Polo del Conocimiento

Pol. Con. (Edición núm. 56) Vol. 6, No 3
Marzo 2021, pp. 1251-1273
ISSN: 2550 - 682X
DOI: 10.23857/pc.v6i3.2432

Experiencias de seguridad cibernética en países europeos y latinoamericanos. Apuntes hacia la defensa nacional

Cybersecurity experiences in European and Latin American countries. Notes towards national defense

Experiências de segurança cibernética em países europeus e latino-americanos. Notas para a defesa nacional

Sardis Otilia Mosquera-Chere [I]
sardysmosquera@gmail.com
https://orcid.org/0000-0003-3058-920X

Correspondencia: sardysmosquera@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 Docencia y Desarrollo del Currículo, Ingeniero en Sistemas Informáticos, Tecnólogo en Informática, Docente Investigadora de la Carrera de Tecnologías de la Información en la Facultad de Ingenierías de la Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador.

Resumen

En la actualidad los problemas que se viven no solo son sanitarios, sino también de las amenazas cibernéticas que son aprovechadas por la crisis que se experimenta a nivel mundial por la pandemia del Covid-19 o Coronavirus y el confinamiento en las casas de habitación. Estas ciberanemazas, se hacen pasar por organismos oficiales e institucionales y de esa manera poder obtener la información personal o de las redes corporativas y gubernamentales, y esto debido a que las personas están trabajando desde espacios que son poco seguros, lo cual conlleva a la vulnerabilidad de la ciberseguridad de un Estado. En este sentido, se plantea a continuación un estudio sobre las experiencias de seguridad cibernética en países de Europa y de América Latina, con la finalidad de cumplir con el propósito de formular lineamientos o apuntes que se vean reflejados a mejorar la defensa nacional de Ecuador. La metodología se fundamenta desde el enfoque cualitativo, bajo la comparación de experiencias de varios países, tomando desde a revisión documental la recopilación de fuentes para el desarrollo del tema y posteriormente establecer aspectos importantes para el país.

Palabras claves: Amenazas cibernéticas; ciberamenazas; seguridad cibernética; defensa nacional; ciberseguridad.

Abstract

Currently, the problems that are experienced are not only health, but also cyber threats that are taken advantage of by the crisis that is experienced worldwide by the covid 19 coronavirus pandemic and the confinement in houses of residence. These cyber threats pose as official bodies and institutions and thus be able to obtain personal information or from corporate and government networks, and this because people are working from spaces that are not very secure, which leads to the vulnerability of the cybersecurity of a State. In this sense, a study on cyber security experiences in European and Latin American countries is presented below, in order to comply with the purpose of formulating guidelines or notes that are reflected in improving the National defense of Ecuador. The methodology is based on the quantitative approach, comparing the experiences of several countries, taking from the documentary review the compilation of sources for the development of the subject and later establishing important aspects for the country.

Keywords: Cyber threats; cyber threats; cyber security; national defense; cyber security.

Resumo

Atualmente, os problemas vividos não são apenas de saúde, mas também de ameaças cibernéticas que se aproveitam da crise vivida mundialmente pela pandemia de Covid-19 ou Coronavirus e do confinamento em residências. Essas gangues cibernéticas, se passam por órgãos oficiais e institucionais e, assim, podem obter informações pessoais ou de redes corporativas e governamentais, e isso porque as pessoas estão trabalhando em espaços pouco seguros, o que leva à vulnerabilidade da cibersegurança de um Estado. Nesse sentido, apresenta-se a seguir um estudo sobre as experiências de segurança cibernética em países europeus e latino-americanos, a fim de cumprir o propósito de formular diretrizes ou notas que se reflitam no aprimoramento da defesa nacional do Equador. A metodologia baseia-se em uma abordagem qualitativa, comparando experiências de diversos países, partindo de uma revisão documental a compilação de fontes para o desenvolvimento do tema e, posteriormente, estabelecendo aspectos importantes para o país.

Palavras-chave: Ameaças cibernéticas; Ameaças cibernéticas; Segurança cibernética; Defesa nacional; Segurança cibernética.

Introducción

Estudios e investigaciones han caracterizado al "ciberespacio" como un dominio de naturaleza militar, por lo que es necesario desarrollar capacidades militares de "ciberdefensa" por parte de los Estados, lo cual ha estado ocupando espacios en los debates sobre la defensa nacional y el diseño de las fuerzas militares (Eissa et al., 2012).

Estos autores detalla, que, a diferencia de los tradicionales escenarios de batallas en tierra, mar y aire, el espacio (este nuevo dominio militar no es físico, sino "virtual") (Joyanes, 2010), lo que da apertura a un abanico de interrogantes desde el punto de vista de la Defensa Nacional: pensar al ciberespacio como un entorno con sus propios medios y reglas, con la particularidad de no poseer locación física específica, implicaría un cuestionamiento a la utilidad de las categorías tradicionales con las que se aborda una "guerra real".

Por lo cual, para Eissa et al. (2012), el carácter novedoso y contemporáneo de los fenómenos vinculados al ciberespacio constituye el principal obstáculo a la hora de dilucidar sus

implicancias para la Defensa Nacional, debido a que la ausencia de consensos a la hora de definir las operaciones sobre seguridad cibernética reproduce sus efectos en el nivel político, obstaculizando la atribución de responsabilidades y la toma de decisiones.

Por ende, desde hace varias décadas, las tensiones que surgen por la diversidad de puntos de vista sobre la gobernanza del ciberespacio, que han sido evidentes entre las naciones (Preciado, 2021). Indica el mismo autor que en el año 2020, se observaron más intervenciones gubernamentales destinadas a localizar los servicios en la nube, a razón de temores de seguridad nacional y privacidad, y es que la pandemia por Covid-19 solo ha exacerbado estas tensiones, con naciones nerviosas que se acusan cada vez más entre sí de ciberespionaje e interferencia en sus asuntos internos.

