ESCUELA CPRI

EL CAMBIO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA OCURRIDAS POR LA CREACIÓN DE NUEVAS INSTITUCIONES A PARTIR DEL AÑO 2013 EN EL ECUADOR

AUTOR

María Fernanda Carrera Celi

AÑO

2019

ESCUELA DE CIENCIAS POLÍTICAS Y RELACIONES INTERNACIONALES

EL CAMBIO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA OCURRIDAS POR LA CREACIÓN DE NUEVAS INSTITUCIONES A PARTIR DEL AÑO 2013 EN EL ECUADOR

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Licenciada en Ciencias Políticas y Relaciones Internacionales.

Profesor Guía:
Alegría Donoso Vallejo

Autora:
María Fernanda Carrera Celi

Año:
2019

DECLARACIÓN DE LA PROFESORA GUÍA

“Declaro haber dirigido el trabajo, “El cambio de las políticas de seguridad informática ocurridas por la creación de nuevas instituciones a partir del año 2013 en el Ecuador”, a través de reuniones periódicas con la estudiante María Fernanda Carrera Celi, en el semestre 2019-2, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Alegría Donoso

C.I. 170461429

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, “El cambio de las políticas de seguridad informática ocurridas por la creación de nuevas instituciones a partir del año 2013 en el Ecuador”, de María Fernanda Carrera Celi, en el semestre 2019-2, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Ian Burdette Keil

C.I. 1754975108

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

María Fernanda Carrera Celi

C.I. 1311689440

AGRADECIMIENTOS

A mi madre, que es la fuente principal de mi inspiración, quien me motiva cada día a cumplir mis objetivos y me brinda todo el apoyo para realizarlos.

A mi hermana, por ser mi rayito de sol en mis días nublados, porque con ella la tristeza no es una opción.

A mis amigos, por nunca dejar de creer en mí y enseñarme lo más maravilloso de una amistad, la confianza.

A Alegría Donoso, por ser mi mentora y soporte durante todo este proceso, para que esta investigación sea posible

DEDICATORIA

Este trabajo va dedicado a mi madre y hermana, que son los pilares de mi vida, por siempre brindarme apoyo, creer en mí y darme fuerzas para lograr metas. El camino ha sido muy duro sin ustedes, pero desde lejos sentía su amor muy presente.

RESUMEN

Lo que motivó esta investigación es la necesidad de analizar el cambio de las políticas de seguridad informática en el Ecuador desde el año 2013 y cómo nacen nuevas instituciones que adoptan medidas de seguridad informática. Es por ello que esta investigación se enfocará en el estudio del cambio de políticas en seguridad informática en el período del gobierno de Rafael Correa y su implementación en las instituciones públicas.

Con esta investigación se espera aportar a la comprensión de la importancia que tiene la seguridad informática en el Estado y cómo la nueva era tecnológica podría ocasionar un desbalance. Este estudio se ha enfocado desde la teoría de la securitización, para ello se analiza el discurso del expresidente Rafael Correa y como se configuraron los cibercrímenes como una amenaza existencial para el Estado ecuatoriano. También se identifica las posibles motivaciones que llevaron al gobierno a implementar regulaciones en este ámbito. Se realiza una recopilación de leyes, reglamentos, acuerdos etc., en la que se explica el cambio y su enfoque hacia la seguridad informática. El reciente suceso en el Ecuador, el retiro del asilo de Julian Assange, tuvo gran relevancia para este tema, debido a los sinnúmeros de ataques que vivió el país, por lo que analizará su repercusión y como se transformó en una amenaza real dentro del país.

Palabras claves: ciberseguridad, políticas, cibercrímenes, ciberdefensa, seguridad informática, ciberespacio.

ABSTRACT

This research aims at analyzing the changes in computer security policies in Ecuador since 2013 and how new institutions adopted computer security measures are born. That is why this research will focus on the study of the change in information security policies in the period of Rafael Correa and its implementation in public institutions.

This research is expected to contribute to the understanding of the importance of computer security in the State and how the new technological age could cause an imbalance. This study is focused on the theory of securitization, for this purpose, the speech of former President Rafael Correa is analyzed and how cybercrimes become real threats to the Ecuadorian State. It also identifies the possible motivations that led the government to implement regulations in this area. A compilation of laws, regulations, agreements, etc. is made, in which the change and its approach towards computer security is explained. The recent success in Ecuador, the retirement of the asylum of Julian Assange, had great relevance for this subject, due to the countless attacks that the country experienced, so, it will analyze its repercussion and how it was formed in a real threat within the country.

