DOI: http://dx.doi.org/10.23857/dc.v7i1.1771

Ciencias técnicas y aplicadas

Artículo de revisión

Propuesta de estrategias de seguridad cibernética. Aproximaciones teórico – prácticas hacia el aprestamiento en países latinoamericanos

Proposal of cyber security strategies. Theoretical - practical approaches towards readiness in Latin American countries

Proposta de estratégias de segurança cibernética. Abordagens teórico-práticas para a prontidão nos países latino-americanos

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

Correspondencia: alanleyvamendez@gmail.com

***Recibido:** 10 de enero de 2021 ***Aceptado:** 20 de enero de 2021 *** Publicado:** 27 de febrero 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

El artículo de revisión tuvo por objetivo analizar las estrategias de seguridad cibernética implementadas en países de Latinoamérica por medio de los indicadores de la Organización para la Cooperación y el Desarrollo Económico, a fin de contextualizar la situación en materia de ciberseguridad de la República del Ecuador por medio del Índice Nacional de Ciberseguridad. Se empleó una metodología de tipo documental, con un diseño de tipo bibliográfico que permitió estructurar la información recopilada. Se analizaron documentos publicados en revistas científicas, llevando a cabo la conceptualización de las temáticas referidas a ciberamenazas, ciberseguridad, seguridad cibernética y las estrategias de seguridad cibernética, ello con el propósito de identificar los aspectos relevantes que fundamenten la formulación de propuesta de estrategias de seguridad cibernética basadas tanto en la realidad latinoamericana como en el contexto ecuatoriano.

Palabras Clave: Ciberamenazas; ciberseguridad; estrategias de seguridad cibernética.

Abstract

The review article aimed to analyze the cybersecurity strategies implemented in Latin American countries through the indicators of the Organization for Economic Cooperation and Development, in order to contextualize the cybersecurity situation of the Republic of Ecuador by middle of the National Cybersecurity Index. A documentary-type methodology was used, with a bibliographic-type design that made it possible to structure the information collected. Documents published in scientific journals were analyzed, carrying out the conceptualization of the themes related to cyber threats, cybersecurity, cybersecurity and cybersecurity strategies, with the purpose of identifying the relevant aspects that base the formulation of the proposed security strategies cybernetics based on both the Latin American reality and the Ecuadorian context.

Keywords: Cyber threats; cybersecurity; cybersecurity strategies.

Resumo

O artigo de revisão teve como objetivo analisar as estratégias de cibersegurança implementadas nos países latino-americanos por meio dos indicadores da Organização para Cooperação e Desenvolvimento Econômico, a fim de contextualizar a situação da cibersegurança da República do Equador a meio do Índice Nacional de Cibersegurança. Foi utilizada uma metodologia do tipo

documental, com desenho do tipo bibliográfico que possibilitou estruturar as informações coletadas. Foram analisados documentos publicados em periódicos científicos, realizando a conceituação dos temas relacionados às ameaças cibernéticas, cibersegurança, cibersegurança e estratégias de cibersegurança, com o objetivo de identificar os aspectos relevantes que fundamentam a formulação das propostas de estratégias de segurança cibernéticas baseadas tanto no latim A realidade americana e o contexto equatoriano.

Palavras-chave: Ameaças cibernéticas; segurança cibernética; estratégias de segurança cibernética.

Introducción

Desde finales del siglo XX, la sociedad ha sufrido una transformación drástica debido a la irrupción del internet y las nuevas tecnologías. Esto ha supuesto toda una evolución que ha generado una interrelación entre los individuos, los estados y los comercios. Esta evolución va de la mano del surgimiento de la dimensión del denominado ciberespacio. El mismo, ha trascendido todo tipo de limitaciones, permitiendo que los ciudadanos interaccionen e intercambien información e ideas con libertad (Gazapo y Machín, 2016)

La diversificación de usuarios del internet ha provocado que en los últimos años se incrementen de manera acelerada las interconexiones a nivel global, implementando relaciones cibernéticas en tiempo real, generando una amplitud del mundo virtual, el cual comúnmente se denomina ciberespacio.

De acuerdo con Dammert y Núñez (2019), América Latina, es una región que no está exenta de este proceso, siendo inclusive una de las regiones donde la comunidad de cibernautas (usuarios) se ha incrementado de una forma amplia. Con ello, se tiene que la interconexión entre usuarios conlleva aspectos positivos para el desarrollo de la sociedad, como lo son la comunicación constante entre personas, organizaciones e instituciones de todo tipo y nivel, tales como: Gobierno electrónico, comercio electrónico, comunicaciones e información instantánea, sistemas de banca en línea, servicios públicos y privados de diversa índole.

Sin embargo, como todo lo positivo, siempre se presentan aspectos negativos, como lo son: la producción y desarrollo de delitos cibernéticos, donde por las características del ciberespacio, se

permiten condiciones como el anonimato, la capacidad de actuación a distancia y la permisibilidad de la vulnerabilidad de los usuarios de la red.

