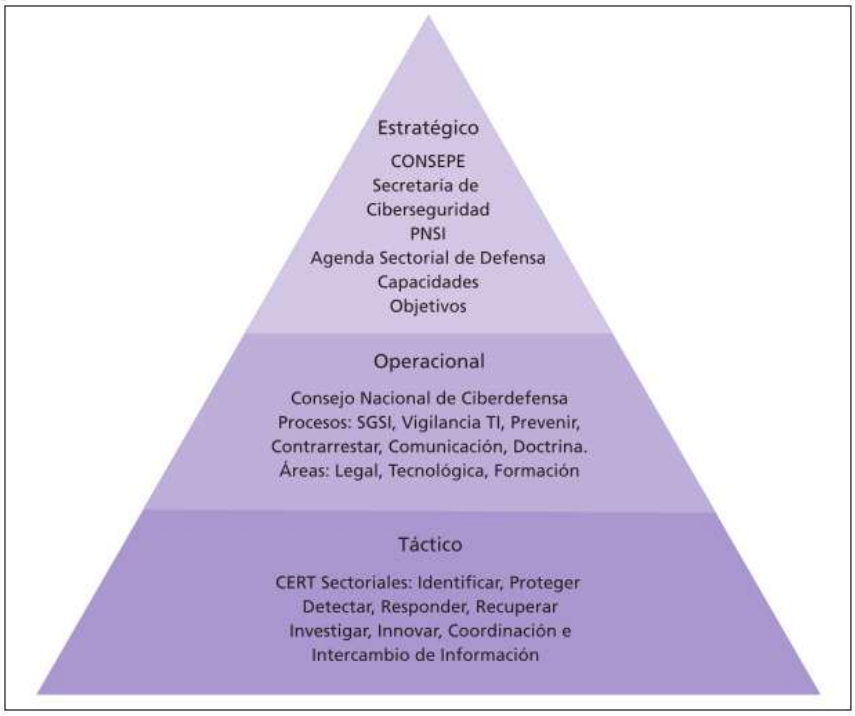
Tabla 1: Propuesta de conformación del COSEPE.

Miembros actuales	Miembros propuestos para tratar asuntos de ciberseguridad
• Presidente de la República • Vicepresidente de la República • Presidente de la Asamblea Nacional • Presidente de la Corte Nacional de Justicia • Ministro Coordinador de Seguridad • Ministro de Defensa Nacional • Ministro del Interior • Ministro de Relaciones Exteriores • Jefe del Comando Conjunto de las FF.AA. • Comandante General de Policía	• Ministerio Coordinador de Sectores Estratégicos • Ministro de Telecomunicaciones y Sociedad de la Información • Ministro de Electricidad y Energía renovables • Ministro de Recursos no renovables • Ministro Coordinador de la Política Económica • Ministro de Justicia, DD.HH y cultos • Secretario General de Gestión de Riesgos • Ministro Coordinador de Producción empleo y competitividad • Ministro de Conocimiento y Talento Humano • Secretario Nacional de Comunicación • Secretario Nacional de la Administración Pública. • Agencia de Control y Regulación de las Telecomunicaciones • Proveedores de Telecomunicaciones y de Internet • Academia

Fuente: Vargas, Recalde y Reyes (2017).

Por último Vargas, Recalde y Reyes, (2017), consideran como parte importante de su planteamiento, que para iniciar una discusión nacional de los temas de ciberseguridad y ciberdefensa, es necesario integrar al seno del mencionado Consejo (además de los miembros ya definidos en Ley) a los representantes de distintas instituciones ecuatorianas, las cuales se muestran en la tabla 1, considerando como énfasis que el ámbito de las TIC es transversal a las organizaciones públicas y privadas del Estado; y que las instituciones citadas aquí tiene gran relevancia en la gestión de los sectores estratégicos del país y son los órganos rectores de la política pública en sus respectivos ámbitos. Sobre la base de una estructura piramidal, nuestra sugerencia es que se jerarquice la gestión de la ciberdefensa en tres niveles: nivel estratégico, nivel operacional y/o gerencial, y nivel táctico y/o técnico, tal como se muestra en la figura 1, que corresponde al direccionamiento estratégico de la ciberseguridad y la ciberdefensa en el Ecuador.