Key words: cibersecurity, policies, cibercrimes, ciberdefense, informatic security, ciberspace.

ÍNDICE

1. INTRODUCCIÓN 1

2. ESTADO DEL ARTE 3

3. MARCO TEÓRICO 10

3.1 Escuela de Copenhague 10

4. DISEÑO METODOLÓGICO 13

5. ANÁLISIS DE CASO 14

5.1 Alineación de acciones para trabajar de manera armoniosa 18

5.2 Coordinación de la cooperación de los sectores públicos y privados 22

5.3 Transmisión de responsabilidades, directivas y establecer relaciones entre todas las partes involucradas 24

5.4 Las consecuencias de haber dado el asilo a Julian Assange y las consecuencias de haberlo retirado 27

6. CONCLUSIONES 30

REFERENCIAS 33

1. INTRODUCCIÓN

A lo largo de la historia han existido algunos ciberataques que han ocasionado problemas serios para infraestructuras públicas de los países. En 2017 se dio el ataque WannaCry, que se basó en infectar a computadoras con un programa que en encriptaba archivos y para poder recuperarlos se pedía dinero. Con este ataque más de 230 mil ordenadores se vieron afectados en más de 140 países como Rusia, Gran Bretaña, España, Alemania (Jaimovich, 2018), donde diversos sectores se vieron comprometidos (salud pública, telefonía, empresa de transporte). Ese mismo año se dio el ataque NotPetya, el cual contaminó a más de 16 mil máquinas, con un costo de más de mil millones de dólares, siendo el ciberataque más costoso hasta la fecha (Johnson, 2018). El país más afectado fue Ucrania, puesto que oficinas gubernamentales, centros nucleares y otras instituciones más se vieron afectadas por NotPeyta. Es así que se puede apreciar que dicho ataque afectó al normal funcionamiento de los estados. En 2018, más de la mitad de la población utilizaba internet, donde los Estados también hacían uso del ciberespacio, lo que significa que cada vez más se solidifica una sociedad informática más integradora (Unión Internacional de Telecomunicaciones, 2018). Según la Unión Internacional de Telecomunicaciones, el desarrollo de banda ancha internacional y el tráfico de Internet ha tenido mayor aumento que el número de personas que usa Internet.

El Ecuador no queda exento de los ciberataques, en 2017 WannaCry afectó al país, siendo Ecuador el tercer país más afectado de Latinoamérica (Ecuavisa, 2017). Por esta razón los países tienen nuevos retos que son prevenir y prepararse para enfrentar cualquier tipo de ataque en la esfera cibernética.

Se debe pensar en cómo esto afecta a la realidad actual del Ecuador y cómo un ataque podría afectar al aparato gubernamental del Estado y dejarnos sin comunicación y sin luz. De aquí que se debe pensar en los nuevos retos que esto implica para la Seguridad Pública del Estado. Si bien existen organismos encargados de proteger la información del Estado, como Arcotel, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, el Centro de Respuesta

a Incidentes Informáticos del Ecuador, es importante analizar cómo se da este cambio en las políticas de seguridad informática dentro de las diferentes instituciones del Ecuador a partir de su creación.

Las políticas públicas implementadas en el Ecuador han tenido deficiencias que han ocasionado que el sistema gubernamental sea vulnerable en varias ocasiones. Como en abril de 2019 que tras retirar el asilo a Assange el Ecuador sufrió más de 40 millones de ataques cibernéticos. De aquí nace la pregunta ¿Qué tan preparado está para enfrentar un ataque cibernético?, es una pregunta mandatoria, ya que, si bien en el país existen políticas y estrategias de ciberdefensa y ciberseguridad, es necesario saber su nivel de pragmatismo.