El uso de las tecnologías de la información en el funcionamiento de todas las actividades de las naciones y de la sociedad en general, han hecho que la dependencia del internet y el uso del ciberespacio constituya la puerta de ingreso para que se produzcan ciberdelitos y aparezcan nuevas amenazas tecnológicas (hibridas), en este nuevo escenario de confrontación no existen fronteras, ni actores, ni límites y estas nuevas amenazas pueden afectar a la seguridad del Estado y de las personas, paralizando la infraestructura crítica del Estado ocasionando grandes pérdidas económicas. El entorno digital en el que se desarrolla el mundo actual debe considerar los riesgos que se presenta en el uso de las redes (internet) en casi todos los procesos de producción. La ciberseguridad representa un dilema de seguridad para todos los estados porque su zona de acción es el ciberespacio, la cual es considerada una zona anárquica (Tates y Recalde, 2019)

Los riesgos y amenazas, producidos mayoritariamente por la globalización, representan la proliferación de las denominadas Nuevas Amenazas o Amenazas No Convencionales, que afectan la seguridad de los Estados, a partir de la utilización de los espacios de vulnerabilidad producidos por la dependencia de las sociedades contemporáneas a los sistemas de información. Sin embargo, a pesar de los diferentes riesgos que significan para una sociedad cada vez estar más interconectada digitalmente y estar cada vez más alejada de los procedimientos tradicionales, la tendencia parece ser imparable.

En contexto, Castro y Monteverde (2018) señalan que los riesgos y amenazas son numerosos y dinámicos. Entre ellos destacan, una mayor y más compleja actividad delictiva desarrollada transnacionalmente por organizaciones o incluso individuos y que afectan directamente la seguridad nacional de los Estados. También, se percibe el incremento de actividades de terrorismo, espionaje, sabotaje y robos de información confidencial, que utilizan el ciberespacio y las plataformas de información para enriquecerse, afectando no solo la seguridad de los Gobiernos, sino también a las Empresas Multinacionales, Organismos Internacionales Gubernamentales, No Gubernamentales e inclusive a cada individuo.

Actualmente, se percibe que los delitos cibernéticos se han vuelto mucho más sofisticados, se han complejizado las actividades de ciberespionaje militar, industrial y político y, se han incrementado los ciberataques a estructuras críticas, tanto por grupos organizados como por individuos (ya sea

por ignorancia, diversión, curiosidad, reto intelectual o lucro). Esto se debe a lo atractivo que resulta el ciberespacio por ser un ambiente anárquico y complejo, que ofrece un camuflaje anónimo casi total a los autores de los ataques.

En concordancia, Leiva (2015) refiere que los ciberataques a estructuras críticas o a sistemas informáticos pueden tener graves repercusiones en la sociedad y su economía; es decir, pueden afectar a todos los niveles de la sociedad. Esto permite ver como es que, a medida que las sociedades dependen más de las tecnologías de información y comunicación (TICs), la ciberseguridad se vuelve uno de los retos más importantes del siglo y un tópico de interés para todo Estado.

En fundamento, la Unión Internacional de Telecomunicaciones – UIT (2017) considera al ciberespacio como el nuevo ámbito de guerra, e indica que es un campo de operaciones igual a la tierra, mar, aire o espacio y, por ende, igualmente sujeto a ser escenario de maniobras defensivas y, si es necesario, ataques preventivos y represalias. Frente a este nuevo escenario global es prioritario que los Estados tomen medidas de ciberseguridad y ciberdefensa, considerando que este tipo de ataques pueden afectar tanto a la seguridad nacional como a la seguridad internacional.

De igual manera, se refiere que, para evitar dar oportunidades al incremento de la delincuencia, las infraestructuras de telecomunicaciones existentes deben contar con medidas de seguridad adecuadas, de naturalezas tanto técnicas como jurídicas.

En tal sentido, Mayorga (2016) define a la ciberseguridad como “la capacidad que tiene un Estado de minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética”. De igual manera, Azcona (2017) la define como “la protección de activos 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”.

En contexto, Bayuk, Healey, Rohmeyer, Sachs, Smitdt y Weiss (2012) establecieron que la ciberseguridad se torna como una prioridad para la seguridad de los Estados, pues representa la clave para su supervivencia y la entienden como “la capacidad de controlar el acceso a los sistemas en red y a la información que contienen. Donde los controles de ciberseguridad son efectivos, el ciberespacio se considera una infraestructura digital fiable, resistente y confiable. Cuando los controles de seguridad cibernética están ausentes, incompletos o mal diseñados, el ciberespacio se

considera el salvaje oeste de la era digital. Incluso aquellos que trabajan en la profesión de la seguridad tendrán una visión diferente de la seguridad cibernética en función de los aspectos del ciberespacio con los que interactúan personalmente".

De tal manera, Cárdenas (2020) detalla que, en el Ecuador, las estadísticas relacionadas a violaciones a la ciberseguridad en su mayoría han sido dirigidas al sector financiero, ya que se busca la afectación de los sistemas de banca virtual, sistemas de tarjetas de créditos y cajeros electrónicos, así como también los ataques direccionados a la prensa, específicamente en sus plataformas digitales.

Con esto, se tiene que la puntualización en el contexto de la seguridad cibernética se dirige a la formulación de alternativas de estrategias en este ámbito de estudio, donde el artículo que se presenta tiene como objetivo la revisión a manera documental de propuestas que enfoquen aproximaciones teórico – prácticas en materia de ciberseguridad tanto en la región latinoamericana como específicamente en el Ecuador, basándose en la implementación de la metodología documental de diferentes autores y/o fuentes que nutran el contexto, para finalmente focalizar en unas consideraciones finales y referencias bibliográficas.

Materiales y métodos

Se llevó a cabo una investigación de tipo documental, en tal sentido, la búsqueda de información se realizó en la base de datos electrónica: Dialnet, Redalyc y Google Scholar. Se analizaron documentos publicados en revistas científicas. Siendo empleado como parámetro de búsqueda: estrategias de seguridad cibernética en países latinoamericanos y específicamente en la República del Ecuador.

Según Pallela y Martins (2012), la investigación documental "se concreta exclusivamente en la recopilación de información en diversas fuentes. Indaga sobre un tema en documentos, escritos u orales".

