Universidad Andina Simón Bolívar

Sede Ecuador

Área de Estudios Sociales y Globales

Maestría Profesional en Relaciones Internacionales

Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento

Respuestas del Estado ecuatoriano en el período 2013-2022

María Dolores Santos Vidal

Tutor: César Montúfar Mancheno

Quito, 2022

Cláusula de cesión de derecho de publicación de tesis

Yo, María Dolores Santos, autora de la tesis intitulada “Marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento. Respuestas del Estado ecuatoriano en el período 2013-2022”, mediante el presente documento dejo constancia de que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno de los requisitos previos para la obtención del título de Magíster Profesional en Relaciones Internacionales en la Universidad Andina Simón Bolívar, Sede Ecuador.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Ecuador, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, durante 36 meses a partir de mi graduación, pudiendo, por lo tanto, la Universidad utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en formato virtual, electrónico, digital u óptico, como usos en red local y en internet.
2. Declaro que en caso de presentarse cualquier reclamación de parte de terceros respecto de los derechos de autor/a de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y a la Universidad.
3. En esta fecha entrego a la Secretaría General, el ejemplar respectivo y sus anexos en formato impreso y digital o electrónico.

12 de enero de 2023

Firma:_____

Resumen

Los avances que han realizado varios países en materia legislativa con relación a la ciberseguridad y ciberdefensa facilitarían la gobernanza del ciberespacio; así como las regulaciones de la Unión Europea, y la legislación que regula la participación del sector privado en el mismo, el interés de los legisladores en desarrollar controles eficientes para la ciberseguridad y ciberdefensa y la delimitación y regulación del sector militar. Esta investigación tiene como objetivo fundamental determinar qué instrumentos estratégicos de la ciberseguridad y ciberdefensa: políticas, legislación e instituciones se han generado en Ecuador para enfrentar las amenazas cibernéticas en el campo de la seguridad y defensa. Esto por medio de la identificación de su origen, escenarios, actores estatales y paraestatales, el marco regulatorio supranacional en seguridad cibernética, políticas y estrategias internacionales, en América Latina y en Ecuador; así como retos y desafíos en la ciberdiplomacia para fomentar el uso pacífico de las tecnologías y de la comunicación, los debates de las ciberamenazas y sus proyecciones. También, evidencia cuál es el rol del Estado frente a la incidencia de las nuevas amenazas y el control del ciberespacio. La conclusión general muestra el deber que Ecuador tiene para contrarrestar las ciberamenazas, ciberataques, salvaguardar la infraestructura crítica digital, los servicios esenciales del Estado, la infraestructura crítica digital de defensa, protección de datos personales; así como la protección de derechos en el ciberespacio.

Palabras clave: inteligencia artificial, estrategia, política pública, ciberespacio, ciberdiplomacia

Al Ser Supremo Dios, nuestro creador. A mi querido esposo, fuente de inspiración, a mis padres, hermanos.

A mi querida Universidad, por permitirme alcanzar mis sueños, plasmados en esta investigación.

A mis familiares y amigos, que de una u otra manera contribuyeron a la consecución de este grado académico.

A Elenita, compañera de batallas y amiga incondicional, que siempre me ha impulsado, mil gracias por tenderme tu mano.

Finalmente, a Chucho y Milki, por ser mi compañía en las perseverantes jornadas de estudio y trabajo al compartir su amor leal.

Agradecimientos

A la Universidad Andina Simón Bolívar, Sede Ecuador, por la confianza puesta en mí puesta como estudiante para el desarrollo de este proceso investigativo y de aprendizaje de vanguardia.

Al doctor César Montúfar, quien me ha brindado su apoyo y guía, motivándome a lograr mi objetivo: culminar la presente investigación.

Tabla de contenidos

Figuras y tablas

Introducción

Nunca se pensó en que los inventos y adelantos científicos del siglo diecinueve pudiesen ser el tema de discusión geopolítica luego de un par de décadas. Esto, por la utilización del ciberespacio. Más aún hoy en día que el uso de las Tecnologías de la Información y de la Comunicación son la base de la vida cotidiana de todos los Estados, en los que se involucran nuevos actores en escenarios multidimensionales complejos, donde existen facilidades inimaginables para el intercambio de información y comunicación, pero, al mismo tiempo, conlleva serios riesgos, incertidumbre y caos, que pueden afectar a la seguridad de las personas, de las instituciones y del Estado (Leiva 2015, 161–75).

A través del avance acelerado de las tecnologías de la información versus el relacionamiento con las personas, se supondría la existencia de sociedades del conocimiento completamente desarrolladas, con dos fines totalmente definidos, tal como lo menciona la Unesco, la información para todos y la libertad de expresión:

> El auge de las nuevas tecnologías de la información y la comunicación ha creado nuevas condiciones para la aparición de sociedades del conocimiento. La *sociedad mundial de la información* en gestación sólo cobrará su verdadero sentido si se convierte en un medio al servicio de un fin más elevado y deseable: la construcción a nivel mundial de *sociedades del conocimiento* que sean fuentes de desarrollo para todos, y sobre todo para los países menos adelantados. Para lograrlo, dos desafíos planteados por la revolución de la información revisten una importancia particular: el acceso a la información para todos y el futuro de la libertad de expresión. (Bindé 2005, 29; énfasis en el original)

Bajo este razonamiento, las sociedades de la información y el conocimiento, constituidas como una innovación de la información y las comunicaciones, no hubiesen sido el sueño de Alexander Graham Bell. Él perfeccionó y dio a conocer su invento sin considerar cómo sería su evolución, que a partir de un electroimán surgiría uno de los inventos más revolucionarios de la historia, tal como lo refiere:

> *The Telegraphic Journal*, de Londres, el 1 de junio de 1876. [...] …de un electroimán en un extremo de un único alambre se oyen salir los sonidos de la voz humana —tonos y palabras hablados o cantados delante de una membrana conectada con un electroimán en el otro extremo del alambre. (Sánchez Miñana y Sánchez Ruiz 2011, 36)

El propósito de comunicarse de un punto a otro solamente con un sistema de voz se transformó en lo que hoy es la 5ta generación de la telefonía móvil. Esta permite tener

la interrelación entre personas y dispositivos conectados en cualquier lugar del mundo y en cualquier momento, que a decir de los investigadores de la Universidad Internacional de Valencia sus alcances se evidenciarán a través de las aplicaciones comerciales, cuyo objetivo transformará el mundo real a una zona *WiFi*. Para lo cual la red 5G tendrá las siguientes características:

> Dirección IP para móviles asignada de acuerdo con la red conectada y la posición geográfica. Señal de radio también a mayor altitud. Múltiples servicios paralelos, con los que se puede saber el tiempo meteorológico y en la posición geográfica mientras hablas. La educación será más fácil. Un estudiante que se sienta en cualquier parte del mundo puede asistir a la clase. El diagnóstico remoto es una gran característica de 5G. Un Médico puede tratar al paciente situado en la parte remota del mundo. El seguimiento será más fácil, una organización gubernamental y otros investigadores pueden monitorear cualquier parte del mundo. Se hace posible reducir la tasa de criminalidad. La visualización del universo, galaxias y planetas serán posibles. Posible también detectar más rápidamente desastres naturales incluyendo tsunamis, terremotos, etc. (Universidad Internacional de Valencia 2018, párr. 12)

De este modo, los Estados y sus ciudadanos hoy cuentan con una poderosa herramienta que permite que la comunicación, la información y el conocimiento se encuentren al alcance de sus manos, producto de la evolución y desarrollo tecnológico. Cabe resaltar que la interrelación persona-dispositivo electrónico requiere de un medio importantísimo que es el internet, el cual permite la interconexión descentralizada de computadoras, además posibilita el poder compartir información por medio de páginas, sitios u otros tipos de software. *Esto significa que este mundo virtual se desarrolla en el ciberespacio, un territorio digital, en donde los Estados ejercen soberanía en la parte del ciberterritorio que le corresponde.*

De hecho, no solamente los Estados son los actores que tienen el control y dominio del ciberespacio, hoy en día los delincuentes cibernéticos luchan por la supremacía tecnológica y global, generándose una serie de amenazas y ataques cibernéticos que buscan robar y destruir información, anular el funcionamiento de los sistemas, entre otros. Es decir, se ha desencadenado una ciberguerra para identificar vulnerabilidades técnicas en equipos o redes informáticas enemigas para poder infiltrarlas y atacarlas, así como revelar información y datos confidenciales (Sain 2016, 1).

Ante estas amenazas surge la necesidad de los Estados de implementar estrategias nacionales e internacionales con el fin de mantener el control y dominio del ciberespacio, ejemplo de lo mencionado es la Estrategia Europea de Seguridad y Defensa, la misma que se plasma en la resolución del Parlamento Europeo y plantea dentro de sus

consideraciones generales e intereses europeos “la seguridad de su vecindad y la protección de sus fronteras exteriores y de infraestructuras críticas, así como la mejora de su ciberseguridad” (Parlamento Europeo 2009, 63).

Así mismo, los efectos de los ataques cibernéticos son causales para la adopción de medidas y acuerdos de índole multilateral, tal como se lo propuso en la Unión Europea (UE) en el año 2009, en la resolución aprobada en la Cumbre de Lisboa y en la que se plasmó el “Concepto Estratégico de la OTAN” (Arteaga 2010, 1), donde se concibe a los ataques cibernéticos como uno de los principales riesgos a nivel mundial.

Frente a esta problemática mundial, Ecuador no podía estar exento de sufrir vulneraciones a sus sistemas por lo que a través de la Secretaría Nacional de la Administración Pública (SNAP), con el Ministerio de Telecomunicaciones y de la Sociedad de la Información y la Secretaría Nacional de Inteligencia (SENAIN), conformaron en el *2011 una Comisión para la Seguridad Informática*, cuya atribución fue “establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional” (EC Secretaría Nacional de la Administración Pública 2013a, 1), estableciendo que el Esquema Gubernamental de Seguridad de la Información tendría un horizonte para su implementación en 2015 en todas las instituciones públicas.

De las evidencias anteriores surge la importancia de la presente investigación, tomando en consideración el avance acelerado de los medios tecnológicos, escenarios presentes y futuros, riesgos y amenazas a la seguridad de la información y a los recursos estratégicos de los Estados y sus habitantes, así como la implementación de políticas públicas estatales para enfrentar estas dificultades en pos de construir una sociedad propositiva, donde se permita evidenciar un manejo responsable y seguro de la información, en un entorno de libertad de expresión y respeto a los Estados y a sus habitantes. Las ideas y reflexiones propuestas en esta investigación se plasman en los siguientes capítulos:

Capítulo I: La ciberseguridad en el contexto mundial. Marco regulatorio, aquí se realiza un breve análisis de cómo se concibe a la ciberseguridad en el contexto mundial, partiendo del origen, los escenarios y actores. Del mismo modo, se pone en evidencia el marco regulatorio supranacional en seguridad cibernética, las políticas y estrategias internacionales que gobiernan dentro de la administración del ciberespacio. En

consecuencia, se tendrá una visión externa de las realidades del Estado ecuatoriano que permitirán determinar cómo se trató este tema en particular.

Capítulo II: Respuestas del Estado ecuatoriano en el período 2013-2022. Se inicia con el marco regulatorio en seguridad cibernética en América Latina, hasta llegar al marco legal y regulatorio de la ciberseguridad y ciberdefensa en Ecuador. Además, se presentan los retos y desafíos en la ciberdiplomacia para fomentar el uso pacífico de las Tecnologías de la Información y de la Comunicación. Estos elementos se suman a los debates de las ciberamenazas y sus proyecciones.

Finalmente se establece las conclusiones, que son el resultado de la presente investigación y se anexan algunos escenarios de amenazas de seguridad cibernética en Ecuador

Planteamiento del problema

El mundo está sumido en una guerra no convencional que se libra en el ciberespacio, donde existen caídas en los sistemas informáticos de los gobiernos e instituciones, con una rapidez impresionante. Adicionalmente hay una acelerada cantidad de información manipulada en tiempo real a través de las redes sociales, que ha influido incluso, por ejemplo, en las elecciones de los EE. UU. de 2016 por parte de Rusia (Giannetti 2017, 1–8). Otro ejemplo son las noticias falsas, que han llegado a desestabilizar la toma de decisiones estratégicas a nivel mundial (Becerril et al. 2018, 6–7).

Frente a estas nuevas amenazas, los estados han desarrollado una gran cantidad de estrategias. Todas ellas buscan mantener un adecuado sistema de seguridad y defensa informáticas, con el fin de combatir al crimen organizado viralizado en la red, que afecta directamente a las personas y estados, que violan sus derechos y su privacidad y que ejercen acoso mediante el robo de información en una escala que traspasa la frontera estratégica y territorial (Moncayo Gallegos 2016, 108–9, 113, 202, 224).

En este contexto, varios estados han definido políticas intersectoriales de seguridad informática para limitar el accionar de las amenazas propagadas por las redes digitales, sean estas directamente vinculadas al internet o la intranet. En la búsqueda de lo que se ha llamado “ciberseguridad” intervienen muchos actores como el Estado, los ciberdelincuentes, grupos terroristas, cibervándalos, hacktivistas, actores internos, ciberinvestigadores y organizaciones privadas. De acuerdo con su nivel de peligrosidad, se establecen estrategias estatales para enfrentar las amenazas y minimizar su incidencia en el contexto nacional y regional (Villalba Fernández 2015, 50–60, 387).

Esta investigación describe las estrategias adoptadas por los estados de América Latina, con énfasis en Ecuador, frente a la acelerada proliferación de amenazas globales que usan al ciberespacio como una autopista para la consecución de sus objetivos en el marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento.

Pregunta de investigación

Frente al surgimiento de las nuevas amenazas cibernéticas y su incidencia en la seguridad de las personas y los estados, ¿qué marco regulatorio de la ciberseguridad y ciberdefensa se implementó en Ecuador en el período 2013-2022 que neutralice las amenazas en el ciberespacio?

Objetivos específicos

- Identificar el origen, los principales escenarios y actores de las amenazas que se configuran en el ciberespacio, y que constituyen la base para la generación de políticas, estrategias, regulaciones y legislación de ciberseguridad que se han desarrollado a nivel internacional.
- Determinar qué instrumentos estratégicos de la ciberseguridad y ciberdefensa: marco regulatorio, políticas, legislación e instituciones se han generado en Ecuador para enfrentar las amenazas cibernéticas en el campo de la Seguridad y Defensa.

Justificación de la investigación e importancia académica y social

Esta investigación busca evidenciar cuál es el rol del Estado frente a la incidencia de las nuevas amenazas y el control del ciberespacio. En relación con ello, existen estrategias definidas por líderes políticos y autoridades institucionales, que no escatiman recursos para presentar soluciones inmediatas para frenar el uso indiscriminado e ilegal del ciberespacio. Hay que considerar también que, actualmente el rumbo que han tomado los Estados, en materia de ciberseguridad, se encuentra asociado a la velocidad en la que mutan las amenazas y los escenarios multidimensionales en que estos se desarrollan.

Las disputas en torno al ciberespacio influyen en las relaciones de poder entre los estados, modificando el criterio de territorialidad que históricamente tenía una gran relevancia, y en la que se podía identificar de cierta manera al enemigo (Moncayo Gallegos 2016, 81, 220, 242).

Acopio y procesamiento de información

Dentro del análisis de la presente investigación, el enfoque propuesto permitirá de manera inductiva contrastar la información y contenidos que se articulan a la importancia

del ciberespacio en la seguridad y defensa de los Estados como un problema que pasa por encima de las fronteras nacionales.

En el caso particular ecuatoriano, por tratarse de temas que expresamente pueden influir en la seguridad y defensa nacional, exclusivamente serán expuestos los que puedan ser manejados con un rigor académico, evitando mantener un sesgo ideológico que afecte a la investigación y a los objetivos establecidos anteriormente. Sin embargo, se puede indicar que este trabajo es una investigación sobre políticas, estrategias, regulaciones y legislaciones institucionales para enfrentar los nuevos desafíos de la ciberseguridad y ciberdefensa, la metodología desarrollada fue la cualitativa a través de la recopilación de diferente bibliografía.

Capítulo primero
La ciberseguridad en el contexto mundial. Marco regulatorio

Esta investigación titulada marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento. Respuestas del Estado ecuatoriano en el período 2013-2022, tiene como pregunta de investigación: *¿qué marco regulatorio de la ciberseguridad y ciberdefensa se implementó en Ecuador en el período 2013-2022 que neutralice las amenazas en el ciberespacio?* En ese marco, este capítulo, la ciberseguridad en el contexto mundial desarrolla la investigación del origen, escenarios, actores y el marco regulatorio supranacional en seguridad cibernética, políticas, estrategias internacionales, con el que se alcanza el primero objetivo:

Identificar el origen, los principales escenarios y actores de las amenazas que se configuran en el ciberespacio, y que constituyen la base para la generación de políticas, estrategias, regulaciones y legislación de ciberseguridad que se han desarrollado a nivel internacional.

1. Origen

Para realizar una aproximación a la investigación es imperativo ver a la ciberseguridad desde el punto de vista epistemológico, más aún cuando esta se desarrolla en base al conocimiento científico del ser humano desde su concepción o desde el inicio de su existencia. Las distintas corrientes epistemológicas del conocimiento han versado esencialmente sobre la posibilidad de representación del conocimiento humano, de hecho, el surgimiento de la nueva era de la información de la sociedad y el conocimiento transporta al nacimiento de los sistemas de información basados en la inteligencia artificial, la misma que se encuentra en pleno auge sin conocer hacia donde conducirá, especialmente en el uso o aprovechamiento de este medio en el dominio del ciberespacio.

La relación existente entre persona y conocimiento, desde el punto de vista de los especialistas, puede tener diferentes grados, ya que esta puede ser percibida desde el pensamiento racional o desde el sencillo razonamiento. Sin embargo, lo más importante radica en que el conocimiento sea desde el criterio racionalista, empirista o de la epistemología contemporánea. Sobre la base racionalista de René Descartes, ligado al pensamiento matemático, desde su percepción mente racional y cuerpo mecánico. La

mente trae consigo el conocimiento certero desde que el hombre nace. Desde el empirismo de John Locke, opuesta al racionalismo, se destaca el conocimiento verdadero desde los datos de los sentidos y la experiencia, pues destaca que el conocimiento se lo adquiere posterior al nacimiento (Rendueles Mata y Dreher Grosch 2007).

No obstante, un criterio que abarca las dos percepciones racionalistas y empiristas descritas por Kant a partir de su obra "Crítica de la razón pura", explica cómo es posible el conocimiento científico de la aritmética, la geometría, la física newtoniana y la lógica tradicional. Entrelazada en concepto de lo sintético, lo analítico lo a priori y lo a posteriori (Kant 2012). Una vez en el siglo veinte, en el problema del conocimiento científico se gestaron nuevas corrientes epistemológicas, tales como: el empirismo criticismo alemán y el empirismo lógico, replanteándose ideas y conceptos fundamentales desde la perspectiva de Noam Chomsky y de Jean Piaget. El primero en base a la lingüística y el otro desde la epistemología genética.

Punto aparte merece el cognoscitivismo propuesto por Jerry Fodor, donde inicia el planteamiento de los desarrollos de la inteligencia artificial a más de la inteligencia natural (Giraldo Montoya 2004). Desde la lógica epistemológica tomada como referencia, es mucho más fácil comprender el rol del ser humano dentro del desarrollo de la información, desarrollo conceptualizado en el año 1968 por Marshall McLuhan[1] como "Aldea Global" (greisbaris 2016, párr. 1).

En este sentido, van tomando una singular importancia los sistemas de información y la sociedad del conocimiento a la cual se ha llegado de manera acelerada, y mucho más con estas expresiones de la creciente interconectividad humana a escala global. Generada por los sistemas de información para ser aprovechadas en la comunicación y el aprendizaje. De aquí la importancia que se le atribuye al espacio donde se van a ejecutar todas las interacciones e interrelaciones necesarias para obtener un fin deseado. Empleando la técnica y el método que cada organización lo crea conveniente, a partir del siguiente criterio:

> El espacio está formado por un conjunto indisoluble, solidario y también contradictorio, de sistemas de objetos y sistemas de acciones, no considerados aisladamente, sino como el contexto único en el que se realiza la historia. Al principio la naturaleza era salvaje, formada por objetos naturales, pero a lo largo de la historia van siendo sustituidos por objetos fabricados, objetos técnicos, mecanizados y, después, cibernéticos, haciendo que

[1] Filósofo canadiense que utilizó el término "Aldea Global" "como expresión de la exponencialmente creciente de interconectividad humana a escala global generada por los medios electrónicos de comunicación" (greisbaris 2016, párr. 1).

> la naturaleza artificial tienda a funcionar como una máquina. A través de la presencia de esos objetos técnicos: centrales hidroeléctricas, fábricas, haciendas modernas, puertos, carreteras, ferrocarriles, ciudades, el espacio se ve marcado por esos agregados, que le dan un contenido extremadamente técnico. (Santos 2000, 54)

Los requerimientos y necesidades de comunicación del ser humano permitieron interactuar una gran cantidad de datos a través de la velocidad de las comunicaciones con las máquinas. Dejando a un lado medios de almacenamiento no confiables y de muy bajo nivel. Es así como a mediados del siglo veinte surge la computadora como la mayor recolectora y procesadora de información. Permitiendo de este modo a toda la sociedad humana transformarse, convirtiendo su estilo de vida similar a la de una aldea.

El progreso y desarrollo de la ciencia y tecnología, como consecuencia del surgimiento de la computadora, ha hecho posible la implementación de procesos informáticos y tecnológicos insospechables que se encuentran al alcance de todos los habitantes del planeta. Puesto que la comunicación hoy en día es efectiva, de persona a persona, de manera instantánea y directa. Los avances significativos de la radio, la televisión, telefonía celular y satelital contribuyen en el mantenimiento de vínculos estrechos en el campo económico, político y social. Donde se hizo evidente la necesidad de mejorar las técnicas de procesamiento de datos, información y comunicación, siendo la solución más eficiente el acceso a una red global que hoy en día parece no tener límites dentro del dominio espacial, el internet.

Internet, concebida como una de las primeras descripciones registradas de las interacciones sociales escritas por J.C.R. Licklider (1962) donde lo describe como "red galáctica".[2] Una de las características del mundo actual es la velocidad de las cosas, anclada a la necesidad y exigencia de fluidez de la circulación de datos, mensajes, ideas, productos, servicios, recursos y capitales que interesan a las personas y a grupos hegemónicos (Leiner et al. 1997).

No obstante, estas necesidades requieren de técnicas aún más eficaces que le permitan obtener una mayor fluidez, tanto en la información como en el flujo de recursos, siendo al mismo tiempo una causa, una condición y un resultado. En este sentido se acerca al concepto de ciberespacio, que a decir de (Casarin et al. 2018) es un constructo social,

[2] J.C.R Licklider, describe Red galáctica: "Imaginó un conjunto de ordenadores interconectados globalmente, a través de los que todo el mundo podría acceder rápidamente datos y programas desde cualquier sitio. En espíritu, el concepto era muy similar a la Internet de hoy en día" (Leiner et al. 1997, párr. 5).

como sociedad red, como ámbito de los flujos y de los lugares. Siendo de manera particular el quinto dominio luego del terrestre, naval, aéreo y el espacio ulterior.

Dentro de estos dominios se han extrapolado objetos y lugares destinados a contribuir a la fluidez de las cosas. Tal es el caso de la construcción de autopistas, aeropuertos, oleoductos, gaseoductos, edificios inteligentes, ciudades inteligentes, donde existe la necesidad y requerimientos de la información al más alto nivel, para su óptimo funcionamiento. De la cual se espera la administración responsable como paradigma en un mundo globalizado. En efecto, para mantener el control de estos dominios anteriormente citados, los Estados han realizado varias acciones con el fin de controlar el acceso a las redes de información, así como a sus sistemas informáticos, desprendiéndose en este caso, el criterio de ciberseguridad.

De este modo, Rusia y los Estados Unidos de América (EE. UU.) con el fin de impulsar una taxonomía útil que beneficie a la humanidad, a la paz y a la estabilidad. Forman una asociación bilateral de trabajo, por cuanto ambos países son respetados por su competencia en el campo de las tensiones nucleares, la era moderna y los intereses en el control y dominio del espacio. Conceptualmente este término fue introducido a principios de 2011, por parte de este grupo bilateral de trabajo del *East West Institute* (EWI) y la Universidad de Moscú, quienes elaboraron un marco referencial de terminología internacional (Anchundia Betancourt 2017). "***Cybersecurity**: is a property of **cyber space** that is an ability to resist intentional and unintentional threats and respond and recover*" (Rauscher y Yaschenko 2011, 31; énfasis en el original; énfasis añadido).

Esta definición es citada por varios autores dentro de las estrategias nacionales de ciberseguridad como "una propiedad del ciberespacio, que tiene la capacidad de resistir las amenazas intencionales y no intencionales, responder y recuperarse" [Rauscher y Yashenko, 2011]. (Leiva 2015, 162).

Atendiendo a estas consideraciones, es muy importante mencionar los debates académicos establecidos en los últimos años en torno a la ciberseguridad, ya que los estados han incorporado dentro de sus agendas de Seguridad y Defensa, a la ciberseguridad como un objeto de estudio y análisis dentro del bilateralismo y multilateralismo regional. "Ciberseguridad o también denominada seguridad informática: es el área que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente, la información contenida o circulante" (Duarte 2018, párr. 3).

> 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 pueden efectuarse en forma más rápida y económica en comparación con otras formas conocidas de intercambio de información. (Sancho Hirare 2017, 8)

> la ciberseguridad y ciberdefensa han evolucionado de ser temas netamente técnicos, para convertirse en una capacidad estratégica clave en la conducción de un Estado dentro de los diversos niveles de decisión o niveles internacionales cuando se habla de proyectos de ciberseguridad regional (Samper 2015). […] en Ecuador […] se evidencia la necesidad de implementar esta capacidad estratégica, lo que se convierte en la oportunidad de establecer un modelo local y propio de gobernanza para la seguridad y defensa en el ciberespacio. (Vargas Borbúa, Recalde Herrera, y Reyes Chicango 2017, 35–36)

Information Systems Audit and Control Association (ISACA) también da una definición de Ciberseguridad. "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (Corletti Estrada 2017, 28).

> la importancia de la Seguridad en el ciberespacio y asumir su complejidad, pues las amenazas en el ciberespacio pueden tener diversos orígenes (estatal o no estatal), pero el mismo efecto de perjudicar a las personas, dañar a las organizaciones e impedir el normal funcionamiento de instituciones. (Sancho Hirare 2017, 11)

> **La ciberseguridad** ha adquirido una relevancia cada vez mayor en las agendas de los gobiernos y los actores privados, pasando de ser un tema de exclusiva incumbencia de los técnicos del área de la informática, a un foco de política pública en donde intervienen académicos, empresas, periodistas, políticos y miembros de la sociedad civil. (Viollier 2017, 5; énfasis en el original)

Dentro de esta lógica del origen de la ciberseguridad y ciberdefensa es necesario establecer algunos conceptos fundamentales del ambiente en la que esta se desarrolla y que contribuyen al tema de investigación, por tanto, se presentan algunos de los principales conceptos usados:

Ciberseguridad

> La ciberseguridad es 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 ciberentorno. (Actualidades de la UIT 2010, 20)

Ciberamenaza

"Las ciberamenazas son amenazas planteadas por medio de Internet o el ciberespacio" (Mogollón Flores 2017, 66).

Cibercrimen

"son los actos delictuales donde el ciberespacio es el objeto del delito o su principal herramienta para cometer ilícitos contra individuos, organizaciones, empresas o gobiernos" (CL Ministerio del Interior y Seguridad Pública y CL Ministerio de Defensa Nacional 2015, 14).

Ciberdefensa

> se orienta a las acciones de un Estado para proteger y controlar las amenazas, peligros o riesgos de naturaleza cibernética, con el fin de permitir el uso del ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía y la integridad territorial; (Vargas Borbúa, Recalde Herrera, y Reyes Chicango 2017, 35)

Seguridad multidimensional

> El fundamento y razón de ser de la seguridad es la protección de la persona humana […] Las condiciones de la seguridad humana mejoran mediante el pleno respeto de la dignidad, los derechos humanos y las libertades fundamentales de las personas, así como mediante la promoción del desarrollo económico y social, la inclusión social, la educación y la lucha contra la pobreza, las enfermedades y el hambre…el concepto y los enfoques tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales…. (Stein 2009, 31)

Seguridad cibernética

> Con el surgimiento de Internet y la extensión de su uso a nivel masivo en la región durante la última década, surgieron nuevas amenazas y formas de cometer delitos. Con el fin de apoyar a los Estados Miembros en su lucha contra el crimen cibernético, la Organización, a través del Comité Interamericano contra el Terrorismo (CICTE) y del Programa de Seguridad Cibernética, está trabajando en el desarrollo de una agenda sobre seguridad cibernética en las Américas. En cooperación con una amplia gama de entidades nacionales y regionales de los sectores público y privado, tanto en asuntos políticos como técnicos, la OEA fomenta y fortalece las capacidades de seguridad cibernética entre los Estados Miembros a través de asistencia técnica y capacitación, mesas redondas sobre política, ejercicios de gestión de crisis e intercambio de mejores prácticas para el uso de tecnologías de la información y la comunicación. (Organización de los Estados Americanos 2022, párr. 1)

Políticas de ciberseguridad

una política de ciberseguridad es necesaria por las siguientes razones: 1. Resguardar la seguridad de las personas en el ciberespacio. […] 2. Proteger la seguridad del país. […] 3. Promover la colaboración y coordinación entre instituciones. […] 4. Gestionar los riesgos del ciberespacio. […]. (CL Ministerio del Interior y Seguridad Pública y CL Ministerio de Defensa Nacional 2015, 10)

Amenaza:

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad. (ES Instituto Nacional de Ciberseguridad 2021, 14)

Amenaza avanzada persistente (APT):

También conocido como APT, acrónimo en inglés de *Advanced Persistent Threat*, consiste en un tipo de ataque informático que se caracteriza por realizarse con sigilo, permaneciendo activo y oculto durante mucho tiempo, utilizando diferentes formas de ataque. Suelen estar patrocinados por compañías, mafias o un estado. El objetivo principal es vigilar, exfiltrar datos o modificar los recursos de una empresa u organización de forma integrada y continuada en el tiempo. Generalmente, este tipo de *malware* hace uso de *exploits* o ejecutables, aprovechando vulnerabilidades de tipo *Zero Day* presentes en el *software* de la víctima. (ES Instituto Nacional de Ciberseguridad 2021, 14; énfasis en el original)

Infraestructura crítica:

Activos de carácter esencial e indispensable cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales (ES Instituto Nacional de Ciberseguridad 2021, 51).