Figura 1: Direccionamiento estratégico de la ciberseguridad y ciberdefensa.



Fuente: Vargas, Recalde y Reyes (2017). Elaboración propia, (2021).

Los autores señalan que, estas nuevas generaciones tienen que tener claro que acciones del mundo virtual tienen sus consecuencias en el mundo real. Con ello, la problemática de seguridad cibernética como consecuencia del uso del ciberespacio, no solo se concentra en temas de técnicos de seguridad en dicho ámbito, sino que implica las consecuencias en el mundo real y sociedad actual, que socaban su continuidad.

El fenómeno está en todos los países del mundo y no solo al nivel del Estado. Sin embargo, para el Ecuador, tras la insuficiente previsión gubernamental en relación al tema, se ha abierto la posibilidad de que se fortalezca la gestión tecnológica de infraestructura e información nacional desde el exterior hacia el país. De ahí que es imprescindible rediseñar la organización de la política pública de la seguridad cibernética en todos sus niveles y su debida implementación, ya que son vitales para la propia existencia del Estado y la sociedad ecuatoriana (Vargas, Recalde y Reyes, 2017).

Posteriormente Moncayo (2019), esboza en su trabajo lo siguiente:

La ciberseguridad de la infraestructura crítica de la información en Ecuador: ¿Qué hacer?

Para que un país tenga una adecuada ciberseguridad de su ICI debe contar con las herramientas jurídicas-institucionales necesarias para poner en marcha la mejora de sus necesidades en este tema. Dentro de las cuales se tiene la Agenda de Política Exterior 2017-2021, a cargo del Ministerio de Relaciones Exteriores y Movilidad Humana, y tiene como objetivo la consolidación del Ecuador en el escenario internacional promoviendo la participación de este en diferentes actividades. Sin embargo, no aborda la ciberseguridad como tema en la política exterior del Ecuador. Es de asombrarse que con la importancia que tiene el uso de las TIC en la actualidad, esta agenda no incluya un parámetro relacionado a la ciberseguridad. Al comprobar que el texto ni siquiera menciona la palabra de ciberseguridad o ciberdefensa (se ha tratado de encontrar la palabra ciberseguridad mediante la opción de búsqueda en la que no se tiene éxito ya que no arroja ningún resultado en temas de ciberseguridad).

Como ya se mencionó anteriormente, es difícil hablar de IC cuando el gobierno central no ha definido cuáles son las infraestructuras críticas de un país. Ecuador no se aleja de esta realidad ya que no existe ningún lineamiento o política en la cual se definan cuáles son las infraestructuras críticas y peor aún cuales son las ICI. El gobierno central maneja una gran cantidad de información de los ciudadanos que ya se encuentra en medios digitales, como por ejemplo las diferentes plataformas creadas por diferentes instituciones del Estado. Esta información corre un grave peligro si no se la protege de una manera adecuada y para esto es necesario una correcta implementación de la ciberseguridad.

Al no tener claro cuáles son los sectores que pertenecen a la infraestructura crítica de la información en el Ecuador es necesario señalar algunos ejemplos en donde esta infraestructura se afectaría de manera significativa y cumpliría con la denominación de que los daños o destrucción de esta tendría serias consecuencias:

- La pérdida de información o eliminación de los datos que tiene a su cargo el Servicio de Rentas Internas (SRI), conlleva a que tanto los contribuyentes como la propia institución dejen de cumplir sus obligaciones y el sector tributario tendría graves pérdidas en el país;
- Otro sector que ser vería afectado es el de la seguridad social, ya que como es de conocimiento de varias personas el Instituto Ecuatoriano de Seguridad Social (IESS), en sus servicios de salud ya se maneja en su mayoría solo de manera electrónica, es decir todos los datos de los pacientes son almacenados en sus redes de datos y la perdida de esta

información tendría graves consecuencias para los afiliados ya que toda su información contenida en sus historias clínicas se perderían y eso generaría una grave consecuencia para el país en general.