La investigación documental tiene la peculiaridad de utilizar como fuente primaria de insumos, el documento escrito en sus diferentes formas: documentos impresos, electrónicos y audiovisuales más no es la única y exclusiva. De la misma forma, en atención al diseño de la investigación bibliográfico, Palella y Martins, (2012) señalan que:

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.

En función de lo trazado, se planteó como objetivo, analizar las estrategias de seguridad cibernéticas implementadas en países latinoamericanos a fin de contextualizar el panorama del Estado Ecuatoriano.

Resultados

La presentación de los resultados se realiza a través de las tablas que se muestran a continuación, las cuales permiten precisar la información para realizar el análisis temático y de contenido. Las tablas 1, 2 y 3, recopilan la conceptualización de las terminologías referidas a las ciberamenazas, la ciberseguridad, la seguridad cibernética y, la tabla 4, teoriza la fundamentación de las Estrategias de Seguridad Cibernética.

Tabla 1: Conceptualización de las ciberamenazas

Autor y año	Título	Tipo de documento	Cita	Análisis por parte del investigador
Fernández, A. y Rodríguez, J. (2017)	Análisis de las ciberamenazas. Cuadernos de estrategia.	Artículo científico publicado en revista	*"Son aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula en el mismo, para la comisión de distintos delitos mediante su utilización, manipulación, control o sustracción. En relación a ello, se pueden identificar al menos nueve actores que pueden generan ciberamenazas, estos son: Estados, ciberdelincuentes, grupos terroristas, grupos yihadistas, cibervándalos, hacktivistas, actores internos, ciberinvestigadores y organizaciones privadas".*	Cada uno de los actores, plantean sus objetivos dependiendo del sector que quieran amenazar y/o atacar y del nivel de peligrosidad que quieran causar. Teniendo en cuenta la diversidad de las ciberamenazas que se puedan realizar por medio del ciberespacio y lo variado que son sus ejecutores, es que se hace necesario contar con medidas de seguridad por parte de las instituciones buscando cumplir con los requerimientos básicos de ciberseguridad.

Fuente: Elaboración propia (2021).

Tabla 2: Conceptualización de la ciberseguridad

Autor y año	Título	Tipo de documento	Cita	Análisis por parte del investigador
Hirare, S. (2017)	Análisis de las ciberamenazas. Cuadernos de estrategia.	Artículo científico publicado en revista	*"la ciberseguridad constituye una condición para permitir que los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio como dimensión, en la cual las relaciones sociales puedan efectuarse en forma rápida y económica en comparación con otras formas conocidas de intercambio de información".*	Resulta fundamental el trabajo mancomunado y colaborativo entre las organizaciones e instituciones, tanto públicas, como privadas, para desarrollar de manera sólida lineamientos políticos y tecnificados que fomenten la ciberseguridad.
Comnimos (2013)	Ciberseguridad en América Latina. Orientación actual de la política hemisférica de seguridad.	Artículo científico publicado en revista	*"en líneas generales se define como la seguridad de la información digital almacenada en redes electrónicas. La ciberseguridad tiene un alcance más político o vinculado a la seguridad nacional".*	Debe diferenciarse los términos de seguridad de la información y de la ciberseguridad, en donde, la primera responde a la actividad de las organizaciones y profesionales de las tecnologías de la información, mientras que la última responde a políticas de Estado.

Fuente: Elaboración propia (2021).

Tabla 2: (Continuación). Conceptualización de la ciberseguridad

Autor y año	Título	Tipo de documento	Cita	Análisis por parte del investigador

Rauscher y Yashenko (2011)	Ciberseguridad.	Artículo científico publicado en revista	*"es una propiedad del ciberespacio, que tiene la capacidad de resistir las amenazas intencionales y no intencionales, responder y recuperarse".*	El prevenir, detectar, responder y recuperarse se señalan como los objetivos de la ciberseguridad, pero tradicionalmente el objetivo principal fue prevenir que se concrete un ataque exitoso.
La Unión Internacional de Telecomunicaciones (2017)	Agenda de Ciberseguridad Global.	Artículo científico publicado en revista	*"como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno".*	En el uso, los procesos y tecnologías para prevenir, detectar y recuperarse de daños en el ciberespacio, las partes involucradas en el tema, ya sea un usuario, un negocio, una institución pública o privada, deben decidir su propia política de seguridad y estas deben estar correlacionadas entre sí y responder a una Estrategia Nacional de Ciberseguridad.

Fuente: Elaboración propia (2021).

Tabla 4: Conceptualización de la seguridad cibernética

Autor y año	Título	Tipo de documento	Cita	Análisis por parte del investigador
Rosario, Y. (2020)	La importancia de la Inteligencia Artificial en la Seguridad Cibernética	Artículo científico publicado en revista	*"es la disciplina que se encarga de proteger la integridad y la privacidad de la información. Se diseñó basada en reglamentos, modelos y estándares para poder proteger las redes, los dispositivos electrónicos, los programas y los datos contra ataques, daños o acceso no autorizado".*	Es importante porque las compañías almacenan datos y generan altas cantidades de transacciones en sus sistemas, donde una parte de esa información puede ser confidencial, por lo cual se pueden generar consecuencias negativas para las instituciones, organizaciones y ciudadanía en general.

Kremmer, J. (2014)	La construcción de seguridad cibernética de Ecuador y Uruguay	Artículo científico publicado en revista	*"el liberalismo considera a la seguridad cibernética no solo como el mecanismo de protección del Estado, sino también como el mecanismo de protección de los derechos individuales".*	Se busca mitigar las amenazas a los derechos de los ciudadanos por parte de cualquier actor nacional e interacional.