El tema para tratarse representa un problema, ya que muchas veces la sociedad desconoce asuntos como seguridad informática o se lo toma muy a la ligera sin pensar en las repercusiones que esto pueda tener a futuro y su incidencia en la configuración de la esfera política. Es por ello que es importante analizar el cambio que se dio en las políticas de seguridad informática en el Ecuador, la motivación por parte del Estado en su implementación ya que, dado el crecimiento acelerado de la tecnología en la sociedad, el ciberespacio se volvió fundamental en las relaciones sociales, económicas, políticas etc., registrándose más usuarios que buscan sacar el mayor provecho posible de esta herramienta. No obstante, algunas veces el uso de este medio podría tener otros fines como dañar las infraestructuras estratégicas del país, es por esta razón que el estudio del cambio de políticas de seguridad informática con la creación de nuevas instituciones es fundamental para direccionar las estrategias del Ecuador en esta materia.

Con el retiro del asilo de Julián Assange, el país sufrió varios ataques informáticos, por lo que esta investigación se divide en dos partes, el análisis de las políticas de seguridad informática implementadas y las consecuencias de haber dado el asilo a Julián Assange y las consecuencias de haberlo retirado.

2. ESTADO DEL ARTE

La Guerra fría fue uno de los sucesos históricos que marcó el sistema internacional, surgió una nueva configuración estatal y nació un nuevo desafío para los Estados como lo es la Seguridad Informática, lo que volvió a los Estados vulnerables no solo a amenazas físicas sino también a amenazas cibernéticas.

Con el surgimiento de las tecnologías masivas, el intercambio de la información, y la creación de virus dentro del mundo cibernético. Los países empezaron a prestar atención en cómo afrontar problemas provenientes del uso de tecnologías. Por este motivo, en 1986 en los Estados Unidos se estableció el "Computer Fraud and Abuse Act" que contemplaba cinco tipos de crímenes informáticos. Esta normativa nace para evitar la piratearía informática, ya que con el crecimiento de usuarios que tenían acceso a computadoras la preocupación del Estado fue la de establecer lineamiento para este nuevo campo. Así también, el uso de computadores por parte del Estado motivó a que la implementación de nuevas reglas, debido a que los delitos informáticos eran juzgados como fraude y la ley carecía eficiencia. Alemania en 1986 incluyó la "Computer Kriminalität"; Francia en 1988 adoptó la "Ley Godfrain"; Italia en 1993 adaptó el crimen informático en su Código Penal (Martín, 2003, p. 23). Países que al igual que Estados Unidos, hacían uso de tecnologías en su aparato gubernamental y al existir algún tipo de anomalía tenían que juzgarlo según los delititos tipificados en la ley, es decir los tradicionales, por lo que los Estados recurrieron a la implementación de estos nuevos manuales para que las decisiones sean más efectivas.

Con la aparición de vulneraciones informáticas, se dio origen a debates que se dieron en base al espacio cibernético. Con la creación del Internet se cuestionó si los Estados debiesen o no tener injerencia del Estado y se hablaba de que este espacio debería carecer de dominio estatal (Domínguez, 2013, p.167). Por esta razón, que Jhon Perry Barlow, el famoso activista cibernético estadounidense, cofundador de la Fundación Frontera Electrónica, que su objetivo principal es el defender las libertades civiles en el marco del mundo

digital. Barlow en 1996 realiza una Declaración de Independencia del Ciberespacio, en la cual expresa que de ninguna manera se va a permitir que los gobiernos tengan soberanía en el espacio cibernético. Lawrence Lessig, académico especializado en derecho informático y fundador del “Centro para el Internet y la Sociedad” en la Universidad de Stanford, mata la utopía de que el Internet será completamente libre e irregulado y manifiesta que el ciberespacio se transformará en el lugar más regulado del mundo (Domínguez, 2013, p. 166). El autor opina que, si bien la Organización para la Cooperación de Sangay se utiliza el término de seguridad de la información, en el Occidente se habla de ciberseguridad, lo que lleva al autor a afirmar que es una diferencia meramente nominal.

La creación de una política de seguridad informática nacida del desarrollo y diversificación del uso de las tecnologías en las instituciones implicó también una serie de amenazas y riesgos para la ciudadanía tanto a nivel nacional como internacional. Esto afectó directamente a la seguridad pública, ya sea que haya sido constructiva o destructiva. En este sentido, los países pusieron sus esfuerzos en crear un marco legal base para que sirva de guía a los demás. Así nació el famoso Convenio de Budapest, creado por países europeos pero abierto para que Estados de otros continentes puedan adherirse. En este Convenio se busca penalizar crímenes realizados a través de dispositivos tecnológicos, también se establecen lineamientos para tomar medidas y sobre todo de la cooperación internacional para poder sancionar estos crímenes (Gómez, 2010, p. 195).