Una vez establecida la base epistemológica de la ciberseguridad, se adentra en los escenarios en los que se interrelacionan actores, riesgos y amenazas en el contexto global y regional.

2. Escenarios

Las capacidades técnicas y estratégicas de ciberseguridad y ciberdefensa como respuesta nacional de un estado, y el principal riesgo para el ciberespacio, el Internet. Por lo que no es suficiente el uso legítimo en la centralización de casi total la tecnología en las instituciones estatales. El propio estado se limita aún más al control, por lo que es

fundamental mantener cooperación y colaboración público–privado para enfrentar las amenazas. Una vez establecidas las bases epistemológicas de la ciberseguridad, profundizamos en escenarios donde actores, riesgos y amenazas se interconectan en contextos globales y regionales. En esta sección se describe algunos escenarios ocurridos a nivel global y regional.

2.1. Global

Una filtración de documentos arrancó en el año 2006, a través el sitio *web Wikileaks*, en donde se publican informes y documentos de carácter confidencial en materias sensibles de índole militar, política, religiosa o social. Sus revelaciones han conseguido un gran impacto en la prensa escrita especializada, en televisión y foros de Internet, hasta llegar al gran público. Este sitio *web* ha recibido prestigiosos premios, en 2008, al Medio de Comunicación del Año por la revista *The Economist* y en 2009, el portal y su fundador, Julian Assange, ganaron el premio de Amnistía Internacional en la categoría de Nuevos Medios (Carrasco 2010).

En abril 2007, la decisión del gobierno de Estonia, para trasladar la estatua conocida como el "Soldado de Bronce", generó una polarización entre la sociedad, provocando manifestaciones, actos vandálicos y disturbios conocidos como "la noche de los cristales". Mientras se enfrentaba la policía con grupos de la comunidad rusa, se presenciaron ciberataques a sistemas de información de la infraestructura pública y privada, así como los medios de comunicación locales, nacionales e internacionales que transmitían la información desde diferente punto de vista (Ganuza Artiles 2011).

En el año 2010, los operadores de la planta de enriquecimiento de uranio en Natanz, Irán, fueron sorprendidos con los rotores de varias cascadas de centrífugas a gas que se aceleraron y desaceleraron sin control. Provocando fallas en estas y dejándolas fuera de servicio, estaban siendo víctimas de *Stuxnet*, un gusano informático que ocasiona daños físicos en sistemas SCADA[3] (Rivadeneira 2016).

Estas afirmaciones, muestran las dimensiones a las cuales puede llegar el uso de la tecnología, la digitalización de la información y el uso de la internet dentro de la sociedad de la información y el conocimiento. Puesto que la conectividad global implica el aumento potencial de los escenarios en los que se pueden desarrollar las amenazas y

[3] Supervisory Control and Data Acquisition - Sistema de control de supervisión y adquisición de datos.

actores maliciosos, por consecuente sus daños potenciales. Tal como evidencia el Foro Económico Mundial (FEM), por ejemplo, un ataque cibernético exitoso en el sistema eléctrico de un país podría desencadenar efectos indirectos devastadores. "Un cálculo sugiere que las compañías de servicios de energía eléctrica gastaron USD 1700 millones en el 2017, en la protección de sus sistemas en contra de ataques cibernéticos" (Collins 2019, 83).

Con la presencia de estas amenazas, los gobiernos tienen el desafío de saber lo que se espera del espacio cibernético para poder defenderse en este dominio. Por tal razón, las naciones elaboraron estrategias de ciberseguridad y ciberdefensa a nivel mundial. Las amenazas están ganando presencia, tanto redes civiles como militares son atacadas por hackers, por lo que la protección de las redes es un tema de alta prioridad. En la última década, además de Estados Unidos, países como Brasil, Colombia, España, Francia y Gran Bretaña, han anunciado sus proyectos estratégicos de defensa cibernética. Que les permita prevenir y controlar posibles futuros ataques, así como "incrementar la intensidad informativa y el dinamismo en los sistemas de protección del espacio cibernético" (Vergara et al. 2017, 15).

No obstante, hay que considerar que muchos años atrás la actuación de los Estados en distintos campos de acción que refieren la protección y promoción de la ciberseguridad. Especialmente en el campo educativo, ya estuvo puesta de manifiesto en el 2001 a través de *Children's Internet Protection Act* (CIPA) en los EE.UU. En la que se exigía a las unidades educativas primarias y secundarias, y a la comunidad educativa en general, mantener el control. Sobre todo en los sistemas informáticos, con prioridad al control de amenazas y bloqueos con un porcentaje bastante importante (Federal Communications Commission 2016).

2.2. Regional

Temas de ciberseguridad fueron discutidos a nivel sudamericano por la Unión de Naciones Suramericanas (UNASUR), fue propuesto en las agendas de los Estados, especialmente por parte de Argentina y Brasil.[4]

[4] Esta propuesta de acciones cooperativas en la región tiene sus bases en el pensamiento sudamericano, que se vincula a las decisiones político estratégicas, siendo de este modo que, en el año 2013, "los Ministros de Defensa de Argentina y Brasil suscribieron un acuerdo de cooperación en materia de seguridad cibernética" (Moncayo Gallegos et al. 2014, 74).

En lo que refiere a Argentina, sobre la base de las nuevas amenazas cibernéticas, desarrolló temas a ser tratados en varias conferencias[5] sobre la actualidad informática y ciberseguridad. Apostando a la idea de presentar estrategias para enfrentar las vulnerabilidades, los tipos de ataques comunes en el ciberespacio y los cuidados que se deben tener frente a estas amenazas. Cabe mencionar que, de acuerdo a la política argentina de actualizar permanentemente su estrategia nacional de seguridad, se presentaron proyectos tecnológicos en desarrollo por parte del Ministerio de Defensa Nacional para mejorar la seguridad de sus sistemas y redes, en base a su normativa interna en materia de ciberseguridad (Arredondo 2017).

Un caso similar se dio en Brasil, país en el que la ciberseguridad fue un tema muy preocupante, especialmente a causa de los constantes ataques cibernéticos sufridos en el mundo. Por tal razón, una de sus estrategias fue establecer vínculos con Estados e instituciones académicas con la finalidad de realizar el Seminario Internacional de Defensa Cibernética.[6] Y aprovechar este espacio de diálogo para concienciar a los participantes de la amenaza que significa esta guerra cibernética, ya que en el año 1999 Brasil registró cerca de tres mil incidentes de esta naturaleza, y en 2016 en cambio, llegaron a 600.000 las notificaciones desde los Cert.Br en todo el país (Arredondo 2017).

Otro de los países que presentaron avances en materia de ciberseguridad y ciberdefensa fue Chile, quien, a través de un seminario organizado por la Comisión de Defensa Nacional del Senado,[7] su Subsecretaría de Defensa promulgó el compromiso de promover regímenes internacionales que incrementen la transparencia y la confianza entre los estados en el ámbito del ciberespacio para reducir la incertidumbre y prevenir conflictos.

Finalmente, Colombia, con el fin de evidenciar las prioridades para el gobierno y la Fuerza Pública, presentó los retos en materia de ciberdefensa y ciberseguridad. Temas importantes desde la gestión de Juan Manuel Santos, por cuanto es una política que ha alcanzado resultados muy destacados. Colombia mantiene importantes convenios,

---

[5] Esude-CDS. Para mayor información acceder a http://esude-cds.unasursg.org/index.php/noticias/683-argentina-ministerio-de-defensa-promueve-la-conferencia-actualidad-informatica-y-ciberseguridad.

[6] Esude-CDS. Para mayor información acceder a http://ar.unasursg.org/index.php/academia/investigacion/732-brasil-especialistas-debatem-formas-de-coibir-ataques-ciberneticos

[7] Esude-CDS. Para mayor información acceder a http://esude-cds.unasursg.org/index.php/noticias/57-chile-20-de-mayo-subsecretaria-de-defensa-presenta-avances-en-materia-de-ciberseguridad-y-ciberdefensa

especialmente con la Organización del Tratado del Atlántico Norte (OTAN) y con el Reino Unido, además cuenta con cuatro unidades para contrarrestar las eventuales amenazas a través de sus ColCert,[8] Secop[9] y Centro cibernético de la Policía. Siendo este último con mayor vinculación en materia cibernética y respuesta a los ataques de *hackers* a toda la infraestructura del Estado (CO Ministerio de Defensa Nacional 2017).

3. Actores que amenazan en el ciberespacio

Son varios los actores que amenazan en el ciberespacio, los mismos que se encuentran categorizados como estados y grupos patrocinados por Estados, ciberdelincuentes, terroristas, hacktivistas, insiders (personal interno) quienes pueden afectar a víctimas de interés del sector público, infraestructuras críticas, empresas y ciudadanos, para cada uno de ellos con diferente nivel de peligrosidad: alto, medio y bajo (ES Centro Criptológico Nacional 2020).

Figura 1. Agentes de la amenaza.
Fuente: Ciberamenazas y Tendencias - Edición 2020 CCN-CERT IA-13/20 (citado en Realpe 2022)

[8] ColCert: "grupo de respuestas a emergencias cibernéticas, coordinador a nivel nacional" (CO Ministerio de Defensa Nacional 2017, párr. 6), con sede en la Presidencia de la República de Colombia.

[9] Secop: grupo de respuesta de las "Fuerzas Militares, encargado de prevenir y contrarrestar las amenazas y ataques que afecten a la infraestructura cibernética del Estado colombiano […]" (CO Ministerio de Defensa Nacional 2017, párr. 6).

3.1. Actores estatales

Estados-Grupos patrocinados por Estados

En el sector público pueden afectar por ciberespionaje, manipulación de información, acciones híbridas. Las infraestructuras críticas pueden ser amenazadas por ciberespionaje, interrupción de servicios, espionaje. Las empresas pueden tener vulneraciones a través de ciberespionaje, manipulación de sistemas. Los ciudadanos pueden ser víctimas de influencia, ciberespionaje (ES Centro Criptológico Nacional 2020, 8).

Dentro del escenario multidimensional creado por el dominio del ciberespacio se presentan un gran número de agentes que cuentan con acceso fácil y rápido dentro de la sociedad de la información y el conocimiento debido al gran flujo de información a nuevas herramientas de ataque y la dificultad permanente para probar la autoría. Es así que, dentro de los tipos de actores que utilizan las mismas herramientas, pero con distintos fines, se encuentran a los Estados, los actores paraestatales e internos (ES Centro Criptológico Nacional 2019).

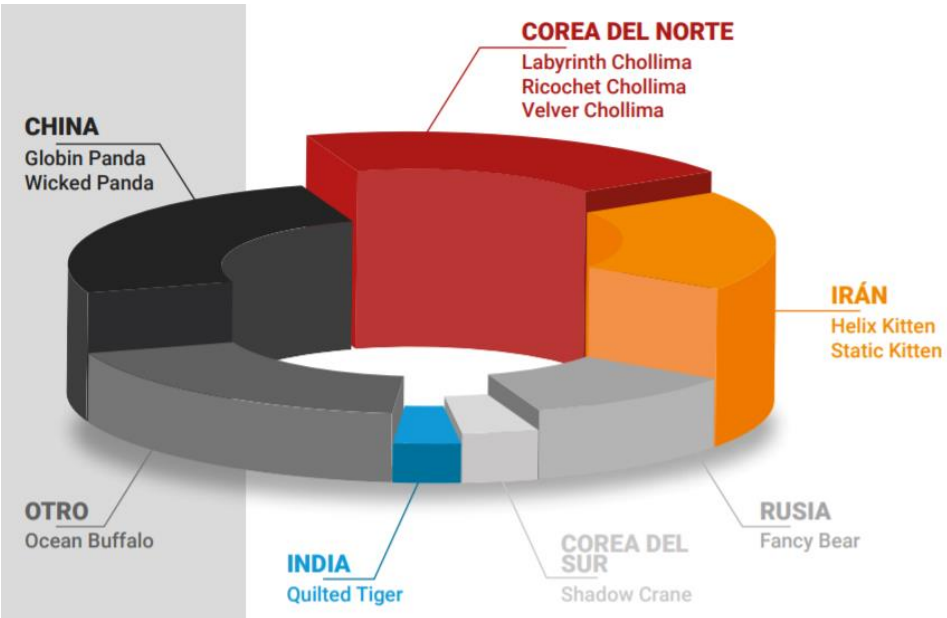

Figura 2. Actores Estatales.
Fuente: 2019 Global Threat Report (citado en ES Centro Criptológico Nacional 2019, 10)

Esta sección del trabajo de investigación se enfoca en los tres grandes actores EE. UU., China y Rusia:

EE. UU.

Con la promulgación de la estrategia de ciberseguridad 2018 por parte del presidente Donald Trump, se evidenció la importancia y preocupación del régimen por articular la primera estrategia nacional de ciberseguridad en quince años (Sputnik Mundo 2018, párr. 1).

Para enfrentar los problemas públicos y privados frente a las actividades maliciosas que cuentan sus ciberdefensas, el Cibercomando del Pentágono cuenta con más de seis mil *hackers* para ejecutar ofensivas cibernéticas. Este Comando estuvo presionado para que en 2019 funcione a plenitud, y apunte a proteger de manera integral los sistemas de información de los EE. UU., mejorar la resiliencia y control del ciberespacio y asegurar su infraestructura crítica. Aumentando la estabilidad cibernética del país con el fin de enfrentar a China, Corea del Norte y otros países de ejecutar ataques cibernéticos contra equipos del gobierno americano, empresas, infraestructura como las redes viales, de transporte y eléctricas del país (Sputnik Mundo 2018).

El USCYBERCOM es la unidad más temida y avanzada del ejército estadounidense, integra, planifica, coordina y realiza operaciones de ciberespacio de espectro completo, guerra electrónica y operaciones de información, posibilitando el accionar de las fuerzas amigas en todos los dominios, garantizando la libertad de acción en el ciberespacio para los EE. UU. y sus aliados, negando esta libertad a sus enemigos (Vergara et al. 2017).

China

China se ha convertido en el eterno sospechoso de grandes ataques cibernéticos, nunca admitidos por el gobierno asiático; sin embargo, China reveló la inversión de decenas de millones para formar un comando especial de 30 soldados cibernéticos, “El Ejército Azul” (Sturm 2011, párr. 2). Entrenados para “mejorar la ciberseguridad de las Fuerzas Armadas […] proteger las redes militares de ataques externos. […] el Ejército Azul existe desde hace 2 años, […] para fines defensivos, no muchos están convencidos con esa historia. Varios gobiernos temen que sea cierto que China esté detrás de los ataques a sus sistemas”(Sturm 2011).

Rusia

El establecimiento de una unidad de operaciones de información por parte del ministro de Defensa ruso, Sergey Shoigu, ha generado preocupaciones de que Rusia sea responsable del pirateo de Estados Unidos y Francia. En medio de acusaciones en curso,

Shoigú ha anunciado la creación de nuevas divisiones en tecnología que están diseñadas para ser transferidas a los estudiantes.

Serguéi Shoigú, ministro de Defensa ruso, informó:

> la creación de **unidades especiales de guerra informativa** […] Rusia es acusada de ciberataques contra […] Estados Unidos y Francia. «Hemos creado unidades **para operaciones de información**, lo que es mucho más eficaz y potente que el denominado departamento de propaganda», afirmó Shoigú […] unidad de guerra electrónica se nutrirá de estudiantes de **informática, matemáticas, robótica, comunicaciones y criptografía.** (ABC Internacional 2017, párr 1,2,7; énfasis en el original)

3.2. Actores paraestatales

Para el propósito de esta investigación se identificaron a los ciberdelincuentes, grupos terroristas, cibervándalos, *hacktivistas*, actores internos, ciberinvestigadores y organizaciones privadas, que se encuentran involucrados en el empleo del ciberespacio, sus objetivos y nivel de peligrosidad que es determinado por el equipo de respuesta a Incidentes de Seguridad de la Información (ISIRT, por sus siglas del inglés). El nivel de peligrosidad se ha identificado como bajo, medio y alto para entregar la información a los estados, empresas públicas y privadas, dentro del contexto mundial, regional y local. Posteriormente se deben establecer las líneas políticas sectoriales de las instituciones y los estados que limiten el accionar y minimicen la amenaza.

Ciberdelicuentes / Cibercriminales

Los ciberdelincuentes en el sector público pueden afectar en la interrupción de los servicios, manipulación de sistemas, robo de información. Las infraestructuras críticas pueden ser amenazadas por la interrupción de servicios y la manipulación de sistemas. Las empresas pueden tener vulneraciones a través de robo de información, manipulación de información, interrupción de servicios, manipulación de sistemas. Los ciudadanos pueden ser vulnerados por la manipulación de información, interrupción de servicios, manipulación de sistemas, robo de información (ES Centro Criptológico Nacional 2020, 8).

Terroristas

Los terroristas prefieren como víctimas al sector público e infraestructuras críticas para cometer actividades de sabotaje(ES Centro Criptológico Nacional 2020, 9).

Hactivistas

Los hacktivistas en el sector público, infraestructuras críticas suelen realizar interrupción de servicios, manipulación de información. En las empresas ejecutan

interrupción de servicios, robo de información, manipulación de información (ES Centro Criptológico Nacional 2020, 9).

Personal interno

Para el caso de los *insiders* (personal interno) afectan al sector público, infraestructuras críticas, empresas con el robo de información, interrupción de servicios (ES Centro Criptológico Nacional 2020, 9).

Visto de esta manera, se concibe a la ciberseguridad como respuesta de los Estados como actores principales, más aún hoy en día que el mayor riesgo para la seguridad del ciberespacio, el internet y sus usos legales se circunscriben en el mismo Estado. Ya que se encuentran centralizando en la tecnología todo el aparataje institucional, con un control casi absoluto.

4. Marco regulatorio supranacional en seguridad cibernética, políticas y estrategias internacionales

Debido a la importancia que reviste el desarrollo de estrategias en las que se identifican áreas de convergencia de los Estados para contrarrestar las amenazas en el ciberespacio y fortalecer los intereses comunes, así como el salvaguardar los valores colectivos, se han identificado mecanismos de cooperación especialmente a nivel internacional como:

4.1. Organización del Tratado del Atlántico Norte (OTAN)

Desde fines de la década de 1990 hasta la actualidad, la OTAN dispone de un sinnúmero de capacidades orientadas a la protección de sistemas, datos, información y análisis de vulnerabilidades, destacándose además las siguientes iniciativas mostradas en la tabla 1.

Tabla 1
Cronología de iniciativas de la OTAN

Año	Evento	Acto
1999	Cumbre de Washington D.C.	Aprobación de capacidades de defensa relacionadas con objetivos de seguridad para sistemas de comunicación e información y análisis de vulnerabilidades.
2002	Cumbre de Praga	Tema central de discusión “la seguridad de la información”.
2004		Aprobada la creación de la *nato Computer Incident Response Capability* (NCIRC).
2005		Protección de infraestructura crítica forma parte de los programas de defensa contra el terrorismo.
2006	Declaración de Riga	Desafíos para la seguridad en el siglo XXI.

Año	Evento	Acto
2007		Publicación de la guía *Comprehensive Political Guidance* y establecimiento de prioridades sobre capacidad, planificación e inteligencia.
	Acuerdo NC3B[10]	Desarrollo para la mejora de la ciberdefensa y el desarrollo del concepto de ciberdefensa.
2008		Aprueba la política de ciberdefensa y el concepto de ciberdefensa.
		Constitución del *Cooperative Cyber Defense Centre Of Excelence* (CCD COE) y la *Nato Cyber Defense Management Authority* (NCDMA).
	Cumbre de Bucarest	Papel de la OTAN en la seguridad del sector energético.
2010	Cumbre de Lisboa	Considera la revisión de la Política de ciberdefensa de la OTAN como hito fundamental. Necesidad de considerar al ciberespacio y adquirir la capacidad de combatir los ciberataques.
2011		Revisión de la Política de ciberdefensa y plan de acción para su implementación.
2012		Revisión de la política de seguridad de la información donde se incluye la defensa cibernética.
		Surge la *Nato Communications and information Agency.*

Fuente: Documentos de Seguridad y Defensa de la Escuela de Altos Estudios de la Defensa. España
Elaboración propia

Como seguimiento de estas actividades, se señala a España, país que es un referente global en términos de ciberseguridad y ciberdefensa, por lo que se destaca el caso del Ministerio de Defensa español respecto a la implementación de la Política de Ciberdefensa de la OTAN, dentro de la que se definen los siguientes puntos principales:

- Integración de las consideraciones de defensa dentro de sus estructuras de la OTAN y los procesos de planificación para poder tener un núcleo de defensa y gestión de crisis.
- Focalización en prevención, resiliencia y defensa de los activos críticos del ciberespacio para la OTAN y sus aliados.
- Desarrollo de capacidades de ciberdefensa robustas y centralización de la protección de las redes de la OTAN.
- Desarrollo de un mínimo de requisitos para la defensa de las redes de las naciones críticas para la OTAN.
- Dar soporte a los aliados para conseguir un nivel mínimo en materia de ciberdefensa y reducir las vulnerabilidades de las infraestructuras críticas de las naciones.
- Cooperación con sus socios, organizaciones internacionales, sector privado y universidad. (ES Ministerio de Defensa 2014, 71–72)

De acuerdo con las especificaciones mencionadas anteriormente, la Política de ciberdefensa de la OTAN requiere el compromiso de las autoridades al más alto nivel, así como de los Estados miembros para cumplir con la misión principal de fortalecer la

[10] NC3B: siglas del inglés *Nato Consultation, Command and Control Board.*

capacidad de ciberdefensa y contribuir con otras organizaciones mediante el desarrollo de doctrinas, investigación y desarrollo.

4.2. Unión Europea (UE)

Una vez aprobada la Estrategia de Ciberseguridad de la UE, la Comisión Europea prepara nuevas propuestas e iniciativas sobre seguridad de redes e información y gestión de riesgos con el fin de "reforzar la ciberseguridad en la UE" (ES Departamento de Seguridad Nacional 2017, párr. 1).

Uno de los aspectos destacados es la presentación de un *roadmap* de ciberseguridad para la UE, denominado *ciber security package*, cuyas características proporcionan un conjunto amplio de medidas para proteger y fortalecer la ciberseguridad y ciberdefensa dentro del contexto europeo. No obstante, en el 2017 el Consejo de la UE solicitó el refuerzo, especialmente en el tema de ciberseguridad y ciberresiliencia, con el fin de garantizar un efectivo sistema que enfrente un incidente o crisis cibernética.

4.3. Naciones Unidas y la Unión Internacional de Telecomunicaciones (UIT)

A nivel internacional, la Unión Internacional de Telecomunicaciones (UIT), de la cual el Ecuador es miembro, apoya la definición de la *sociedad de la información* basada en el avance de las telecomunicaciones y el importante rol que emplea para el progreso de la sociedad, la economía, la cultura y la milicia. También es consciente de la globalización de las telecomunicaciones y de cómo ésta debe ser compatible con las normas, reglamentos y actividades tecnológicas del país anfitrión. Por ello, la Asamblea General de las Naciones Unidas "aprobó la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI)" (EC Ministerio de Telecomunicaciones y la Sociedad de la Información 2018, 12) en dos partes: la primera en Ginebra en 2003 y la segunda en Túnez en 2005.

El propósito de la primera fase es hacer una declaración de intenciones y tomar acciones concretas, de tal manera de llevar a cabo los "fundamentos de la Sociedad de la Información, a través de la Declaración de Principios y el Plan de Acción, que fue aprobado el 12 de diciembre de 2003"(EC Ministerio de Telecomunicaciones y la Sociedad de la Información 2018, 12). En esta participaron los líderes mundiales de 175 países. En la segunda fase, en Túnez en 2005, se da la razón de la importancia del avance de las Tecnologías de Información y Comunicaciones como herramienta de desarrollo.

Como resultado, líderes mundiales de 174 países, así como representantes de organizaciones internacionales, el sector privado y la sociedad civil analizaron la oportunidad de una visibilidad y un sinergia globales para crear un "marco de una Sociedad de la Información integradora y justa" (EC Ministerio de Telecomunicaciones y la Sociedad de la Información 2018, 13). De manera general, estas guías metodológicas están basadas y/o hacen referencia a los estándares, directrices y mejores prácticas.

Como referencia para desarrollar una estrategia nacional de ciberseguridad se cuenta con la guía elaborada entre la "Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial (BM), la Secretaría de la Commonwealth (COMSEC), la Organización de Telecomunicaciones de la Commonwealth (CTO) y el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN)" (Secretaría de la Commonwealth et al. 2018, III–IV), que es el resultado de esfuerzos para utilizar el conocimiento, la experiencia y las capacidades de muchas organizaciones en el desarrollo e implementación de estrategias y políticas de seguridad cibernética.

4.4. Organización para la Cooperación y el Desarrollo Económico (OCDE)

Desde la década pasada, la OCDE ha impulsado leyes para la protección de la privacidad que han sido una tendencia en diferentes países. Siendo así que en 1976 se encargó a un grupo de expertos la elaboración de Directrices que rijan el "flujo transfronterizo y la protección de los datos personales y la privacidad" .

En los albores de 1978, apareció "un nuevo Grupo de Expertos *ad hoc*" enfocado a crear barreras de los "Datos Transfronterizos y la Protección de la Privacidad" (Organisation for Economic Co-operation and Development y ES Ministerio de Administraciones Públicas, Secretaría General Técnica, 2004, 11) para realizar "directrices sobre las normas básicas que regirían el flujo transfronterizo y la protección de los datos personales y la privacidad" (Organisation for Economic Co-operation and Development y ES Ministerio de Administraciones Públicas, Secretaría General Técnica, 2004, 11), y facilitar las legislaciones nacionales, así como realizar un "Convenio internacional […] coordinación con el Consejo de Europa y la Comunidad Europea […] (Organisation for Economic Co-operation and Development y ES Ministerio de Administraciones Públicas, Secretaría General Técnica, 2004, 11–12).

Como parte de los fines y objetivos de la OCDE está el

> compromiso de los Países Miembros de proteger la privacidad y las libertades individuales y de respetar el flujo transfronterizo de datos personales. […] instrumentos internacionales afines que rigen temas como los derechos humanos, las telecomunicaciones, el comercio internacional, el derecho de propiedad intelectual y distintos servicios de información. […] de las políticas sobre información, informática y comunicaciones. (Organisation for Economic Co-operation and Development y ES Ministerio de Administraciones Públicas, Secretaría General Técnica, 2004, 13–14)

4.5. Instituto Nacional de Ciberseguridad (INCIBE)

En Madrid, expertos solicitaron la creación de "un organismo supranacional de ciberseguridad" (La Vanguardia 2015, párr. 1), que permita "mejorar la seguridad digital mundial" (La Vanguardia 2015, párr. 1), reforzando la respuesta a los ataques en la red, considerando que "la actual regulación y las políticas mundiales de gobierno en materia de seguridad digital son "insuficientes" para asegurar un ciberespacio protegido" (La Vanguardia 2015, párr. 2). Que es en donde "las tensiones entre los Estados se reproducen" (La Vanguardia 2015, párr. 5) afectando "al desarrollo técnico, económico mundial" (La Vanguardia 2015, párr. 6) e inestabilidad política de algunos gobiernos puede verse afectada, un marco de gobernanza del siglo veinte, no puede responder a la tecnología del siglo veintiuno. Se debe considerar una "colaboración entre el sector privado, la sociedad civil y responsables políticos para reducir las amenazas cibernéticas" (La Vanguardia 2015, 7). Y con un cambio cultural y de mentalidad de intercambio de información con el sector privado y la conexión de la ciberseguridad con la seguridad multidimensional.

> INCIBE forma parte de los principales foros y grupos de trabajo en ciberseguridad del plano nacional e internacional, colaborando activamente con actores estratégicos que tratan diferentes aspectos de la ciberseguridad, como son la respuesta a incidentes, el intercambio de información, la concienciación, el desarrollo de políticas o el impulso de la normalización, entre otros. (ES Instituto Nacional de Ciberseguridad 2020, párr. 1)

4.6. Organizaciones de normalización y gestión de internet

Partiendo de la lógica de la interconexión persona-máquina que se mencionó al inicio de la investigación, es imprescindible el uso del internet como catalizador para el desarrollo global, más aún cuando se ha definido al internet como el recurso esencial para el desarrollo de las sociedades modernas. En este sentido, el uso efectivo de este recurso depende no solamente de su arquitectura e infraestructura tecnológica, sino de la administración de los servicios críticos, por lo que para su normalización y gestión técnica

existen sociedades que se especializan en este segmento, para ejemplificar se detallan las siguientes:

1. *Internet Corporation for Assigned Names and Numbers* (ICANN)
2. *Internet Engineering Task Force* (IETF)
3. *Internet Governance Forum* (IGF)
4. *Internet Society* (ISOC)

A escala regional, en el 2005 en Rio de Janeiro (Brasil) se realizó:

> la Primera Conferencia Ministerial Regional de América Latina y el Caribe […] aprobó la primera versión del Plan de Acción sobre Sociedad de la Información de América Latina y el Caribe (eLAC), […] visión regional y un compromiso político para reducir la brecha digital. […] para el acceso y uso de las tecnologías de la información y la comunicación (TICS) en la región. (Comisión Económica para América Latina y el Caribe 2020, párr. 1)

4.7. Convenio de Budapest – Convenio de Cibercriminalidad

La oficina de las Naciones Unidades contra la Droga y el Crimen (ONUDC) emitió el reporte TOCTA[11] en el año 2010, en el que contextualiza el "Delito cibernético", mismo que es utilizado para describir una gama de delitos, incluidos los delitos contra datos y sistemas informáticos, falsificación y fraude informáticos, delitos de contenido y delitos de derechos de autor.

Convencidos de la necesidad de llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional (Consejo de Europa 2001).

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, mejor conocido como convenio de Budapest, fue firmado en Hungría el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004, con 56 firmas y 64 firmantes. Fue suscrito por Canadá, Estados Unidos, Japón y Sudáfrica. Son parte también: Argentina, Brasil, Chile, Colombia, Costa Rica, Perú, Filipinas y México (Asociación Ecuatoriana de Ciberseguridad y Acurio Del Pino 2020).

[11] TOCTA: Transnational Organized Crime Threat Assessment (United Nations Office on Drugs and Crime 2010).