Fuente: Elaboración propia (2021).

Tabla 5: Estrategias de seguridad cibernética.

Autor y año	Título del estudio	Tipo de document	Objetivo del estudio	Metodología del estudio	Resumen de resultados
Núñez, C. (2019)	Estrategias nacionales de ciberseguridad en el Cono Sur. Análisis a partir de los indicadores de la Organización para la Cooperación y el Desarrollo Económico	Artículo científico publicado en revista	Analizar la preparación de la ciberseguridad de cada Estado mostrando diferencias y similitudes entre sus respectivas estrategias.	*La investigación se clasificó como cualitativa, la técnica de recolección de datos utilizada fue la revisión documental.*	*Las Estrategias Nacionales de Ciberseguridad buscan responder a las nuevas necesidades de seguridad en el ciberespacio. Para que existan, es indispensable elaborar una política de Estado; en donde se establezcan propósitos, principios rectores, políticas, objetivos a largo plazo, medidas específicas o líneas de acción, un diseño institucional con funciones mínimas, leyes y normativas, instituciones coordinadas y con capacidades, infraestructura, presupuesto, etc., para enfrentar las nuevas amenazas cibernéticas, donde una Estrategia Nacional de Ciberseguridad, debe involucrar al Estado, a la empresa privada, la sociedad, la academia y las relaciones internacionales.*

Fuente: Elaboración propia (2021).

Discusión de resultados

Las ciberamenazas.

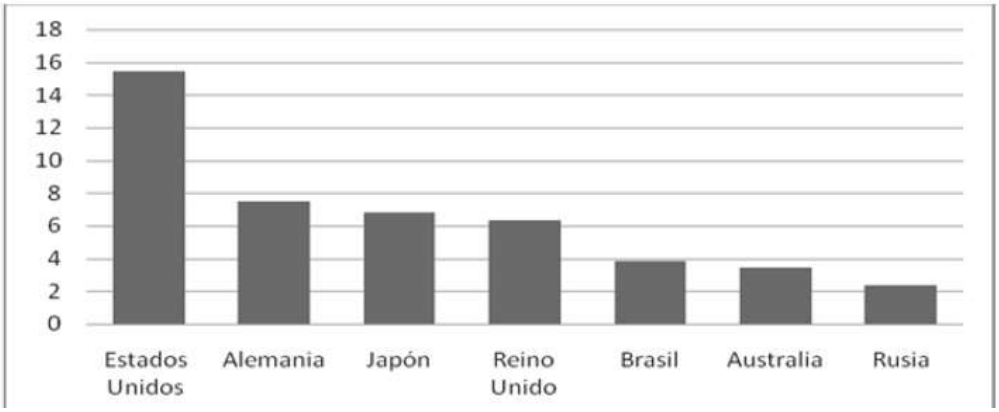
Núñez (2019) refiere que realizar un diagnóstico de los delitos o ataques cibernéticos que han ocurrido en regiones latinoamericanas es una tarea compleja, debido al déficit de registros

sustentables. Sin embargo, se detalla que la tendencia a la ocurrencia de este tipo de amenazas es creciente, destinándose tanto a individuos, como a organizaciones privadas e instituciones estatales.

Dinatale (2018) describe que, en naciones como Argentina, que por años ha estado bajo la sombra de distintos tipos de ciberamenazas las cuales han logrado poner en la palestra la vulnerabilidad de las instituciones públicas, privadas y la ciudadanía en general. Esto se refleja, en los datos oficiales emitidos por el Ministerio de Modernización en el año 2017, el cual detalla que se suscitaron más de tres millones de incidentes informáticos, siendo focalizados a principalmente a las empresas privadas; llegándose a reflejar un incremento de hasta un 700% en los hackeos a los sistemas informáticos.

Asimismo, Arias (2011) establece que Brasil, el país gigante de América Latina ha sido puesto a prueba a nivel de seguridad cibernética, debido a que a recibido directamente ciberataques en su sector público, siendo vulneradas las plataformas tecnológicas de instituciones, ministerios, empresas e inclusive el área militar. Actualmente, la nación brasilera se sitúa en el quinto lugar a nivel mundial de los países que más perdidas perciben por delitos informáticos, acompañando a grandes potencias como Estados Unidos y Alemania, e incluso superando en pérdidas a Rusia.

Gráfico 1: Volumen de pérdidas generadas por los delitos informáticos, en millones de USD.



Fuente: Statista (2019).

Otra nación que ha sido víctima de las ciberamenazas es Chile, que en los últimos años ha sido blanco de diversos ciberataques, en su mayoría destinados a robar información para cometer fraudes económicos. De igual manera Paraguay, es otra nación que ha presentado vulnerabilidad

ante los ciberataques, ya que su plataforma tecnológica es considerada débil para la protección de datos.

La ciberseguridad

El Observatorio de la Ciberseguridad en América Latina en su informe del año 2016, estableció el porcentaje de acceso al internet respecto al desarrollo de políticas y estrategias en el ámbito de la seguridad en el ciberespacio.

Tabla 5: Porcentaje de acceso al internet respecto al desarrollo de políticas y estrategias de América del Sur.