Lo principal que se debe destacar en Ecuador es que no cuenta con una entidad encargada de llevar a cabo la ciberseguridad nacional del país. El Ministerio de Telecomunicaciones y Sociedad de la Información es el encargado de desarrollar planes, proyectos y programas que tengan relación a medios electrónicos, pero por el momento solo en materia de telecomunicaciones ya que no existe ningún lineamiento en el que se le encargue la dirección de la ciberseguridad del país.

Las falencias más notorias de Ecuador según el NCSI son sus indicadores generales de seguridad cibernética, ya que el país no cuenta con suficientes herramientas jurídicas-institucionales para tener una ciberseguridad adecuada, además que tampoco ha ratificado ningún convenio internacional en materia de ciberseguridad (Moncayo, 2019).

La autora indica que con base en la tabla 2 se deduce que Ecuador debe mejorar su ciberseguridad ya que todos los esfuerzos que ha realizado no son suficientes para combatir un ataque de ciberseguridad que sea de gran magnitud. Los más afectados serían los ciudadanos porque su información correría riesgo de perderse y el Estado ya no estaría cumpliendo con los derechos fundamentales que establece la Constitución de la República del Ecuador.

Tabla 2: Síntesis de Ciberseguridad de Ecuador según el NCSI.

DE UN TOTAL DE 77 PUNTOS CONTENIDOS EN EL RANKING NACIONAL DE CIBERSEGURIDAD (NCSI), ECUADOR CUENTA CON 25 PUNTOS.		**TOTAL**
INDICADORES GENERALES DE SEGURIDAD CIBERNÉTICA		6/27 (22.22%)
Desarrollo de políticas de seguridad cibernética	0/7 (0%)	
Análisis e información de amenazas cibernéticas	0/5 (0%)	
Educación y desarrollo profesional	4/9 (44%)	
Contribución a la seguridad cibernética global	2/6 (33%)	
INDICADORES DE CIBERSEGURIDAD DE LÍNEA BASE		7/24 (29.16%)
Protección de servicios digitales	1/5 (20%)	
Protección de servicios esenciales	0/6 (0%)	
Identificación electrónica y servicios de confianza	6/9 (67%)	
Protección de datos personales	0/4 (0%)	
INDICADORES DE GESTIÓN DE INCIDENTES Y CRISIS		12/26 (46.15%)
Respuesta a incidentes cibernéticos	3/6 (50%)	

Pol. Con. (Edición núm. 56) Vol. 6, No 3, marzo 2021, pp. 1229-1250, ISSN: 2550 - 682X

Gestión de la crisis cibernética	1/5 (20%)	
Lucha contra el ciberdelito	4/9 (44%)	
Ciberoperaciones militares	4/6 (67%)	

Fuente: National Ciber Security Index (2018). Elaboración propia (2021).

Así también cuenta con leyes, organismos e instituciones que garantizan la seguridad cibernética en Ecuador.

Leyes y acuerdos:

- Constitución de la República del Ecuador, Ley de Seguridad Pública y del Estado, Ley de Comercio electrónico, firmas electrónicas y mensajes de datos, Acuerdo No. 166, emitido por la Secretaría Nacional de la Administración Pública (SNAP).

Organizaciones e instituciones:

- Ministerio de Defensa Nacional: Agenda Política de Defensa 2014-2017, Acuerdo Ministerial No. 281
- Dirección Nacional de Registro de Datos Públicos: Dato Seguro
- Ministerio de las Telecomunicaciones y Sociedad de la información (MINTEL): Plan Nacional de Gobierno Electrónico, Ecuador Digital, Plan de la Sociedad de la Información y del Conocimiento 2018-2021
- Agencia de Regulación y Control de las Telecomunicaciones: Centro de Respuesta a incidentes informáticos del Ecuador (EcuCERT).

Para finalizar, Moncayo (2019), indica que el primer paso para una adecuada ciberseguridad en Ecuador es la creación de una entidad que esté enfocada únicamente en la protección de la ciberseguridad a nivel nacional. Con la creación de esta entidad el siguiente paso es el de clasificar cuáles son las IC del país para con ello todos los habitantes tengan conocimiento de los sectores que más se verían afectados ante un incidente cibernético.