> El primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que se ocupa especialmente de las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de la red. También contiene una serie de poderes y procedimientos, como la búsqueda de redes informáticas y la intercepción. (Estévez 2020, párr. 3)

> Esta Convención busca como objetivos fundamentales los siguientes: (1) Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático; (2) Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; y (3) Establecer un régimen dinámico y efectivo de cooperación internacional. (Acurio Del Pino 2017, 122)

En la ciudad de Estrasburgo, el 28 de enero de 2003, se suscribe el:

> Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. […] tiene por objeto la lucha contra el racismo, la discriminación racial, la xenofobia y la intolerancia, en el ámbito de los sistemas informáticos -y en particular, a través de Internet-, penalizando jurídicamente los actos racistas y xenófobos. (CL Biblioteca del Congreso Nacional 2014, 3)

Una vez culminado la descripción de la investigación en este capítulo primero podemos mencionar que la *ciberseguridad* es un área de investigación que requiere un profundo análisis epistemológico, basado en el conocimiento científico sobre el uso, concientización y educación con que los seres humanos la emplean. Las necesidades y demandas de la comunicación del ser humano para manipular y almacenar grandes cantidades de datos a velocidades de comunicación de máquina. Han hecho que las computadoras se conviertan en los mayores recolectores y procesadores de información, transformando sociedades humanas enteras, siendo las tecnologías de la computación, la información y la comunicación los medios más efectivos para acceder a las redes globales como el modus vivendi en los negocios, la política y la interacción social a través de la interconexión a escala mundial.

Para garantizar esta evolución tecnológica y que sea más eficiente en causa, condición y efecto, al mismo tiempo que aumente la fluidez del proceso de información y recursos. Se acerca al concepto de ciberespacio, es decir, al ámbito de la construcción social, la sociedad red, el flujo y el lugar. De manera especial, se convierte en el quinto dominio después de la Tierra, el Mar, el Cielo y el Espacio.

Con este avance tecnológico, también se han desarrollado escenarios de amenazas cibernéticas tanto a nivel global como regional. Algunos escenarios a nivel global que dieron mucho de qué hablar son el caso Julian Assange y su sitio web WikiLeaks, en el cual publicaba documentos e informes que contienen información confidencial, los

ataques cibernéticos en infraestructura, medios y sistemas en toda Estonia a causa de la estatua del Soldado de Bronce que fue trasladada de lugar, la propagación del gusano Stuxnet que dañó el sistema SCADA de una centrífuga a gas en la planta de enriquecimiento de uranio en Irán.

Para lograr neutralizar las amenazas en el ciberespacio, los países de todo el mundo han desarrollado estándares, políticas, estrategias y demás normativa de ciberseguridad y ciberdefensa. Para este trabajo de investigación se ha considerado los casos de Argentina, Brasil, Chile y Colombia por los avances en sus estrategias de seguridad cibernética a nivel regional.

Las amenazas cibernéticas son provocadas por muchos actores que atenta el mundo digital. Se clasifican como actores estales y actores paraestatales. Se consideró detallar los actores estatales como Estados Unidos, China y Rusia. Así como también se mencionó como actores paraestatales a los ciberdelincuentes, terroristas, hacktivistas, insiders personas con información privilegiada que trabajan en gobiernos e infraestructuras críticas, corporaciones y ciudadanos. En la sociedad de la información y el conocimiento estos actores tienen fácil y rápido acceso a la información y el conocimiento. Estos agentes o vectores de ataque existen dentro del dominio del ciberespacio en el cual no existe fronteras. Hacen uso de herramientas para la manipulación de los sistemas de información, ciberacoso, espionaje cibernético y acciones híbridas contra las infraestructuras críticas: sector bancario, telecomunicaciones, centrales eléctricas, sector salud, sistemas de transporte, sistemas de agua y otras.

Para combatir con las amenazas de ciberseguridad y ciberdefensa a más de los países, existen organizaciones, instituciones que contribuyen con la cooperación, colaboración internacional dentro de las cuales en este capítulo primero se nombra a la Organización del Tratado del Atlántico Norte, Unión Europea, Naciones Unidas y la Unión Internacional de Telecomunicaciones, la Organización para la Cooperación y el Desarrollo Económico, el Instituto Nacional de Ciberseguridad, la Organización de normalización y gestión de internet y el Convenio de Budapest.

Para aterrizar a nuestro país Ecuador una vez que hemos comprendido que la ciberseguridad concierne a todos. En este primer capítulo se presentó un marco regulatorio de ciberseguridad global, abordando los orígenes de la ciberseguridad, así como los diferentes actores y situaciones que existen en este ámbito. Esto nos permite comprender la perspectiva del mundo de las políticas y estrategias internacionales que influirían en el Estado ecuatoriano.

Capítulo segundo

Respuestas del Estado ecuatoriano en el período 2013-2022

Esta investigación titulada marco regulatorio de la ciberseguridad y ciberdefensa dentro de la sociedad de la información y el conocimiento. Respuestas del Estado ecuatoriano en el período 2013-2022, tiene como pregunta de investigación: ¿qué marco regulatorio de la ciberseguridad y ciberdefensa se implementó en Ecuador en el período 2013-2022 que neutralice las amenazas en el ciberespacio? En este capítulo se desarrolla la investigación del marco regulatorio de seguridad cibernética en América Latina, marco legal y regulatorio de ciberseguridad en Ecuador, retos y desafíos en la ciberdiplomacia para fomentar el uso pacífico de las Tecnologías de la información y de la comunicación, debates y desafíos de las ciberamenazas y sus proyecciones con el que se cubre el segundo objetivo:

Determinar qué instrumentos estratégicos de la ciberseguridad y ciberdefensa: políticas, legislación e instituciones se han generado en Ecuador para enfrentar las amenazas cibernéticas, en el campo de la Seguridad y Defensa.

1. Marco regulatorio de seguridad cibernética en América Latina

Para el desarrollo de este trabajo de investigación se procedió con la revisión de instrumentos internacionales existentes, las misma que se listan en la tabla 2. Base Legal América Latina:

Tabla 2

Base legal Internacional

Instrumentos Internacionales
Carta de las Naciones Unidas.
Convenio de Ginebra y sus Protocolos adicionales.
Resolución AG/RES 2004 (XXXIV-O / 04) de la OEA: Adopción de una Estrategia de Seguridad Cibernética.
Resoluciones UNGA 55/63 y 56/121 de las Naciones Unidas sobre la lucha contra el uso de la tecnología de la información con fines delictivos.
Resoluciones UNGA 57/239, 58/199 y 64/211 de las Naciones Unidas sobre la creación de una cultura mundial de seguridad cibernética y la protección de infraestructuras críticas de la información.
Resolución UNGA 73/266 sobre Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional.
Declaración para la protección de infraestructura crítica ante las amenazas emergentes – Comité Interamericano contra el Terrorismo de la OEA.
Resolución CICTE/RES. 1/19 del 24 de mayo de 2019 sobre Medidas Regionales de Fomento de Cooperación y Confianza en el Ciberespacio (MFCS) del Comité Interamericano contra el Terrorismo.

Fuente: Política Nacional de Ciberseguridad (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2021, 22)
Elaboración: Ministerio de Telecomunicaciones y de la Sociedad de la Información

El panorama actual de ciberseguridad refleja los sistemas legales de todos los países de la región y las necesidades de cada profesión. Esta historia influye en los esfuerzos actuales para asegurar el sistema, incluidos los desafíos y los esfuerzos competitivos. Además, las consideraciones de desarrollo histórico y la falta de defensa, privacidad y libertad de expresión afectan la capacidad de proteger los sistemas de manera efectiva. Las personas necesitan seguridad en sus vidas digitales. Por lo tanto, los sectores público y privado deben trabajar juntos para proporcionar esto. Necesitamos crear un marco de ciberseguridad y ciberdefensa coherente para la región. Esto se debe a que ambos están diseñados para proteger intereses comunes y generar intereses comerciales.

> El desarrollo histórico de los sistemas legales en los países, enfocado en los tres sistemas existentes y utilizados en la región: sistema civil, común y la combinación de ambos, así como el contraste de los esfuerzos y los desafíos para los tres sistemas, se consideran elementos contribuyentes a la actual falta de capacidades reguladoras.
> La regulación de las funciones de ataque, defensa, resiliencia, privacidad y libertad de expresión, entre otras de los sectores público y privado, es esencial para ejercer la ciberseguridad nacional y global. El sector público, enfocado en el principio de proteger el bien común, y el sector privado, enfocado en la generación de ganancias comerciales, deben converger y unirse bajo un marco regulatorio común para cumplir sus objetivos de seguridad. […] A manera de idea general del estado de la cuestión de las regulaciones de seguridad cibernética en la región, la tabla 3 describe cada país y el marco de legislación de seguridad cibernética o regulaciones relacionadas con: protección de datos, cibercrimen, gobierno electrónico, tecnología de la información (TI), comunicaciones, infraestructura crítica y varias áreas adicionales, así como el sistema legal empleado y la fecha de implantación. (Boris 2020, 197–98)

Tabla 3
Regulaciones de seguridad cibernética en América Latina

País	Sistema Legal	Título de la legislación en ciberseguridad	Año
Argentina	Derecho civil	Ley de Protección de Datos Personales Ley de Delitos Informáticos	2000 2008
Bolivia	Derecho civil	Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación Plan de Implementación de Gobierno Electrónico	2011 2017
Brasil	Derecho civil	Estrategia Nacional de Seguridad de las Comunicaciones de Información y Seguridad Cibernética Ley General de Protección de Datos	2015 2020
Chile	Derecho civil	Ley General de Telecomunicaciones Ley de Protección de la Vida Privada Política Nacional de Ciberseguridad	1982 1999 2017
Colombia	Derecho civil	Ley de la Protección de la Información y de los Datos Lineamientos de Política para la Ciberseguridad y Ciberdefensa Acta de Protección de Datos Personales Ley de Protección de Datos Política Nacional de Seguridad Digital	2009 2011 2011 2012 2016
Costa Rica	Derecho civil	Estrategia Nacional de Ciberseguridad	2017

Cuba	Derecho civil	Reglamento de Seguridad para las Tecnologías de Información	2007
República Dominicana	Derecho civil	Ley sobre Crímenes y Delitos de Alta Tecnología Ley de Protección de Datos Personales Estrategia Nacional de Ciberseguridad	2007 2013 2018
Ecuador	Derecho civil	Ley de Comercio Electrónico, Firmas y Mensajes de Datos Plan Nacional de Gobierno Electrónico	2002 2017
El Salvador	Derecho civil	Ley Especial Contra los Delitos Informáticos y Conexos	2016
Guatemala	Derecho civil	Estrategia Nacional de Seguridad Cibernética	2018
Guyana	Derecho mixto	Proyecto de Ley sobre Delitos Electrónicos	2018
Honduras	Derecho civil	Ley de Transacciones Electrónicas Ley de Ciberseguridad Agenda Digital de Honduras	2006 2010 2013
México	Derecho civil	Ley Federal de Protección de Datos Personales Estrategia Nacional de Ciberseguridad	2010 2017
Nicaragua	Derecho civil	Ley de Protección de Datos Personales	2012
Panamá	Derecho civil	Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas	2013
Paraguay	Derecho civil	Ley que modifica el Código Penal Ley de Protección de Datos Plan Nacional de Ciberseguridad	2011 2015 2017
Perú	Derecho civil	Ley de Protección de Datos Personales Política Nacional de Gobierno Electrónico Ley de Delitos Informáticos	2011 2013 2014
Puerto Rico	Derecho mixto	Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información Ley para Descartar Información Personal de Consumidores	2005 2014
Trinidad y Tobago	*Common law*	Ley de Protección de Datos Estrategia Nacional de Ciberseguridad	2011 2012
Uruguay	Derecho civil	Ley de Protección de Datos Decreto de Seguridad de la Información para Organismos de la Administración Pública Estandarización de los Nombres de Dominio de la Administración Central Agenda Digital 2020	2008 2009 2014 2017
Venezuela	Derecho civil	Ley Especial contra los Delitos Informáticos Ley sobre Mensaje de Datos y Firmas Electrónicas Ley de Infogobierno	2001 2011 2014

Fuente: Estado de Derecho en el Ciberespacio: La actualidad en Latinoamérica y El Caribe (Boris 2020, 199–202)
Elaboración: Boris Saavedra

Todos los ecosistemas de ciberseguridad actuales reflejan los sistemas legales locales y las necesidades de cada país. Esta historia explica por qué los esfuerzos actuales para asegurar el sistema enfrentan dificultades. Esto se debe a la falta de privacidad, defensa y libertad de expresión dentro del sistema. Además, las consideraciones de desarrollo previo y la competitividad afectan la seguridad del sistema en general. Finalmente, las consideraciones afectan negativamente los esfuerzos de la ciberseguridad por falta de protección para la privacidad y la libertad de expresión. El sector público como el privado deben proporcionar confianza en su entorno de ciberseguridad por lo que trabajando juntos podrán brindarla. Debemos crear un marco coherente de ciberseguridad

para la región. Su finalidad es proteger los intereses comunes y otros intereses económicos.

1.1. Organización de los Estados Americanos (OEA)

La Organización de los Estados Americanos (OEA) en su reporte de ciberseguridad del 2020 se enfoca en el *modelo de madurez de la capacidad de ciberseguridad* (CMM) aplicado a los países en América Latina y el Caribe: Antigua y Barbuda, Argentina, Mancomunidad de las Bahamas, Barbados, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Dominica, *Ecuador*, El Salvador, Grenada, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Saint Kitts y Nevis, San Vicente y las Granadinas, Santa Lucía, Suriname, Trinidad y Tobago, Uruguay, Venezuela.

Este CMM del del GCSCC[12] está conformado por 5 dimensiones: 1) Política y Estrategia de Ciberseguridad; 2) Cultura Cibernética y Sociedad; 3) Educación, Capacitación y Habilidades en Ciberseguridad; 4) Marcos Legales y Regulatorios; y 5) Estándares, Organizaciones y Tecnologías. Y cada dimensión cuenta con un conjunto de factores que describen y definen la capacidad de ciberseguridad de un país de acuerdo a la etapa de avance. Para el caso de Ecuador al 2020, se puede analizar que en forma general se encuentra en una etapa inicial,[13] formativa,[14] y consolidada[15] con respecto al estado de la madurez en seguridad cibernética, como se indica en la Tabla 4 (Banco Interamericano de Desarrollo y Organización de los Estados Americanos 2020).

---

[12] El Centro Global de Capacidad en Seguridad Cibernética (GCSCC, por sus siglas en inglés) de la Universidad de Oxford, en consulta con más de 200 expertos internacionales provenientes de gobiernos, la sociedad civil y la academia, desarrolló el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés). (Banco Interamericano de Desarrollo y Organización de los Estados Americanos 2020, 42)

[13] Inicial: En esta etapa no existe madurez en ciberseguridad o bien se encuentra en un estadio muy embrionario. Puede haber discusiones iniciales sobre el desarrollo de capacidades de ciberseguridad, pero no se han tomado medidas concretas. Falta evidencia observable de la capacidad de seguridad cibernética. (Banco Interamericano de Desarrollo y Organización de los Estados Americanos 2020, 42)

[14] Formativa: Algunos aspectos han comenzado a crecer y formularse, pero pueden ser ad hoc, desorganizados, mal definidos, o simplemente nuevos. Sin embargo, se puede demostrar claramente evidencia de este aspecto. (Banco Interamericano de Desarrollo y Organización de los Estados Americanos 2020, 42)

[15] Consolidada: Los indicadores están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero la etapa es funcional y está definida. (Banco Interamericano de Desarrollo y Organización de los Estados Americanos 2020, 42)

Tabla 4

Indicadores Ecuador: Madurez de la Capacidad de Seguridad Cibernética

Dimensiones	Factores	Etapas 2020				
		Inicial	Formativa	Consolidada	Estratégica	Dinámica
Dimensión 1: Política y Estrategia de Seguridad Cibernética	D1.1 Estrategia Nacional de Seguridad Cibernética	X	X			
	D1.2 Respuesta a Incidentes	X	X	X		
	D1.3 Protección de Infraestructura Crítica (IC)	X	X			
	D1.4 Manejo de Crisis	X				
	D1.5 Defensa Cibernética	X	X			
	D1.6 Redundancia de Comunicaciones	X				
Dimensión 2: Cultura Cibernética y Sociedad	D2.1 Mentalidad de Seguridad Cibernética	X	X			
	D2.2 Confianza y Seguridad en Internet	X	X			
	D2.3 Comprensión del Usuario de la Protección de Información en Línea	X				
	D2.4 Mecanismos de Denuncia	X				
	D2.5 Medios y Redes Sociales	X				
Dimensión 3: Formación, Capacitación y Habilidades Seguridad Cibernética	D3.1 Sensibilización	X	X			
	D3.2 Marco para la Formación	X	X			
	D3.3 Marco para la Capacitación Profesional	X	X			
Dimensión 4: Marcos Legales y Regulatorios	D4.1 Marcos Legales	X	X	X		
	D4.2 Sistema de Justicia Penal	X	X			
	D4.3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético	X	X			
Dimensión 5: Estándares, Organizaciones y Tecnologías	D5.1 Cumplimiento de los Estándares	X	X	X		
	D5.2 Resiliencia de Infraestructura de Internet	X	X	X		
	D5.3 Calidad del Software	X				
	D5.4 Controles Técnicos de Seguridad	X	X			
	D5.5 Controles Criptográficos	X	X			
	D5.6 Mercado de Seguridad Cibernética	X				
	D5.7 Divulgación Responsable	X				

Fuente: Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe (Banco Interamericano de Desarrollo y Organización de los Estados Americanos 2020, 94–95)
Elaboración propia

2. Marco legal y regulatorio de la ciberseguridad y ciberdefensa en Ecuador. Escenarios

Se desarrolla y describe el marco legal y regulatorio general que se relacionan con el *entorno digital y ámbito de la ciberseguridad y ciberdefensa* en Ecuador, también se mencionará, en la sección anexos, algunos *escenarios* que ha sufrido el Ecuador referente a estas temáticas:

La reforma al Sistema de Inteligencia del Ecuador inició en el año 2008, en el Gobierno de Rafael Correa, la razón para hacerlo fue la sospecha de que había injerencia de la Central de Inteligencia de Estados Unidos (CIA) en los servicios policiales y

militares del país, y que se evidenció en el ataque colombiano de Angostura el 1 de marzo de 2008 (INREDH 2008).

La reforma legal motivada desde el Ejecutivo fue la creación de la Secretaría Nacional de Inteligencia (SENAIN), la misma que se sustenta en el Primer Informe sobre la Penetración de la CIA en los sistemas de inteligencia tanto militar y policial (INREDH 2008).

El funcionamiento inicial la SENAIN, en los primeros tres meses, se sustentó legalmente con el Decreto Ejecutivo N°1768, firmado el 8 de junio de 2009 por el presidente Rafael Correa, con este Decreto toma el control total del Sistema Nacional de Inteligencia (El Universo 2009).

El 28 de septiembre de 2009 se publica la Ley de Seguridad Pública y del Estado en el Registro Oficial Suplemento 35, con lo cual se legalizó la creación de la Secretaria Nacional de Inteligencia (EC Asamblea Nacional 2009).

En la Ley de Seguridad Pública y del Estado se resalta la siguiente consideración:

> es necesario renovar la doctrina de seguridad para adaptarla a las demandas del mundo contemporáneo, al marco constitucional vigente, siendo menester contar con un nuevo Sistema de Seguridad Integral bajo una óptica civilista, dinámica y adecuada para el nuevo entorno geopolítico internacional. (EC Asamblea Nacional 2009, 2)

La Ley de Seguridad Pública y del Estado estable en su artículo 1:

> regular la seguridad integral del Estado democrático de derechos y justicia y todos los habitantes del Ecuador, garantizando el orden público, la convivencia, la paz y el buen vivir, en el marco de sus derechos y deberes como personas naturales y jurídicas, comunidades, pueblos, nacionalidades y colectivos, asegurando la defensa nacional, previniendo los riesgos y amenazas de todo orden, a través del Sistema de Seguridad Pública y del Estado. (EC Asamblea Nacional 2009, 2)

La primera función del Sistema Nacional de Inteligencia se detalla en el Artículo 15, literal a:

> Elaborar el Plan Nacional de Inteligencia, bajo los lineamientos y objetivos de estado y de gobierno establecidos por el Presidente de la República, plan que entre otros aspectos deberá contener las metas periódicas de sus acciones y los procedimientos de coordinación entre las diversas entidades que conforman el Sistema Nacional de Inteligencia. Plan que deberá ser aprobado por el Presidente de la República. (EC Asamblea Nacional 2009, 7)

El 30 de septiembre de 2010 se publica el Reglamento a la Ley de Seguridad Pública y del Estado en el Registro Oficial Suplemento 290, expedido por Rafael Correa (EC Presidencia Constitucional de la República 2010).

Del Reglamento a la Ley de Seguridad Pública y del Estado, se enfatizan los siguientes artículos: art. 6, art. 7, art. 8, y art. 9, lit. d, detallados a continuación:

> Art. 6.- Del Sistema Nacional de Inteligencia.- Es el conjunto de organismos de inteligencia independientes entre sí, funcionalmente coordinados y articulados por la Secretaría Nacional de Inteligencia, que ejecutan actividades específicas de inteligencia y contrainteligencia, para asesorar y proporcionar inteligencia estratégica a los niveles de conducción política del Estado, con el fin de garantizar la soberanía nacional, la seguridad pública y del Estado, el buen vivir y defender los intereses del Estado. (EC Presidencia Constitucional de la República 2010, 3)

> Art. 7.- De los organismos que conforman el Sistema Nacional de Inteligencia.- Conformarán este Sistema, las siguientes instituciones: a. La Secretaría Nacional de Inteligencia; b. Los Subsistemas de Inteligencia Militar; c. Los Subsistemas de Inteligencia Policial; d. La Unidad de Inteligencia Financiera; e. El Servicio de Protección Presidencial; f. El Departamento de Inteligencia Tributaria del Servicio de Rentas Internas; g. La Dirección Nacional de la Unidad de Vigilancia Aduanera del Servicio Nacional de Aduana del Ecuador; y, h. Unidad de Gestión de Seguridad Interna de la Presidencia de la República. (EC Presidencia Constitucional de la República 2010, 3)

> Art. 8.- De la Secretaría Nacional de Inteligencia.- La Secretaría Nacional de Inteligencia es el órgano rector del Sistema Nacional de Inteligencia, con rango de Ministerio de Estado, responsable de producir inteligencia, inteligencia estratégica y contrainteligencia. (EC Presidencia Constitucional de la República 2010, 3)

Se indica en el lit. d del art. 9, correspondiente a la competencia de la Secretaría Nacional de Inteligencia: “Realizar la adquisición de equipos y tecnología, y contratar la prestación de servicios de acuerdo con la normativa especial establecida para la ejecución de operaciones encubiertas de inteligencia y seguridad” (EC Presidencia Constitucional de la República 2010, 3).

Como se ha mencionado y frente a los eventuales riesgos y amenazas en el ámbito del ciberespacio, Ecuador no se ha mantenido ajeno a este tema en particular, puesto que a partir del año 2009 creó sus propios mecanismos de respuesta anclados a redes informáticas con aplicaciones relacionadas a la seguridad y defensa. Acorde a la política del gobierno de Rafael Correa, Ecuador promulgó como tema de interés y vanguardia la inversión en tecnología, especialmente en el acceso al internet y universalización de acceso a redes (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2014).

En este ámbito, se evidenció la mejora sustancial de trámites ciudadanos, así como la conectividad a nivel nacional para datos abiertos y el uso de la banca y comercio electrónico. Sin embargo, para potenciar este sector se requiere del establecimiento de políticas, regulaciones y estrategias claras para lograr niveles óptimos de control del ciberespacio, que contribuyan a la seguridad y defensa del Estado. Ecuador apostó a los datos abiertos como parte de la transparencia en la gestión pública, información que según el Centro Andino de Estudios Estratégicos no compromete la Seguridad Nacional, ni la privacidad de los ciudadanos, ya que el *Open Data* en nuestro caso, está normado y solo se puede publicar lo que la Ley Orgánica de Transparencia y Acceso a la Información Pública faculta (Ramos 2014).

Seguidamente se mencionan algunas políticas, instrumentos estratégicos nacionales relacionados a la ciberseguridad y ciberdefensa, en el Ecuador, se inicia en el 2013 con la expedición del primer esquema gubernamental de seguridad de la información (EGSI) basado en la norma ISO 27001:2013, por la Secretaría Nacional de la Administración Pública (SNAP) que buscaba brindar seguridad en el uso de *internet* a los usuarios, y tenía como objetivo implementar controles para garantizar la confidencialidad, integridad y disponibilidad de la información que se gestionan en las instituciones de Estado (EC Secretaría Nacional de la Administración Pública 2013b).

En el 2014 se crea el Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT) (EC Centro de Respuesta a Incidentes de la ARCOTEL 2014), "creado mediante Resolución ST-2014-0247 del 18 de julio de 2014 (EC Ministerio de Telecomunicaciones y la Sociedad de la Información 2018, 43), el mismo que al tomar un grado de madurez, llegó a formar parte de *FIRST* (*Forum of Incident Response and Security Teams*) (Foro de equipos de seguridad y respuesta a incidentes) (Forum of Incident Response and Security Teams 2014).

El Equipo del Centro de Respuesta a Incidentes de Seguridad Nacional (EcuCERT) opera bajo la Agencia para la Regulación y Control de las Telecomunicaciones (ARCOTEL) está regida por la Ley Orgánica de Telecomunicaciones, es el punto de contacto nacional e internacional para la coordinación de la respuesta de gestión de incidentes cibernéticos. Actualmente se limita a los operadores de redes de telecomunicaciones, por lo que no tiene mandato ni competencias suficientes para operar completamente a nivel nacional. Existen otros CERT o CSIRT en los sectores académicos, privado y financiero y un CERT militar. Sin embargo, falta una instancia para reaccionar a los incidentes cibernéticos de manera centralizada y

coordinada, así como tampoco existe un enfoque unificado para la notificación de incidentes y los mecanismos son variables entre los CERT. A nivel internacional EcuCERT es socio activo de CSIRTAmericas de la OEA y mantiene una relación de colaboración con otros CERT regionales (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022b, 24).

En el mismo año 2014, en base al Acuerdo Ministerial 281, del Ministerio de Defensa Nacional, se crea el Sistema de Ciberdefensa, dentro del cual se crea el Comando de Ciberdefensa (COCIBER), integrado por personal técnico de las tres ramas de las Fuerzas Armadas (El Universo 2014).

En el Plan Estratégico Institucional de la Defensa 2017-2021 se establece que aunque hay pocas posibilidades de una guerra convencional en la región sudamericana, el Ecuador enfrenta muchas amenazas a su seguridad y soberanía: "la inseguridad ciudadana, el crimen transnacional organizado, corrupción, ataque cibernético, el narcotráfico; […] nuevos factores de riesgo: explotación ilegal de recursos naturales y biodiversidad, contrabando de combustibles, minería ilegal" (EC Ministerio de Defensa Nacional 2017, 33–34), por lo que, para combatir esta amenaza, el país necesita un ejército fuerte capaz de construir un aparato de seguridad adecuado para apoyar los esfuerzos contra esta nueva amenaza.

Debido a la antigüedad de varios sistemas tecnológicos, muchos de sus registros pueden ser fácilmente destruidos o accedidos por terceros. Esto tiene el potencial de eliminar o reemplazar actualizaciones de datos importantes y medidas de seguridad defectuosas. Esto afectaría la organización y los intereses de seguridad nacional. Es necesario desarrollar un plan de mejora de la seguridad informática de acuerdo con las medidas de ciberseguridad. Esto requiere la creación de leyes, directrices y lineamientos internacionales para el uso de tecnología y sistemas de información, incluida la seguridad cibernética.

Debido al monitoreo constante de amenazas por parte de las Fuerzas Armadas, deben mejorar constantemente sus capacidades de seguridad cibernética. Esto es importante para proteger los activos digitales en los sectores de gobierno y defensa. El Comando de Ciberdefensa actualmente protege estas áreas de especialización y seguridad cibernética.

Dentro de los objetivos estratégicos del Plan Estratégico Institucional de la Defensa 2017-2021 se considera "Fortalecer las capacidades de ciberdefensa para

proteger las áreas críticas y objetivos estratégicos del Estado" (EC Ministerio de Defensa Nacional 2017, 85).

El 21 de septiembre de 2018, mediante Decreto Presidencial N° 526, se crea el Centro de Inteligencia Estratégica (CIES) que consta en el Suplemento del Registro Oficial N° 358, del 30 de octubre de 2018 (EC Presidencia Constitucional de la República 2018). A continuación, se hace referencia a los arts.1 y 2 del decreto:

> Art. 1.- Suprímase la Secretaría de Inteligencia.
> Art. 2.- Créase el Centro de Inteligencia Estratégica (CIES) como el ente rector del Sistema Nacional de Inteligencia. Es una entidad de derecho público, con personalidad jurídica, patrimonio propio, autonomía administrativa y financiera, con sede en la ciudad de Quito. (EC Presidencia Constitucional de la República 2018, 7)

En el año 2018, la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), expide una "Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de las redes y servicios de telecomunicaciones" (EC Agencia de Regulación y Control de las Telecomunicaciones 2018, 7).

En el Libro Blanco de la Sociedad de la Información y del Conocimiento 2018, se menciona sobre el Estudio 2017, realizado por la empresa Deloitte a empresas nacionales y multinacionales. De igual manera el Estudio 2017 realizado por la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA) a varias universidades ecuatorianas en materia de Seguridad de la Información. Dichos estudios indican que se "debe mejorar la gestión de la seguridad de la información tanto en la Academia, así como en las empresas" (EC Ministerio de Telecomunicaciones y la Sociedad de la Información 2018, 41).

El Índice Global de Ciberseguridad (GCI), publicado por la Unión Internacional de Telecomunicaciones (UIT), en 2017, señala que Ecuador ocupa el puesto 66 de 193 países a nivel mundial y el 6° de América Latina y el Caribe (EC Ministerio de Telecomunicaciones y la Sociedad de la Información 2018, 42).

El Esquema Gubernamental de Seguridad de la Información (EGSI), requiere que todas las organizaciones sigan sus pautas de gestión de seguridad de la información. Estos lineamientos requieren que todas las organizaciones utilicen las Normas Técnicas Ecuatorianas, NTE INEN-ISO/IEC 27000 (EC Servicio Ecuatoriano de Normalización 2016), para la gestión de la seguridad de la información. Hasta el 25 de abril de 2018, solo el 16,36% de las organizaciones obtuvieron un buen resultado y cumplieron con el

esquema de cumplimiento del EGSI. Las autoridades competentes están realizando esfuerzos futuros para aumentar la implementación de las reglas del esquema (EC Ministerio de Telecomunicaciones y la Sociedad de la Información 2018, 42–43).

Los niños, niñas y adolescentes corren un mayor riesgo de exposición a cualquier amenaza relacionada con las Tecnologías de la Información y la Comunicación (TIC). Esto se debe a que la calidad de vida de las personas depende de la utilidad de las TIC. Los niños y adolescentes son vulnerables a los riesgos que implican el uso inadecuado de Internet. También corren un mayor riesgo de sufrir: "ciberadicción (IAD), *cybergrooming*, *sexting*, *sextortion*, *cyberbullying*, pornografía infantil […] delitos como violación a la intimidad personal y familiar […] violencia sexual, explotación sexual […]" (EC Ministerio de Telecomunicaciones y la Sociedad de la Información 2018, 44; énfasis añadido).