Ecuador 43%	Colombia 53%	Brasil 58%	Chile 72%	Argentina 65%
NO ha desarrollado una **ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA**. Ecuador ha hecho avances en los últimos años para fortalecer su capacidad para abordar amenazas informáticas.	Estableció **LA POLÍTICA NACIONAL DE SEGURIDAD CIBERNÉTICA**	En el año 2010 publicó las **ESTRATEGIAS NACIONALES DE SEGURIDAD DE LAS COMUNICACIONES DE INFORMACION Y SEGURIDAD CIBERNÉTICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL**	Se establecieron **LAS POLÍTICAS DE SEGURIDAD CIBERNÉTICA A NIVEL GUBERNAMENTAL**	Desarrollaron el proyecto de **ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA**

Fuente: Observatorio de la Ciberseguridad en América Latina (2016)

El Ecuador no cuenta con una estrategia específica de ciberseguridad. Si bien el Estado ha desarrollado mecanismos que permitan hacer frente a las ciberamenazas, no se han logrado consolidar políticas de seguridad que se enfoquen en esta materia. A pesar de estas limitaciones, existen varios actores de seguridad que han buscado impulsar, en sus ámbitos respectivos, ciertos proyectos de seguridad cibernética. Los principales actores gubernamentales están estrechamente relacionados con las tecnologías de la información y la comunicación.

Estrategias de seguridad cibernética.

Las Estrategias Nacionales de Ciberseguridad buscan responder a las nuevas necesidades de seguridad en el ciberespacio. Para que exista, es indispensable elaborar una política de Estado; considerándola como una Estrategia de Seguridad Nacional, en donde se establezcan propósitos,

principios rectores, políticas, objetivos a largo plazo, medidas específicas o líneas de acción, un diseño institucional con funciones mínimas, leyes y normativas, instituciones coordinadas y con capacidades, infraestructura, presupuesto, etc., para enfrentar las nuevas amenazas cibernéticas, donde una Estrategia Nacional de Ciberseguridad, debe involucrar al Estado, a la empresa privada, la sociedad, la academia y las relaciones internacionales.

Asimismo, para poder establecer estrategias de seguridad cibernética efectivas, las organizaciones necesitan coordinar sus esfuerzos en todos los sistemas que utilizan, como: la seguridad de la red, la seguridad de datos, seguridad de aplicaciones, gestión de identidad, seguridad de la infraestructura, bases de datos, seguridad de la nube, seguridad móvil y recuperación de desastres. Algunos países latinoamericanos han empezado a desarrollar políticas para enfrentar este fenómeno, entre las cuales se tienen:

Tabla 6: Estrategias Nacionales de Ciberseguridad implementadas en países latinoamericanos.

País	Nombre de la Estrategia Nacional de Ciberseguridad	Año de publicación
Argentina	Estrategia Nacional de Ciberseguridad	2015
Brasil	Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal	2015
Chile	Política Nacional de Ciberseguridad	2017
Paraguay	Plan Nacional de Ciberseguridad de Paraguay	2017

Fuente: Dammert y Núñez (2019).

En función a los indicadores de ciberseguridad de la Organización para la Cooperación y el Desarrollo Ecónomico – OECD (2012), se analizan las Estrategias Nacionales de Ciberseguridad de los países referenciales de la región latinoamericana, agrupados según sus fines, ya sean de: protección, cooperación y/o estratégicos (ver Tabla 7).

Tabla 7: Análisis comparativo de Estrategias Nacionales de Ciberseguridad

	INDICADORES DE CIBERSEGURIDAD OECD / PAISES	ARG	BR	CHL	PAR	URU
Protección	Seguridad del gobierno	X	X	X	X	X
	Infraestructura de información críticas	X	X	X	X	X
	Monitoreo en tiempo real					
	Desarrollo de industrias de seguridad cibernética		X	X	X	
	Consideración de soberanía		X	X		
	Lucha contra el ciberdelito	X		X	X	X
	Respuesta	X	X	X	X	X
Cooperación	Cooperación internacional	X	X	X	X	X
	Coordinación gubernamental - Multiagencia para un enfoque interinstitucional	X	X	X	X	X
	Cooperación público – privada	X	X	X	X	X
	Diálogo de multiactores interesados			X	X	X
	Asociaciones con proveedores de servicios de internet (ISP)	X				
Estratégicos	Enfoque de política flexible	X	X		X	X
	Sensibilización	X	X	X	X	X
	Educación, Investigación y Desarrollo	X	X	X	X	X
	Resiliencia		X	X	X	
	Desarrollo de marcos de identidad digital	X		X		X
	Políticas específicas para la protección de niños en línea	X			X	
	Respuesta de los valores fundamentales			X		

Fuente: Dammert y Núñez (2019).

En el ámbito de protección, las naciones adoptaron el indicador de seguridad del Gobierno; donde el Estado Argentino, propuso la elaboración de normas destinadas a incrementar los umbrales de seguridad, tanto en los recursos como en los sistemas que están relacionados con tecnologías informáticas del sector público nacional. Por su parte la nación brasilera, cuenta con una agencia especializada para la seguridad del gobierno denominada Agencia Brasileña de Inteligencia, la cual funge como el órgano encargado de proporcionar al presidente y a los ministros, información y análisis estratégico, necesarios para la toma de decisiones. En concordancia, el Estado Chileno, estableció normas técnicas sobre sistemas y sitios web de los órganos de la administración del Estado y direccionado por el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT Chile). Al respecto, el Estado Paraguayo coordina con los agentes representantes o responsables de cada sección gubernamental, apelando de esta manera a la correcta función de los altos cargos, teniendo conciencia situacional referente a la ciberseguridad.