Passman (2020), señala que en la actualidad, no es de sorprender que las amenazas cibernéticas aumenten y los ataques se vuelvan cada vez más sofisticados, y es que en esta época, la información sobre cada persona, datos jurídicos, de instituciones y organizaciones, tanto públicas como privadas se encuentra en un canal que no vemos a través del internet y el ciberespacio, lo que cada país debe tener en cuenta para proteger y salvaguardar sus recursos y sus ciudadanos de amenazas y ataques cibernéticos.

Por otro lado, la Organización de los Estados Americanos – OEA (2013), señaló que en un mundo que permanece interconectado, es necesario buscar un equilibrio que permita disfrutar la comodidad que ofrecen las tecnologías de la información y comunicación (TIC) y minimizar las oportunidades que su uso ofrece a los delincuentes cibernéticos.

Un informe de Motorola Solutions, Inc. (2015), menciona que la seguridad cibernética permite implementar políticas, procedimientos y mecanismos técnicos para proteger, detectar y corregir problemas que amenacen la seguridad de su red.

Asimismo, el informe refleja que un objetivo frecuente de los hackers son las redes gubernamentales, pues su objetivo es conseguir propiedad intelectual muy valiosa, y por ello cada vez más, los ataques se originan en países extranjeros.

Por lo cual, en un panorama que cambia vertiginosamente y que se caracteriza por una combinación de ataques, como virus, suplantación de identidad (phishing) y robo de identidad, es importante implementar anillos concéntricos de protección. Este enfoque holístico debe tener en cuenta todo el ciclo de vida de la protección de la seguridad: desde la evaluación de la seguridad,

la integración y los servicios gestionados, como la supervisión del firewall y la protección contra intrusiones, hasta el desarrollo de políticas (Motorola Solutions, Inc., 2015).

Así, Motorola Solutions, Inc. (2015), indica que un error común que se repite en muchas personas, organizaciones e instituciones es la falta de planificación. Señalan que no es suficiente implementar un control de seguridad y quedarse tranquilo, es preciso realizar un mantenimiento y una revisión de los controles con regularidad, en especial porque las amenazas al entorno cambian continuamente, tal como expresa Barrera (2020), el problema es que la ciberseguridad no le hacen tanto caso, porque no se ve, no se percibe el riesgo, y no lo vemos hasta que lo tenemos encima, porque el internet es una gran malla de información y es incontrolable, por lo que la mejor solución es la prevención, la cual hay que tomarla muy en serio, que es de verdad, que no se ve pero si se siente, porque lo físico pasa a lo virtual y a veces lo que se pueda crear o generar actualmente en los ciudadanos, organismos e instituciones, pueden marcar la vida en el futuro y no se sabe cómo en el día de mañana puede evolucionar.

Por lo cual, es fundamental tomar esta temática desde el punto de vista de relacionar experiencias de seguridad cibernética en países europeos y de latinoamérica, con el propósito de formular lineamientos o apuntes que se vean reflejados a mejorar la defensa nacional de Ecuador.

En tal sentido se plantea la investigación desde un enfoque cualitativo, basado en un método comparado, debido a que se realizó una comparación de las experiencias de países de Europa y de América Latina, para luego reflejar lineamientos para Ecuador. Para ello, fue necesario recurrir a la revisión y recopilación de información de fuentes primarias documentales y de páginas web sobre los conceptos básicos respecto a: cibernética, ciberespacio, ciberriesgo, ciberdelitos, ciberdefensa y ciberseguridad, así también lo referente a la infraestructura crítica del Estado y la necesidad de seguridad cibernética en América Latina.

Fundamentación teórica

A continuación, se presenta el basamento o fundamentación teórica que sustenta el tema de esta investigación.

Conceptos básicos sobre: cibernética, ciberespacio, ciberriesgo, ciberdelitos, ciberdefensa y ciberseguridad

De acuerdo a Barbosa (2004), en 1948 Norbert Wiener, en su libro Cybernetics, or control and communication in the animal and the machine , propone el concepto de cibernética para reunir

toda una gama de teorías que se venían desarrollando antes y durante la segunda guerra mundial: "la cibernética es la ciencia de la dirección y comunicación en los organismos vivos y en las máquinas", donde indica que "hemos decidido llamar a toda la materia referente al control y teoría de la comunicación, tanto en la máquina como en el animal, con el nombre de cibernética", detallando además que "hasta hace muy poco tiempo no existía una voz que comprendiera ese conjunto de ideas; para poder expresarlo todo mediante una palabra, me vi obligado a inventarla". Sin embargo, advierte que dicho término fue tomado de los griegos y especialmente de Platón: "Ciertamente que ya Platón empleó la palabra en el sentido de forma de pilotar una nave... La palabra, en fin, procede etimológicamente del griego Kybernetes, piloto, timonel, de ahí su sentido actual" (p.174).

No obstante, describe Barbosa (2004), la cibernética no se circunscribe al helénico "arte de gobernar un timón" (p. 177), si no que incluye todo el contexto de: la nave, su capitán, el piloto y timonel, donde coloca como ejemplo al piloto quien es el pensamiento cibernético, ya que está situado entre el capitán que fija el objetivo y el timonel que lleva el buque, elige el programa de acción y da las órdenes al timonel. El piloto, es quien controla, gobierna u ordena el rumbo del barco, tiene, previamente, que estar informado no sólo de a dónde ha de dirigirse (orden del capitán), sino del estado de la mar, velocidad y dirección de los vientos, entre otros, recibe toda esta información y toma una decisión: el rumbo. Así es como la cibernética, en su acepción actual, se extiende al estudio del funcionamiento de toda clase de sistemas (Barbosa, 2004).

Posteriormente, el propio Wiener, indica en 1951 su segunda obra The human use of human being: cybernetics and society, que:

"cuando controlo las acciones de otra persona le comunico un mensaje y aunque este sea de naturaleza imperativa, la técnica de la comunicación no difiere de la técnica de la transmisión de un hecho. Por demás, si deseo que mi control sea eficaz, debo informarme de todos los mensajes procedentes de la persona, capaces de advertirme que la orden ha sido comprendida y ejecutada" (p. 23).