Según Libro Blanco de la Sociedad de la Información y del Conocimiento del 2018 hasta esta fecha, Ecuador era uno de los países de América de Sur que no tenía una Ley de Protección de Datos Personales, así como Venezuela, Bolivia, Surinam, Guyana. El tratamiento de datos personales sin el pensamiento y la consideración adecuados, la información de las personas se ve comprometida. La recopilación, el procesamiento y la transferencia irresponsables de datos pueden causar daños graves. Los datos se pueden recopilar, procesar y transferir sin el conocimiento del público, esto puede dar lugar a graves violaciones de los derechos humanos, como el derecho a la vida, la salud y el acceso a los servicios públicos entorpeciendo las operaciones esenciales de la sociedad. Pero, esto puede generar una gran cantidad de beneficios si se aplica el tratamiento de datos personales de manera adecuada.

Para la Política de la Defensa Nacional del Ecuador "Libro Blanco" 2018, la infraestructura digital y los servicios esenciales del estado, requieren protección contra ataques cibernéticos que pueden socavar la seguridad nacional. Para evitar las violaciones de la infraestructura crítica, los estados también pueden reforzar sus capacidades de ciberdefensa, así como obtener beneficios de la cooperación internacional. Los ciberataques paralizantes y los ciberdelitos basados en la explotación de sistemas digitales a través de métodos "[…] tecnológicos de ciberterrorismo, ciberdelito, cibercrimen, ciberespionaje, e infiltración de los sistemas informáticos […]" (EC Ministro de Defensa Nacional 2018, 53). Estos se clasifican como herramientas de agresión contra infraestructuras críticas y pueden ser dañinas para la seguridad nacional.

Debido al estado actual del sistema internacional y la creciente popularidad de la palabra "seguridad", todo tipo de inteligencia debe reflexionar sobre sus ideas y métodos. Los agentes de inteligencia deben incorporar múltiples procesos y niveles de análisis para comprender los riesgos y amenazas a nivel estratégico y político. También tienen la tarea de comprender y anticipar futuras amenazas al país para prevenirlas. En tiempos de paz, las agencias de inteligencia también deben comprender la posibilidad de utilizar los problemas en beneficio del gobierno. En el Plan Específico de Inteligencia 2019-2030 se plasma el siguiente concepto:

> inteligencia estratégica como la actividad de obtención, sistematización, análisis y difusión oportuna de inteligencia, para alertar y asesorar en la toma de decisiones en el más alto nivel, buscando prevenir, evitar o desactivar amenazas y riegos que afecten a la seguridad integral e identificar oportunidades para el Estado que logren condiciones de gobernabilidad al interior y su posicionamiento estratégico en el entono regional y mundial. (EC Centro de Inteligencia Estratégica 2019, 31)

Es importante también resaltar el concepto:

> **amenaza para el Estado ecuatoriano a todo fenómeno o condición en la que uno o más actores con capacidad y fines específicos generan un daño, pérdida o consecuencia negativa directa contra los ejes de protección de la seguridad integral del Estado, entendiendo a estos como ser humano, Estado y naturaleza.** (EC Centro de Inteligencia Estratégica 2019, 33; 35; énfasis en el original)

Tabla 5
Determinación de amenazas para el Estado ecuatoriano

AMENAZAS PARA EL ESTADO ECUATORIANO
Agresión armada externa de actores no estatales
Incidencia del crimen organizado transnacional en Ecuador
Acciones terroristas con diversas motivaciones
Acciones contra el Estado en el ciberespacio
Degradación ambiental
Limitación en el desarrollo económico sostenido y sustentable por presencia de flujos económico ilícitos

Fuente: Centro de Inteligencia Estratégica (EC Centro de Inteligencia Estratégica 2019, 35)
Elaboración: Centro de Inteligencia Estratégica

Para nuestro trabajo de investigación podemos referirnos a la amenaza: Acciones contra el Estado en el ciberespacio listada en la Tabla 5.

De acuerdo al Plan Específico de Seguridad Pública y Ciudadana 2019-2030 se plantea trabajar sobre los delitos transnacionales, entre ellos ciberdelitos, así como reforzar tecnológicamente a la Unidad de Ciberinteligencia. Los delincuentes utilizan tecnología integrada en las redes informáticas para llevar a cabo sus delitos cibernéticos. Esto se debe a la introducción de nuevas tecnologías de la información y la comunicación

que están causando grandes problemas en la seguridad global. Muchos países no han encontrado soluciones efectivas para investigar estas amenazas a la ciberseguridad, por lo que, se genera una falta de confianza en las instituciones y una disminución en la confianza por parte del público en general. En Ecuador, se reporta un aumento en el fraude en línea debido al aumento en el número de usuarios de Internet y el uso de métodos de pago electrónico (EC Ministerio del Interior 2019).

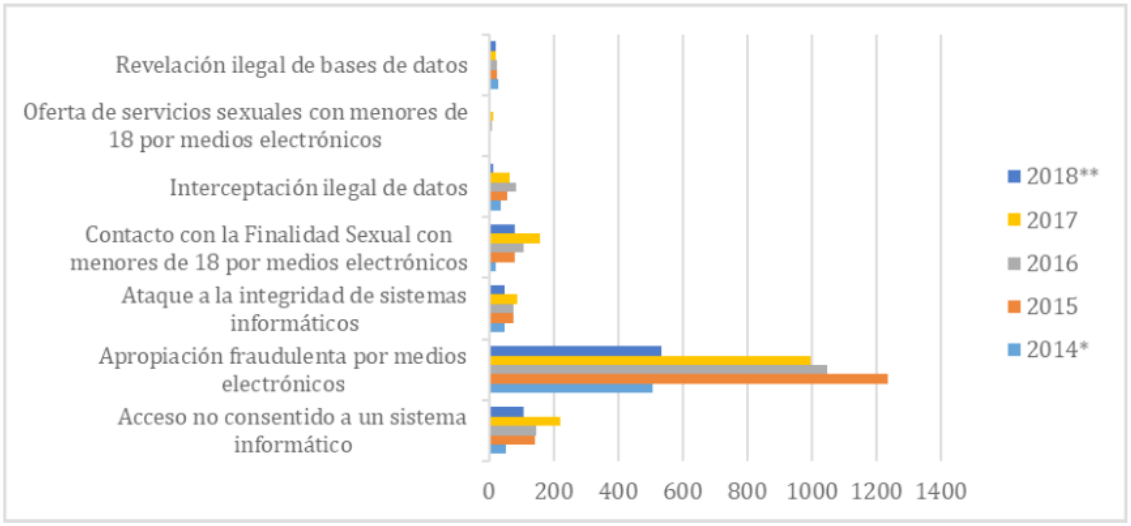

Figura 3. Evolutivo noticias del delito registradas en fiscalía general del Estado.
Fuente: Sistema Integrado de Actuación Fiscal-SIAF, 2018. Elaboración: DCD0, 2019 (EC Ministerio del Interior 2019, 42)

Mantener una economía positiva requiere una presencia segura en Internet y cooperación internacional. En el Plan Específico de Relaciones Exteriores y Movilidad Humana 2019-2030 se resalta que las amenazas en el ciberespacio tienen implicaciones económicas, por lo cual, Ecuador está considerando unirse a la Convención de Budapest sobre Ciberdelincuencia (EC Ministerio de Relaciones Exteriores y Movilidad Humana 2019).

Las amenazas cada vez más misteriosas y globales exigen la cooperación internacional para manejarlas. Estas amenazas incluyen desastres ambientales, explotación de recursos naturales, tráfico de armas, tráfico de drogas, ataques cibernéticos a la infraestructura crítica nacional, grupos hostiles, grupos armados, crimen organizado transnacional y armas e incluso ataques espaciales y marítimos. Además de estas amenazas globales, se dimensionan los territorios nacionales que incluyen el ciberespacio. Esto requiere planificación, preparación y operaciones en todos los dominios del combate: tierra, aire, mar y espacio.

Se identifica como problemática de la defensa según el Plan Específico de Defensa 2019-2020:

> Las amenazas que atentan contra el Estado ecuatoriano son la agresión armada perpetrada por otro Estado concebidas como amenazas tradicionales poco factibles, los grupos irregulares armados, la delincuencia organizada transnacional, el tráfico de armas, municiones y explosivos, el narcotráfico, la degradación ambiental, los desastres naturales, la explotación ilegal de los recursos naturales, los *ciberataques a la infraestructura crítica del Estado* entre otros. […] El ciberespacio implica ampliar la territorialidad, lo que conlleva el incremento de actividades ilegales en esta dimensión. El empleo del manejo de las tecnologías de la información y comunicaciones (TIC) y redes informáticas vulneran la seguridad y defensa de los Estados, a través de ciberataques como: *phishing, hacking, cracking* hasta ciberterrorismo, los cuales pueden afectar la infraestructura crítica del Estado. *Una de las debilidades del Ecuador es la carencia de una política nacional de ciberseguridad*, en relación a la protección de la población, redes informáticas y sistemas de la infraestructura critica. […] *El Estado participará activamente* en el control efectivo del territorio nacional (espacios terrestres, marítimos, aéreos y el ciberespacio) *impulsando el desarrollo de políticas y estrategias para la ciberseguridad, ciberdefensa y defensa aeroespacial*, permitiendo que estas se encuentren en las mejores condiciones para afrontar la amenazas y riesgos que atenten a la paz y seguridad. […] En el ámbito de ciencia y tecnología para la seguridad y defensa se fomentará la cooperación en investigación, desarrollo e innovación (I+D+i), […] de gestión de riesgos, de relaciones internacionales y capacidades de ciberseguridad. (EC Ministerio Defensa Nacional 2019, 22, 24, 49, 50; énfasis añadido)

Como otro documento importante para el avance en torno a las tecnologías digitales en el país es la política Ecuador Digital:

"**La política Ecuador Digital se puso a disposición de la ciudadanía el 17 de mayo de 2019, en el marco del Día Mundial de las Telecomunicaciones, bajo la disposición del ex Presidente de la República, Lenin Moreno Garcés, y del ex Ministro de Telecomunicaciones y de la Sociedad de la información, Andrés Michelena Ayala**" (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2019a, párr.10; énfasis en el original); sin embargo, fue expedida con Acuerdo Ministerial No. 15-2019, del 18 de julio del 2019 y publicado en el Registro Oficial 69 de 28-oct.-2019 (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2019c).

> El programa Ecuador eficiente y ciberseguro tiene como objetivo proteger a la sociedad frente a las amenazas cibernéticas, generar confianza en el uso del internet y fomentar el desarrollo económico y social basado en el uso de las Tecnologías de la Información y Comunicaciones (TIC). (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2021, 4)

Para el año 2020, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), con Acuerdo Ministerial No. 025-2019, emite una segunda

versión del esquema gubernamental de seguridad de la información (EGSI) versión 2.0. (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2020). Incluyendo nuevos requisitos normativos a tener en consideración para la actualización e implementación de EGSI, mismo que difiere de manera considerable respecto a las disposiciones emitidas en su primera versión. Añade el ciclo de mejora continua: planificar, hacer, verificar, actualizar y que busca preservar la confidencialidad, integridad y disponibilidad de la información.

Mediante la aplicación de un proceso de gestión de riegos de seguridad de la información y la sección de controles para el tratamiento de los riesgos identificados con las Normas ISO 27000/27001, 27032 respecto a ciberseguridad, concienciación de Riesgos de Seguridad. Definir una mejora continua con la implantación, mantenimiento y revisión de riesgos y controles orientados a la protección de la información, y tendrá relación con el proyecto de ley para la Protección de los Datos Personales en Ecuador.

A finales del 2020, el Comando Conjunto de las Fuerzas Armadas, dentro de las competencias que tiene, actualizó y generó 33 cuerpos doctrinarios al nivel estratégico militar, creando el Manual Militar de Operaciones de Ciberdefensa 2020. El cual "describe el ciberespacio como dominio de la guerra, su relación con las operaciones militares en los otros dominios. Además, explica las operaciones de ciberdefensa y las tareas del Comando de Ciberdefensa" (EC Comando Conjunto de las Fuerzas Armadas 2020, vi).

El gobierno electrónico se refiere a la prestación eficiente y eficaz de servicios mediante el uso de la tecnología de la información. En particular, esto se aplica a la provisión de beneficios a empresas y ciudadanos a través de las TIC. Al integrar operaciones y procesos, el gobierno electrónico reduce el costo y el tiempo de las transacciones públicas. Esto da como resultado una productividad general mejorada a través de una mejor integración del esfuerzo y los procesos de trabajo con un uso eficiente de los recursos.

El Plan Nacional de Desarrollo 2021-2025 describe la condición económica deseada para Ecuador. Una institución eficiente y eficaz que proteja la libertad individual al mismo tiempo que se esfuerza por lograr una economía competitiva es uno de los requisitos de la política. Además de estas exigencias, el programa prevé el establecimiento de instituciones eficaces que salvaguarden la libertad individual para producir una economía competitiva. El Plan Nacional de Desarrollo de Ecuador señala cómo gestionar los ingresos y el empleo. También pretende mejorar la seguridad de

Internet y la integración nacional de las TIC. También se mejorarán los servicios de calidad, así como la conectividad a Internet (EC Secretaría Nacional de Planificación 2021, 2021–25).

Actualmente el Ecuador, a través del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), con Acuerdo Ministerial 006-2021, documentado en el No. 479 del Quinto Suplemento del Registro Oficial, del 23 de junio de 2021, publicó la Política Nacional de Ciberseguridad (PNC), aunque fue creado el 17 de mayo, aún bajo el gobierno del presidente Lenin Moreno, y contiene siete pilares:

> I) Gobernanza de la ciberseguridad […] II) Sistemas de información y gestión de incidentes […] III) Protección de la infraestructura crítica digital y servicios esenciales […] IV) Soberanía y defensa […] V) Seguridad pública y ciudadana […] VI) Diplomacia en el ciberespacio y cooperación internacional […] VII) Cultura y educación de ciberseguridad […]. (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2021, 39-42)

El desafío que se tiene es la implementación, monitoreo y evaluación. A pesar de haber alcanzado la generación de la Política Nacional de Ciberseguridad (PNC), aún existe consciencia qué como país, Ecuador, se tiene mucho por avanzar para llegar a consolidar un ciberespacio más seguro.

Tabla 6

Pilares, objetivos y responsabilidades de la Política Nacional de Ciberseguridad del Ecuador

PILAR	OBJETIVO	INSTITUCION RESPONSABLE
I. Gobernanza de la ciberseguridad	OBJETIVO 1	Ministerio de Telecomunicaciones (MINTEL)
II. Sistemas de información y gestión de incidentes	OBJETIVO 2	Ministerio de Telecomunicaciones (MINTEL)
III. Protección de la infraestructura crítica digital y servicios esenciales.	OBJETIVO 3	Ministerio de Defensa Nacional (MDN)
IV. Soberanía y defensa.		
V. Seguridad pública y ciudadana.	OBJETIVO 4	Ministerio de Gobierno (MDG)
VI. Diplomacia en el ciberespacio y cooperación internacional	OBJETIVO 5	Ministerio de Relaciones Exteriores (MREMH)
VII. Cultura y educación de la ciberseguridad	OBJETIVO 6	Ministerio de Telecomunicaciones (MINTEL)

Fuente: Política Nacional de Ciberseguridad del Ecuador (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2021, 46)
Elaboración: Ministerio de Telecomunicaciones y de la Sociedad de la Información

Con la Política Nacional de Ciberseguridad vigente se plantea pilares, objetivos, coordinación estratégica con las instituciones responsables en temas de ciberseguridad:

1. Gobernanza de la ciberseguridad.

Articular lineamientos y acciones de ciberseguridad nacional (Comité de Ciberseguridad).[16]

2. Sistemas de información y gestión de incidentes.

Proteger sistemas de procesamientos de datos y manejo de incidentes informáticos a través de EcuCERT[17] y CSIRT.[18]

3. Protección de la infraestructura crítica digital y servicios esenciales.

Construir las condiciones necesarias de robustez y resiliencia (MINTEL, MDN, actores públicos y privados involucrados).

4. Soberanía y defensa.

Reconocer el ciberespacio como el quinto dominio donde se cumplen operaciones militares para la defensa del estado (MDN).

5. Seguridad pública y ciudadana.

Proteger derechos y libertades, remediación ante espectro de delitos informáticos en el ciberespacio (MDG, PN,19 Fiscalía y Sistemas Judicial).

6. Diplomacia en el ciberespacio y cooperación internacional.

Fomentar la ciberseguridad internacional, derechos humanos, desarrollo sostenible, comercio mundial. Seguridad de la información en servicios exteriores (MREMH).

7. Cultura y educación de la ciberseguridad.

Desarrollar educación en el ámbito de seguridad en el ciberespacio, para fomentar la cultura de ciberseguridad (MINTEL, ME,20 Academia).

De igual manera, en junio 2021, el Ministerio de Defensa, mediante acuerdo ministerial 199, expide su Estrategia de Ciberdefensa 2021, la misma que "[…] se enlaza con los diferentes documentos[21] de planificación nacional vigentes en el ámbito de la seguridad y defensa […]" (EC Ministerio de Defensa Nacional 2021b, 23).

---

[16] Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), Secretaría Nacional de la Administración Pública (SNAP), Ministerio de Gobierno (MDG), Ministerio de Defensa Nacional (MDN), Centro De Inteligencia Estratégica (CIES), Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH)

[17] Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones, ARCOTEL. https://www.ecucert.gob.ec/

[18] Listado CSIRTS EC. https://csirt.ec/csirts-en-ecuador/listados/

[19] Policía Nacional del Ecuador.

[20] Ministerio de Educación.

[21] El Plan Sectorial de Defensa 2017-2021 […]. La Política de Defensa Nacional 2018 […]. El Libro Blanco de la Sociedad de la Información y del Conocimiento (2018), […]. El Libro Blanco de Línea de Investigación, Desarrollo e Innovación y Transferencia de Conocimiento en TIC

Esta Estrategia de Ciberdefensa 2021 dentro de su alcance tiene como propósito:

> Establecer lineamientos que orienten el fortalecimiento de la ciberdefensa como una capacidad necesaria en el cumplimiento de la misión constitucional de la Defensa, para estar en condiciones de realizar operaciones de defensa, exploración y respuesta a los efectos producidos por los ciberataques, asegurando una defensa efectiva de las infraestructuras digitales consideradas críticas. (EC Ministerio de Defensa Nacional 2021b, 33)

Los gobiernos, las organizaciones privadas y las involucradas en la seguridad cibernética tienen objetivos comunes: proteger a las personas que realizan actividades y generan conocimiento en el ciberespacio. Todos interactúan y comparten información a través de plataformas y repositorios comunes. Los países que mejoran la capacidad de defensa contra los ataques cibernéticos pueden aprovechar la cooperación y el liderazgo transfronterizos. "La ciberdefensa y la ciberseguridad son parte de la seguridad digital" (EC Ministerio de Defensa Nacional 2021b, 38).

> El Ministerio de Defensa Nacional tiene la responsabilidad de la rectoría de la ciberdefensa en el Ecuador, con la finalidad de defender la infraestructura crítica digital y servicios esenciales del Estado e infraestructura crítica digital del sector Defensa en el ciberespacio, emplear la ciberdefensa en la defensa de la soberanía e integridad territorial, contrarrestar el ciberterrorismo, y fortalecer la inteligencia y contrainteligencia en el ciberespacio. (EC Ministerio de Defensa Nacional 2021b, 40)

Seguidamente se desarrolla la Guía Política – Estratégica de Ciberdefensa 2021, que dentro de su contenido hace referencia al ciberespacio como escenario de confrontación, detalla los activos a defender. Describe algunas definiciones de amenazas, presenta el fundamento político–estratégico de la ciberseguridad y ciberdefensa en la sociedad de la información y del conocimiento y presenta la aplicación de la ciberdefensa en Ecuador. Esta Guía Política-Estratégica de Ciberdefensa 2021 está sustentada en los documentos de políticas, estrategias y planes: "el Plan Nacional de Seguridad Integral 2019-2030, el Plan Específico de Defensa Nacional 2019-2030, el Plan Específico de Inteligencia 2019-2030, la Política de Defensa Nacional 2018" .

Las Fuerzas Armadas tienen su misión establecida en el ciberespacio para combatir con amenazas externas estatales o transnacionales: delincuencia organizada, ataques asimétricos mediante el terrorismo y ciberataques, las mismas que se ven

---

> (2019), […]. El Plan Nacional de la Sociedad de la Información del Conocimiento 2018-2021, […]. El Plan Nacional de Seguridad Integral 2019-2030, […]. El Plan Específico de Defensa Nacional (PED) 2019-2030, […]. La Política Nacional de Ciberseguridad 2021, […]. (EC Ministerio de Defensa Nacional 2021b, 23–25)

afectadas a las políticas, planificación estratégica y toma de decisiones. Por lo que se establece un nuevo "*enfoque de gestión de ciberdefensa*" (EC Ministerio de Defensa Nacional 2021a, 63; énfasis añadido) en el cual conlleva a la protección de infraestructuras críticas digitales y servicios esenciales, análisis de riesgo, y mantener una cooperación interinstitucional e internacional.

Figura 4. Modelo de aplicación de la Ciberdefensa.
Fuente: Subsecretaría de Defensa (citado en EC Ministerio de Defensa Nacional 2021a, 64)

El 26 mayo 2021, la Asamblea Nacional expide la Ley Orgánica de Protección de Datos Personales de Ecuador, de la cual es importante conocer su objeto y finalidad de acuerdo al artículo 1:

> El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela. (EC Asamblea Nacional 2021b, 9)

Dentro de esta Ley Orgánica de Protección de Datos Personales de Ecuador se considera fundamental conocer los integrantes que forman parte del sistema de protección de datos personales, los mismos que se describen en el artículo 5:

1) Titular;
2) Responsable del tratamiento;
3) Encargado del tratamiento;
4) Destinatario;
5) Autoridad de Protección de Datos Personales; y,
6) Delegado de protección de datos personales. (EC Asamblea Nacional 2021b, 14)

Esta ley busca la protección para el titular de los datos personales, mientras exista un consentimiento para el tratamiento de sus datos, será el único medio para hacer uso de los datos personales de los titulares. Esta ley de protección de datos personales determina los principios de:

> a) Juridicidad […]. b) Lealtad […]. c) Transparencia […]. d) Finalidad […]. e) Pertenencia y minimización de datos personales […]. f) Proporcionalidad del tratamiento […]. g) Confidencialidad […]. h) Calidad y exactitud […]. i) Conservación […]. j) Seguridad de datos personales […]. k) Responsabilidad proactiva y demostrada […]. l) Aplicación favorable al titular […]. m) Independencia del control […]. (EC Asamblea Nacional 2021b, 16–19)

Se incluye también medidas relacionados con la seguridad, protección, análisis de riesgo, amenazas y vulnerabilidades, emergencias a incidentes informáticos de datos personales. De acuerdo a la ley se establece un Registro Nacional de protección de datos personales en el cual estará liderada por la Autoridad de Protección de Datos Personales o Superintendente de Protección de Datos quien:

> […] es el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, […] se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley y en su reglamento de aplicación […]. (EC Asamblea Nacional 2021b, 60)

Y quien recibirá la información actualizada por parte del responsable del tratamiento de datos personales. Incluye temáticas sobre las obligaciones del responsable, encargado y delegado de protección de datos personales, medidas correctivas, infracciones y régimen sancionatorio; en el caso de incumplimiento de la ley de protección de datos hasta mayo 2023 se aplicará el régimen sancionatorio.

En la sección anexos se mencionan algunos escenarios de amenazas de seguridad cibernética los mismos por lo cual el "asambleísta Rodrigo Fajardo (ID) entrega Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia" (EC Asamblea Nacional 2021a), el 19 de octubre de 2021.

De acuerdo a portal web de la Asociación de Bancos del Ecuador (ASOBANCA) se tiene el siguiente extracto:

> Establece un sistema de seguridad digital, bajo componentes o subsistemas de ciberseguridad y ciberdefensa, que permitan enfrentar los riesgos y amenazas cibernéticas, con la y coordinación participación del sector público y privado. Se proponen reformas, por ejemplo en el Código Monetario, para que la Junta de Política y Regulación Financiera, tenga la función de prevenir y erradicar delitos informáticos en la operación y funcionamiento de las entidades financieras, y otras, mediante la

> implementación de buenas prácticas de ciberseguridad y estándares internacionales y el avance tecnológico. Y que la Superintendencia de Bancos pueda exigir que las entidades controladas implementen medidas correctivas en delitos informáticos y tecnológicos, e imponer sanciones por incumplimiento en políticas de ciberseguridad. (Asociación de Bancos del Ecuador 2021, párr. 1)

Este Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia 2021 que entrará en vigencia a partir de la publicación en el Registro Oficial, a la fecha actual es un proyecto que se encuentra en revisión por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). Es importante resaltar los siguientes artículos para tener una visibilidad de este proyecto en curso.

> **Artículo 1.- Objeto.-** El objeto de la presente Ley es establecer un Sistema de Seguridad Digital, con los componentes o subsistemas de ciberseguridad, ciberdefensa que permita prevenir, combatir, reaccionar, neutralizar, manejar la o las crisis y recuperar información en caso de amenazas, riegos y/o ataques informáticos con la participación de los diferentes organismos públicos y privados para coordinar las acciones del Estado y promover la seguridad digital en los distintos niveles del gobierno y de la ciudadanía en el ciberespacio […]. (Rodrigo 2021, 7–8)

> **Artículo 2.- Ámbito.-** El ámbito de aplicación de la ley está encaminada a la facultad de ejecución de políticas públicas, operaciones de ciberseguridad, ciberdefensa, ciberinteligencia dentro del territorio nacional y en el exterior con la colaboración internacional respectiva, teniendo como finalidad la de prevenir y mitigar toda actividad cibernética maliciosa que ponga en riesgo la seguridad integral del estado ecuatoriano, la soberanía y la protección de los derechos de la ciudadanía en general. (Rodrigo 2021, 8)

> **Artículo 5.- Sistema Nacional de Seguridad Digital.-** Es el conjunto de subsistemas, instituciones, políticas, estrategias, normativas, planes, programas, con el fin de efectuar la conducción estratégica de la seguridad digital del Estado en la prevención y respuesta, para enfrentar los desafíos, riesgos y amenazas que afectan al ejercicio de los derechos y libertades de sus ciudadanos en el ciberespacio, sistemas informáticos y la red. (Rodrigo 2021, 9)

Este proyecto propone también la reforma a la "Ley Orgánica de Datos Personales, en su artículo 76.- Funciones atribuciones y facultades" (Rodrigo 2021, 19), incorporando el literal: "18) Entregar un informe trimestral de riesgos, ataques informáticos registrados en relación a la protección de datos, al ente rector del Sistema Nacional de Seguridad Digital, para su análisis y decisión en la generación de políticas públicas" (Rodrigo 2021, 19).

Una vez detallados los conceptos de ciberseguridad en el capítulo primero, es importante realizar la descripción de la ciberseguridad a nivel del Estado ecuatoriano, la cual se define como "la capacidad del Estado para proteger a las personas, sus bienes activos de información y servicios esenciales ante riesgos y amenazas que se identifiquen

en el ciberespacio" (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2021, 15; énfasis añadido).

En el Gobierno del presidente Guillermo Lasso, el 16 de junio del 2022, se presenta la Estrategia Nacional de Ciberseguridad a través de la ministra de Telecomunicaciones y de la Sociedad de la información, Vianna Maino, con el cual se espera fortalecer la ciberseguridad del Ecuador, esta estrategia fue elaborada con la asesoría técnica del "Proyecto de Resiliencia Cibernética para el Desarrollo de la Unión Europea (Cyber4Dev) y el programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos (CICTE/OEA)" (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022a, párr. 2).

Participaron actores de sector privado, académico, expertos en ciberseguridad y representantes del Comité Nacional de Ciberseguridad conformado por los "Ministerios de Telecomunicaciones y de la Sociedad de la Información, Defensa Nacional, Gobierno, Interior, Relaciones Exteriores y Movilidad Humana, Centro de Inteligencia Estratégica y Secretaría General de la Administración Pública de la Presidencia" (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022b, 3).

Esta estrategia contempla los siguientes seis ejes de acción: "Gobernanza y coordinación nacional; Resiliencia cibernética; Prevención y combate a la ciberdelincuencia; Ciberdefensa; Habilidades y capacidades de ciberseguridad; y Cooperación internacional" (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022b, 3). Los mismos que tendrán que ser aplicados en el período de 3 años desde el 2022 al 2025.

Tabla 7

Pilares, objetivos de la Estrategia Nacional de Ciberseguridad del Ecuador

<table>
<tr><td colspan="3">PILAR 1:
GOBERNANZA Y COORDINACIÓN NACIONAL</td></tr>
<tr><td colspan="3">Objetivo 1.1: Establecer un marco integral de gobernanza de la ciberseguridad
Objetivo 1.2: Fomentar una comunidad sólida y articulada con expertos en ciberseguridad de las múltiples partes interesadas
Objetivo 1.3: Desarrollar un marco legal y regulatorio integral que permita la gobernanza nacional de la ciberseguridad y la ciberdefensa</td></tr>
<tr><td>PILAR 2:
RESILIENCIA CIBERNÉTICA</td><td rowspan="2">PILAR 3:
PREVENCIÓN Y COMBATE A LA CIBERDELINCUENCIA</td><td rowspan="2">PILAR 4:
CIBERDEFENSA</td></tr>
<tr><td>Objetivo 2.1: Establecer un proceso integral para la gestión de riesgos de ciberseguridad y preparación para afrontar crisis cibernéticas con el fin de fortalecer dichas capacidades a nivel nacional

Objetivo 2.2: Adoptar un marco integral para la identificación, orientación y supervisión de los operadores de infraestructuras de información crítica nacionales

Objetivo 2.3: Continuar desarrollando capacidades de respuesta y gestión de incidentes cibernéticos y del CERT nacional

Objetivo 2.4: Maximizar el uso de tecnologías avanzadas y la innovación en el diseño de políticas y procesos ágiles para el desarrollo de capacidades de Ciberinteligencia</td><td>Objetivo 3.1: Actualizar el marco legal y regulatorio de Ecuador en materia de ciberdelincuencia para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio

Objetivo 3.2: Fortalecer la respuesta oportuna y las capacidades operacionales de investigación y judicialización de la cibercriminalidad.</td><td>Objetivo 4.1: Incrementar y fortalecer las capacidades de Ciberdefensa del Estado ecuatoriano para alcanzar la actitud estratégica defensiva definida en la Política de la Defensa Nacional, para la protección de la infraestructura crítica digital (ICD) y servicios esenciales en el ciberespacio.</td></tr>
<tr><td colspan="3">PILAR 5:
HABILIDADES Y CAPACIDADES DE CIBERSEGURIDAD</td></tr>
<tr><td colspan="3">Objetivo 5.1: Mejorar y ampliar la concientización sobre la ciberseguridad a todos los niveles de la sociedad
Objetivo 5.2: Reforzar las habilidades en materia de ciberseguridad necesarias con las múltiples partes interesadas
Objetivo 5.3: Asegurar que el sistema educativo imparta conocimientos y fortalezca habilidades en materia de ciberseguridad</td></tr>
<tr><td colspan="3">PILAR 6:
COOPERACIÓN INTERNACIONAL</td></tr>
<tr><td colspan="3">Objetivo 6.1: Identificar las prioridades internacionales de Ecuador y desarrollar la capacidad de participar en la ciberdiplomacia regional e internacional
Objetivo 6.2: Fortalecer la participación de Ecuador en la cooperación bilateral, regional e internacional en respuesta a las amenazas en el ciberespacio</td></tr>
</table>

Fuente: Estrategia Nacional de Ciberseguridad del Ecuador (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022b, 15)

Elaboración: Ministerio de Telecomunicaciones y de la Sociedad de la Información

Ecuador cuenta con una Estrategia Nacional de Ciberseguridad que delinea un plan inicial de ciberseguridad. No obstante, la estrategia señala que las empresas todavía luchan con el desarrollo digital y la gobernanza nacional, se han visto afectadas en gran medida por los ataques cibernéticos. Una visión nacional de ciberseguridad debe incluir objetivos claros, un plan de acción y un marco para la gobernanza de la ciberseguridad. Actualmente no existe un marco a nivel nacional. La ciberseguridad no tiene roles, responsabilidades o funciones definidas. Además, no existe una propuesta de plan de cooperación internacional en materia de reparto de responsabilidades en ciberseguridad.