Así también, los países latinoamericanos referidos establecen un nivel prioritario a la protección de infraestructura de información crítica, vinculando a un equipo de tratamiento de ciberamenazas a los diferentes órganos de seguridad de Estado. En contraposición a ello, ninguna nación ha desarrollado el monitoreo en tiempo real, el cual requiere de la detección inmediata a nivel

operativo de las ciberamenazas mediante el establecimiento de Centros de Operaciones de Seguridad Cibernética.

Por su parte, la estrategia de desarrollo de industrias de seguridad cibernética se ha arraigado en Brasil, Chile y Paraguay, en donde se busca el desarrollo tecnológico e innovación, por medio de la implementación de programas piloto de ciudades inteligentes y/o de energías renovables, que requieren de manera estricta fuertes sistemas de seguridad cibernética para proporcionar protección a nivel nacional e internacional.

Entre tanto, Brasil y Chile han manejado el enfoque de consideración de soberanía, dándole el enfoque militar y de defensa respecto al reconocimiento de las amenazas cibernéticas, exigiendo políticas que fomenten la seguridad desde esta perspectiva. Así también, se fundamenta la lucha contra el ciberdelito, en donde Argentina, Chile y Paraguay, se direccionan hacia la investigación y el procesamiento de los ciberdelitos y los cibercrímenes; sustentándose todo ello en base a una capacidad de respuesta por parte de las naciones latinoamericanas con la formación de sus respectivos Equipos de Respuesta a Incidentes de Seguridad Cibernética.

La cooperación en sus distintas dimensiones, ya sea internacional, intergubernamental y/o cooperación público – privada es determinante para que un país cumpla con estándares mínimos de seguridad cibernética, pues la ciberseguridad no será efectiva si solo nutrimos un marco legal entorno a lo nacional, descuidando los quehaceres internacionales en materia cibernética, ya que, las ciberamenazas y todo lo relacionado con el ciberespacio, rompe fronteras. Al respecto, la coordinación gubernamental – multiagencia, genera un enfoque interinstitucional, planteándose una coordinación y una cooperación entre los órganos gubernamentales, la cual sumada a la cooperación público – privada, es de suma importancia para la ciberseguridad, debido a que los incidentes cibernéticos, en su mayoría van dirigidos a instituciones privadas, afectando primordialmente al sector financiero.

Ante la presencia del diálogo multipartes interesadas, Chile y Paraguay, recogen los conocimientos de los diversos actores a los que compromete la ciberseguridad. Se solicitan constantemente la ayuda de expertos en seguridad cibernética, ya sea del sector privado, la academia y/o la sociedad civil para ampliar la capacidad de respuesta ante factores de riesgo. Es de hacer notar, que solo el Estado Argentino a generado asociaciones con proveedores de servicios de internet, lo que facilita

el intercambio de información entre el sector gubernamental y los proveedores de internet, sobre todo ante situaciones de fraudes, ciberdelitos o cibercrimen.

A nivel estratégico, donde es necesaria la toma de decisiones rápida e informada, el constante aprendizaje, retroalimentación y mejoramiento, son esenciales para optimizar recursos y tiempo. Precisamente, el enfoque de política flexible en la ciberseguridad que adoptan países latinoamericanos, busca el repercutir en la buena utilización de los recursos, generando una rendición anual de la situación de la cibernética de una nación. Asimismo, se plantea mayor control, por medio de mecanismos de mapeo sistemático de los activos que afecten al Estado y a la sociedad que componen la infraestructura crítica de la información.

En tal sentido, se plantea la sensibilización para fortalecer a la población en el uso responsable de las tecnologías e internet, promoviendo la concientización en base a los riesgos que conlleva el uso de medios digitales y tecnologías de información y comunicación. De la mano con ello, naciones latinoamericanas han puesto en la educación, la investigación y el desarrollo todos sus esfuerzos, en donde algunos países tienen una educación en materia cibernética más robusta en comparación con otros países. En conjunto, las naciones ven a la resiliencia como la capacidad de los sistemas de red gubernamentales y privados de estar preparados o recuperarse ante ciberincidentes, siendo esta una de las direccionales principales para medir la efectividad de la ciberseguridad de un país.

Por tanto, frente a los indudables avances tecnológicos, los marcos de identidad digital son una necesidad tanto para el Estado como para los ciudadanos para optimizar recursos en los trámites que se soliciten. Con estos marcos de identidad, se establecen sistemas de identidad digital, lo cual proporciona la autentificación en línea, permitiendo el libre acceso a documentos personales y servicios de gobierno de manera remota, en tiempo real y desde cualquier dispositivo. Esto, además proporciona la capacidad de protección de niños y niñas, que, sin mayor conocimiento son blanco fácil de la inseguridad en las redes, puntualizando en medidas que eviten el ciberacoso, el ciberbullying, entre otros.

Ante los indudables riesgos de la web, los países tienen la obli¬gación de resguardar la seguridad de las personas en el ciberespacio, incluso de sus propios Estados, pues en lo inmediato, son los ciudadanos los que no cuentan con las herramientas ni cono¬cimientos idóneos para enfrentar la vulneración de su desarrollo personal en internet. La respuesta de valores fundamentales precisamente apunta a que las personas puedan realizar sus actividades personales, sociales y

comunitaria vía web respetándoles la privacidad, la libertad de expresión y el libre flujo de información.

En contexto, la República del Ecuador, un país considerado con ciberseguridad deficiente a nivel general, a presentado aspectos positivos en la gestión de incidentes y crisis, además cuenta con otro aspecto a su favor como es la generación de la identificación electrónica y servicios de confianza, con ello, el Índice Nacional de Ciberseguridad, por sus siglas en inglés NCSI, le proporciona un 67% en este ámbito, pero eso no exonera a la nación de ubicarse para el año 2018 en el puesto 82 del ranking del NCSI, en donde se detallan los indicadores que sigue el Estado Ecuatoriano en cuanto a la seguridad cibernética (ver Tabla 8).