Por este motivo es que se debe entender el concepto de seguridad, para ello se tomará el concepto del realista George F. Kennan quien manifiesta que el gobierno es un mero agente mas no un patrón, ya que su tarea principal es hacer respetar los intereses de la sociedad a la cual representa, mas no a los intereses particulares (Kennan, 1986, p. 206) El autor sostiene que el gobierno en la seguridad pública va a defender los intereses colectivos mas no a los intereses particulares de la sociedad. De tal manera que la seguridad informática no se

trata de proteger solo a las instituciones públicas que poseen información del Estado, sino también a los ciudadanos, ya que todos estos actores están expuestos a un ataque que, si bien puede llegar a ser de poco alcance, también puede ser de gran impacto.

El autor Arnold Wolfers establece que la seguridad nacional tiene por objetivo la protección de los intereses de la nación de las amenazas externas, y su objetivo es superior al de los intereses particulares (1952). Es decir, se observa la existencia de una superioridad del interés nacional, característica que comparte con el autor Kennan. De este modo, surge la pregunta ¿Cuáles son los parámetros para establecer el tema que cabe dentro de la Seguridad Pública

A causa de lo mencionado con anterioridad, el historiador americano Richard Smoke expresa que existen dificultades para definir la seguridad nacional, ya que en general los estudios se basan en problemas de seguridad que enfrentan las naciones y los procesos son diferentes en cada una de ellas (Brena, 2006). Dicho argumento en la actualidad sería un tanto ambiguo, pues si bien no se habla de seguridad en sí, dentro de la seguridad nacional se encuentra la seguridad informática, y tanto en la seguridad nacional como seguridad informática existen ciertos lineamientos bases establecidos, debido a que se han logrado varias resoluciones de la Unión Internacional de Telecomunicaciones que han ido construyendo el concepto de ciberseguridad (Unión Internacional de Telecomunicaciones, 2007). Otros actores internacionales como la Organización Internacional de Normalización y algunos países en su legislación interna han establecido su definición en base a los principios propuestos por estas organizaciones.

Carolina Sancho Hirare, Doctora en Conflictos, Seguridad y Solidaridad por la Universidad de Zaragoza, explica cómo la nueva configuración del sistema internacional, con toda esta revolución tecnológica y gran uso del ciberespacio da nacimiento a la seguridad informática dentro de la seguridad gubernamental. De igual manera hace un análisis de los diferentes tipos de ataques y grados de

conocimiento del tema dentro de un Estado. Esto ayuda a identificar qué ataques pueden ser dañinos para el aparato gubernamental del Estado, ya que no todos los ataques cibernéticos significan una amenaza de alta magnitud para el gobierno (Hirare, 2017, p. 8).

La seguridad informática es definida por Purificación Aguilera, como una disciplina dentro de un sistema de información encargada del diseño de normas, métodos, técnicas y procedimientos que hacen de éste confiable y seguro. Al sistema de información esta autora se refiere a la agrupación de elementos organizados y conectados entre sí, facilitando su funcionamiento para cumplir con sus objetivos. Esta autora explica que para poder establecer un sistema de información es importante conocer; 1) los elementos que integran el sistema; 2) los peligros que pueden dañar al sistema ya sean de forma accidental o provocados 3); las medidas a implementarse para prevenir, reducir, impedir y controlar riesgos (Aguilera, 2010, p.9). Por otra parte, describe dos tipos de seguridad informática, como son la activa y la pasiva; la primera se refiere a las medidas tomadas para prevenir amenazas al sistema. La segunda en cambio son medidas que se implementan una vez originado el acontecimiento de peligro para disminuir las repercusiones de este, permitiendo la recuperación del sistema (Aguilera, 2010, p. 10).

De igual modo José Fabián Buendía en su libro expresa que se la seguridad informática pretende resguardar el procesamiento, almacenamiento y transmisión de la información digitalizada (Buendía, 2013, p. 8). Este autor también hace una clasificación entre lo que es la seguridad activa y pasiva, en donde los conceptos no difieren mucho del de Aguilera, ya que conceptualiza a la seguridad activa como la que protege al sistema de ataques mediáticos a través de regulaciones que protejan activos de la empresa, en este caso del Estado (Buendía, 2013, p.14). En cambio, la seguridad pasiva la denota como todos aquellos mecanismos que, en caso de sufrir un ataque, posibilita una recuperación razonable.