Ecuador necesita una estrategia nacional de ciberseguridad para gestionar adecuadamente su entorno digital. Además, se deben tener en cuenta los marcos legales y regulatorios vigentes relacionados con el mundo digital. Esto es importante para garantizar la gobernanza eficaz general del sector. Los planes de adaptación del ciclo de vida deben evaluarse y revisarse continuamente. Esto es para determinar la eficacia de cada fase y para asegurar la continuidad adecuada entre las fases. Además, el seguimiento y la planificación adecuados están respaldados por datos. Por lo tanto, los sectores público y privado deben trabajar juntos en los niveles estratégico y operativo. Los avances en ciberseguridad se basan en procesos nacionales, medidas clave y decisiones estratégicas. Mediante el uso de la planificación presupuestaria, los gastos operativos, las inversiones específicas, los mecanismos de apoyo al presupuesto nacional y los indicadores clave de acción y progreso, los países pueden aprovechar sus recursos para mejorar la ciberseguridad.

La Comisión Nacional de Ciberseguridad es el órgano que toma las decisiones y tiene en cuenta las consideraciones estratégicas. Sus funciones principales son comprender el intercambio de conocimientos, facilitar el desarrollo estratégico y facilitar la colaboración entre comunidades. Para lograr estos objetivos, el comité está coordinado por miembros de la comunidad de ciberseguridad para apoyar a la ciberseguridad con el intercambio de información. También se espera crear cooperación operativa, estructuras legales y regulatorias transparentes, academia y gobierno de la sociedad civil. Las empresas privadas y otras organizaciones no gubernamentales y ONG también forman parte de la ciberseguridad.

La resiliencia cibernética nacional de un país incluye la preparación, la respuesta y la recuperación de una crisis cibernética. Esto es necesario para identificar y gestionar adecuadamente los riesgos de seguridad cibernética junto con capacidades efectivas de preparación y respuesta, así como para la protección de infraestructura crítica gestionando

los riesgos relacionados con la transformación digital, las amenazas nuevas y complejas, los nuevos desarrollos socioeconómicos y la competitividad industrial. También gestiona los riesgos asociados a la competitividad industrial y la dependencia digital, así como la gestión de amenazas externas.

En todo el mundo, tanto los daños naturales a los activos de información como las amenazas a los sistemas de información y los servicios digitales se enfrentan a la ciberseguridad. Las dependencias digitales, la geopolítica y la infraestructura crítica de los países hacen que sus riesgos de seguridad sean únicos. Comprender estas tendencias globales permite a los analistas de seguridad abordar adecuadamente las amenazas.

Cualquier crisis digital implica interrupciones en las operaciones y el entorno de un país. También puede tener repercusiones negativas, como la pérdida de vidas y de ingresos. Para evitar que ocurran crisis digitales, la infraestructura operativa y ambiental crítica debe monitorearse y evaluarse periódicamente.

Después de los eventos recientes, la recuperación del país depende de probar los límites de sus defensas cibernéticas. Se implementa un enfoque de gestión de riesgos para la ciberseguridad a través de un marco de gobernanza. Esto incluye el análisis continuo de amenazas y riesgos potenciales. Tanto la infraestructura digital nacional como los proveedores de servicios de telecomunicaciones requieren evaluaciones continuas de gobernanza. Tanto el sector privado como el gobierno se benefician de los estándares y las mejores prácticas de seguridad cibernética en curso. Cada escenario de indicador de riesgo incluye un plan de contingencia nacional que facilita la capacitación estandarizada en ciberseguridad al personal que labora en cada organización.

Los CERT proporcionan a los gobiernos centrales de información sobre vulnerabilidades e incidentes en sus ciberespacios. También detectan amenazas, investigan cómo identificarlas, desarrollan estrategias para mitigar riesgos, apoyan a los afectados por una amenaza, mantienen la resiliencia y coordinan acciones conjuntas entre varias agencias.

Los ciberdelincuentes utilizan soluciones y plataformas digitales innovadoras para ganar dinero a través de actividades ilegales. Las transacciones en tiempos de la pandemia como el COVID-19 que se realizaron en línea esto ha llevado a un aumento de la ciberdelincuencia en línea en Ecuador, así como el Fraude informático, el robo de identidad y la violación de datos personales y la pornografía infantil. Las investigaciones y la ejecución en Ecuador toman demasiado tiempo debido a la limitada capacidad de aplicación de la ley en delito cibernético.

Ecuador es miembro de INTERPOL y AMERIPOL. El país está actualizando recientemente su sistema legal para facilitar mejor la cooperación con otros países durante el proceso de adhesión a la Convención de Budapest sobre Delitos Cibernéticos. Esto permitirá a Ecuador mejorar las técnicas de investigación y armonizar las leyes con otros signatarios. A pesar de tener una unidad nacional de delitos cibernéticos bajo la Dirección General de Investigación de la Policía Nacional de Ecuador, la unidad carece de los recursos y la mano de obra necesarios para sostenerse. Debido a la falta de recursos, se puede recopilar poca evidencia sobre el delito cibernético. Esto se debe a normas procesales y leyes obsoletas que dificultan la investigación, prevención y sanción de estos delitos, así como la capacidad para rastrear el delito cibernético y producir evidencia.

Originalmente estaba destinado a proteger áreas tradicionales tierra, mar, aire, espacio y ciberespacio. Las ideas para proyectos de desarrollo económico, social y tecnológico de defensa provienen conceptualmente del ciberespacio. Desde sus inicios, la coalición de defensa cibernética ha crecido para incluir intereses más amplios, como organizaciones para la paz y la estabilidad colectivas e incluso infraestructura crítica. El intercambio de información, la investigación y las nuevas ideologías para la defensa cibernética surgen de la investigación académica y los ejercicios militares con cooperación internacional. A través de la cooperación con países y organizaciones extranjeras, el ciberespacio mitiga las amenazas a la ciberseguridad.

Se considera que los usuarios frecuentes de Internet son los principales objetivos para los ciberdelincuentes. Para que Ecuador sea un país ciberseguro, se requiere incrementar profesionales en ciberseguridad. Se puede alentar a ciertos grupos de personas a participar en un comportamiento consciente de la ciberseguridad a través de programas implementados en plataformas y servicios digitales.

Ecuador necesita aumentar la conciencia y la comprensión de la ciberseguridad. No hay suficientes escuelas y programas para abordar este problema. Actualmente no existe un plan nacional formal para abordar esta necesidad. Además, el país carece de recursos para la educación en ciberseguridad. Se necesita más investigación para mejorar las habilidades y el conocimiento de la seguridad cibernética de las personas en los campos de la tecnología de la información, administración y legal.

Para Ecuador es necesario crear leyes y tratados coordinados para obtener un ciberespacio armonioso. Los países deben trabajar juntos para crear espacios seguros de diálogo transfronterizo. Estos marcos brindan oportunidades para el diálogo y la colaboración a nivel mundial. Esto nos permite gestionar un ciberespacio seguro y abierto

para la ciberseguridad y el desarrollo global. También con apoyo de la colaboración entre la industria, la sociedad civil y la academia para oportunidades de desarrollo seguro y sostenible que beneficie a todos los involucrados.

Ecuador debe construir su capacidad diplomática digital participando en actividades regionales e internacionales. Esto incluye la cooperación con otras organizaciones nacionales, regionales e internacionales centradas en la recopilación de inteligencia en investigaciones y operaciones transfronterizas en ciberseguridad. Al mismo tiempo, Ecuador debe trabajar con otras autoridades nacionales e internacionales para responder de manera proactiva a los incidentes cibernéticos compartiendo información sobre cómo combatir el delito cibernético.

La Estrategia Nacional de Ciberseguridad de Ecuador requiere una evaluación y seguimiento permanente mediante el Comité Nacional de Ciberseguridad. Este organismo ordena los planes de implementación física y monetaria a través de la supervisión. Con su implementación, el Comité sirve como un órgano de toma de decisiones que garantiza la seguridad general del país. Cada trimestre, el comité revisará los informes trimestrales de los responsables de la implementación de las líneas de acción. A continuación, el Comité Nacional de Ciberseguridad actúa como guardiana de la Estrategia Nacional de Ciberseguridad, realizando un seguimiento de la implementación y elaborando de un informe anual sobre su éxito (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022b).

Cada tres años, el gobierno ecuatoriano actualizará la Estrategia Nacional de Ciberseguridad incluyendo planes, análisis e implementación con la recopilación y el análisis de datos públicos, así como planes de comunicación pública. Además, desarrollará herramientas generales, marcos, procesos y estrategias específicas para abordar los problemas (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022b).

Las entidades del sector público y privado, la sociedad civil y la academia, articuladamente con el Gobierno Nacional del Estado ecuatoriano, con el fin de garantizar la seguridad de los ciudadanos en el ciberespacio, quinto dominio,[22] establecen lineamientos y acciones para generar capacidades para enfrentar los riesgos y amenazas digitales. Para el desarrollo de este trabajo de investigación se procedió con la revisión de

[22] Dominios para el arte de guerra son: Tierra, Mar, Aire, Espacio, Ciberespacio (Corletti Estrada 2017, 17–18) .

instrumentos nacionales existentes, la normativa nacional vigente, las mismas que se listan en la tabla 8. Base Legal del Estado ecuatoriano:

Tabla 8
Base legal del Estado ecuatoriano

Instrumentos Nacional
Constitución de la República Art. 16, 66 (Num. 19 y 21), 158, 313 y 393
Ley de Seguridad Pública y del Estado Art. 2, 3, 10, 11, 38, 41 y 43
Reglamento a la Ley de Seguridad Pública y del Estado
Código Orgánico Integral Penal Art. 103, 170, 178, 190, 194, 202.1, 202.2, 229 - 234, 262, 353.1, 415.1, 415.2, 472, 476, 526, 553.2
Ley Orgánica de la Identidad y Datos Civiles Art. 1 y 3 (Num. 4 y 6)
Ley Orgánica de Telecomunicaciones Art. 76, 77, 78, 79, 80, 81, 82, 83, 84 y 85
Ley Orgánica de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Art. 5, 7,8, 9,10, 29, 51, 54, 58, 62, 63, 64
Ley de Propiedad Intelectual
Normas Técnicas: Familia de NTE INEN-ISO/IEC 27000, principalmente; NTE INEN-ISO/IEC 27005, Tecnología de la Información - Técnicas de Seguridad - Gestión del Riesgo en la Seguridad de la información. NTE INEN-ISO/IEC 27032, Tecnologías de la Información – Técnicas de seguridad– Directrices para Ciberseguridad. Resolución ARCOTEL-2018-0652, Norma técnica para coordinar la gestión de incidentes y vulnerabilidades que afecten a la seguridad de las redes y servicios de telecomunicaciones, publicado en el Registro Oficial No. 331, del 20 de septiembre de 2018. Resolución No. SB-2018-771 de la Superintendencia de Bancos, se reforma la Norma de Control para la Gestión del Riesgo Operativo, Suplemento del Registro Oficial No. 325, del 12 de septiembre de 2018.
Plan Nacional de Telecomunicaciones y tecnologías de Información del Ecuador 2016-2017
Plan Nacional de Desarrollo 2017-2021 “Toda una Vida”
Plan Sectorial de Defensa 2017-2021
Plan Estratégico Institucional de la Defensa 2017-2021
Plan Nacional de Seguridad Integral 2019 – 2030
Plan Específico de Defensa Nacional 2019-2030
Plan Nacional de Gobierno Electrónico 2018-2021
Libro Blanco de la Sociedad de la Información y del Conocimiento 2018
Plan Nacional de la Sociedad de la Información del Conocimiento 2018-2021
Agenda de Coordinación Intersectorial de Seguridad
Política de la Defensa Nacional del Ecuador “Libro Blanco” 2018
Plan Específico de Seguridad Pública y Ciudadana 2019-2030
Plan Específico de Inteligencia 2019-2030
Plan Específico de Relaciones Exteriores y Movilidad Humana 2019-2030
Libro Blanco de Línea de Investigación, Desarrollo e Innovación y Transferencia de Conocimiento en TIC (2019)
Plan Nacional de Seguridad Ciudadana y Convivencia Social Pacífica 2019 – 2030
Manual Militar de Operaciones de Ciberdefensa (MM-DCS-12)
Plan Nacional de Desarrollo 2021-2025
Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal sobre la Violencia Sexual Digital y el Ciberacoso (AN-PVP-2021-0143-M) 03-05-2021: Resolución No. 2019-2021-486
Proyecto de Ley Orgánica Reformatoria del Código Orgánico Integral Penal, para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos (Trámite unificado / 292-2020-MMV-AN). Proyecto de ley aprobado por el Pleno. 10-05-2021
Ley Orgánica de Protección de Datos Personales. Ley publicada en el R.O. No. 459, Quinto Suplemento, de 26 de mayo 2021.

Acuerdo Ministerial 006-2021, documentado en el No. 479 del Quinto Suplemento del Registro Oficial, del 23 de junio de 2021, publicó la Política Nacional de Ciberseguridad.
Estrategia de Ciberdefensa 2021
Guía Política Estratégica de Ciberdefensa 2021
Revisión: Proyecto Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia
Política Pública para una Internet segura para Niñas, Niños y Adolescentes.
Construcción: Ley Orgánica de Seguridad Integral del Estado.
Construcción: Reglamento de la Ley Orgánica de Protección de Datos Personales.
Actualización: Política Pública de Ciberseguridad.
Estrategia Nacional de Ciberseguridad
Agenda de Transformación Digital 2022-2025
Construcción: Política de la Agenda de Transformación Digital
Futuro: Reglamento de la Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia

Fuente: Marco legal y regulatorio relacionados al entorno digital, ciberseguridad y ciberdefensa del Ecuador
Elaboración propia con base en (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2021, 19–21, 23–25)

La Estrategia Nacional de Seguridad Cibernética es una descripción general integral de las áreas clave del gobierno ecuatoriano, incluidas las responsabilidades, funciones y regulaciones. Se presenta en forma de un plan de implementación que describe los objetivos del gobierno y los recursos necesarios para alcanzarlos. Para analizar adecuadamente el marco legal y regulatorio actual, es necesario la contribución de todas las partes interesadas relevantes, incluidas las ONG, la academia, las instituciones públicas y las empresas privadas. Esto incluye un análisis en profundidad de los ministerios clave, las regulaciones nacionales de seguridad cibernética y los marcos legales y regulatorios vigentes.

CERT es una organización que proporciona las mejores prácticas, estándares y metodologías para gestionar las amenazas del ciberespacio. Está integrado por autoridades federales y estatales, así como por organizaciones del sector privado y sin fines de lucro. Cada miembro del CERT recopila datos sobre amenazas cibernéticas actuales e informa sobre nuevos métodos y patrones. Producen informes de cumplimiento del gobierno y recopilan datos sobre patrones, métodos y amenazas emergentes. Los CERT deben trabajar con los operadores de infraestructura pública para implementar programas que presenten riesgos socioeconómicos, ambientales y de seguridad bajos para el sector público.

Existen muchos instrumentos jurídicos relacionados con la delincuencia, así como instrumentos jurídicos extranjeros relacionados con la ciberdelincuencia. El Convenio de Budapest sobre Ciberdelincuencia proporciona actos jurídicos, órdenes y facultades para hacer cumplir la ley. Las investigaciones criminales relacionadas con el ciberdelito

requieren una importante cooperación internacional. Además, el programa rige facultades como la investigación, el procesamiento, la recopilación, la tecnología de herramientas electrónicas y las pruebas. Las funciones informáticas forenses de datos y logística humana a menudo están involucradas en las investigaciones de delitos cibernéticos. Esto requiere incorporar precauciones estándar y mecanismos de notificación en todas las investigaciones.

Los avances tecnológicos están creando nuevas oportunidades en el ciberespacio. La tecnología avanzada por lo que se espera crear ejercicios cibernéticos nacionales e internacionales para fuerzas cibernéticas conjuntas. La Política sobre Tácticas y Técnicas Cibernéticas, y la Protección de Activos de Infraestructura Digital Crítica y Servicios Esenciales es un plan nacional de contingencia cibernética con pruebas periódicas de resiliencia, y está diseñado para apoyar la cooperación industrial nacional y los objetivos estratégicos en el ciberespacio con organismos internacionales. Además, elaborar una ley internacional de ciberdefensa, un manual de operaciones militares en el ciberespacio, una ley de ciberoperaciones y una doctrina común de ciberdefensa son fundamentales en nuestro país.

El ente rector responsable de implementar la Estrategia Nacional de Ciberseguridad y demás entidades de interés común tienen como objetivo implementar programas coordinados a nivel nacional para aumentar la conciencia pública sobre la cultura cibernética. Además, estos programas apoyarán colaboraciones con otras agencias gubernamentales y empresas privadas para desarrollar mejores capacidades de ciberdefensa y nuevos productos y servicios ecuatorianos. Además, estos programas crearán oportunidades para la colaboración con una variedad de empresas de seguridad de la cadena de suministro cibernético y brindarán experiencia para que los profesionales de riesgo de amenazas desarrollen su experiencia pública y privada en la lucha contra las amenazas. Su objetivo es crear capacitación técnica profesional.

Los profesionales de las TIC son vistos cada vez más como importantes diplomáticos, son esenciales para mantener unas relaciones internacionales y una organización regional adecuadas. Los profesionales de las TIC trabajan con las fuerzas del orden para brindar apoyo técnico e impulsar un cambio positivo. Crean un entorno cibernético seguro y confiable al capacitar a los futuros embajadores cibernéticos y compartir conocimientos. Los profesionales de las TIC también mantienen canales diplomáticos formales para organizaciones regionales e internacionales.

La Agenda de Transformación Digital del Ecuador 2022-2025 también menciona como parte de sus objetivos específicos: “Fortalecer el ciberespacio ecuatoriano procurando garantizar la seguridad de la información personal de los ciudadanos” (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022c, 14).

En la agenda de transformación digital del Ecuador 2022-2025, se establecen los siguientes ejes y pilares:

Tabla 9
Agenda de Transformación Digital del Ecuador 2022-2025

AGENDA DE TRANSFORMACIÓN DIGITAL DEL ECUADOR 2022-2025	
Eje	**Pilar**
Infraestructura digital	▪ Conectividad y Servicios de Telecomunicaciones ▪ Sistemas de Información
Cultura e Inclusión Digital	▪ Educación Digital ▪ Salud Digital ▪ Cultura Digital
Economía Digital	▪ Transformación Digital de estructura productiva ▪ Comercio Electrónico
Tecnologías emergentes para el desarrollo sostenible	▪ Fomento de nuevas tecnologías en las industrias ▪ Fomento de nuevas tecnologías para el medio ambiente ▪ Ciudades Inteligentes y Sostenibles
Gobierno Digital	▪ Simplificación de trámites ▪ Participación ciudadana por medios electrónicos ▪ Gobierno de TI ▪ **Identidad Digital**
Interoperabilidad y tratamiento de datos	▪ Servicios de Interoperabilidad ▪ Datos personales ▪ Datos abiertos
Seguridad Digital y confianza	▪ **Seguridad de la información**

Fuente: Agenda de Transformación Digital del Ecuador 2022-2025 (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022c, 16)
Elaboración propia

Los pilares que se resaltan en esta investigación son la *Identidad Digital*, herramienta que se puede utilizar para identificar a una persona en el mundo digital y para realizar tareas en organizaciones públicas y privadas. Además, para la protección de Datos Personales se debe brindar orientación para proteger mejor la información. El conocimiento se debe dar al público a través de programas de educación y capacitación. Los datos deben manejarse con cuidado mediante la implementación de sistemas seguros. Y en lo referente al pilar *Seguridad de la Información* se establece:

> creación de una Unidad de Gestión […] de la Seguridad de la Información […] la formulación y ejecución de un Sistema de Gestión de Seguridad de la Información […] la evaluación del Esquema Gubernamental de Seguridad de la Información […] Crear e implementar un Cert nacional para responder a las ciberamenazas y contar con servicios de ciberseguridad. […] implementación, evaluación y ejecución de la Estrategia Nacional

> de Ciberseguridad y la actualización de la Política […] cultura de seguridad e innovación de la ciberseguridad […] uso responsable del ciberespacio en el Ecuador. (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022c, 29)

La Unidad Nacional de Ciberdelito en sus investigaciones de delitos investiga los tipificados en el Código Orgánico Integral Penal (COIP):

Tabla 10
Delitos que investiga la CIBERPOL

DELITOS QUE INVESTIGA LA CIBERPOL								
Artículos	**Art. 186**	**Art. 190**	**Art. 230.2**	**Art. 230.4**				
Fraude Digital	Estafa	Apropiación fraudulenta por medios electrónicos	Interceptación ilegal de datos	Interceptación ilegal de datos				
Artículos	**Art. 154.2**	**Art. 168**	**Art. 230**	**Art. 232**	**Art. 234**	**Art. 234.1**	**Art. 477.1**	
Incidentes Informáticos	Hostigamiento	Distribución de material pornográfico a niñas, niños y adolescentes	Interceptación ilegal de datos	Ataque a la integridad de sistemas informáticos	Acceso no consentido a un sistema informático telemático o de telecomunicaciones	Falsificación informática	Interceptación de las comunicaciones en cooperación internacional	
Artículos	**Art. 100**	**Art. 103**	**Art. 104**	**Art. 106**	**Art. 172**	**Art. 173**	**Art. 174**	**Art. 178**
Violencia Digital	Explotación sexual de personas	Pornografía con utilización de niñas, niños o adolescentes	Comercialización de pornografía con utilización de niños, niñas o adolescentes	Acoso sexual	Utilización de personas para exhibición públicas con fines de naturaleza sexual	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.	Violación a la intimidad

Fuente: Los Ciberdelitos en el Ecuador (García Cataña 2022)
Elaboración propia

Se han descrito algunos documentos políticos estratégicos nacionales los cuales mencionan objetivos estratégicos relacionados al entorno digital, ciberseguridad y ciberdefensa con los cuales se da respuesta a la pregunta de investigación planteada: ¿qué marco regulatorio de la ciberseguridad y ciberdefensa se implementó en Ecuador en el período 2013 – 2022 que neutralice las amenazas en el ciberespacio?

3. Retos y desafíos en la ciberdiplomacia para fomentar el uso pacífico de las Tecnologías de la Información y de la Comunicación

Las tecnologías de la información y la comunicación han demostrado ser muy eficaces para promover interacciones pacíficas entre las personas en las sociedades y las relaciones internacionales. Han tenido un gran impacto. Si bien las TIC aportan grandes beneficios, también conllevan riesgos significativos. Con el aumento dramático en el uso indebido de las TIC, el entorno tecnológico global está poniendo en riesgo la paz y la

seguridad internacionales por parte de actores estatales y no estatales. Oscilar entre estos extremos es perjudicial para todas las naciones, sean estatales o no.

Con el propósito de fomentar el uso pacífico de las TIC, es necesario reconocer que pocas tecnologías han sido tan poderosas como las tecnologías de la información y las comunicaciones en la remodelación de las economías, las sociedades y las relaciones internacionales. El ciberespacio toca todos los aspectos de la vida. Si bien los beneficios son enormes, no están exentos de riesgos. El entorno mundial de las TIC se enfrenta a un aumento espectacular del uso malicioso de las mismas por parte de actores estatales y no estatales. El mal uso de las TIC representa un riesgo para todos los Estados y puede dañar la paz y la seguridad internacionales (United Nations Office for Disarmament Affairs 2017) .

En 1998, se presentó a la Primera Comisión de la Asamblea General de las Naciones Unidas un proyecto de resolución sobre las TIC en el contexto de la seguridad internacional. Los grupos de trabajo han producido informes sustantivos y han sido elogiados por todos los Estados miembros de la ONU.

El tema de la seguridad de la información ha estado en la agenda de las Naciones Unidas desde 1998, cuando se presentó un proyecto de resolución sobre el tema en la Primera Comisión de la Asamblea General de la ONU. Desde 2004, cinco Grupos de Expertos Gubernamentales (GGE) continúan estudiando las amenazas que plantea el uso de las TIC en el contexto de la seguridad internacional y cómo deben abordarse estas amenazas. Tres de estos grupos han acordado informes sustantivos con conclusiones y recomendaciones que han sido bien recibidos por todos los Estados miembros de la ONU (United Nations Office for Disarmament Affairs 2017).

Los informes GGE de 2013 y 2015, abordaron los cinco pilares de los informes GGE: amenazas existentes y emergentes; cómo se aplica el derecho internacional al uso de las TIC; normas, reglas y principios para la conducta responsable de los Estados; medidas de fomento de la confianza; y cooperación y asistencia internacionales en materia de seguridad y creación de capacidad en materia de TIC (United Nations Office for Disarmament Affairs 2017).

4. Debates de las ciberamenazas y sus proyecciones

Tal como lo menciona la OEA, uno de los principales debates de la ciberseguridad en la región gira en torno a la detección y análisis de eventos de seguridad digital,

especialmente en el ámbito financiero, por cuanto, las mafias saben que es ahí donde deben acelerar sus actividades criminales para obtener el dinero.

> Los delincuentes cibernéticos están organizados, bien financiados y no tienen limitación geográfica. Los ladrones ya no necesitan ingresar a una sucursal bancaria, ni siquiera al país en el que se encuentra su blanco. Los delincuentes sofisticados atacarán el banco que proporcione el mayor retorno de la inversión, independientemente de dónde esté ubicado. Por lo tanto, todos los Bancos deben asegurarse de tener suficientes recursos técnicos, personal adecuadamente capacitado y procedimientos apropiados para defenderse de los delincuentes cibernéticos y garantizar que el negocio sea lo suficientemente resiliente. En América Latina y en todo el mundo, la resiliencia cibernética requiere un compromiso desde el nivel de junta directiva hasta el nivel de sucursal. (Organización de los Estados Americanos 2018, 20)

Ante este grave problema, Symantec (2017) ratifica que "las instituciones financieras se enfrentan a ataques en múltiples frentes. Los dos tipos principales son ataques contra sus clientes y ataques contra su propia infraestructura" (Organización de los Estados Americanos 2018, 55). De este modo se evidencia que los riesgos cibernéticos que requieren mayor atención por parte de los Estados y la empresa privada son: "i) el robo de base de datos crítica, ii) el compromiso de credenciales de usuarios privilegiados, y, iii) la pérdida de datos" (Organización de los Estados Americanos 2018, 55).

Este esfuerzo conjunto debe poner fin a las amenazas y riesgos permanentes al sistema, puesto que la utilización de recursos ilegales se encuentra a la orden del día, especialmente en los intentos de inyectar capitales mediante transacciones fraudulentas de pago de facturas mensuales o por transferencias, siendo de este modo el sector financiero tres veces más susceptible a ciberataques en comparación con otras industrias, tal como lo muestra la Figura 5.

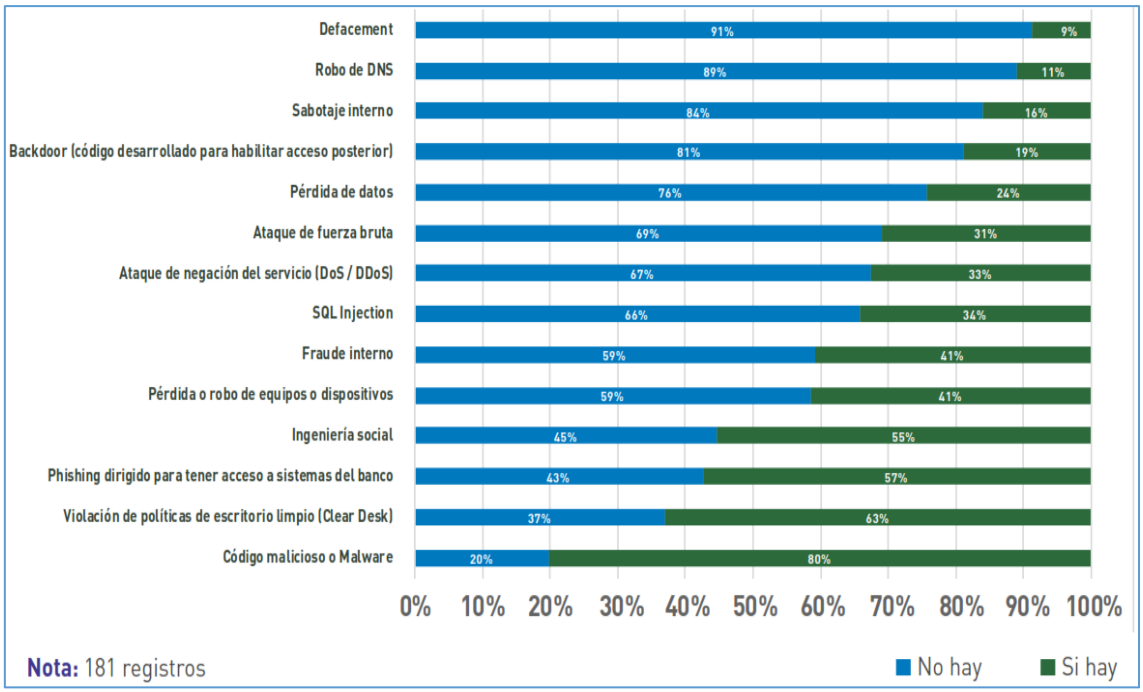

Figura 5. Eventos de seguridad digital contra entidades bancarias 2017.
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe (citado en Organización de los Estados Americanos 2018, 57)

Otro punto importante a considerar, en base al apartado anterior, es que la sociedad en general debe fortalecer su cultura de ciberseguridad en un contexto global, puesto que el objetivo deberá cumplirse con el apoyo interagencial y coordinado, especialmente, con el sector público y privado, poniendo de manifiesto que se debe frenar la evolución acelerada de las amenazas mediante estrategias y políticas multisectoriales que garanticen minimizar estos riesgos y amenazas presentes.