Tabla 8: Síntesis de Ciberseguridad el 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%)	
Gestión de la crisis cibernética	1/5 (20%)	
Lucha contra el ciberdelito	4/9 (44%)	
Ciberoperaciones militares	4/6 (67%)	

Fuente: Alvarado (2020)

Es de hacer notar, que el Ecuador cuenta con herramientas jurídico – institucionales, que fundamentan legal y técnicamente las acciones de ciberseguridad que se llevan a cabo en la nación (ver Tabla 9).

Tabla 9: Herramientas jurídico – institucionales que garantizan la ciberseguridad en Ecuador.

Leyes/acuerdos y Organizaciones
a) Constitución de la República del Ecuador
b) Ley de Seguridad Pública y del Estado
c) Ley de Comercio electrónico, firmas electrónicas y mensajes de datos
d) Acuerdo No. 166, emitido por la Secretaría Nacional de la Administración Pública (SNAP)
1. Ministerio de Defensa Nacional:
- Política de la Defensa Nacional "Libro Blanco"
- Acuerdo Ministerial No. 281
2. Dirección Nacional de Registro de Datos Públicos:
- DatoSeguro
3. 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
4. Agencia de Regulación y Control de las Telecomunicaciones:
- Centro de Respuesta a incidentes informáticos del Ecuador (EcuCERT)

Fuente: Alvarado (2020).

Para lograr una seguridad cibernética, se propone que el Estado Ecuatoriano considere una serie de líneas de acción que conlleven a minimizar las ciberamenazas y los ciberataques, para lo cual se recomienda:

- Capacidad del Estado para enfrentar las ciberamenazas.
- Seguridad de la información de la administración pública.
- Seguridad de la infraestructura crítica.
- Cibercriminalidad.
- Ciberdefensa.
- Capacidad del sector privado ante ciberamenazas.
- Sociedad y cultura de ciberseguridad.
- Investigación, desarrollo e innovación.

El cumplimiento de dichas líneas de acción va de la mano del logro de los objetivos que se formulan a continuación:

- Fortalecer la ciberseguridad a nivel nacional

- Diseño e implementación de un marco nacional interinstitucional para proteger la información, sistemas y servicios del Estado de las diferentes ciberamenazas.
- Actualización de la normativa jurídica nacional y desarrollo de normas técnicas necesarias para la ciberseguridad nacional.
- Determinación del impacto de la interrupción de los servicios digitales públicos e identificar la infraestructura crítica nacional.
- Fortalecer la capacidad de respuesta ante incidentes.
- Fortalecer la seguridad ciudadana y del Estado en el ámbito digital a nivel nacional.
  - Recopilar información estadística actualizada referente a las amenazas y riesgos a la seguridad ciudadana y del Estado.
  - Implementar en las comunidades normas y procedimientos que contribuyan a la administración de los recursos informáticos y digitales.
  - Localizar posibles actores que atenten a la seguridad de las personas y del Estado, especialmente en el ámbito de la ciberseguridad.
- Fortalecer la ciberdefensa para contribuir con la ciberseguridad nacional e incrementar la resiliencia del país, protegiendo la infraestructura critica digital priorizada del Estado.
  - Proteger la infraestructura critica digital de las Fuerzas Armadas y priorizada del Estado para garantizar el normal funcionamiento del país.
  - Fortalecer la capacidad de protección en el ciberespacio de la infraestructura critica de Fuerzas Armadas y la priorizada del Estado.
  - Incrementar la investigación e innovación para el desarrollo de la capacidad de ciberdefensa.
  - Apoyar a los demás sectores del Estado en la protección de la infraestructura critica nacional en caso de grave conmoción o crisis.
  - Fortalecer los lazos de cooperación internacional en materia de ciberdefensa.
- Construir una red público - privada para potenciar las capacidades nacionales para la ciberseguridad.
  - Fortalecer el sector público - privado del Estado en la implementación de protocolos y planes de contingencia en el ciberespacio desde un enfoque colectivo.

  - Promover el fortalecimiento del centro de operaciones gubernamental para el intercambio de la información sensible del Estado.
  - Incentivar el ingreso de talento humano contratado, altamente calificado, en el ámbito de ciberseguridad.
- Incrementar la concientización en materia de ciberseguridad.
  - Difusión de las directrices existentes sobre seguridad del manejo de la información.
  - Fomentar el intercambio de buenas prácticas nacionales e internacionales para incrementar la seguridad de la información de Estado.
  - Diseñar programas y campañas para fomentar la cultura de seguridad cibernética en el sector público y privado.

Conclusiones

La digitalización de la información se ha convertido en un aspecto de fundamental importancia para cualquier Estado, motivado a que las empresas públicas han digitalizado casi en su totalidad la documentación estratégica que manejan y han automatizado todos sus procesos. En concordancia, la ciudadanía ha hecho lo propio y su información confidencial y la mayoría de sus operaciones y/o transacciones las realizan a través de las redes. Esto representa una amplia inquietud por parte de los Estados y sus ciudadanos, porque están propensos a la acción de organizaciones, hackers, otros Estados y grupos terroristas, que están en disposición de realizar ciberataques; poniendo esto como prioridad de Estado a la ciberseguridad.

La ciberseguridad se ha tornado en una necesidad real para la seguridad de las naciones, tanto para proteger sus plataformas tecnológicas a nivel público y privado, como el proteger y permitir el desenvolvimiento cotidiano de los ciudadanos en las redes.