Seguidamente en este contexto, Barbosa (2004), refiere que luego de la propuesta de Wiener surgieron líneas de investigación dedicadas al campo cibernético en diversas áreas y que para el momento abarcaba, al menos, tres grandes esferas: los mecanismos guiados (palabras en el sentido de: regulación), personal que maneja máquinas (palabras con el sentido de: piloto) y sociedades autorreguladas (palabras como: gobierno).

Y es que de acuerdo a Siles (2007), la cibernética, consiste en una ciencia de las leyes generales de la comunicación, aplicadas a una diversidad de entidades, en la cual el concepto de información ocupa un lugar privilegiado en las formas de comprender al ser humano y sus relaciones con el ambiente. (p. 3).

El autor antes mencionado, expresa que, según el enfoque cibernético, la comunicación representa el "modo de ser" de todos los fenómenos y, por lo tanto, su estudio no debe asumirse como un saber más, sino como el elemento común de todas las disciplinas, donde la comunicación es la ciencia de las relaciones entre los fenómenos que permite distinguir su parte esencial, su naturaleza.

Ahora, respecto al término ciberespacio, el Consejo Argentino para las Relaciones Internacionales - CARI (2013), lo define como "la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos cualesquiera sean estos y las telecomunicaciones que los vinculan" (p. 4).

Por otro lado, se encuentra el concepto de ciberriesgo, donde López (2018), considera que no es un riesgo específico, es un grupo de riesgos, que difieren en tecnología, vectores de ataque, medios, etc., por lo que dicho autor plantea estos riesgos de acuerdo a dos características similares, primeramente todos tienen un gran impacto potencial y posteriormente todos fueron considerados una vez improbables; en este sentido, la ciberseguridad para el mencionado autor, es la suma de los esfuerzos invertidos en abordar el ciberriesgo, gran parte de lo cual, hasta hace poco, se consideraba tan improbable que apenas requería de atención.

En este mismo orden de ideas, se encuentra el término de ciberdelito, el cual para los autores Rayón y Gómez (2014), se entiende por "ciberdelito o cibercrimen" cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito (p. 3).

En este contexto, Sánchez (2019) indica que los Estados organizan la Defensa de la Seguridad mediante el establecimiento de Estrategia Nacional, de acuerdo con las amenazas y los consiguientes riesgos se planean y definen unas estrategias de defensa abordando diferentes frentes como el territorial, aéreo, fronterizo, económico y el del ciberespacio, razón por la cual tiene que existir una Ciberdefensa que garantice la Ciberseguridad (p. 38). Por lo cual el autor expresa que la ciberdefensa es:

"el conjunto de acciones u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticos de la Defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos, a la vez que se impide que Fuerzas enemigas los utilicen para cumplir los suyos" (p. 39).

Por otra parte, se encuentra el concepto de ciberseguridad, donde Koch (2015) la define como "la situación de ausencia de amenazas realizadas por medio de, o dirigidas a las tecnologías de la comunicación y de la información y a sus redes" (p. 89). En tal sentido, la ciberseguridad es definida en líneas generales como la seguridad de la información digital, que es reservada en redes electrónicas, la cual debe distinguirse del concepto de seguridad de la información, que, si bien son similares, el último apunta a la actividad de las organizaciones y profesionales de las tecnologías de la información, mientras que la Ciberseguridad tiene un alcance más político o vinculado a la seguridad nacional (Comnimos, 2013).

Por último, ciberseguridad es sinónimo de seguridad cibernética y para la Red Local de Puerto Rico Colmena66 (2021), significa que es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático y por su parte el Gobierno de los Estados Unidos, en su campaña nacional de servicio público Ready (2021), considera que la seguridad cibernética consiste en la prevención, detección y respuesta a los ataques cibernéticos que pueden causar efectos de gran alcance en las personas, organizaciones, y a nivel comunitario y nacional.

Infraestructura crítica del Estado

Para Moncayo (2019), la Infraestructura Crítica (IC), es utilizada por los Estados para definir instalaciones y sistemas en los cuales se encuentran servicios esenciales y su funcionamiento no permite que se generen soluciones alternativas. Por lo cual, la autora también indica que son aquellas instalaciones, redes, servicios, equipos físicos y de tecnología de la información, cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado.

Ahora bien, de acuerdo al Centro de Ciberseguridad Industrial (2013), la IC existente en un Estado son agrupadas dentro de sectores estratégicos, los cuales son necesarios para la seguridad nacional de un país (p. 8).

Por otro lado, de acuerdo a lo señalado por el proceso MERIDIAN del Gobierno Holandés (2016), en la actualidad, los daños físicos (o incluso la destrucción) de elementos esenciales de las IC no son la única amenaza para el correcto funcionamiento de éstas, indican que, los servicios basados en las tecnologías de la información y comunicación (TIC) son cada vez más importantes para el funcionamiento de las IC, por lo que un fallo en la infraestructura relacionada con la información puede tener repercusiones muy serias para un país y por tanto, surge el concepto de Infraestructura Crítica de la Información (ICI), que no es mas que la "información interconectada e infraestructuras de comunicación esenciales para el mantenimiento de los servicios básicos de la sociedad (salud, seguridad, bienestar económico o social de las personas) cuyos daños o destrucción tendría serias consecuencias" (MERIDIAN, 2016).

Necesidad de seguridad cibernética En América Latina

la Comisión Económica para América Latina y el Caribe – CEPAL, (2020), señala que la seguridad cibernética representa un esfuerzo coordinado a nivel nacional, la cual demanda un marco normativo e institucional y una política pública con lineamientos claros sobre la protección de datos, para ello requiere de la cooperación internacional, ya que es clave para enfrentar las amenazas cibernéticas y las alianzas entre el sector público y privado es indispensable para una estrategia efectiva de seguridad cibernética.