Álvaro Gómez Vieites define a la seguridad informática como cualquier medida adoptada para impedir operaciones no autorizadas en el espacio informático y donde los efectos pueden arriesgar la integridad de los usuarios, así como su rendimiento (Vieites, 2011). Concepto que no tiene mucha distinción del de Aguilera y Buendía, solo que este autor no clasifica o menciona los dos diferentes tipos de seguridad informática como los dos anteriores. Desde otro punto de vista, Jeimy J. Cano, enfoca a la seguridad informática como aquella que "comprende las propiedades emergentes de los sistemas (analizados) bajo condiciones y realidades extremas" (Cano, 2004, p. 42). Es así como se puede apreciar que este autor difiere su pensamiento con Bertalanffy en cuanto a la visión de la Seguridad Informática, ya que este último autor lo ve como un todo, mientras que Cano lo ve como una propiedad dentro del sistema, aparte de que abarca las relaciones entre los objetos y tiene en cuenta las reacciones en los modelos causales.

Siendo la seguridad informática un elemento relativamente nuevo que afecta la construcción de los Estados, se ha creído conveniente hablar de Ludwig quien introduce la idea de la Teoría de Sistemas quien vio que el esquema mecanicista no era suficiente para explicar problemas teóricos. Este autor básicamente habla sobre el estudio de organismo como un sistema, en donde se tienen múltiples perspectivas de la realidad, sin aislar fenómenos (Bertalanffy, 1968). Es importante entender esta visión porque es así como es analizada la seguridad informática, como un sistema que se compone de diferentes sectores. Este panorama multidimensional también lo comparten Francisco Solarte, Edgar Rosero, Mirian del Carmen Benavides, que hablan sobre los riegos de aplicación de la seguridad informática y cómo el complemento de ciertos factores hace posible de la seguridad informática una realidad. Por consiguiente, conceptualizan el concepto de vulnerabilidad informática como "las debilidades del sistema o activo informático en cuanto a seguridad", amenazas informáticas "como los ataques cometidos por personas internas o externas, que pueden ocasionar daños a la infraestructura tecnológica, a los sistemas de información o a la misma información que circula en la organización."; de riesgos informáticos

los defines como los “problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo.”, todo lo anterior son conceptos fundamentales para poder comprender la seguridad informática (Solarte, Rosero, Benavides, 2015)

Es importante entender al ciberespacio desde una perspectiva tecnológica ya que de esta manera se podrá entender cómo funciona, la forma en la que se desenvuelve el ciberespacio y cuál es la función de la seguridad informática, así como también sus vulnerabilidades.

De igual manera se necesita una visión más política en el tema, debido a que, si bien pueden existir múltiples leyes, normas, reglamentos ligados a la seguridad informática, pero la consonancia de estas es indispensable. Estos autores hablan de que, así como hay políticas orientadas a la seguridad cibernética, también existen otras que promueven el libre uso del internet. Es por ello que en este texto se plantea hasta qué punto los ciudadanos tienen libertad de usar el internet y si las medidas usadas por el gobierno afectan la libertad de expresión, puesto que existen normativas tanto de protección y liberalización del uso del internet. (Richero, Cerbino, 2006).

Ciro Antonio Dussan Clavijo conceptualiza sobre la política de seguridad informática, y menciona criterios para la promulgación de una política de seguridad informática. Uno de los factores que resalta este autor es la claridad que se debe tener en cuanto a las amenazas que se está expuesto, ya que esto facilitará al Estado la implementación de medidas preventivas y correctivas informáticas. Este autor identifica tres elementos indispensables que deben acompañar a la política de seguridad informática: La cultura organizacional, las herramientas y el monitoreo. Igualmente manifiesta que una política de seguridad no funciona por sí sola, sino que requiere del acompañamiento de varios elementos para que su desempeño logre los objetivos deseados (Dussan, 2006). Dentro de los parámetros para la elaboración de esta política Dussan

establece que se deben considerar lo siguiente la integración de un comité especializado que ayudará a la formulación de la política informática.