La herramienta jurídica más importante que se debe implementar en el Ecuador es la Estrategia de ciberseguridad, la cual debe estar enfocada en la protección de los riesgos que conlleva el ciberespacio en Ecuador, enfocada a una realidad que se vive todos los días y que tenga la participación de los sectores público, privado, la academia y los profesionales expertos en esta materia; posteriormente con ello proceder con una participación internacional en materia de ciberseguridad, así como también, incrementar los protocolos de ciberseguridad al momento de

seleccionar a los proveedores de servicios de internet y que todos los ecuatorianos deben estar conscientes de los riesgos que trae el ciberespacio, por lo que la entidad correspondiente debe publicar un informe anual de todos los ataques cibernéticos que han combatido, empezando por una explicación de la amenaza combatida y de las acciones que se tomaron para que no genere un daño grave.

Conclusiones

La seguridad es una definición que está en un constante proceso evolutivo, debido a que se ha convertido en un eje fundamental del desarrollo de las naciones. En tal sentido, la seguridad cibernética se establece como una terminología amplia, que enfrenta el reto de lograr establecer un balance estratégico entre los ámbitos que se relacionan y que requieren directrices, espacios y prioridades.

El Estado ecuatoriano por medio de alineaciones jurídicas, institucionales y políticas ha formulado lineamientos básicos sobre el espectro del ciberespacio y la seguridad cibernética, la cual se enlaza como eslabón de la ciberdefensa nacional. En este contexto, se vislumbran limitaciones que, por la naturaleza transformadora y evolutiva de los actores y de las amenazas, impiden que el potencial de cada una de las funciones se aproveche al máximo.

En cuanto a la seguridad cibernética, el Ecuador ha sustentado una estructura institucionalidad que ha fomentado la proliferación de entidades, entre las cuales se resalta el Comando de Ciberdefensa Nacional y, el conocimiento a nivel básico de una cibercultura de parte del Gobierno. Pese a ello, la inexistencia de acuerdos técnico – metodológicos, queda entre los aspectos pendientes por analizar, para lograr configurar puntos de referencia para orientar la seguridad cibernética y la ciberdefensa.

La República del Ecuador requiere de políticas públicas basadas en un modelo de gobernanza en seguridad cibernética, que integre y materialice de manera efectiva los esfuerzos aislados, que a lo largo del tiempo no han supuesto una solución global al objetivo de la ciberseguridad y ciberdefensa del Ecuador. Recordemos que, si bien la seguridad por teoría es tratada individualmente, no es eficiente si no se logra con la participación de todos.

Tanto es así que, para el Ecuador tras la insuficiente previsión gubernamental en relación al tema, se ha abierto la posibilidad de que se fortalezca la gestión tecnológica de infraestructura e

Pol. Con. (Edición núm. 56) Vol. 6, No 3, marzo 2021, pp. 1229-1250, ISSN: 2550 - 682X

información nacional desde el exterior hacia el país. De ahí que es imprescindible rediseñar la visión de la política pública en función de la seguridad cibernética en todos sus niveles, con el fin de establecer una política de privacidad y de gestión de la información en la sociedad ecuatoriana y con ello el mejoramiento de la seguridad en las infraestructuras críticas vitales para la propia existencia del Estado y la sociedad ecuatoriana en su conjunto.