La CEPAL (2020), indica que se requiere un marco regulatorio e institucional y una política clara que asegure la gobernanza efectiva relacionado a:

- Una estrategia nacional de ciberseguridad requiere de un ente de coordinación centralizado que pueda definir y dirigirla
- La ciberseguridad tiene varias formas y grados de impacto sobre: personas, empresas, gobiernos.

Las distintas amenazas al uso y mal uso de los datos requieren de mecanismos de respuesta operativa y de esfuerzos conjuntos dentro de un país y entre países, para abordar los ciber riesgos:

- El tratamiento a los programas informáticos maliciosos: malware, spyware, data breaches y ransomware, los cuales incluyen: robo de datos especialmente sensibles, manipulación de datos, obstaculizar el funcionamiento de sistemas informáticos (incluidos los que controlan infraestructuras críticas), borrar y suprimir o bloquear el acceso a datos, programas de extorsión, espionaje cibernético, entre otros.

De igual forma la CEPAL (2020), menciona la dimensión de la importancia de los sistemas críticos de datos y seguridad cibernética, lo que conlleva a la construcción de una agenda holística de ciberseguridad, a saber:

- Incluye infraestructura crítica: clave para los países desde la perspectiva de: defensa, seguridad nacional, economía, salud, orden público y política
- Impactos sobre sectores: servicios públicos y gubernamentales, alimentación, combustible, transporte, comunicaciones, finanzas e industrias.
- Impacto sobre la sociedad: agota fondos del tesoro público, atentar contra los servicios públicos, red eléctrica, telecomunicaciones y el suministro de bienes y servicios esenciales.

En este mismo orden de ideas, la CEPAL (2020), también hace mención sobre la capacidad de respuesta de los gobiernos frente ataques cibernéticos en distintos ámbitos, de la siguiente manera:

- El tamaño, diversidad y dinamismo estructuras económico – sociales, clave para mitigar los efectos de los ataques cibernéticos. Particularmente el impacto sobre las instituciones.
- Sobre los riesgos cibernéticos: ataques a distintos niveles de gobierno hay consideraciones variadas, que muestra entre otras cosas la diversificación económica para atender dichos riesgos.
- En términos de estructura “política” un ataque se dirige al uso de datos personales para fines políticos obtenidos de manera ilícita.
- Sistemas de datos efectivos que protejan a personas de robo de identidad, y a organismos públicos de posible fraude.
- Construcción de talento y tecnología de ciberseguridad para enfrentar los desafíos.

La CEPAL (2020), reseña que ciberseguridad en el flujo transfronterizo de datos, requiere de esfuerzos multilaterales, en concordancia a:

- La cooperación internacional entre actores públicos y privados que involucra temas como: privacidad y protección de datos personales (sensibles), el acceso a los datos almacenados en jurisdicciones extranjeras o en la nube y aspectos relacionados con soberanía nacional.

- Limitar el poder de los monopolios de datos. Los efectos de la red, la falta de portabilidad de datos y derechos de usuario sobre sus datos y la débil protección de la privacidad ayudan a los "data-opolies" a mantener un dominio.
- Se requiere de una mayor coordinación entre los encargados de hacer cumplir las leyes antimonopolio y los funcionarios de protección de la privacidad y del consumidor para garantizar que existan las condiciones para una competencia de privacidad efectiva y una economía inclusiva.

Metodología

Este tema de investigación inicia desde un enfoque cualitativo, tal como lo refiere Hernández (2014), "los procesos cualitativos son aquellos que se orientan a aprender de experiencias y puntos de vista de los individuos, para valorar procesos y generar teorías fundamentadas las cuales se basan en las perspectivas de aquellos que participan en dicho proceso" (p. 361).

Así también, el método comparado es el fundamento para la investigación, que de acuerdo a Morlino (2018), expresa que el primer objetivo de la comparación es muy simple, donde las realidades de varios países se investigan para comprender mejor los fenómenos involucrados (p. 21), y, por ende, para este trabajo, se realizó una comparación de las experiencias de varios países y tomar los apuntes para nuestra nación.

De igual manera se realizó una revisión y recopilación de información de fuentes documentales y de páginas web respecto a la seguridad cibernética, ciberseguridad y experiencias vividas por diferentes países en Europa, en Latinoamérica y en lo que respecta a esta área tan importante para la defensa nacional de Ecuador.

Resultados y discusión

De acuerdo a un informe emanado por la Organización de Estados Americanos - OEA (2018), señala que los países a nivel mundial, las organizaciones y los gobiernos han comenzado a desarrollar marcos (gubernamentales, internacionales, de comunidades técnicas y academia), puntos de referencia y estrategias nacionales más amplias para comprender mejor sus dependencias y vulnerabilidades de infraestructura de internet, y para asegurar las redes nacionales, las infraestructuras y los servicios de los que dependen su futuro digital y su bienestar económico, las cuales pueden ser tomadas como referencia para los países latinoamericanos.

Por ejemplo, respecto a un marco gubernamental, en Holanda, estimaron que para 2020, al menos el 25% de su producto interno bruto (PIB) estaría compuesto por la economía digital (es decir, bienes digitales y servicios electrónicos). Por otro lado, los Países Bajos han afirmado que su futuro depende de la capacidad de asegurar su economía digital, y están realizando algunas de las inversiones necesarias y reformas estructurales para lograr ese objetivo.

Otros países, como Estados Unidos y Alemania, están identificando las principales compañías que representan más del 2% del PIB del país y están trabajando con ellas para garantizar que la gestión del riesgo y la resiliencia sean parte de sus procesos generales de planificación comercial. La mayoría de los otros países, sin embargo, han adoptado un enfoque más amplio exigiendo la protección de las "infraestructuras críticas", es decir, los activos, sistemas y redes esenciales que se considera que se están volviendo vulnerables a través de una mayor interconexión y confianza en Internet, y como tal, quedan susceptibles a fallas en los equipos, errores humanos, clima y otras interrupciones causadas naturalmente, y ataques físicos y cibernético.