Es así que el pensamiento de Dussan coincide con el de Ricardo M. Mata y Martín quienes determinan que la creación de un “departamento especializado en la seguridad del sistema informático” (Martín, 2003, p. 40), es importante puesto que de esta forma se pueden planificar y ejecutar medidas para este fin. También manifiesta que para que la seguridad informática esté a salvo, se debe poner especial énfasis en las personas. Este pensamiento podría basarse en la posible venta de información sobre este tema a los cibercriminales como lo ocurrido con los episodios de WikiLeaks y Julián Assange a quien la prensa internacional ha calificado como pirata informático asilado en la embajada ecuatoriana por siete años. Julián Assange es australiano y cofundador de la página web WikiLeaks, sitio web usado para filtrar información política y financiera de potencias mundiales, lo que constituyó una amenaza para la soberanía de los países. El país que más protagonismo tuvo en este sitio web fue Estados Unidos, país con el que tiene problemas legales pendientes, ya que la información vertida por la WikiLeaks afectó a la seguridad nacional estadounidense y al último proceso electoral.

Al hablar de Seguridad, también se debe mencionar qué son los delitos informáticos. El Dr. Santiago Acurio del Pino, profesor de derecho informático en la Pontificia Universidad Católica del Ecuador, recoge los conceptos de Nidia Callegari y Davara Rodríguez. La primera define al delito informático como “aquel que se da con la ayuda de la informática o de técnicas anexas” (Pino, 2006, p.10), el segundo lo conceptualiza como la realización de una acción que reuniendo todas las características del concepto de delito se desarrolla en el espacio cibernético. Es así que estos conceptos son de fundamental ayuda para que más adelante se pueda identificar los tipos de delitos informáticos que el Ecuador ha tenido en los últimos años.

En el VI encuentro de Seguridad Integral en España se habla que las amenazas dentro del ciberespacio son cada vez más difíciles de combatir debido a que los crímenes informáticos han adquirido carácter de profesionalización. Además de que existe una estrecha conexión entre el crimen en la esfera virtual como física. Este factor se da debido al poco conocimiento del tema que tienen tanto las empresas como consumidores, en el encuentro también se habló que el resultado de estos cibercrímenes es por la escaza cooperación que existe entre el Estado y las instituciones, ya sean públicas o privadas (Llorente et al., 2014).

3. MARCO TEÓRICO

Las relaciones internacionales centraron su atención en los desafíos que la desaparición del sistema bipolar ocasionó en la esfera internacional. Es así que nacen la teoría de la securitización con la Escuela de Copenhague, que quiebra con los enfoques tradicionales dentro de las relaciones internacionales, ya esta teoría muestra una nueva perspectiva de cómo se configura una amenaza.

Existen algunas formas de entender la seguridad, según Francisco J. Verdes, investigador predoctoral del departamento de Estudios Internacionales de la Universidad Complutense de Madrid. Estas formas se traducen en la objetiva y subjetiva, por la cual se da una concepción discursiva de este término en consecuencia de lo social-constructivista que cuestiona que la seguridad pueda ser totalmente objetiva y las amenazas e inseguridades son resultados de construcciones sociales, rechazando los pensamientos tradicionales del estudio de la seguridad (2014, p. 282).

3.1 Escuela de Copenhague

La escuela de Copenhague se levanta sobre tres pilares: “securitisation, sectores y complejos de seguridad regional” (Idiart, 2013, p. 2). Cuando se habla de sectores significa las diferenciaciones que existen en el sector económico, político, militar, social y ambiental. Con respecto a complejos de seguridad regional, la significación de este término radica en los “niveles regionales del

análisis de la seguridad" (Idiart, 2013, p. 3). Esta teoría se compone de; a) Actor o actores securitizadores; b) objeto referente; c) Speech act (acto del habla o discurso); d) audiencia.

Ole Waever uno de los investigadores de la Escuela de Copenhague define que la seguridad social es aquella en la que se conserva las condiciones del ciudadano de forma aceptable en temas de evolución, lengua, cultura, asociación, identidad nacional, religiosa y de costumbres. Donde la seguridad se construirá como un tema que habla a través de los actos de los diferentes actores del Estado, ya sean líderes del gobierno, de la sociedad civil, de organizaciones, etc. (Wæver, 1998). Estos actores dentro de la teoría son denominados "actores securitizadores", pues estos son los que determinan la urgencia de un tema a tratarse, ellos son los que califican a un fenómeno como peligroso o amenazante. Demostrando así que la seguridad nacional se configura por aquellos que tienen el poder de tomar decisiones dentro del estado.