En este sentido, es imperante concienciar a los ciudadanos sobre la necesidad de manejar adecuadamente la información calificada, preservando la cadena de custodia, contribuyendo de este modo al cambio en la percepción de las ciberamenazas y sus consecuencias, mediante la promoción de la seguridad de los datos, la información, la educación, el intercambio de buenas prácticas y la competencia dentro de la sociedad de la información y el conocimiento. Es muy importante resaltar que las llamadas ciudades inteligentes serán el horizonte para la sociedad en general, considerando a ellas como la interacción de salud y bienestar, transporte inteligente, edificios inteligentes, agricultura, energía inteligente y medio ambiente (Brea Sánchez 2018).

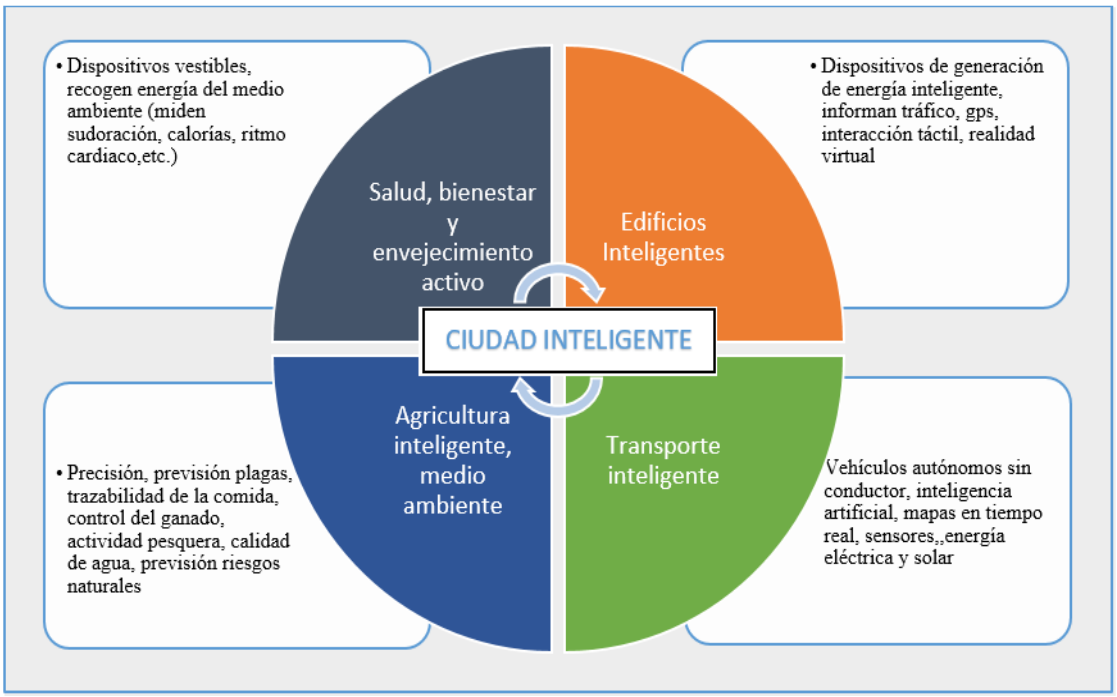

Figura 6. Ciudad Inteligente.
Fuente: Instituto Español de Estudios Estratégicos, 2018. Elaboración propia

Este tema en particular ya ha sido puesto de manifiesto en la UE, especialmente en España, donde es importante la cultura de ciberseguridad en todo nivel, y es a partir del año 2011 en la que se realizan aportes importantes como:

> Un cambio de cultura para adaptar la cultura de seguridad de una organización a las realidades actuales de la ciberseguridad supone una labor increíblemente dura a menos que se empiece desde cero. Normalmente las organizaciones tienen ya establecida su cultura de seguridad e incluso los individuos aportan ya una cultura de ciberseguridad preestablecida. (Pulido Alonso y Rosell Tejada 2017, 228)

Tal como sugiere el autor, cada empresa tiene una cultura de ciberseguridad, sea esta precaria o avanzada, por lo que será de vital importancia generar una estrategia sinérgica entre el sector público y privado. Además, deberán existir estructuras legales capaces de administrar en tiempo real la red global desde el ámbito de la comunicación pública, la asesoría legal, la gestión documental e informática, la capacitación técnica especializada, la inversión en ciencia y tecnología orientada a la investigación, desarrollo e innovación (i + D + I), entre otros.

El último tema mencionado anteriormente, es causa obligada de debate en el contexto de la ciberseguridad, especialmente en la región Sudamericana, puesto que se constituye en una de las principales opciones a las que recurren los gobiernos para establecer una relación de interdependencia con Estados hegemónicos, especialmente con

dominio global, siendo los más conocidos EE. UU., China, India, Reino Unido de Gran Bretaña, entre otros. De hecho, es una necesidad urgente de los Estados, puesto que requieren de una solución inmediata para proteger a sus habitantes y los recursos estratégicos de actos delictivos y ataques por parte de ciberdelincuentes, tal como refiere el siguiente apartado:

> A principios del mes de enero de 2016, el Departamento de Seguridad Interior de los Estados Unidos (DHS, *Department of Homeland Security*) informaba acerca de la manipulación ilícita de vehículos aéreos no tripulados (*UAV*) del servicio de protección de fronteras. Por medio del envío de señales GPS falsas que aparentaban ser genuinamente procedentes de los satélites NAVSTAR, lo que se conoce como GPS *spoofing*, narcotraficantes mejicanos lograban manipular la misión de drones a fin de poder cruzar libremente la frontera entre Estados Unidos y México y así conseguir libertad de acción en su actividad criminal. (Hinarejos Rojo y De la Peña Muñoz 2017, 249; énfasis en el original)

Tal como se puede interpretar, tanto los Estados como las estructuras ilegales pueden tener el dominio del ciberespacio, por lo que a futuro se mantendrá una disputa del poder a través de medios coercitivos y el uso del monopolio legítimo de la violencia que, a decir de Max Weber, este se encuentra materializado en sus FF.AA. y Policía Nacional, que de manera particular representa el caso ecuatoriano.

Siguiendo esta línea de la legalidad, el futuro muestra una gran incertidumbre, puesto que se evidencian adelantos en materia prospectiva, en la que se ven a los grandes ejércitos emplear su inteligencia artificial multidimensional para contrarrestar las amenazas futuras de agentes ilegales y de los propios Estados, tal como se manifiesta a continuación:

> *On the morning of May 17, 2024 U.S. and Chinese leaders authorized a limited nuclear exchange in the western Pacific. No one, including those who made the decision, is completely sure what caused the flash war. However, historians are confident that neither side deployed fully autonomous weapons or intentionally violated the law of armed conflict. Each side acted in anticipatory self-defense. Irrespective of the intent, in less than two hours, the technologies in use prompted a conflict that killed millions*. (Price, Walker, y Wiley 2017, 93; énfasis añadido)

De hecho, se desconoce cómo será el futuro próximo cercano, pero si es claro que los Estados y sus ciudadanos deben enfrentarse a este tema con determinación y seriedad, puesto que las implicaciones en varios ámbitos, que no han sido considerados como el aspecto socioeconómico, la privacidad y confianza, tendrán la misma importancia dentro de las ciudades del conocimiento y el internet de las cosas, siendo adicionalmente ejes transversales que también serán causa de afectación a los recursos e infraestructura crítica

que poseen los Estados. La ciberseguridad es un desafío global que incluye al internet de las cosas y el reto está en diagnosticar sus fortalezas, vulnerabilidades e impactos en el uso de las tecnologías con 5G y muy pronto 6G.

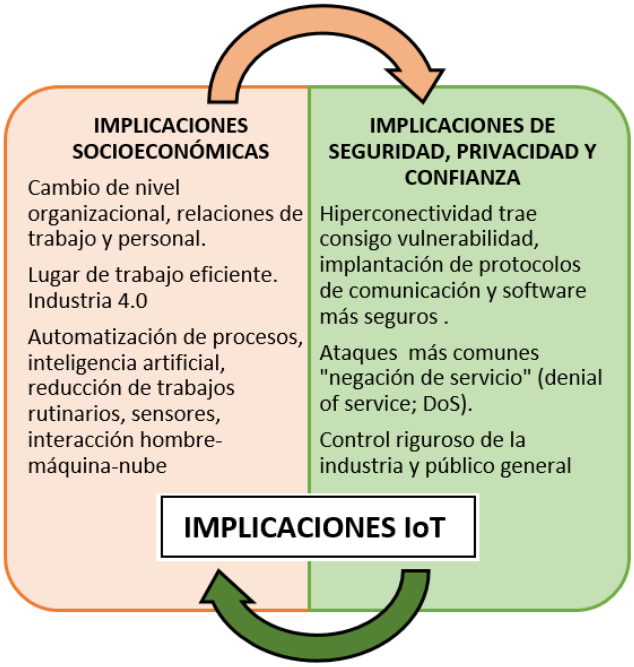

Figura 7. Implicaciones del internet de las cosas
Fuente: Internet de las cosas. Horizonte 2050 (Brea Sánchez 2018, 13–14). Elaboración propia

En este segundo capítulo se trató el marco legal y regulatorio de Ecuador en materia de ciberseguridad y ciberdefensa, herramientas y normativas utilizadas en Ecuador en el nuevo proceso de ciberseguridad incluyendo mecanismos legales, administrativos e institucionales, dando respuesta a la pregunta de investigación ¿qué marco regulatorio de la ciberseguridad y ciberdefensa se implementó en Ecuador en el período 2013-2022 que neutralice las amenazas en el ciberespacio?, también se describió el sistema de ciberseguridad en América Latina, se revisó la ciberdiplomacia como mecanismo para considerar las amenazas que plantean y proporcionan conocimiento sobre las tecnologías de la información y la comunicación, así como algunas proyecciones en torno a las ciberamenazas.

Conclusiones

Para los países de América del Sur, la región enfrenta muchas amenazas cibernéticas, por lo que, para combatir se necesita un contingente de recursos profesionales, fuerte, capaz de desarrollar herramientas de evaluación relacionadas con las nuevas amenazas. Las organizaciones públicas y privadas en sus sistemas que tiene fallas técnicas lo cuales pueden perderse o acceder a ellos terceros afectando la continuidad de las operaciones digitales, por lo que es necesario desarrollar un programa de mejora de conocimientos informáticos, para trabajar con medidas de ciberseguridad. Esto requiere el desarrollo de leyes, reglamentos y directrices internacionales para el uso de tecnologías y sistemas.

El procesamiento de los datos sin reflexión y razonamiento conduce a la pérdida de la información. La recopilación, el procesamiento y la transmisión de datos no planificados y sin el conocimiento del propietario, a lugar a graves violaciones de los derechos humanos que pueden afectar las actividades de las empresas, la comunidad, etc.

Las amenazas globalizadas que son cada vez más omnipresentes requieren una cooperación global para resolverlas estas pueden ser tráfico de armas, tráfico de drogas, ataques cibernéticos a infraestructura nacional crítica, desastres ambientales, crimen organizado transnacional y ataques marítimos y espaciales. El ciberespacio existe más allá de las fronteras nacionales. Por lo tanto, las fuerzas militares deben prepararse para operaciones en todas las dimensiones del combate: en el aire, la tierra, el mar, el espacio y ciberespacio. Además, estas amenazas requieren una planificación y preparación global para las operaciones en todas las áreas de jurisdicción de los países.

El uso de la fuerza además del bélico, como amenaza tradicional, se suman las amenazas cibernéticas. Por lo que, el papel preponderante de las FF.AA. para enfrentar ciberriesgos se enfoca en la necesidad de fortalecer el reclutamiento de nuevos miembros, con capacidades tecnológicas previas y que mantengan una constante capacitación para brindar respuestas en el aspecto multidimensional.

Los sectores público y privado ecuatorianos, tienen importantes activos de infraestructura crítica digital: sector bancario, telecomunicaciones, centrales eléctricas, sector salud, sistemas de transporte, sistemas de agua y otras, que, en la era digital actual, estos activos se enfrentan a amenazas, es prioritario que los datos se recopilen y gestionen

desde toda la infraestructura digital. Se debería levantar un inventario de estas infraestructuras digitales en la se tenga visibilidad e información y puedan ser protegidos por los marcos legales y regulatorios, mitigando los riesgos de ciberseguridad y se apliquen mecanismos de coordinación y cooperación. Además, estas infraestructuras se deberían monitorear y evaluar por ser puntos de datos clave. Esta información se comparte para permitir una comunicación más amplia y una mejor comprensión. Los países establecen objetivos para los aspectos económicos, sociales y ambientales de la infraestructura digital. Lo hacen trabajando con partes interesadas públicas y privadas para identificar prioridades críticas de infraestructura digital.

Para limitar posibles infracciones cibernéticas, debemos fortalecer nuestra seguridad digital. Además, la resiliencia digital requiere preparación, respuesta y recuperación constantes ante incidentes y crisis cibernéticos. Hacemos esto al hacer cumplir públicamente los estándares de seguridad de la información.

Los CERT permite a los gobiernos centrales recopilar, analizar, clasificar y medir información sobre incidentes y vulnerabilidades en el ciberespacio. También detectan amenazas, investigan cómo identificarlas, desarrollan formas de mitigar los riesgos, manteniendo la resiliencia y brindando soporte de respuesta a incidentes. Los CERT coordinan la acción conjunta entre las agencias para proteger el ciberespacio, articulan y abogan por decisiones estratégicas, operativas y tácticas en la toma de decisiones.

La capacidad limitada de aplicación de la ley de delitos cibernéticos de Ecuador está retrasando las investigaciones y la aplicación. Esto ha llevado a un aumento de los delitos cibernéticos en línea, como ganar dinero ilegalmente a través de plataformas y soluciones digitales. Además, las actividades delictivas como el fraude informático, el robo de identidad, violación de datos personales y la distribución de material de explotación sexual infantil se llevan a cabo a través de plataformas y soluciones en internet.

Las personas que acceden a Internet a menudo se convierten en objetivos fáciles para los descargadores de canales digitales profesionales. Conocen el sistema, lo que lo hace aún más fácil de explotar. En Ecuador se debe superar la escasez de profesionales de ciberseguridad y ciberdefensa para aumentar la conciencia, cultura de seguridad cibernética en la sociedad, a través de programas dirigidos a grupos específicos. Estos pueden implementarse a través del acceso a las plataformas y servicios digitales más importantes.

La falta de capacitación y concienciación es un problema global, los países de la región son muy vulnerables. La mayoría de los incidentes cibernéticos se ven reflejados por causa de vectores humanos y pueden ser evitados con capacitación, educación de calidad, previniendo a los malos actores, mitigando los riesgos y ataques cibernéticos y considerando el recurso humano, conversando y analizando sobre el producto, procesos, y personas.

Hoy en día con la tecnología, se realizan compras en línea, se tiene acceso a salud, a educación, se potenció el teletrabajo, se construye una vida paralela a través de las redes sociales: WhatsApp, TikTok, Instagram, YouTube, Facebook, Twitter; por ello tener alta conciencia sobre la seguridad cibernética es inminente, se puede empezar con prácticas simples como, por ejemplo, mantener una buena higiene de cambio de contraseñas, haciendo un buen uso de los dispositivos que se tienen conectados en el Internet de las cosas, para potenciar un trabajo digital más seguro. Se recuerda que los atacantes se concentran en la gente haciendo uso de la ingeniería social.

Desde el enfoque de políticas, ciberdiplomacia, a la cultura de ciberseguridad se la tiene que canalizar desde los puntos de vista organizativo-gobernanza, técnico y humano, siendo así a nivel político y ciber diplomático con un enfoque multidisciplinario, en roles de ciberseguridad y ciberdefensa.

No hay ciberseguridad sin cooperación, actualmente Ecuador cuenta con acuerdos de cibercrimen con Interpol, acuerdos bilaterales en lucha contra el cibercrimen, pero está pendiente que Ecuador logre tener la adhesión al acuerdo del convenio de Budapest. Es importante generar alianzas público-privada, contar con colaboración inter e intra institucional, tener aliados bilaterales y multilaterales que fortalezcan las capacidades de los estados miembros, participar en foros internacionales. Realizar emprendimientos, proyectos, innovación, desarrollo, que ayuden a generar estrategias y políticas públicas, promoviendo y generando conocimiento, manteniendo una coordinación y liderazgo nacional, para disfrutar de un internet abierto y seguro para todos. Se ha incrementado el uso de plataformas para estudiar, trabajar, hacer compras, se ha tenido que reinventar la vida, inventar nuevos hábitos, esto no es temporal, esto es ya el futuro.

El convenio de cibercriminalidad se compone principalmente de varios puntos, entre ellos: contiene definiciones de términos que permiten comprender la finalidad del convenio; en su artículo primero se incorporan los conceptos de “sistema informático”, “datos informáticos”, “proveedor de servicios”, “datos relativos al tráfico”, que ayudan a comprender su definición y a estar de acuerdo en los conceptos.

Hoy en día se debe tener en cuenta que el crimen organizado transnacional ha evolucionado a través del uso de la tecnología y del ciberespacio, generando nuevos desafíos a nivel global, similar a la globalización del narcotráfico, tráfico de personas, rutas de migración irregular, tráfico mundial de armas, alta tasa de violencia en América Latina. Los flujos financieros ilícitos del crimen organizado y de terrorismo, la economía ilícita empodera por la darknet y la criptomoneda, por lo que se necesita la cooperación interagencial e internacional para combatir el crimen organizado transnacional en el nuevo orden mundial.

Es importante mencionar que como país se debe contrarrestar las ciberamenazas, ciberataques, salvaguardar la infraestructura crítica digital, servicios esenciales del Estado, infraestructura crítica digital de defensa, así como la protección de derechos en el ciberespacio. Para ello se cuenta con una estrategia de ciberdefensa dinámica y resiliente para proteger desde el ámbito de la defensa nacional, la cual plantea objetivos, directrices, estructura y conceptualizaciones.

La Estrategia Nacional de Ciberseguridad describe las áreas clave del gobierno ecuatoriano. Proporciona un plan de cómo el gobierno espera lograr sus objetivos y los recursos necesarios para hacerlo. La clave para comprender las leyes y los estándares regulatorios actuales radica en analizar las actividades de varias comunidades, incluidas la academia, las ONG, las empresas privadas y las instituciones públicas. Estos análisis requieren información importante de todos estos grupos, así como las regulaciones de seguridad cibernética actuales.

CERT es un acrónimo de Computer Emegency Response Team, por sus siglas en inglés. Esta es una junta de organizaciones del sector público y privado y ONG. CERT recopila datos de amenazas y crea analistas de nuevas técnicas y patrones en el ciberespacio. Para recopilar datos, compartir información con otros miembros. CERT recopila datos sobre nuevas amenazas, métodos y patrones. También proporciona informes de cumplimiento que los gobiernos y los operadores de infraestructura pública pueden usar al implementar programas de bajo riesgo cibernético. A nivel del país contamos con el Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT).

Hay una serie de instrumentos legales en el derecho penal, así como leyes extranjeras sobre ciberdelincuencia. El Convenio de Budapest sobre Ciberdelincuencia contiene leyes, órdenes y facultades para hacer cumplir la ley. Las investigaciones criminales relacionadas con el ciberdelito requieren una cooperación internacional complementaria. Para supervisar aspectos de las investigaciones criminales tales como:

Tecnología de herramientas electrónicas y recopilación de pruebas y la aplicación de la ley, las investigaciones sobre delitos cibernéticos deben incorporar precauciones estándar y mecanismos de notificación en todas las investigaciones. Esto se debe a que se debe comprender la logística humana y el análisis forense de datos informáticos que significa incorporar estas habilidades en cada investigación.

La tecnología avanzada trae nuevas oportunidades en línea. Esto conducirá a la creación de nuevos ejercicios cibernéticos nacionales e internacionales por fuerzas cibernéticas conjuntas. La Política sobre amenazas cibernéticas y contramedidas, y Protección de recursos de infraestructura digital crítica y servicios esenciales es una emergencia cibernética nacional, con pruebas periódicas y sólidas para respaldar la cooperación industrial nacional y los objetivos estratégicos en el ciberespacio. La elaboración de leyes internacionales de defensa cibernética, manuales militares sobre operaciones en el ciberespacio y leyes sobre la realización de operaciones cibernéticas son importantes para el desarrollo futuro de nuestro país. Además, la creación de una doctrina común de ciberdefensa también es necesaria para llevar a cabo con éxito esta tarea.

Las agencias gubernamentales responsables de implementar la Estrategia Nacional de Ciberseguridad y otros organismos de interés común tienen como objetivo implementar programas coordinados a nivel nacional para aumentar la conciencia pública sobre la cultura cibernética. Además, estos programas apoyan la colaboración con otras agencias gubernamentales y empresas privadas para desarrollar mejores capacidades de defensa cibernética y nuevos productos y servicios ecuatorianos. Además, estos programas crean oportunidades para trabajar con una variedad de empresas de seguridad cibernética. Dentro de la cadena de suministro cibernético y aportan la experiencia a los profesionales de riesgo de amenazas para aumentar sus capacidades en la lucha contra los incidentes cibernéticos en los sectores públicos y privados.

Actualmente la tendencia en los tiempos modernos es considerar a los profesionales de las TIC como los nuevos diplomáticos esenciales. Como tales, juegan un papel vital en las relaciones internacionales y las organizaciones regionales. Impulsan un cambio positivo a través de la colaboración con múltiples partes interesadas y el conocimiento compartido, así como la asistencia técnica en la aplicación de la ley. Los profesionales de las TIC abordan el delito cibernético y ayudan a crear un entorno de seguridad y confianza mediante el desarrollo de embajadores cibernéticos e intercambian

conocimientos, información transfronteriza y mantienen canales diplomáticos formales para organizaciones regionales e internacionales.

Se puede mencionar también que los gobiernos cuando conocen la importancia de las políticas de la ciberseguridad y ciberdefensa, toman la decisión e inmediatamente las crean, de tal manera de obtener un marco de gobernanza. La cual describe a las instituciones que son parte de las políticas cibernéticas. Se inicia desde los ministerios, viceministros, subsecretarias, expertos técnicos en temas de ciberseguridad y ciberdefensa. Los estados generalmente crean un centro nacional de respuesta como los CERT. Los mismos que son considerados también actores individuales de los sectores privados, academia e industria.

Se puede considerar también algún consejo asesor ministerial el cual asesora a nivel presidencial para la toma de decisiones en temas de ciberseguridad y ciberdefensa. También actúa como intermediario en las instituciones con recurso personal técnico a nivel estratégico-político. Este consejo asesor ministerial se integra por los ministerios de telecomunicaciones, defensa, interior, finanzas, relaciones exteriores, justicia, gobierno.

Compartir la información es muy indispensable cuando se trata de la ciberseguridad y ciberdefensa. De tal forma de proteger al estado de las ciberamenazas, salvaguardar las infraestructuras críticas, protección de datos personales, nuevas tendencias, generación de normas, marco regulatorio. Esta información es analizada por los grupos de trabajo cibernética nacional, desarrollando las recomendaciones técnicas para emitirlas al consejo asesor ministerial.

Se recomienda que los estados creen el rol de un coordinador nacional cibernética quien se encargará de informar el enfoque cibernético a toda una nación. Este coordinador podría ser parte de un centro de coordinación cibernética nacional lugar en donde todos los actores se reunirían para resolver conflictos entre todas las agencias, es decir, permite la integración para generar la concienciación. Este centro se diferencia de las funciones que cumple un CERT. Este centro estaría integrado de personal multidisciplinario, debe cumplir las habilidades de un “campeón” para logar el nexo a un alto nivel en la toma de decisiones, con una excelente credibilidad y con capacidades para emitir respuestas.

Establecer los cimientos de una estrategia nacional de ciberseguridad es importante para que pueda continuar a largo plazo, tiene un costo, sacrificio, disciplina. Para que un estado se pueda empoderar de esta cultura cibernética, incluyendo la coordinación, cooperación con diferentes actores nacionales e internacionales. Esto ayudará a tener una gobernanza fortaleciendo la sostenibilidad, flexibilidad y

actualización permanente, de tal manera que todos podemos trabajar organizados en comparación a los ciberdelincuentes que ellos si se comparten información y se apoyan entre sí para cometer sus ciberdelitos.

Es más fácil impulsar, desarrollar e implementar metodologías de esquemas de seguridad, en los sectores públicos y privados, los cuales cuentan con estrategias de protección de datos personales y que han llegado a un nivel de madurez alto en ciberseguridad y ciberdefensa y poseen un mecanismo de protección de datos. Esto es considerado un ecosistema de la ciberseguridad en temas de protección de datos personales, facilitando y optimizando los esfuerzos y recursos económicos que se invierten de forma aislada ahora se puede gestionar de una manera integral.

Para Ley de Protección de Datos Personales a nivel de Ecuador, aún está pendiente la creación del Registro Nacional y la designación respectiva del Superintendente de Protección de Datos. Se espera que se estabilice la situación política interna en Ecuador para que las autoridades de turno, el presidente de la República, designe una terna de acuerdo a lo que establece la Constitución de la República que cumpla con los requisitos y méritos correspondientes.

El marco legal y regulatorio general relacionado con el entorno digital, ciberseguridad y ciberdefensa en Ecuador de acuerdo a la recolección de documentos que conforman la base legal del Estado ecuatoriano se puede mencionar que ha sido muy débil y escasa. Si bien se cuenta con la constitución, diferentes leyes, reglamentos, código orgánico integral penal, leyes orgánicas, normas técnicas, resoluciones, planes nacionales, planes sectoriales, planes estratégicos, planes específicos, Libros Blancos, Agendas, Políticas, Manuales, Acuerdos Ministeriales, no ha sido suficiente para neutralizar las amenazas en el ciberespacio en el Ecuador.

Se resalta que desde el 2021 se da prioridad política para iniciar con normativa propiamente establecida para el entorno digital, ciberseguridad y ciberdefensa. el 26 de mayo de 2021 se publica la Ley Orgánica de Protección de Datos Personales, el 23 de junio de 2021 es publicada la Política Nacional de Ciberseguridad, así como la Estrategia de Ciberdefensa 2021. En curso de análisis en la Asamblea Nacional se encuentra el Proyecto Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia presentado el 19 de octubre de 2021. Y el 16 de junio de 2022 es presentada la Estrategia Nacional de Ciberseguridad, documentos que tienen el desafío para la implementación, monitoreo y evaluación.

Mientras tanto durante esta línea de tiempo del desarrollo de la normativa se han evidenciado escenarios de amenazas: SENAIN, Tropas Cibernéticas, Ataques informáticos a Ecuador, CONSEP, SENESCYT & ANT, GEA, Plan Toda Una Vida, Ola Bini, Novaestrat, CNT, Ministerio de Salud, Agencia Nacional de Tránsito, Operación Pulpo Rojo, Acceso ilegal a datos personales en sistemas del CIES, los mismo que se desarrollan en la sección de anexos. En algunos de los casos como: fraude digital, incidentes informáticos, violencia digital en los que se han aplicado los artículos tipificados en el código orgánico integral penal (COIP). Adicionalmente, se ha tenido como avance la Ley Orgánica Reformatoria del Código Orgánico Integral Penal, para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos y la Ley Orgánica Reformatoria del Código Orgánico Integral Penal sobre la Violencia Sexual Digital y el Ciberacoso aprobados en el 2021.

El marco regulatorio de la ciberseguridad y ciberdefensa que se implementó en Ecuador en el período 2013-2022 que neutralice las amenazas en el ciberespacio para el caso ecuatoriano no ha logrado neutralizar las amenazas en el ciberespacio. Se espera implementar, evaluar, monitorear la Estrategia Nacional de Ciberseguridad vigente; así como fomentar, impulsar la concienciación, educación y la cultura en temas de ciberseguridad y ciberdefensa de forma integral sumando sinergias en capacidades técnicas y estratégicas desde de los sectores público-privado, y gestionando la cooperación, colaboración internacional.

Lista de referencias

ABC Internacional. 2017. “Rusia crea unidades especiales de guerra informativa”. https://www.abc.es/internacional/abci-rusia-crea-unidades-especiales-guerra-informativa-201702231029_noticia.html.

Actualidades de la UIT. 2010. “Ciberseguridad”, nº 9.

Acurio Del Pino, Santiago. 2017. “Derecho Penal Informático: Una visión general del Derecho Informático en el Ecuador con énfasis en las infracciones informáticas, la informática forense y la evidencia digital”. Pontificia Universidad Católica del Ecuador. https://www.academia.edu/19803737/Derecho_Penal_Inform%C3%A1tico.

Anchundia Betancourt, Carlos E. 2017. “Ciberseguridad en los sistemas de información de las universidades”. *Fundación Dialnet*.

Arredondo, Gustavo Aimone. 2017. “UNASUR y el Consejo de defensa Suramericano en su Primer Lustro 2011-2016”. *Revista de Marina*, nº 957: 18–25.

Arteaga, Félix. 2010. “El Nuevo Concepto Estratégico de la OTAN: lógica y estructura”. *Real Instituto Elcano,* nº 2/2010: 10.

Asociación de Bancos del Ecuador. 2021. “Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia”. https://asobanca.org.ec/Legal/8443-2/.

Asociación Ecuatoriana de Ciberseguridad, y Santiago Acurio Del Pino. 2020. “#Charla12 - ‘Convenio de Budapest en el #Ecuador’”. Charlas de Concienciación. https://www.youtube.com/watch?v=382Mg-vVEZA.

Banco Interamericano de Desarrollo y Organización de los Estados Americanos. 2020. “Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe”. doi:http://dx.doi.org/10.18235/0002513.

Becerril, Soledad, Amancio Fernández, Helena Resano, José Manuel González Huesa, Bárbara Ruiz, Juan José Morodo, Justo Villafañe, Francisco Sierra, Carlos Fernández Guerra, y Rosa Yagüe. 2018. “Influencia de las Noticias Falsas en la Opinión Pública”. *Estudio de Comunicación*. https://www.servimedia.es/sites/default/files/documentos/informe_sobre_fake_news.pdf.

Bindé, Jérôme. 2005. *Hacia las sociedades del conocimiento: informe mundial de la Unesco*. Paris(Francia): UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000141908.

Boris, Saavedra. 2020. "Estado de Derecho en el Ciberespacio: La actualidad en Latinoamérica y El Caribe". En *La seguridad en el marco del Estado de derecho*. Universidad de las Américas Puebla.

Bradshaw, Samantha, y Philip N Howard. 2017. "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation". *University of Oxford*, nº 12: 37.