Establece la OEA (2018) que las organizaciones internacionales también están opinando en diversos debates a nivel mundial sobre la gestión del riesgo cibernético y están trabajando para acelerar la adopción de medidas efectivas de seguridad cibernética utilizando sus propios marcos y recomendaciones, así como también las instituciones académicas, los grupos de expertos y la comunidad técnica también han comenzado a involucrarse y han propuesto diversas metodologías para acelerar la preparación cibernética y los niveles de madurez de los países más vulnerables y las organizaciones.

Por otro lado, se presentan otras experiencias que valen la pena mencionar, como son: República Checa y España, países que se encuentran dentro de los primeros cinco lugares según el Índice Nacional de Ciberseguridad (NCSI). Por su parte la República Checa, es un país que cuenta con un avanzado desarrollo de políticas de ciberseguridad (Moncayo, 2019). La autora mencionada indica que posee una Agencia Nacional de Seguridad Informática y Cibernética (National Cyber and Information Security Agency - NCISA), que es asesorada por el Primer Ministro sobre seguridad cibernética y se encarga de mantener una buena cooperación entre República Checa y organizaciones internacionales que trabajan en el campo de la ciberseguridad; además, informa a los ciudadanos con publicaciones que realizan una vez al año donde describen y explican la situación ante amenazas cibernéticas del país.

Asimismo, Moncayo (2019), expresa que para la protección de la infraestructura crítica de su información cuentan con un proveedor de servicios digitales para que presten un servicio a la ciudadanía, mediante una gestión de la continuidad de las actividades, seguimiento, auditoría, pruebas y cumplimiento de la normativa internacional y la organización encargada de la defensa cibernética de este país es el Centro Nacional de Operaciones Cibernéticas (NCKO), cuya función es realizar operaciones militares en el ciberespacio, mientras desempeña un papel activo en el entorno internacional.

Por otro lado, España, en su desarrollo de estrategia de ciberseguridad, cuenta con un Consejo Nacional de ciberseguridad, el cual tiene una condición de Comisión Delegada del Gobierno para la Seguridad Nacional y forma parte del Departamento de Seguridad Nacional, el cual fue creado para reforzar las relaciones de colaboración, cooperación, y coordinación entre las diversas organizaciones de la administración pública con competencias en materia de ciberseguridad, así como también con los sectores públicos y privados, cuya estrategia de ciberseguridad nacional está alineada con su estrategia de seguridad nacional, que fueron planteadas en el año 2013 (Moncayo, 2019).

De esta forma, la ciberdefensa está a cargo del Mando Conjunto de Ciberdefensa (MCCD), que es catalogado como un órgano de estructura operativa y éste a su vez, está subordinado al Jefe de Estado Mayor de la Defensa y que cumple con la planeación y ejecución de todas las acciones que tengan relación a la ciberdefensa en las redes y sistemas de las TIC del Ministerio de Defensa y así encontrar una respuesta apropiada frente amenazas o agresiones que puedan poner en riesgo a la Defensa Nacional en el ciberespacio (Moncayo, 2019).

Ciberseguridad en Chile

Chile es uno de los países con mayor responsabilidad en esta área, tal como lo indica el National Cyber Security Index – NCSI, sitúa a Chile en el primer lugar en el ranking Internacional de protección de ciberseguridad en América Latina (Ciberseguridad, 2018). En este sentido, este país, cuenta con una plataforma web denominada DataChile la cual contiene la recopilación de los datos públicos chilenos. De acuerdo a Moncayo (2019), el objetivo de esta plataforma es optimizar la eficiencia y la eficacia de todas las decisiones públicas mediante la recopilación de datos.

Por otro lado, la misma autora indica que en 2017, Chile ratificó la Convención del Cibercrimen de Budapest, cuyo convenio es un instrumento internacional, conocido como el Convenio sobre la Ciberdelincuencia y es un tratado internacional vinculante en materia penal y su objetivo es el establecer herramientas legales para poder combatir aquellos delitos cometidos en contra de sistemas o medios informáticos, el cual ha sido ratificado por más de 50 naciones de todo el mundo.

Lo anteriormente mencionado, fue debido a que informaciones dadas a conocer a través de periódicos digitales de este país señalan que la ciberseguridad tuvo su auge a raíz de que el 24 de mayo de 2018 se produjo un millonario ciberataque al Banco de Chile por parte de piratas informáticos de una banda de Europa del Este o Asia, en el que sustrajeron alrededor de 10 millones de dólares de los cuales la mayoría acabó en cuentas de bancos de Hong Kong (Moncayo, 2019).

Posteriormente, detalla la autora antes mencionada que los funcionarios encargados de la investigación señalaron que se trataba de un virus de tipo SWAPQ (denominado virus del día zero ya que sus vulnerabilidades no son conocidas o reportadas hasta que descubren su funcionamiento por lo que los expertos en el tema no cuentan con actualizaciones de seguridad para su control y prevención). El objetivo constaba en despistar a los funcionarios del banco para poder realizar transacciones fraudulentas. Los funcionarios al proteger la información de sus clientes descuidaron otros aspectos de la plataforma y los atacantes lograron la sustracción del dinero (ADNradio.cl, 2018).

Luego de todo ello, el país posee unos aspectos importantes que deben tomar en consideración otros países y es la declaratoria del Mes de la Ciberseguridad, fruto de una moción presentada en el año 2018 por varios senadores, donde en el mes de octubre de cada año se realizan actividades de fomento y ejercicios nacionales relacionados con la ciberseguridad de Chile (Cámara de Diputados de Chile, 2018).