Referencias

1. Acosta, O., Pérez, J., Arnáiz, D. y Ballesteros, P. (2009). Seguridad nacional y ciberdefensa. https://n9.cl/gg60y
2. Andes (2013). Sistema informático electoral del Ecuador sufrió ciberataque desde un país del primer mundo. https://n9.cl/4d6ai
3. Bañon, R., y Carrillo, E. (1997). El Análisis de las políticas públicas en La Nueva Administración Pública. https://n9.cl/f7bsh
4. Corporación del Seguro de Depósitos, Fondo de Liquidez y Fondo de Seguros Privados (COSEDE). (2014). Plan de Gobierno Electrónico. http://www.cosede.gob.ec/?p=3677
5. Cortés, R (2015). Estado actual de la politica pública de ciberseguridad y ciberdefensa en Colombia. https://n9.cl/6ubla
6. Cárdenas, S. (2020). Estrategia Nacional de Ciberseguridad.
7. Delgado, A. (2014). Gobernanza de Internet en Ecuador: Infraestructura y acceso. repositorio.educacionsuperior.gob.ec/handle/28000/1579.
8. Ecuador Universitario. (2012). El contexto de la Ciberseguridad. https://n9.cl/4we7a
9. El Comercio. (2012). Anonymous inicio ataque a web oficiales en Ecuador. https://n9.cl/kxfrl
10. El Comercio. (2014). Ecuador implementará un Comando de Ciberdefensa. https://n9.cl/8a6ng
11. El Comercio. (2016). Hackers de Rusia, China, EE.UU. y Francia dirigen ataques a Ecuador. https://n9.cl/481ku
12. El Telégrafo (2014). Ecuador escala 9 puestos en ranking de aplicación de las TIC. https://n9.cl/0iew
13. El Universo. (2009). Ciberataques a sitios web de Ecuador. https://n9.cl/ximef
14. El Universo. (2014). Formación militar prevé ciberdefensa. https://n9.cl/xb3i
15. El Universo. (2016). Tres portales web de Ecuador denuncian ciberataques. https://n9.cl/clrvh
16. Finnemore y Hollis (2016). Constructing Norms for Global Cybersecurity. https://n9.cl/v6ylc
17. Freire, B. (2016). Aplicación de la Ciberdefensa en la Seguridad Nacional. Revista Presencia la Asociación de Generales: 59-65.

18. Guerrero, L. (2007). Los Derechos Humanos como Politica Publica (Primera ed.). Bogota: Universidad Nacional, Facultad de derecho, Ciencias Poltiicas y Sociales.
19. Instituto Nacional de Estadísticas y Censo (INEC). (2016). Tecnologías de la Información y Comunicaciones 2015. https://n9.cl/wqpf
20. Inteligencia, Secretaría. (2014). Plan Estratégico Institucional 2015-2016. https://goo.gl/WE7WYu
21. Ministerio Coordinador de Seguridad. (2014). Ciberseguridad escenarios y recomendaciones. Revista Digital del Ministerio Coordinador de Seguridad.
22. Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. https://n9.cl/pp1f2
23. Ley de Seguridad Pública y Estado. (2009). https://www.wipo.int/edocs/lexdocs/laws/es/ec/ec049es.pdf
24. Luiijf, E., Besseling, K., & De Graaf, P. (2013). Nineteen National Cyber Security Strategies. International journal of critical infrastructures, 9(1), 3-31.
25. Martínez, P. (2006). El método de estudio de caso. Estrategia metodológica de la investigación científica. https://n9.cl/qw0p
26. Mogollón, F. (2017). Desafíos de la Ciberseguridad y Respuestas Estatales: El caso del Estado Ecuatoriano en el Período 2008 – 2015. https://n9.cl/yavg
27. Moncayo, P. (2019). Herramientas jurídicas para garantizar la ciberseguridad del Estado. Análisis comparado de Colombia, Chile y Ecuador. https://n9.cl/i1ye
28. National Ciber Security Index. (2018). Ecuador. https://ncsi.ega.ee/country/ec/
29. Organización para la Cooperación y el Desarrollo Económico (2012). Índice Nacional de Ciberseguridad.
30. Palella, S. y Martins, F. (2012). Metodología de la investigación cuantitativa.
31. Salinas, N. (2018). Ciberdefensa en el Estado Ecuatoriano Período 2013 – 2016.
32. Sancho, C. (2017). Ciberseguridad. Presentación del dossier.
33. Subirats, J., Knoepfel, P., Larrue, C., y Varonne, F. (2008). Análisis y Gestión de Políticas Públicas. Barcelona: Editorial Ariel, S. A.
34. Valdez, A. (2019). Introducción a la ciberseguridad. https://n9.cl/3q7xr
35. Vargas, R., Recalde, L. y Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. https://n9.cl/e8rb2.