Bravo, Diego. 2015. "La Senain dice que no ha contratado a Hacking Team". *El Comercio*. https://www.elcomercio.com/actualidad/senain-contratato-hacking-team-ecuador.html.

Brea Sánchez, Víctor Manuel. 2018. "Internet de las cosas. Horizonte 2050". Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/docs_investig/2018/DIEEEINV17-2018_Internet_de_las_Cosas_Horizonte_2050.pdf.

Campaña, Marieta. 2022. "Un detenido en Loja por posible acceso ilegal a información que el CIES tenía de cientos de ciudadanos". *expreso*. https://www.expreso.ec/actualidad/detenido-loja-posible-acceso-ilegal-informacion-cies-tenia-cientos-ciudadanos-132497.html.

Carrasco, Luís de Salvador. 2010. "Internet, Filtraciones y Wikileaks". *Documentos de opinión del IEEE*, nº 25. https://www.ieee.es/Galerias/fichero/docs_opinion/2010/DIEEEO25_2010Wikileaks.pdf.

Casarin, Marcelo, Fernando Calderón, Paola Bonavitta, Iván Gustavo Baggini, Félix Caballero, Fernando Fraenza, Luis Ignacio García Sigman, et al. 2018. *En torno a las ideas de Manuel Castells: discusiones en la era de la información*. 1a ed revisada. 4. Universidad Nacional de Córdoba: Centro de Estudios Avanzados, Facultad de Ciencias Sociales. https://rdu.unc.edu.ar/handle/11086/6454.

CL Biblioteca del Congreso Nacional. 2014. "Convenio de Budapest". *Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia*. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20810/5/Convenio%20N%20185%20del%20Consejo%20de%20Europa%20sobre%20la%20Ciberdelincuencia%20(Convenio%20de%20Budapest).pdf.

CL Ministerio del Interior y Seguridad Pública y CL Ministerio de Defensa Nacional. 2015. “Bases para una Política Nacional de Ciberseguridad*”. *CL Ministerio del Interior y Seguridad Pública, CL Ministerio de Defensa Nacional*. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/0EE2B41802BD1CE80525831D005FBE91/$FILE/Bases_Pol%C3%ADtica_Nacional_sobre_Ciberseguridad.pdf.

CO Ministerio de Defensa Nacional. 2017. “Ciberdefensa y ciberseguridad: prioridades para el Gobierno y la Fuerza Pública”. https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido/listadomdn?date=16072017.

Código Vidrio. 2020. “Desinformación”. *Código Vidrio*. https://www.codigovidrio.com/code/category/desinformacion/.

Collins, Aengus. 2019. *Informe de riesgos mundiales 2019*. 14ª ed. Ginebra (Suiza): Foro Económico Mundial.

Comisión Económica para América Latina y el Caribe. 2020. “Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe”. https://www.cepal.org/es/organos-subsidiarios/conferencia-ministerial-la-sociedad-la-informacion-america-latina-caribe.

Congreso Nacional. 2002. “Ley Orgánica de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos”.

Consejo de Europa. 2001. “Convenio sobre la Ciberdelincuencia”. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.

Corletti Estrada, Alejandro. 2017. *Ciberseguridad. Una estrategia informático/militar*. Madrid.

CyberSecure. 2021. “Grupo Hotarus Corp evidenciado en campañas que afectarían a importantes empresas de Ecuador”. https://portal.cci-entel.cl/Threat_Intelligence/Boletines/962/.

Duarte, Mario Ramón. 2018. “La ciberseguridad: una temática global y un desafío estratégico en Latinoamerica”. *Revista Globalización*. http://rcci.net/globalizacion/2018/fg3623.htm.

EC Agencia de Regulación y Control de las Telecomunicaciones. 2018. *Resolución ARCOTEL-2018-0652 La Agencia de Regulación y Control de las Telecomunicaciones*. Registro Oficial 331, 20 de septiembre.

https://www.arcotel.gob.ec/wp-content/uploads/downloads/2018/08/ARCOTEL-2018-0652-2018-07-31-TELECOMUNICACIONES-MATRIZ.pdf.

EC Asamblea Nacional. 2009. *Ley de Seguridad Pública y del Estado*. Registro Oficial 35, Suplemento, 28 de septiembre. https://www.oas.org/juridico/pdfs/mesicic5_ecu_panel5_sercop_1.3._ley_seg_p%C3%BAblica.pdf.

———. 2021a. "Asambleísta Rodrigo Fajardo (ID) entrega Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia, en Modalidad Presencial. Ecuador 19 de octubre de 2021." *Asamblea Nacional*. https://www.flickr.com/photos/asambleanacional/sets/72157720039928633.

———. 2021b. *Ley Orgánica de Protección de Datos Personales*. Registro Oficial 459, Quinto Suplemento, 26 de mayo. https://www.registroficial.gob.ec/index.php/registro-oficial-web/publicaciones/suplementos/item/14857-quinto-suplemento-al-registro-oficial-no-459.

EC Centro de Inteligencia Estratégica. 2019. "Plan Específico de Inteligencia 2019-2030". *Centro de Inteligencia Estratégica*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-nacional-inteligencia-web.pdf.

EC Centro de Respuesta a Incidentes de la ARCOTEL. 2014. "RFC 2350 español". *EcuCERT*. https://www.ecucert.gob.ec/rfc2350/.

EC Comando Conjunto de las Fuerzas Armadas. 2020. *Manual Militar de Operaciones de Ciberdefensa MM-DCS-12*. Resolución N.° CCFFAA-SG-A-2020-006-O, 14 de septiembre.

EC Consejo de la Judicatura. 2019. "232 Ataque a la Integridad de Sistemas Informáticos, Num. 1". *No. proceso 17282-2019-01265*. abril 13. http://consultas.funcionjudicial.gob.ec/informacionjudicial/public/informacion.jsf.

EC Ministerio de Defensa Nacional. 2017. "Plan Estratégico Institucional de la Defensa 2017-2021". *Ministerio de Defensa Nacional*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/02/PEI-2017-2021.pdf.

———. 2021a. "Guía Político - Estratégica de Ciberdefensa 2021". *Ministerio de Defensa Nacional*.

———. 2021b. "Estrategia de Ciberdefensa 2021 del Ecuador". *Ministerio de Defensa Nacional*. Acuerdo Ministerial 199.

EC Ministerio de Relaciones Exteriores y Movilidad Humana. 2019. “Plan Específico de Relaciones Exteriores y Movilidad Humana 2019-2030”. *Ministerio de Relaciones Exteriores y Movilidad Humana*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-nacional-min-exteriores-web.pdf.

EC Ministerio de Telecomunicaciones y de la Sociedad de la Información. 2014. “Presidente Rafael Correa destacó el crecimiento de la conectividad en el Ecuador”. https://www.telecomunicaciones.gob.ec/presidente-rafael-correa-destaco-el-crecimiento-de-la-conectividad-en-el-ecuador/.

———. 2019a. “Ecuador Digital”. *Ministerio de Telecomunicaciones y de la Sociedad de la Información*. https://www.telecomunicaciones.gob.ec/25693-2/.

———. 2019b. “Más de 40 millones de ataques al Ecuador neutralizados desde el retiro del asilo a Julian Assange”. https://www.gobiernoelectronico.gob.ec/mas-de-40-millones-de-ataques-al-ecuador-neutralizados-desde-el-retiro-del-asilo-a-julian-assange/.

———. 2019c. *Política Ecuador Digital*. Acuerdo Ministerial 15, Registro Oficial 69, 28 de octubre. http://www.pge.gob.ec/images/documentos/LeyTransparencia/2019/octubre/a2/politica_ecuador_digital.pdf.

———. 2020. *Esquema Gubernamental de Seguridad de la Información -EGSI- version-2.0*. Acuerdo Ministerial No. 025-2019, Registro Oficial 228, Edición Especial, 10 de enero. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/01/Registro-Oficial-Acuerdo-Ministerial-No.-025-2019-EGSI-version-2.0.pdf.

———. 2021. *Política Nacional de Ciberseguridad*. Acuerdo Ministerial 006-2021, Registro Oficial 479, Quinto Suplemento, 23 de junio. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-Anexo-Politica-de-Ciberseguridad..pdf.

———. 2022a. “El Gobierno Nacional presentó la Estrategia Nacional de Ciberseguridad”. *Ministerio de Telecomunicaciones y de la Sociedad de la Información*. https://www.telecomunicaciones.gob.ec/el-gobierno-nacional-presento-la-estrategia-nacional-de-ciberseguridad/.

———. 2022b. “Estrategia Nacional de Ciberseguridad del Ecuador”. <i>Ministerio de Telecomunicaciones y de la Sociedad de la Información<i>. https://www.gobiernoelectronico.gob.ec/wp-

content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf.

———. 2022c. “Agenda de Transformación Digital 2022-2025”. <i>Ministerio de Telecomunicaciones y de la Sociedad de la Información<i>. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf.

EC Ministerio de Telecomunicaciones y la Sociedad de la Información. 2018. “Libro Blanco de la Sociedad de la Información y del Conocimiento”. <i>Ministerio de Telecomunicaciones y la Sociedad de la Información<i>. julio. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/07/Libro-Blanco-de-la-Sociedad-del-Informaci%C3%B3n-y-del-Conocimento.pdf.

EC Ministerio Defensa Nacional. 2019. “Plan Específico de Defensa Nacional 2019-2030”. *Ministerio Defensa Nacional*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-nacional-defensa-web.pdf.

EC Ministerio del Interior. 2019. “Plan Específico de Seguridad Pública y Ciudadana 2019-2030”. *Ministerio del Interior*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-nacional-min-interior-web.pdf.

EC Ministro de Defensa Nacional. 2018. “Política de Defensa Nacional Libro Blanco 2018”. *Ministro de Defensa Nacional*. https://www.defensa.gob.ec/wp-content/uploads/2019/01/Pol%C3%ADtica-de-Defensa-Nacional-Libro-Blanco-2018-web.pdf.

EC Presidencia Constitucional de la República. 2010. *Reglamento a la Ley de Seguridad Pública y del Estado*. Decreto Ejecutivo 486, Registro Oficial 290, Suplemento, 30 de septiembre. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/06/Reglamento-a-la-Ley-de-Seguridad-Publica-y-del-Estado.pdf.

———. 2018. *N° 526 Suprímese la Secretaría de Inteligencia*. Registro Oficial 358, Suplemento, 30 de octubre.

EC Secretaría Nacional de la Administración Pública. 2013a. “Esquema Gubernamental de Seguridad de la Información EGSI”. Acuerdo Ministerial 166, Registro Oficial 88, Suplemento 25 de septiembre de 2013.

———. 2013b. *Esquema Gubernamental de Seguridad de la Información (EGSI) versión 1.0*. Acuerdo Ministerial 166, Registro Oficial 88, Suplemento 25 de septiembre de 2013. https://www.gobiernoelectronico.gob.ec/wp-

content/uploads/2018/10/Acuerdo-Nro-166-Seguridad-de-la-Informaci%C3%B3n.pdf.

EC Secretaría Nacional de Planificación. 2021. "Plan de Creación de Oportunidades 2021-2025". *Secretaría Nacional de Planificación*. Resolución 002-2021-CNP. https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/Plan-de-Creaci%C3%B3n-de-Oportunidades-2021-2025-Aprobado_compressed.pdf.

EC Servicio Ecuatoriano de Normalización. 2016. Tecnologías de la Información — Técnicas de Seguridad — Sistemas de Gestión de Seguridad de la Información – Descripción General y Vocabulario. (ISO/IEC 27000:2016, IDT). NTE INEN-ISO/IEC 27000, Cuarta Edición.

El Comercio. 2015. "Ecuador asegura que 'respeta la privacidad' tras revelaciones sobre supuesto espionaje". *El Comercio*. https://www.elcomercio.com/actualidad/politica/ecuador-espionaje-privacidad-hackingteam-wikileaks.html.

———. 2018. "Lenín Moreno denuncia el robo de la base de datos del Plan Toda Una Vida". *El Comercio*. https://www.elcomercio.com/actualidad/politica/leninmoreno-denuncia-robo-basededatos-plan.html.

———. 2019. "'Hackers' lanzaron ofensiva global para atacar web estatales". *El Comercio*. https://www.elcomercio.com/actualidad/hackers-ofensiva-global-ataque-ecuador.html?fbclid=IwAR02_3Am2nbcWgJQWzG88uJcoBsIKl-wHS0TkwPfSX8BSMhuInQ7wzngPjo.

———. 2021. "ANT sufrió ataque cibernético a su sistema AXIS". *El Comercio*. https://www.elcomercio.com/actualidad/ecuador/ant-ataque-cibernetico-sistema-axis.html.

El Universo. 2009. "Cambios en el Sistema Nacional de Inteligencia". *El Universo*. https://www.eluniverso.com/2009/06/09/1/1355/C16AF3BA14674C4DB113E41FD46FD8D2.html?src=web.

———. 2014. "Comando de Operaciones de Ciberdefensa para el 2015, anuncian Fuerzas Armadas de Ecuador". *El Universo*. https://www.eluniverso.com/noticias/2014/09/09/nota/3805401/ffaa-anuncian-2015-comando-operaciones-ciberdefensa/.

———. 2018. “Total Digital abasteció a instituciones de control”. *El Universo*. https://www.eluniverso.com/noticias/2018/03/27/nota/6686836/total-digital-abastecio-instituciones-control/.

Enríquez, Luis. 2021. “Caso Ola Bini: la presunción de inocencia en entornos digitales y el derecho al cifrado”. Univesidad Andina Simón Bolívar. https://www.uasb.edu.ec/ciberderechos/2021/06/15/caso-ola-bini-la-presuncion-de-inocencia-en-entornos-digitales-y-el-derecho-al-cifrado/.

ES Centro Criptológico Nacional. 2019. “Ciberamenazas y Tendencias 2019 CCN-CERT IA-13/19 Resumen Ejecutivo”. *Centro Criptológico Nacional*. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html.

———. 2020. “Ciberamenazas y Tendencias - Edición 2020 CCN-CERT IA-13/20”. *Centro Criptológico Nacional*. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.html.

ES Departamento de Seguridad Nacional. 2017. “La UE reforzará la ciberseguridad”. https://www.dsn.gob.es/es/actualidad/sala-prensa/ue-reforzar%C3%A1-ciberseguridad.

ES Instituto Nacional de Ciberseguridad. 2020. “Membresías”. https://www.incibe.es/que-es-incibe/con-quien-trabajamos/membresias.

———. 2021. “Glosario de términos de ciberseguridad: una guía de aproximación para el empresario”. <i>Instituto Nacional de Ciberseguridad<i>. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf.

ES Ministerio de Defensa. 2014. *Documentos de Seguridad y Defensa 60. Estrategia de la información y seguridad en el ciberespacio*. https://www.uma.es/foroparalapazenelmediterraneo/wp-content/uploads/2014/07/dsegd_60.pdf.

eset. 2022. “ESET”. *Wikipedia*. https://es.wikipedia.org/wiki/ESET.

Estévez, Juan Carlos. 2020. “En qué consiste el convenio de Budapest y cómo regula la ciberdelincuencia”. *Telefónica Tech*. https://empresas.blogthinkbig.com/convenio-budapest-ciberdelincuencia/.

Federal Communications Commission. 2016. “Ley de Protección de la Infancia en Internet (Children’s Internet Protection Act, CIPA)”. *Federal Communications*

Commission. https://www.fcc.gov/consumers/guides/ley-de-proteccion-de-la-infancia-en-internet-childrens-internet-protection-act-cipa.

Forum of Incident Response and Security Teams. 2014. “EcuCERT. FIRST Teams”. https://www.first.org/members/teams/ecucert.

Fundación Mil Hojas. 2022. “Fundación Mil Hojas”. Accedido septiembre 2. https://m.facebook.com/milhojasfundacion/photos/a.715049835260793/1158291684269937/?type=3&locale2=ja_JP.

Ganuza Artiles, Néstor. 2011. “La Situación de la Ciberseguridad en el Ámbito Internacional y en la OTAN”, 166–214.

García Cataña, Héctor Gonzalo. 2022. “Los Ciberdelitos en el Ecuador”. Día del INTERNET SEGURO. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjtr9Pm-oD7AhVSTDABHdLJAucQFnoECAsQAQ&url=https%3A%2F%2Fwww.gobiernoelectronico.gob.ec%2Fwp-content%2Fuploads%2F2022%2F02%2F5.-Gonzalo-Garcia-Unidad-Nacional-de-Ciberdelito.pptx&usg=AOvVaw346cXzHepW2wadvkJzKUxf.

Giannetti, Mayor William. 2017. “Cómo ayudar a EE.UU. a luchar contra la desinformación rusa”. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-30_Issue-1/2018_1_04_giannetti_s.pdf.

Giraldo Montoya, Gladys. 2004. “Hacia una Epistemología Evolucionista”. *Universidad de Chile*, nº 20: 27.

greisbaris. 2016. “McLuhan y la aldea global”. https://greisbaris.wordpress.com/2016/11/04/mcluhan-y-la-aldea-global/.

Hinarejos Rojo, Aurelio, y José De la Peña Muñoz. 2017. “I+D+i y ciberseguridad: análsis de una relación de interdependencia”. En *Cuadernos de Estrategia 185. Ciberseguridad: la cooperación público-privada*. Cuadernos de estrategia 185. Madrid: Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/cuadernos/CE_185.pdf.

Hora 32. 2022. “La Fiscalía y Policía de las unidades de Ciberdelitos de Pichincha detuvieron a presunto ‘hacker’ de información confidencial”. *Hora 32*. https://hora32.com.ec/la-fiscalia-y-policia-de-las-unidades-de-ciberdelitos-de-pichincha-detuvieron-a-presunto-hacker-de-informacion-confidencial/.

INREDH. 2008. “Ecuador: Informe de penetración de la CIA en Fuerzas Armadas y Policía Nacional. Informe comisión para la investigación de los servicios de inteligencia militares y policiales”. https://inredh.org/informe-de-penetracion-de-la-cia-en-fuerzas-armadas-y-policia-nacional/.

Kant, Immanuel. 2012. *Crítica de la razón pura*. Traducido por Pedro Ribas. Primera edición en Taurus. Pensamiento. Madrid: Taurus. https://trabajosocialucen.files.wordpress.com/2012/05/kant-critica-de-la-razon-pura-ribas.pdf.

La República. 2015. “Hackean compañía italiana de espionaje informático. Revelan a Ecuador entre supuestos clientes”. https://www.larepublica.ec/blog/2015/07/07/compania-de-espionaje-hacking-team-es-atacada-por-hackers/.

La Vanguardia. 2015. “Expertos piden un organismo supranacional de ciberseguridad”. https://www.lavanguardia.com/vida/20151009/54438006255/expertos-piden-un-organismo-supranacional-de-ciberseguridad.html.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, y Stephen Wolff. 1997. “Breve historia de Internet”. https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/.

Leiva, Eduardo Alfredo. 2015. “Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local”. *Revista Latinoamericana de Ingeniería de Software* 3 (4). doi:10.18294/relais.2015.161-176.

Loaiza, Yalilé. 2021. “Un ataque informático apagó las computadoras de la Corporación Nacional de Telecomunicaciones del Ecuador”. *infobae*. https://www.infobae.com/america/america-latina/2021/07/19/un-ataque-informatico-apago-las-computadoras-de-la-corporacion-nacional-de-telecomunicaciones-del-ecuador/.

Mena Mena, Paúl. 2021. “Se publicaron los datos privados de más de 1,5 millones de personas custodiados por el Ministerio de Salud del Ecuador”. *El Universo*. https://www.eluniverso.com/noticias/politica/base-datos-privados-covid-19-coronavirus-ministerio-salud-publica-ecuador-nota/.

Mogollón Flores, Francis Stephanía. 2017. “Desafíos de la ciberseguridad y respuestas estatales: el caso del estado ecuatoriano en el período 2008 - 2015”. Tesis Grado,

Pontificia Universidad Católica del Ecuador. http://repositorio.puce.edu.ec/handle/22000/14104.

Moncayo Gallegos, Paco. 2016. *Geopolítica Espacio y Poder*. Universidad de las Fuerzas Armadas ESPE.

Moncayo Gallegos, Paco, François Houtart, Oswaldo Jarrín Román, Miguel Ángel Barrios, Rosario Rodrígez Cuitiño, Daniel Gudiño Pérez, Óscar Montero De la Cruz, et al. 2014. *Geopolítica y estrategia sudamericana Perspectivas Académicas*. Primera. Comisión Editorial de la Universidad de las Fuerzas Armadas - ESPE. https://cespe.espe.edu.ec/wp-content/uploads/2019/03/Geopolitica.pdf.

Naranjo, Lorena. 2022. "Ley Orgánica de Protección de Datos, un logro conjunto". Presentado en Congreso "Desafíos emergentes de la ciberseguridad", Quito.

Organisation for Economic Co-operation and Development y ES Ministerio de Administraciones Públicas, Secretaría General Técnica,. 2004. "Directrices de la OCDE que regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales". http://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf.

Organización de los Estados Americanos. 2018. "Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe". Organización de los Estados Americanos.

———. 2022. "Seguridad Cibernética". https://www.oas.org/es/temas/seguridad_cibernetica.asp.

Ortiz, Sara. 2016. "Hackers registraron 366 títulos universitarios en la Senescyt y entregaron 600 licencias de conducir". *El Comercio*. https://www.elcomercio.com/actualidad/hackers-registraron-titulos-universitarios-falsos.html.

Parlamento Europeo. 2009. "Estrategia Europea de Seguridad y PESD". Diario Oficial de la Unión Europea.

Plan V. 2018. "La Polémica por los Descuentos de GEA Reaviva por Debate por la Privacidad de los Datos". *Plan V*. https://www.planv.com.ec/historias/politica/la-polemica-descuentos-gea-reaviva-debate-la-privacidad-datos.

———. 2019. "La peor filtración de datos en la historia del Ecuador al descubierto". Plan V. https://www.planv.com.ec/historias/sociedad/la-peor-filtracion-datos-la-historia-del-ecuador-al-

descubierto#:~:text=La%20firma%20VPN%20Mentor,corresponden%20a%20menores%20de%20edad.

Price, Matthew, Stephen Walker, y Will Wiley. 2017. “The Machine Beneath: Implications of Artificial Intelligence in Strategic Decisionmaking”. *Features*, nº 4. https://cco.ndu.edu/Portals/96/Documents/prism/prism7_4/181204_Price_PDF.pdf?ver=2018-12-04-161238-277.

Pulido Alonso, Gregorio Miguel, y Rafael Rosell Tejada. 2017. “La cooperación público-privada en el fomento de la cultura de ciberseguridad”. En *Cuadernos de Estrategia 185. Ciberseguridad: la cooperación público-privada*. Cuadernos de estrategia 185. Madrid: Instituto Español de Estudios Estratégicos. https://www.ieee.es/Galerias/fichero/cuadernos/CE_185.pdf.

Ramos, Mario. 2014. “Acerca de la soberanía del Ecuador en el ciberespacio”. Centro Andino de Estudios Estratégicos CENAE. https://www.cenae.org/uploads/8/2/7/0/82706952/acerca__soberania_ecuador_en_el_ciberespacio.pdf.

Rauscher, Karl Frederick, y Valery Yaschenko. 2011. “Russia-US Bilateral on Cybersecurity Critical Terminology Foundations”. *EastWest Institute and the Information Security Institute of Moscow State University*. https://www.files.ethz.ch/isn/130080/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2)-1.pdf.

Realpe, TCRN. Milena. 2022. “La ciberdefensa, sus implicaciones para la seguridad nacional y el rol femenino en la ciberseguridad y ciberdefensa”. Seminario Web Internacional. El rol de la mujer en la ciberseguridad y ciberdefensa.

Rendueles Mata, Miguel, y Mercedes Dreher Grosch. 2007. “La Epistemología y los Sistemas de Información Basados en Inteligencia Artificial”. *Universidad Privada Dr. Rafael Belloso Chacín* 6 (1): 158–69.

Rivadeneira, Erwin Frederick. 2016. “Stuxnet, la Primera Ciberarma”. *Ciencia y Tecnología*, nº 2. https://revistamarina.cl/revistas/2016/2/efrederickr.pdf.

Rodrigo, Fajardo. 2021. *Proyecto de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia*. Memorando Nro. AN-PR-2021-0431-M, 22 de octubre. http://ppless.asambleanacional.gob.ec/alfresco/d/d/workspace/SpacesStore/8ccd13d5-a886-4099-a810-007c7fae7bc0/pp-seg-dig-410903-fajardo(1).pdf.

Sain, Gustavo. 2016. "¿Qué es la ciberguerra?" *Revista Pensamiento Penal*. https://www.pensamientopenal.com.ar/system/files/2016/02/doctrina42952.pdf.

Sánchez Miñana, Jesús, y Carlos Sánchez Ruiz. 2011. "Sobre la difusión del teléfono de Bell en sus comienzos (1876-1877)". *Actes D'història de la Ciència I de la Tècnica*, nº 4: 33–53. doi:10.2436/20.2006.01.161.

Sancho Hirare, Carolina. 2017. "Ciberseguridad. Presentación del dossier". *URVIO - Revista Latinoamericana de Estudios de Seguridad*, nº 20: 8–15. doi:http://dx.doi.org/10.17141/urvio.20.2017.2859.

Santos, Milton. 2000. *La naturaleza del espacio*. 1ª ed. Barcelona: Ariel, S.A. https://docer.com.ar/doc/x0s8v80.

Secretaría de la Commonwealth, Organización de Telecomunicaciones de la Commonwealth, Deloitte, Centro de Política de Seguridad de Ginebra, Centro Global de Capacitación en Ciberseguridad de la Universidad de Oxford, Unión Internacional de Telecomunicaciones, Microsoft, et al. 2018. "Guía para la elaboración de una estrategia nacional de ciberseguridad". https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf.

Sputnik Mundo. 2018. "Presidente de EEUU promulga estrategia nacional de ciberseguridad". https://mundo.sputniknews.com/america_del_norte/201809201082142659-presidente-eeuu-promulga-estrategia-nacional-ciberseguridad/.

Stein, Abraham. 2009. "El concepto de Seguridad multidimensional". *Centrales*, 31–37.

Sturm, Cony. 2011. "China tiene un equipo especial de soldados entrenados para la guerra cibernética". *FayerWayer*. https://www.fayerwayer.com/2011/05/china-tiene-un-equipo-especial-de-soldados-entrenados-para-la-guerra-cibernetica/.

Tableau Public. 2022. "Bienvenido a Tableau Public". Accedido octubre 26. https://public.tableau.com/app/discover.

Tavella, Fernando. 2022. "Operación Pulpo Rojo: campaña de malware dirigida a organismos de alto perfil de Ecuador". *eset*. https://www.welivesecurity.com/la-es/2022/08/30/campana-malware-dirigida-organismos-alto-perfil-ecuador/.

United Nations Office for Disarmament Affairs. 2017. "Cyberdiplomacy Course: Furthering the peaceful use of ICTs". *United Nations Office for Disarmament Affairs*. https://cyberdiplomacy.disarmamenteducation.org/home.

United Nations Office on Drugs and Crime. 2010. *Transnational Organized Crime Threat Assessment*. Vienna. https://www.unodc.org/documents/data-and-analysis/Studies/TOCTA_draft_2603_lores.pdf.

Universidad Internacional de Valencia. 2018. "Evolución de la red de comunicación móvil, del 1G al 5G". *Universidad Internacional de Valencia*. https://www.universidadviu.com/int/actualidad/nuestros-expertos/evolucion-de-la-red-de-comunicacion-movil-del-1g-al-5g.

Usuarios Digitales, y Fundación Mil Hojas. 2016. "Coalición por la Defensa del Derecho de Privacidad y Seguridad Digital Contribución Conjunta para el Tercer Ciclo del Examen Periódico Universal a Ecuador". https://sobrevivientes.planv.com.ec/wp-content/uploads/2019/06/11.-EPU-Informe-sobre-privacidad-i-acceso-al-internet-Mil-hojas-y-Derechos-Digitales.pdf.

Vargas Borbúa, Robert, Luis Recalde Herrera, y Rolando P. Reyes Chicango. 2017. "Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa". *URVIO, Revista Latinoamericana de Estudios de Seguridad*, nº 20: 31–45. doi:https://doi.org/10.17141/urvio.20.2017.2571.

Vergara, Evergisto de, Gustavo Adolfo Trama, Marcelo Noel Uriona, Javier Ulises Ortiz, y Lucia Alejandra Destro. 2017. "Operaciones militares cibernéticas: Planeamiento y Ejecución en el Nivel Operacional". *CEFADIGITAL*. http://www.cefadigital.edu.ar/bitstream/1847939/939/1/CAVIII%20-%20OMC%20DE%20VERGARA.pdf.

Villalba Fernández, D. Aníbal. 2015. "La Ciberseguridad en España 2011 – 2015 Una Propuesta de Modelo de Organización". Tesis doctoral, Madrid: Universidad Nacional de Educación a Distancia. http://e-spacio.uned.es/fez/eserv/tesisuned:CiencPolSoc-Avillalba/VILLALBA_FERNANDEZ_Anibal_Tesis.pdf.

Viollier, Pablo. 2017. "La participación en la elaboración de la Política Nacional de Ciberseguridad: Hacia un Nuevo Marco Normativo en Chile". https://www.derechosdigitales.org/wp-content/uploads/ciberseguridad.pdf.

Anexos

Anexo 1: Escenario SENAIN

De acuerdo al trabajo realizado por el periodismo de investigación de la Fundación Mil Hojas, en el 2013 la Secretaría Nacional de Inteligencia (SENAIN) "[…] realizó la contratación de varios equipos de espionaje a la compañía "500 *Smart Solutions* LLC", […] *Hacking Team*, empresa italiana especializada en vender sistemas de seguridad a gobiernos que quieren espiar a sus ciudadanos"(Fundación Mil Hojas 2022, párr 13; 16; énfasis añadido).

En el hackeo a *Hacking Team* se revela a Ecuador como cliente **"Ecuador:** SENAIN está usando su tecnología para recolectar inteligencia para el gobierno ecuatoriano. Más de $535.000 pagados al grupo *Hacking Team*"(La República 2015, párr. 8; énfasis en el original ; énfasis añadido).

WikiLeaks, fundada por Julian Assange, "reveló los correos interceptados a *Hacking Team* y sus conexiones con gobiernos alrededor de mundo". (El Comercio 2015, párr. 3; énfasis añadido) Lo que reveló que "*Hacking Team*, es una empresa que ofrece servicios de vigilancia en Internet a gobiernos y compañías privadas […]." (El Comercio 2015, párr. 3; énfasis añadido).

Otro de los datos revelados fue que, posterior a la creación de la SENAIN, contratos públicos importantes se realizaron entre "la empresa ecuatoriana *Total Digital* S.A. que sirvió de nexo entre la Secretaría Nacional de Inteligencia (SENAIN) y la firma italiana *Hacking Team* (HT)" (El Universo 2018, párr. 1; énfasis añadido).