Diversos actores públicos y privados participan en la creación de herramientas para garantizar la ciberseguridad del país mediante sus entidades adscritas a los diferentes ministerios y organismos e instituciones privadas (Moncayo, 2019), a continuación, se mencionan algunos de ellos:

- Universidad de Chile:
  - Equipo de Respuesta ante Emergencias Informáticas (Computer Emergency Response Team, CERT) CL – CERT

- NIC Chile
- Comité Interministerial sobre Ciberseguridad (CICS)
- La Política Nacional de Ciberseguridad tiene como objetivos el diseño, implementación y búsqueda de alternativas para proteger la seguridad y la libertad de los usuarios en el ciberespacio.
- Ministerio del Interior y Seguridad Pública (MISP):
- Subsecretaría del Interior
- Policía de Investigaciones de Chile
- Agencia Nacional de Inteligencia
- Equipo de Respuesta ante Incidencias de Seguridad Informáticas (Computer Security Incident Response Team, CSIRT Chile)
- El Ministerio de Defensa Nacional:
- Subsecretaría de Defensa:
- Estado Mayor Conjunto y Fuerzas Armadas
- Política de Ciberdefensa esta dispone la creación de un Comando Conjunto de Ciberdefensa; creación de un Equipo de Respuestas a Incidentes Informáticos (CSIRT) de la Defensa Nacional; creación de una Oficina de Ciberdefensa y Seguridad de la Información en el Gabinete del Ministro de Defensa Nacional.
- Clave Única, el cual es un servicio de confianza y auto identificación que permite a los ciudadanos elegir una contraseña única para identificarse en todos los servicios en línea del Estado y poder realizar trámites.

Ciberseguridad en Colombia

Este fue el primer país en Latinoamérica que adoptó una "Estrategia de Ciberseguridad" (Moncayo, 2019). De acuerdo a la autora mencionada, para Colombia, la temática de ciberseguridad y ciberdefensa fue incluido por primera vez en el Plan Nacional de Desarrollo 2010-2014 denominado "Prosperidad para Todos" y que estaba incluido en el Plan Vive Digital, a través del Ministerio de Tecnologías de la Información y las Comunicaciones.

Posteriormente, el Ministerio de Defensa de la República de Colombia ha propuesto tres áreas para el mejoramiento de ciberseguridad y ciberdefensa en Colombia, a saber:

- Compromiso internacional,

- Educación, capacidades de investigación y desarrollo, y
- Doctrina (normativa)

Por lo cual considera, que éstas áreas son parte fundamental de una ciberseguridad adecuada que debe ser puesta en práctica no solo en Colombia sino en todos los países que quieran tener una adecuada ciberseguridad (Camacho, 2016).

Indica Moncayo (2019), que Colombia no es un país que ha estado exento de ataques informáticos, en donde el más conocido fue el ataque de Anonymus a los sitios web del Ministerio de Educación, el Senado, el Ministerio de Defensa, la Presidencia de la República y el sitio personal del expresidente colombiano Juan Manuel Santos (Pérez, 2014, p. 4), y por lo cual todos estas plataformas web sufrieron caídas temporales de sus sistemas, pero el sitio web del Ministerio de Defensa colombiano fue el único ataque que duró todo el día (p.47).

Más recientemente, en el 2018 Colombia fue catalogada como el país de Latinoamérica con más ataques cibernéticos de secuestro de información, utilizando el virus ransomware (Mocayo, 2019), cuyo ataque consistía en descargar un archivo PDF que suponía contener el pago de una deuda de una empresa de cobranzas; al descargar este archivo que en realidad era un link, descargaban el virus mencionado anteriormente, lo cual a sus víctimas mediante la encriptación de sus datos otorgándole un límite de tiempo para cancelar cantidades de dinero y así poder recuperar su información (Tecnósfera, 2018).

A pesar de que Colombia cuenta con varias herramientas jurídicas e institucionales para garantizar una ciberseguridad adecuada no han podido combatir a las ciberamenazas desde la raíz. Un ejemplo de ello, detalla Mocayo (2019), es el Sector Financiero, el cual se considera como uno de los sectores más sensibles de la ciberseguridad. En este sentido, la autora, muestra algunas de las organizaciones e instituciones comprometidas con la ciberseguridad en Colombia:

- Ministerio de Tecnologías de la Información y las Comunicaciones:
  - En TIC confío
  - Política de Gobierno Digital
- Ministerio de Defensa Nacional:
  - Política de Defensa y Seguridad 2019 (PDS)
- Consejo Nacional de Política Económica y Social:
  - Departamento de Planeación Nacional:

- Lineamientos de Política para Ciberseguridad y Ciberdefensa
- Política Nacional de Seguridad Digital
- Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT)
- Centro de Coordinación de Atención a Incidentes de Seguridad Informática Colombiano (CSIRT-CCIT)
- Comando Conjunto Cibernético
- Centro cibernético policial de Colombia:
- Centro Cibernético Policial Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL

Ciberseguridad en Ecuador

Especifica Mocayo (2019), que Ecuador no cuenta con una entidad encargada de llevar a cabo la ciberseguridad nacional del país. En este sentido, el Ministerio de Telecomunicaciones y Sociedad de la Información es el encargado de desarrollar planes, proyectos y programas que tengan relación a medios electrónicos, no obstante, en este momento solo se fundamenta en lo relacionado a las telecomunicaciones, debido a que no existe ningún lineamiento en el que se le indique la dirección de la ciberseguridad de la nación.

La autora relata que, en el año 2009, crearon la Secretaría Nacional de Inteligencia como ente coordinador del Sistema Nacional de Inteligencia, cuya función primordial es la coordinación de los subsistemas de inteligencia que pertenezcan a las Fuerzas Armadas y de la Policía Nacional para que se puedan realizar labores en la ejecución de contrainteligencia.

Aunque esta institución prometía mucho para una adecuada protección de la defensa nacional del Ecuador, en el año 2018, el actual presidente del Ecuador, mediante el Decreto 526, suprime la Secretaría de Inteligencia y a su vez crea el Centro de Inteligencia Estratégica (CIES), que adquiere todas las funciones que pertenecían a la Secretaría Nacional de Inteligencia (Mocayo, 2019).