Las amenazas a la seguridad cibernética afectan de manera directa, teniendo un impacto global, por lo que la comunidad internacional, representada por los organismos internacionales se han puesto del lado de los Estados para apoyarlos en el desarrollo e implementación de estrategias que optimicen sus niveles de ciberseguridad. Con esto, la instauración de Estrategias de Seguridad Cibernética en la región latinoamericana, teniendo como referencia indicadores de ciberseguridad establecidos por la Organización para la Cooperación y el Desarrollo Económico.

Con ello, se visualiza que Chile es el país que cumple con la mayoría de los indicadores de ciberseguridad, lo que lo convierte en la vanguardia en los procesos de establecimiento de unas estrategias de seguridades cibernéticas coherentes y ajustadas a los lineamientos de los organismos internacionales.

En la actualidad, la seguridad dejó de ser el último elemento para considerar y está siendo parte de todo proceso de desarrollo y pruebas. Pese a ello, los tiempos que puede demandar corregir vulnerabilidades o debilidades en los sistemas son extensos.

Considerando todas las experiencias de muchos países de la región en cuanto a las estrategias creadas en función de las amenazas que circundan en el ciberespacio, es una necesidad imperiosa del Estado Ecuatoriano frente a estas nuevas amenazas "híbridas", crear un organismo de Ciberseguridad que garantice el principio de individualidad de los ciudadanos y de la infraestructura crítica del estado evitando la pérdida de recursos garantizando la seguridad y paz interna en forma preventiva y proactiva considerando la experiencia de países que lideran este campo y ya tienen en funcionamiento sus políticas nacionales y estrategias de Ciberseguridad.

El Ecuador tiene un acceso al internet del 43% de la población permitiendo estar conectados a la información que está en el ciberespacio lo cual es una puerta de entrada para los delincuentes aumentando el riesgo a la seguridad, por lo cual se debe adaptar su política y estrategias de seguridad cibernética, considerando los modelos implementados en países de la región.

Es fundamental que el Estado cuente un marco legal contra los delitos informáticos, que puede afectar la infraestructura crítica y proteja la información, este marco jurídico debe estar basado en precedentes tomados de acuerdos internacionales y de la legislación de otros países.

Se necesita ahondar en la concientización de todos los nacionales sobre los hábitos cibernéticos y la sensibilidad general hacia la seguridad de la información, lo cual dificultará que los ciberdelincuentes puedan perpetuar fácilmente ataques. El ciberespacio nunca estará seguro al cien por ciento, aunque se implementen estrategias de seguridad, ya que junto con ellas evoluciona una alta tendencia a las ciberamenazas.

Referencias

1. Alvarado, J. (2020). Análisis de ataques cibernéticos hacia el Ecuador.
2. Arias, J. (2015). Brasil sufre un ciberataque a gran escala.

3. Azcona (2017). Definiciones sobre ciberseguridad.
4. Bayuk, J., Healey, J., Rohmeyer, P., Sachs, M., Smitdt, J. y Weiss, J. (2012). Cyber security policy guidebook.
5. Cárdenas, S. (2020). Estrategia nacional de ciberseguridad.
6. Castro, H. y Monteverde, A. (2018). Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito.
7. Comnimos (2013). Ciberseguridad en América Latina. Orientación actual de la política hemisférica de seguridad.
8. Dammert, L. y Núñez, C. (2019). Enfrentando las ciberamenazas: estrategias nacionales de ciberseguridad en el Cono Sur.
9. Dinatale, M. (2018). Incremento de los hackeos en la Argentina.
10. Fernández, A. y Rodríguez, J. (2017). Análisis de las ciberamenazas. Cuadernos de estrategia.
11. Gazapo, M. y Machín, N. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea.
12. Hirare, S. (2017). Análisis de las ciberamenazas. Cuadernos de estrategia.
13. Kremmer, J. (2014). La construcción de seguridad cibernética de Ecuador y Uruguay.
14. Leiva, E. (2015). Estrategias nacionales de ciberseguridad: Estudio comparativo basado en enfoque Top – Down desde una visión global a una visión local.
15. Mayorga, A. (2016). Lineamientos, tendencias y estrategias sobre ciberseguridad y ciberdefensa en Colombia.
16. Mogollón, F. (2017). Desafíos de la ciberseguridad y respuestas estatales: el caso del Estado Ecuatoriano en el periodo 2008 – 2015.
17. Núñez, C. (2019). Estrategias nacionales de ciberseguridad en el Cono Sur. Análisis a partir de los indicadores de la Organización para la Cooperación y el Desarrollo Económico.
18. Observatorio de la Ciberseguridad en América Latina (2016). Porcentaje de acceso al internet respecto al desarrollo de políticas y estrategias de América del Sur.

19. Orellana, C. (2017). De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales.
20. Organización para la Cooperación y el Desarrollo Económico (2012). Estrategias Nacionales de Ciberseguridad implementadas en países latinoamericanos.
21. Palella, S. y Martins, F. (2012). Metodología de la investigación cuantitativa.
22. Rauscher y Yashenko (2011). Ciberseguridad.
23. Rosario, Y. (2020). La importancia de la Inteligencia Artificial en la Seguridad Cibernética.
24. Statista (2019). Volumen de pérdidas generadas por los delitos informáticos en determinados países en agosto de 2015.
25. Tates, C. y Recalde, L. (2019). La ciberseguridad en el Ecuador, una propuesta de organización.
26. Unión Internacional de Telecomunicaciones (2017). Agenda de ciberseguridad global (GCA).