Según el portal digital Código Vidrio, en 2014, la SENAIN contrató a la empresa *Emerging* MC "para proteger el perfil digital de Rafael Correa y su familia" (Código Vidrio 2020, párr. 74). Políticos de oposición denunciaban que fue contratada para perseguir y difamar en redes sociales a quienes pensaban diferente. Es así, que la empresa *Illuminati Lab* "cumplió una tarea de asesoría en estrategia de redes" (Código Vidrio 2020, 82), copando las redes y aplastando a los críticos del gobierno, difundiendo "todo tipo de mensajes y ***fake news***" (Código Vidrio 2020, 80; énfasis en el original) y fue escogido "para que sea representante en las negociaciones con *Hacking Team*" (Código Vidrio 2020, 82; énfasis añadido). También se conoce de la empresa *Eye Watch*

contratada también por la SENAIN encargada de "enfilar ataques digitales" (Código Vidrio 2020, 86).

Sin embargo, la Secretaría Nacional de Inteligencia publicó un comunicado sobre la relación del Gobierno y la firma *Hacking Team* en el que indica que no existe relación contractual con dicha empresa; así como también que es "[…] falso que alguna **contratación** de la Senain, haya servido para atacar **medios digitales** u otros objetivos políticos […]" (Bravo 2015, párr. 4; énfasis en el original).

En octubre 2016, Ecuador fue denunciado en la Sede de las Naciones Unidas en Ginebra, Suiza, como parte del Examen Periódico Universal (EPU) por espionaje y seguimientos ilegales a ciudadanos disidentes del gobierno a políticos y periodistas. Las organizaciones civiles prepararon un informe y participó en representación la organización Usuario Digitales. Usuarios Digitales conjuntamente con Fundación Mil Hojas presentaron un informe del estado de Internet, los ataques que sufrían los ciudadanos, así como el ciber acoso con el tema del *troll center*, bloqueo de acceso al Internet y la compra de equipos de espionaje a *Hacking Team* por la SENAIN. Dichas organizaciones se vinculan "con el derecho al acceso a internet, y la investigación y defensa de la intimidad y privacidad, tanto a nivel personal como virtual" (Usuarios Digitales y Fundación Mil Hojas 2016, 1) y el informe destaca la "afectación a la privacidad personal […] derecho al Internet y derecho a la privacidad […] acceso y uso de Internet en Ecuador […]" (Usuarios Digitales y Fundación Mil Hojas 2016, 5, 13, 14).

Se indica en el informe del Examen Periódico Universal (EPU) que el portal Ecuador Transparente dio a conocer 31 documentos de la SENAIN, "[…] fechadas del año 2012 y 2014, que documentan el espionaje sistémico a políticos de oposición y activistas por parte del gobierno" (Usuarios Digitales y Fundación Mil Hojas 2016, 7). Se habla de fichas de investigación: empresarios, políticos y periodistas que tenía la SENAIN para investigar y que habría solicitado información a la plataforma gubernamental datoseguro.gob.ec.

Anexo 2: Escenario Tropas Cibernéticas

Ecuador está entre las naciones cuyos gobiernos tienen 'tropas cibernéticas' (*bots*) para manipular la crítica en redes sociales, asegura el estudio "*Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*" (Bradshaw y Howard 2017, 1; énfasis añadido) elaborado por la Universidad de Oxford. La manipulación organizada de las redes sociales ocurre en muchos países alrededor del

mundo. En varios de ellos, las tropas cibernéticas tienen múltiples afiliaciones, financiadores o clientes. Sin duda, la organización de las cibertropas seguirá evolucionando. Es probable que permanezca, sin embargo, como un fenómeno global. El estudio mencionado se realizó para 28 países: Argentina, Azerbaiyán, Australia, Bahréin, Brasil, China, República Checa, Ecuador, Alemania, India, Irán, Israel, México, Corea del Norte, Filipinas, Polonia, Rusia, Arabia Saudita, Serbia, Corea del Sur, Siria, Taiwán, Turquía, Ucrania, Reino Unido, Estados Unidos, Venezuela y Vietnam. (Bradshaw y Howard 2017).

> *In Ecuador, individual targeting is coordinated through the government using the web-based platform Somos +* (Morla, 2015a). […] *In Ecuador, the government launched a website called Somos + to investigate and respond to social media users who criticize the government. The website sends updates to subscribers when a social media user criticizes the government, allowing pro-government supporters to collectively target political dissidents* (Morla, 2015a). […] *Other cyber troops are employed under the executive branch of government. For example, in Argentina and Ecuador, cyber troop activities have been linked to the office of the President* (Rueda, 2012; Morla, 2015a, 2015b). […] *For example, Ecuador, which contracts out cyber troop activity to private firms, spends, on average, USD200,000 per contract.* (Morla, 2015) (Bradshaw y Howard 2017, 10, 11, 15, 19; énfasis añadido)

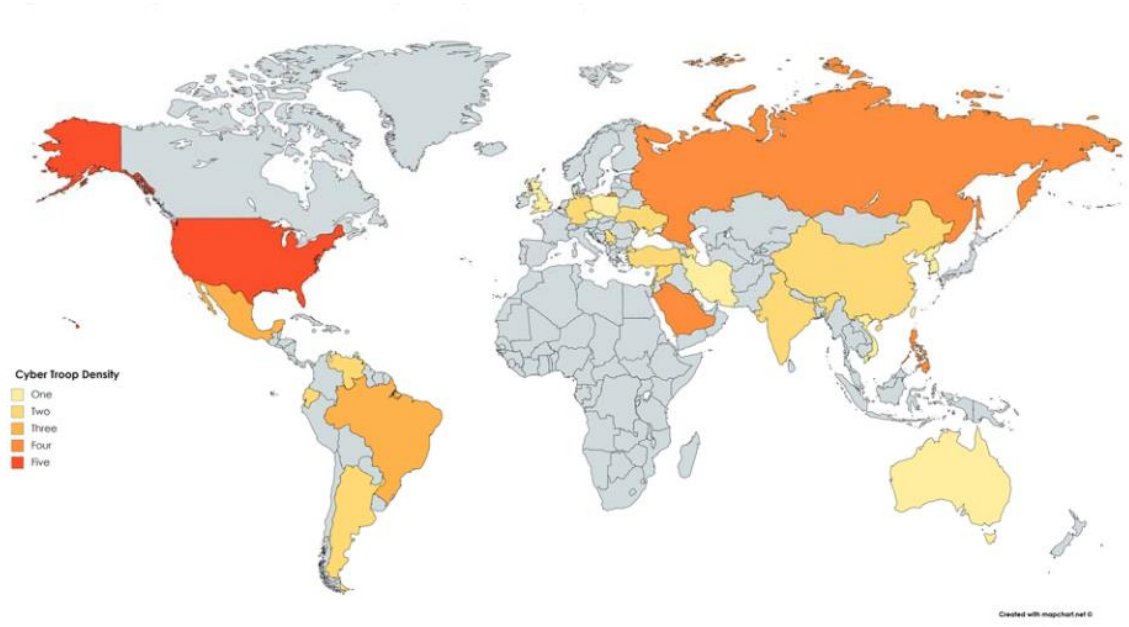

Figura 8. Densidad organizativa de las cibertropas.
Fuente: Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation (Bradshaw y Howard 2017, 22)

Anexo 3: Escenario Ataques informáticos a Ecuador

> acciones implementadas por parte del Gobierno Nacional ante los más de 40 millones de ataques informáticos recibidos por el país desde la decisión soberana de retirar el asilo diplomático a Julian Assange. […] "a tal punto fueron los ataques al Ecuador que, el 11 de abril en horas de la tarde, pasamos del puesto 51 al 31 a escala mundial en el volumen de ataques cibernéticos". […] instituciones como el IESS, sistema de salud pública, SRI, Banco Central, CNEL, CELEC y todas aquellas que brindan servicios ciudadanos fueron priorizados para la implementación del Protocolo y se mantendrá activado indefinidamente. […] las principales instituciones que recibieron los intentos de intrusión fueron: Cancillería, Banco Central, Presidencia de la República, ministerio del Interior, Servicio de Rentas Internas, CNT, varios GAD, Consejo de la Judicatura, ministerio de Telecomunicaciones y de la Sociedad de la Información, ministerio de Turismo, ministerio de Ambiente y algunas universidades. (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2019b, párrs. 1, 2, 5, 6)

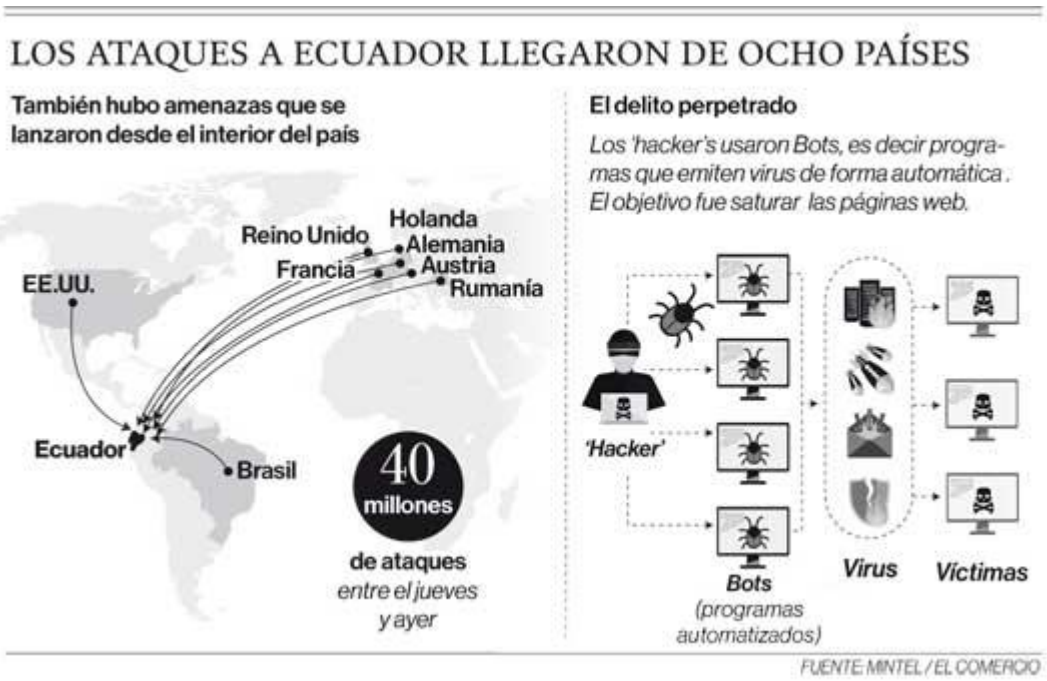

Figura 9. Los ataques a Ecuador llegaron de ocho países.
Fuente: 'Hackers' lanzaron ofensiva global para atacar web estatales (El Comercio 2019)

Anexo 4: Escenario CONSEP

Desde el 2015 se evidencia ciertos casos en los cuales se ven afectados los datos personales y se analiza que el derecho a la protección de datos es primordial, de tal manera de mitigar los incidentes en el país.

El Consejo Nacional de Control de Sustancias Estupefacientes y Psicotrópicas (CONSEP) manejaba una lista de consumidores de drogas que eran usados para temas de salud pública y para evitar que estén registrados privados de libertad. Porque si detenían con droga a una persona, se consideraba que eran traficantes o micro traficantes, pero si

estaban en la lista se consideraban que eran consumidores y por lo tanto no eran detenidos. El CONSEP vendió esta base de datos a un banco, el cual la usó para análisis crediticio, este banco fue denunciado y tuvo conocimiento la Defensoría del Pueblo. Desde la perspectiva de la "No Discriminación" logró que efectivamente se resarza esta "Violación del derecho a la honra"; así como también el Derecho a la "Protección de la Personalidad y Dignidad Humana", por lo que no se estaría solucionando la problemática, se necesita verificar que ese ciudadano que fue afectado no siga siendo. El uso ilegítimo de la base de datos, las finalidades indebidas en otras situaciones similares y determinar quién es el encargado para resolver esto y evitar que no se repita convirtiéndose en una condición general, nace la necesidad para determinar la defensa de estos derechos y de la protección de datos personales (Naranjo 2022).

Anexo 5: Escenario: SENESCYT & ANT

En el 2016, la Policía y la Fiscalía evidenció que "Hackers registraron 366 título universitarios en la Senescyt y entregaron 600 licencias de conducir" (Ortiz 2016, párr. 1). En el operativo "Impacto inicial", una banda de supuestos hackers, fue desarticulada, habrían cobrado por registrar títulos falsos en el sistema informático de la Secretaría Nacional de Educación Superior (SENESCYT), así como también habrían atacado los sistemas informáticos de la Agencia Nacional de Tránsito (ANT) para la falsificación de licencias de conducir. Algunas entidades financieras como el Banco Central del Ecuador también se vieron afectados; esta red de hackers de los cuales fueron detenidos sus cabecillas, vulneraba las bases de datos de instituciones. Se calcula que con esta banda "movieron USD 1 millón a cuentas bancarias en el país y también derivaron el dinero a Colombia" (Ortiz 2016, 4).

Anexo 6: Escenario GEA

En el 2017, las demasiadas e intensas llamadas telefónicas realizadas por personal de varios *calls centers* a muchos clientes de los bancos del Pacífico y Banco de Guayaquil para ofertas de productos o servicios como: ""Asistencia tarjeta segura", "Asistencia respaldo integral", "Asistencia cuidados hospitalarios", "Asistencia 24 horas conmigo", "Asistencia dental y exequial", "Asistencia médico familiar" entre otros" (Plan V 2018, párr. 25). Por dichas ofertas se realizaban descuentos, algunos sin autorización de débitos automáticos a las cuentas bancarias de los clientes. Este particular fue comentado por el

“presentador de TC Televisión, Mauricio Ayora” (Plan V 2018, párr. 10). Esto se debe a que los bancos mencionados vendieron las bases de datos de sus clientes a la empresa GEA, de la cual Eduardo Jurado, exsecretario del expresidente Lenin Moreno, figura como accionista. Este tipo de llamadas han provocada en algunas personas sentirse ciber acosadas y ha existido la falta de privacidad para el tratamiento de datos personales (Plan V 2018).

Anexo 7: Escenario Plan Toda Una Vida

En el 2018, la base de datos del Plan Toda Una Vida fue robada. Esta base de datos contenía información de ecuatorianos. A través de mensajes maliciosos que recibieron 400.000 personas, jugaron con sus sentimientos, al recibir información de la supuesta asignación de casa. El expresidente Lenin Moreno condenó esto, diciendo que tenían la intención de influir en su proyecto como objetivo de un ataque. Moreno se refirió a los rumores, campañas agresivas y ataques que podrían ocurrir durante el referéndum del domingo 4 de febrero de 2018. Dijo que la gente debería ignorar estos intentos de sembrar discordia (El Comercio 2018).

Anexo 8: Escenario Ola Bini

Como es de conocimiento público, el presidente de la República le ha retirado el asilo al señor Julian Assange. Según el No. Proceso: 17282-2019-01265 de la Función Judicial del Ecuador (EC Consejo de la Judicatura 2019), para el caso de Ola Metodius Martin Bini de nacionalidad sueca, “la ex-Ministra del interior María Paula Romo, declaró el mismo día acerca de intentos de desestabilización del Gobierno, y acerca de que en Ecuador existen *“dos hackers rusos y entre ellos un miembro de wikileaks que tiene contacto directo con Julian Assange”*” (Enríquez 2021, párr. 3; énfasis en el original).

Se genera orden de detención y allanamiento dispuesta por autoridad competente, actas de allanamiento e incautación, acta entrega del inmueble, parte detención con fines investigativos por orden de autoridad competente, formulario único cadena custodia, lectura derechos constitucionales en inglés y español al señor Bini Ola Metodius, correo electrónico al Consulado de Suecia, fijación de indicios, reporte médico detenido, consulta de peritos acreditados al Consejo de la Judicatura, informe movimientos financieros ampliados del señor Bini Ola Metodius, operaciones reportadas en el sistema

financiero nacional, datos de la Unidad de Análisis Financiero y Económico en el que uno de los beneficiarios es TELCONET S.A (EC Consejo de la Judicatura 2019).

> La petición de Audiencia de Formulación de Cargos, por el Delito FLAGRANTE de Tipo de acción: ACCIÓN PENAL PÚBLICA, presentado por: FISCALIA GENERAL DEL ESTADO, En contra de: BINI OLA METODIUS por presunta Infracción: ART. 232 NUMERAL 1 COIP ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS, solicitando la prisión preventiva. LA JUDICATURA LA CONCEDE Y DISPONE SE GIRE LA CORRESPONDIENTE BOLETA CONSTITUCIONAL DE ENCARCELAMIENTO EN SU CONTRA; ASÍ COMO, LA MEDIDA CAUTELAR ESTABLECIDA EN EL ART. 556 DEL COIP; ESTO ES, RETENCIÓN DE CUENTAS BANCARIAS QUE SE ENCUENTREN A NOMBRE DE BINI OLA METODIUS. POR TRATARSE DE UNA FORMULACIÓN DE CARGOS, ESTA AUTORIDAD SE INHIBE DE SEGUIR CONOCIENDO LA PRESENTE CAUSA Y DISPONE QUE LA PRESENTE ACTUACIÓN SEA REASIGNADA A LA UNIDAD CORRESPONDIENTE. (EC Consejo de la Judicatura 2019)

Inicialmente, no ha podido tener acceso a sus abogados, lo que vulnera sus derechos. Ha existido falta de prolijidad en ciertos funcionarios de las respectivas instituciones que deben llevar a cabo la Reinstalación de la Audiencia Evaluatoria y Preparatoria del Juicio, para la designación de peritos de la Dirección Nacional de Peritos de la Policía Nacional, así como, designar peritos de la Dirección Nacional de Peritos de la Policía Judicial. Después de tanto tiempo y demora se tiene fijado la convocada audiencia de juzgamiento para el 11 de noviembre del 2022 del 2022, una vez que se ha logrado el sorteo de perito Interprete Traductor en idioma inglés. En relación con el perito interprete traductor en el idioma sueco, se acepta al señor sugerido por el procesado Ola Metodius Martin Bini, y con respecto a sus honorarios, el peticionario debe correr con los honorarios puesto que dicho traductor no se encuentra acreditado por el Consejo de la Judicatura (EC Consejo de la Judicatura 2019).

Anexo 9: Escenario Novaestrat

A partir del caso Novaestrat[23] en el 2019, los ecuatorianos iniciaron a tomar conciencia sobre la protección de datos personales. A través de un aviso de la firma de seguridad VPN *Mentor*[24] y el portal de tecnología Zdnet.com anunciaron que un servidor, de "propiedad de la empresa Novaestrat" (Plan V 2019, párr. 15), que contiene bases de

[23] "Novaestrat es una empresa ecuatoriana dedicada a reinventar tu empresa en base a los datos procesados, para tomar decisiones acertadas con el menor impacto possible" (Plan V 2019, párr. 15).

[24] "VPN Mentor es el sitio web de revisión de VPN (red privada virtual) más grande del mundo. Su laboratorio de investigación es un servicio que se esfuerza por ayudar a la comunidad en línea a defenderse de las amenazas cibernéticas" (Plan V 2019, párr. 3).

datos del Ecuador, no tiene seguridades y hallaron una filtración de información personal de más de 20 millones de ecuatorianos incluidos menores de edad, información actualizada hasta el 2019. Esta cantidad de registros de usuario superaba a los 16 millones de la población ecuatoriana. "Un equipo dirigido por los investigadores Noam Rotem y Ran Locar descubrió la vulneración que puede incluir datos además de personas fallecidas" (Plan V 2019, párr. 2).

La información filtrada posiblemente correspondía a las instituciones: Registro Civil, Asociación de Empresas Automotrices del Ecuador (AEADE) y BIESS. En esta violación de datos, "Los investigadores también encontraron una entrada sobre Julian Assange, fundador de *WikiLeaks*, con su número de cédula ecuatoriana." (Plan V 2019, párr. 12; énfasis añadido). Esta información se encontraba alojada en un servidor en Miami, la misma que no contenían seguros de protección. Se generó un proceso penal, creando una comisión para que investigue este caso llamado Novaestrat, por la usurpación de la información, la cual detectó que no fue un tema técnico del Esquema Gubernamental de Seguridad de la Información, capacitación o políticas pública, sino que no existía un Ley de Protección de Datos Personales. Exfuncionarios de instituciones públicas del Ecuador constan como socios de la empresa Novaestrat.

La Fiscalía allanó las viviendas de los socios en la que:

> incautaron equipos electrónicos, computadores y dispositivos de almacenamiento […]. Se investiga un presunto delito de violación a la intimidad. […] Andrés Michelena, ministro de Telecomunicaciones, confirmó que no hubo hackeo sino una posible venta de las bases de datos conectadas con el SIN.[25] […] Lorena Naranjo, directora de la Dirección Nacional de Registro de Datos Públicos, informó que en 72 horas enviará a la Asamblea una la ley de protección de datos personas. […]. El portal VPN Mentor apunta a que los datos filtrados podrían crear problemas de privacidad duraderos para las personas afectadas. Es decir, pueden ser víctimas de estafas y ataques de phishing. […] Los ataques de suplantación de identidad pueden adaptarse […] Otro riesgo que identifican es el robo de identidad y fraude financiero porque están los números de identificación nacionales y números únicos de contribuyentes. […] Los datos filtrados incluían información sobre los empleados de muchas compañías, así como detalles sobre algunas compañías y por lo tanto pueden estar en riesgo de espionaje comercial y fraude. (Plan V 2019)

Anexo 10: Escenario CNT

La Corporación Nacional de Telecomunicaciones (CNT) del Ecuador informó que presentó una denuncia ante la fiscalía general del Estado por el delito de "ataque a los

[25] Proyecto emblemático de fortalecimiento del Sistema Nacional de Información (SNI) (Plan V 2019, párr. 16)

sistemas informáticos" para que se realice la investigación previa y se determinen responsables. Así lo anunció el viernes 16 de julio de 2021. La empresa pública había señalado que sus sistemas registraban intermitencias en sus sistemas de atención al cliente, agencias y *Contact Center*. Se supo de fuentes internas de la empresa pública que el ataque informático es de tipo *Ransomware.*[26] Debido al ataque, todo el personal de la empresa pública comenzó a recibir disposiciones de apagar los computadores desde el jueves 15 de julio del 2021 (Loaiza 2021).

Durante el 2021 se evidenciaron más ataques de Ransomware en instituciones financieras como el Ministerio de Finanzas y el Banco Pichincha. Estos ataques han sido realizados por ciberdelincuentes llamados *Hotarus Corp.*[27] Estos han publicado en un portal de extorsión los casos de ataques a las instituciones de Ecuador: Banco Pichincha y Filiales, Petro Ecuador, IESS / SRI.

Anexo 11: Escenario Ministerio de Salud

Durante de la pandemia del COVID-19, en julio 2021, se evidencia una fuja de información de datos personales de ciudadanos ecuatorianos que fueron vacunados. Bajo una presión mediática que los ciudadanos exigían al gobierno que presenten las estadísticas de cómo avanzaba la vacunación en el país. La institución que hizo público los datos fue el Ministerio de Salud (MSP), sin considerar las respectivas seguridades y las implicaciones que se generarían. Esta información fue publicada el domingo 25 de julio del 2021 durante unas horas, luego de ello el mismo día fue bajado. La información que fue publicada contiene:

> nombres y apellidos, número de cédula, teléfono, ocupación profesional, autoidentificación étnica, fecha de nacimiento, parroquia de domicilio, número de historia clínica, diagnóstico médico y otros datos privados de más de 1,5 millones de personas que se han realizado un examen para COVID-19 en Ecuador […]. (Mena Mena 2021, párr. 3)

A través de un mensaje escrito, el MSP afirmó a EL UNVERSO que

> detectó la omisión de un filtro de seguridad que permitió el acceso momentáneo a la base de datos sobre COVID-19. Tan pronto se conoció de hecho, este fue corregido siguiendo

[26] Ransomware: "Este ciberdelito consiste en propagar a los dispositivos un software maligno a través de archivos adjuntos o enlaces fraudulentos en correos electrónicos, sitios web y memorias USB infectadas. Cuando el programa malicioso se activa el sistema se bloquea y se cifran los datos. Para recuperar el sistema y los datos, los ciberdelincuentes exigen un pago a los afectados. Este pago se negocia en la Dark Web" (Loaiza 2021, párr. 6).

[27] "'"Hotarus Corp" ha actualizado su sitio en la Dark Web para presentarse como un nuevo portal de extorsión en Latinoamérica" (CyberSecure 2021, párr. 5).

> los protocolos de protección de datos y se solicitó un informe técnico para establecer las acciones administrativas correspondientes. (Mena Mena 2021, párr. 12)

Una plataforma digital con 1,5 millones de datos fue publicada, se trataba de *Tableau Public,*[28] en donde se visualizaba dos infografías de las cifras de la pandemia. Una de ellas era de sólo visualización, mientras que la otra infografía permitía descargar la información sin restricción alguna.

Anexo 12: Escenario Agencia Nacional de Tránsito

El sistema *AXIS*[29] fue atacado de la Agencia Nacional de Tránsito (ANT), esto ocurrió el jueves 21 de octubre del 2021. Este ataque cibernético dificultó que los ciudadanos realicen los trámites de licencias y matrículas vehiculares.

> La ANT explicó que este **ataque** se produce 24 horas después de establecer medidas de seguridad informática para evitar ilícitos con la entrega de licencias; […] ejecutar **procesos regulatorios** para anular "el alza fraudulenta de puntos, la entrega ilícita de licencias profesionales y no profesionales y la baja de 100 000 procesos de matriculación vehicular entregados sin el pago de las multas correspondientes". (El Comercio 2021, párr. 2; énfasis en el original)

Con los servicios de Firewall y ciberseguridad contratados por la ANT permitieron restituir el servicio a la colectividad, así como garantizó protección a la información de los datos personales. La anulación de "35000 licencias de conducir" (El Comercio 2021, párr. 6) ha generado que la ANT reciba "afectaciones al sistema y a la base de datos, así como amenazas personales al equipo de servidores encargados"(El Comercio 2021, párr. 6).

Anexo 13: Escenario Operación Pulpo Rojo

ESET[30] Latinoamérica con su equipo de investigación descubrió la "Operación Pulpo Rojo" (Tavella 2022) llevada a cabo entre junio y julio de 2022. Esta es una campaña de malware que estaba dirigida a organizaciones en muchos países de América. El equipo encontró que la mayor parte de la campaña fue enviada a Ecuador a empresas privadas, agencias gubernamentales y organizaciones de salud (Tavella 2022).

---

[28] Tableau Public "Una plataforma gratuita para explorar, crear y compartir públicamente visualizaciones de datos en línea"(Tableau Public 2022).

[29] "AXIS es un **sistema interconectado** a escala nacional con la ANT y la Comisión de Tránsito del Ecuador (CTE) cuyos datos están en una sola base integral" (El Comercio 2021, párr. 3).

[30] ESET compañía de software especializada en ciberseguridad (eset 2022).

Remcos,[31] herramienta de software utilizada inicialmente para monitorear y controlar sus dispositivos de forma remota. Los ciberdelincuentes utilizan el Remcos para espiar y robar información confidencial de las víctimas como parte de una estafa (Tavella 2022).

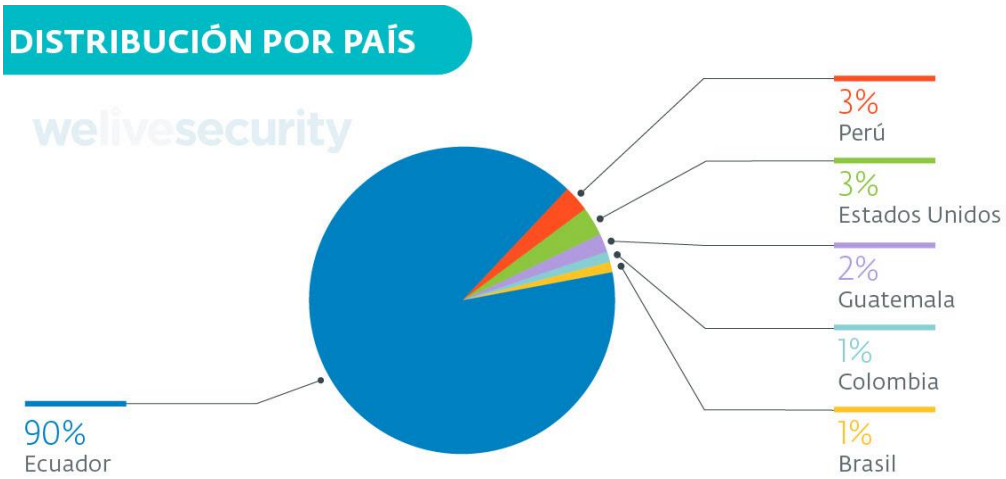

Figura 10. Países afectados por la campaña Operación Pulpo Rojo.
Fuente: welivesecurity by eset (Tavella 2022)

El mecanismo de infección de esta campaña de malware fue a través del correo electrónico, utilizaron correos de phishing. Para el caso de Ecuador existieron supuestos correos enviados desde la fiscalía general del Estado que contenían archivos adjuntos maliciosos.

Anexo 14: Acceso ilegal a datos personales en sistemas del CIES

En la ciudad de Loja, la Unidad de Ciberdelitos de la Policía Nacional, la entidad de Ciberdelitos de la Policía (Ciberpol) y la Fiscalía del Estado detuvo a un sospechoso. Este sujeto habría accedido ilegalmente a los datos personales de ciudadanos ecuatorianos. Esta información correspondía a los sistemas de inteligencia y contrainteligencia del Centro de Inteligencia Estratégica (CIES), la cual consumo datos desde la Dirección Nacional de Registros Públicos. La información sustraída era promocionada a través de redes sociales y vendida a personas naturales y jurídicas (Campaña 2022).

Según Hora 32:

> Si el presunto 'hacker' es declarado culpable por el delito de revelación ilegal de base de datos, de acuerdo al Art. 229 del Código Orgánico integral Penal (COIP), él sería

[31] Troyano de acceso remoto RAT (Tavella 2022, párr. 2).

> condenado de 1 a 3 años de cárcel, según los delitos contra la seguridad de los sistemas de información y comunicación. (Hora 32 2022, párr. 6)

En la Agenda de Transformación Digital del Ecuador 2022-2025 presentada, en agosto del 2022, por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) se establece el objetivo general:

> Instaurar un marco de trabajo multisectorial coordinado que establezca líneas de acción en relación al proceso de transformación digital del país, definiendo su gobernanza e institucionalidad, y considerando para ello la transversalidad de las TIC. (EC Ministerio de Telecomunicaciones y de la Sociedad de la Información 2022c, 14)