Ahora bien, lo cierto es que el NCSI (2018) posiciona a Ecuador en el puesto 82, con una ciberseguridad deficiente, tal como lo indica la tabla 1. Al respecto, Ecuador sobresale en su gestión de incidentes y crisis, al contar con el Comando Cibernético del Comando Conjunto de las Fuerzas Armadas, lo que otorga una ventaja en la protección de los intereses del país, a través de estrategias de ciberdefensa. Otro aspecto en el que se hace notar es en su identificación

electrónica y servicios de confianza, con un porcentaje del 67% con la valoración, donde cada uno de los ecuatorianos cuenta con un número único (número de cédula), con el cual pueden acceder a todos los servicios que son dispuestos por el Estado.

Las carencias que saltan a la vista según el NCSI (2018), son sus indicadores generales de seguridad cibernética, debido a que no existen suficientes herramientas jurídicas e institucionales para tener una ciberseguridad adecuada, aunado a que el país no ha ratificado ningún convenio internacional en materia de ciberseguridad, por lo cual se deben tomar decisiones para mejorar en este aspecto tan importante en la actualidad, donde los ecuatorianos están más conectados a la tecnología y a la información digital en este momento por pandemia Covid-19.

Ecuador se ha visto inmerso en varios ciberataques, en diversas plataformas web públicas y privadas, sin embargo, el Ministerio de Defensa activó un protocolo de seguridad que fue utilizado para fortalecer la ciberseguridad del país, aunque no se conoce su funcionamiento; asimismo, el país ha recibido ofertas de otros países europeos para fortalecer su seguridad informática y el de sus portales web (Ortiz, 2019).

Tabla 1: 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		
Desarrollo de políticas de seguridad cibernética	0/7 (0%)	6/27 (22.22%)
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: National Ciber Security Index (2018).

Pol. Con. (Edición núm. 56) Vol. 6, No 3, marzo 2021, pp. 1251-1273, ISSN: 2550 - 682X

Posteriormente, se muestran las leyes, organismos e instituciones que respaldan la seguridad cibernética en Ecuador, a saber:

Leyes:

- 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:

- DatoSeguro

- 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)

De acuerdo a las experiencias previamente desarrolladas y mencionadas en esta investigación, permiten dar un pequeño paseo por algunos países de Europa y de América Latina, donde se pueden destacar algunas precisiones sobre aspectos para la defensa nacional en Ecuador.

Para iniciar, se detalla que en América existen vacíos en la seguridad cibernética nacional de cada país, las cuales hay que mejorar e incluir en otros. En este contexto, se debe avanzar y desarrollar un nuevo concepto de seguridad cibernética que no solo derive de los dominios militares y de defensa para las naciones, sino también desde cada uno de los ciudadanos en pro y beneficio de su seguridad y la de su país.

Ahora bien, la experiencia de los países mencionados, proporciona fundamentos para tomar apuntes necesarios para la defensa nacional adecuada ante los retos de la seguridad cibernética

presentes en nuestro país. Por lo cual, la ciberseguridad precisa creación de estrategias, normativas, organizaciones e instituciones que tomen con seriedad la seguridad nacional, haciendo el ciberespacio un lugar seguro para sus ciudadanos y para los datos gubernamentales. De esta manera, se observa con los resultados de la información recopilada, que en Europa existe un compromiso y una responsabilidad en resguardar y proteger sus datos y la de su población. Tienen claramente definidos los objetivos de protección en la temática de seguridad cibernética y sus herramientas jurídicas e institucionales, les ayudan a detectar y actuar en caso de eventualidades.

Otro aspecto a mencionar, es que diversos países están participando activamente en convenios internacionales, caso contrario el de Ecuador, que no ha ratificado ningún convenio en este aspecto de ciberseguridad, por lo que se presenta ante el mundo como un país muy vulnerable en el ciberespacio. Por tanto, Ecuador presenta indicadores muy bajos, comparándolo con otros países europeos y latinoamericanos, lo cual debe revertir en el corto y mediano plazo, ya que su protección nacional de sus recursos e instituciones puede estar en peligro o en riesgo.

Con las herramientas adecuadas, Ecuador puede mejorar en muchos aspectos su seguridad cibernética y así proteger y defender a la nación de cualquier imprevisto en esta materia, ya que cuenta con algunos elementos formales de protección en el ciberespacio; sin embargo, hay que fortalecerlos y ampliar en otros, otorgándoles un manejo adecuado y así obtener control de la ICI nacional.

De igual manera, sus ciudadanos deben estar informados de los riesgos que se presentan al utilizar el ciberespacio, sobre todo en este momento coyuntural por la pandemia, donde se utiliza mucho el internet desde diferentes dispositivos y desde lugares poco seguros, donde pueden ubicarse brechas de acceso para los ciberataques, por lo cual hay que fomentar en la población conductas de protección desde lo individual para mejorar las debilidades que puedan presentarse respecto al tema en el país.

Conclusiones

A manera de conclusión, se muestra en líneas generales los lineamientos que debe tomar en cuenta Ecuador para la defensa nacional en relación a la seguridad cibernética.

En Ecuador, es necesaria la seguridad cibernética para la protección de datos, tanto de la IC como de sus ciudadanos; asimismo, se debe ampliar las herramientas jurídicas e institucionales que sirven para garantizar la seguridad cibernética de la ICI en el país. Por otro lado, es necesario generar categorización de las IC de la nación e implementar políticas públicas en materia de seguridad cibernética, los cuales deben ser realizados y desarrollados por especialistas en el área. De la misma forma, también hay que aplicar las herramientas jurídicas e institucionales que garanticen la seguridad cibernética. Es bien conocido que, en la Constitución de la República de Ecuador, en su art. 66 numeral 19, indica que el Estado es el encargado de velar por la protección de los ciudadanos, por lo que de forma obligatoria es responsable de implementar un organismo que coordine la seguridad cibernética a nivel nacional, para la protección de la información de cada ecuatoriano y las instituciones del país, tal como lo han hecho otros países que se han reflejado en esta investigación.

Así también, Ecuador debe dar a conocer públicamente a sus ciudadanos, todo lo concerniente a la seguridad cibernética, así como también sobre las actividades o procesos que tomen en relación al tema y por último, en el país es importante establecer alianzas de cooperación internacional en materia de seguridad cibernética, así como establecer convenios y tratados para mejorar en esta temática tan amplia.

Referencias

1. ADNradio.cl. (2018). Millonario ciberataque al Banco de Chile: la mayoría del dinero robado llegó a Hong Kong. https://n9.cl/zaf69
2. Barbosa, O. (2004). Evolución de una idea: de la cibernética a la cibercultura. La filosofía griega y la cibernética. https://dialnet.unirioja.es/descarga/articulo/5679924.pdf
3. Barrera, S. (2020). La mejor ciberseguridad es la prevención. https://n9.cl/4fr9
4. Camacho, J. (2016). Evolución de la ciberdefensa y la seguridad de la información en Colombia. Bogotá: Universidad Militar Nueva Granada. https://n9.cl/rn4u8
5. Cámara de Diputados de Chile. (2018). Sala aprobó proyecto que declara octubre como el Mes Nacional de la Ciberseguridad. https://n9.cl/wy1n1
6. Centro de Ciberseguridad Industrial. (2013). La Protección de Infraestructuras Críticas y la Ciberseguridad Industrial. https://www.cci-es.org/

7. Ciberseguridad (2018). Chile sube al primer lugar de América latina en ranking Ciberseguridad: internacional de ciberseguridad. https://n9.cl/9q9vq
8. Comisión Económica para América Latina y el Caribe - CEPAL. (2020). La seguridad cibernética en América Latina y el Caribe: un esfuerzo multiateral. https://n9.cl/0isue
9. Comnimos, A. (2013) Una agenda de ciberseguridad para la sociedad civil: ¿qué hay en juego? En: Temas Emergentes. APC. Disponible en: https://n9.cl/t4bwi
10. Consejo Argentino para las Relaciones Internacionales – CARI. (2013). Ciberdefensa-Ciberseguridad Riesgos y Amenazas. https://n9.cl/6n5f1
11. Constitución de la República del Ecuador. (2008). Quito, Pichincha, Ecuador: Registro Oficial 449.
12. Eissa, S., Gastaldi, S., Poczynok, I. y Zacarías, M. (2012). El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino. VI Congreso de relaciones internacionales. https://n9.cl/trzqw
13. Gobierno Estados Unidos - Campaña nacional de servicio público Ready (2021). Seguridad cibernética. https://www.ready.gov/es/ataque-cibernetico
14. Hernández Sampieri, R. (2014). Metodología de la Investigación. México: Mcgraw- Hill / Interamericana Editores, S.A.
15. Joyanes, L. (2010). Introducción. Estado del arte de la ciberseguridad. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. https://n9.cl/z668
16. Koch, S. (2015). La libertad en el ciberespacio: Ciberseguridad y el principio del daño.
17. López, C. (2018). Diferencia entre seguridad informática y ciberseguridad. http://polux.unipiloto.edu.co:8080/00004637.pdf
18. MERIDIAN. (2016). Guía de buenas prácticas de GFCE-MERIDIAN sobreprotección de infraestructuras críticas de la información para responsables de políticas gubernamentales. https://n9.cl/h4xz
19. Moncayo, P. (2019). Herramientas jurídicas para garantizar la ciberseguridad del Estado. Análisis comparado de Colombia, Chile y Ecuador. https://n9.cl/i1ye
20. Morlino, L. (2018). Comparison. A Methodological Introduction for the Social Sciences. Toronto: by Barbara Budrich Publishers, Opladen, Berlin & Toronto.
21. Motorola Solutions, Inc. (2015). Documento Técnico. Seguridad Cibernética: Manejando El Reto y La Complejidad. https://n9.cl/amden

22. Organización de Estados Americanos – OEA. (2013). Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos. https://n9.cl/hetlk
23. Organización de Estados Americanos – OEA. (2018). Gestión Del Riesgo Cibernético Nacional. https://www.oas.org/es/sms/cicte/espcyberrisk.pdf
24. Ortiz, S. (2019). Telecomunicaciones denuncia ciberataques tras la salida de Assange. El Comercio. https://n9.cl/scff
25. Passman, P. (2020). Seguridad Cibernética al alcance de Pequeñas y Medianas Empresas. https://n9.cl/3tenx
26. Pérez, Y. (2014). Importancia de la ciberseguridad en Colombia. https://n9.cl/ifp7w
27. Preciado, P. (2021). La seguridad cibernética. Lo que el 2021 podría traer para la seguridad cibernética. https://n9.cl/0l1bo
28. Rayón, M. y Gómez, J. (2014). Cibercrimen: particularidades en suinvestigación y enjuiciamiento. https://n9.cl/y7ha8
29. Red local de Puerto Rico Colmena66 (2021). Seguridad Cibernética. https://n9.cl/kuom
30. Sánchez, M. (2019). La ciberseguridad y la ciberdefensa, la necesidad de generar estrategias de investigación sobre las temáticas que afectan la seguridad y defensa del Estado. https://n9.cl/z668
31. Siles, I. (2007). Cibernética y sociedad de la información: el retorno de un sueño eterno. https://n9.cl/qtxg
32. Tecnósfera. (2018). Colombia es el país más atacado por ciberextorsión en Latinoamérica. El Tiempo. https://n9.cl/rentk
33. Valdéz, A. (2019). Introducción a la ciberseguridad. https://n9.cl/04o8
34. Wiener, N. (1948). Cybernetics, or control and communication in the animal and the machine. París: Hermann Editions; Cambridge: MIT Press; New York: Wiley & Sons.
35. Wiener, N. (1951) The human use of human being: cybernetics and society. London: Free Association Books.