Se debe tener claro que esta teoría no se refiere meramente a la seguridad del Estado, sino que va a depender del objeto referente al que se esté analizando; este objeto referente debe ser visto de una manera multidimensional. Ole Waever expresa que en la teoría de securitización debe existir una amenaza existencial que afecte directamente al objeto referente aun cuando sean puramente subjetivas, ya que no todo debe ser visto como una amenaza. Esta teoría explica que las amenazas son construidas a través del discurso, es por ello que con anterioridad se manifestó que la seguridad habla a través de las acciones de los líderes. Los actores securitizadores son los que determinan si existe la amenaza al objete referente, estos actores son aquellos que poseen poder dentro de la esfera política. Sin embargo, para que una amenaza sea considerada como tal la audiencia determinada debe aceptarla, ya que es la audiencia la que define qué atenta contra la seguridad del estatal aun cuando resulta difícil determinar cuál es dicha audiencia. Es así que estos actores son los que implantan medidas extraordinarias de carácter urgente y gracias a la aceptación de la audiencia es que las medidas a tomar pueden ser justificadas.

Sin embargo, esto les daría derecho a los agentes securitizadores el derecho de abolir leyes como resultado de implementación de medidas urgentes.

Bjorn Moller, escritor danés en diferentes revistas científicas, analiza la seguridad según el objeto de referencia. Este autor indica que se debe estudiar la seguridad desde diferentes perspectivas, ya que no es estática sino dinámica, y dependerá del contexto y los actores para entender hacia dónde va. Cuando analiza a las dimensiones de la seguridad menciona que, si bien el Estado en un principio fue creado para proteger a sus ciudadanos, éste puede ser también una amenaza para la seguridad (Moller, 1996, p. 777). Uno de los principales problemas que este autor identifica es que en la gran mayoría de los Estados del Tercer Mundo existe una escasez de seguridad desde diferentes perspectivas.

Barry Buzan quien junto a Ole Waever publicaron “A New Framework for Analysis” describen a la seguridad como un campo de negociación entre el pueblo y sus líderes (1998). En otras palabras, la securitización es un proceso de construcción social entre la audiencia y los actores securitizadores. Es decir, un fenómeno es securitizado cuando la audiencia debe apoyar las medidas de los actores securitizadores frente a la amenaza que es aceptada por naturaleza.

Otro de los factores a analizar dentro de la Teoría de la securitización es el speech act que van creando los agentes securitizadores para definir que algo es considerado como una amenaza a la supervivencia del objeto referente. En este sentido, este componente viene a ser el instrumento fundamental para poder securitizar el problema.

Con lo dicho anteriormente, la Teoría de la securitización es la más adecuada para la realización de este estudio reconociendo su incidencia en el que hacer de los Estados. Si bien las diferentes Teorías de las Relaciones Internacionales veían a la seguridad como un tema meramente físico en donde las amenazas podían ser desarrolladas en el aspecto militar, diversos investigadores de la Escuela de Copenhague fueron los que dieron un giro a la visión que se tenía de

la Seguridad, por lo que autores como Ole Waever y Buzan definen a la seguridad teniendo en cuenta otros elementos, como lo es el objeto referente al cual se va a analizar. Uno de los principales postulados de esta escuela es que, a la hora de hablar del sentido de la seguridad, lo que estos pensadores proponen es que la seguridad debe separarse de su contenido instrumental para que de esta manera se pueda determinar su uso ante ciertos problemas. Este proceso de depuración se da para desviar la atención de aquellos temas que en un inicio no demandan intervención militar.

4. DISEÑO METODOLÓGICO

El método para usarse para el estudio de este caso es el cualitativo, ya que se va a realizar una recopilación de información la cual buscará una explicación y una inferencia causal del fenómeno. Con la creación de nuevas instituciones como ARCOTEL, el Ministerio de Telecomunicaciones, el Centro de Respuesta a Incidentes Informáticos del Ecuador, se dio paso a la regulación de temas de la comunicación y que forzaron a la creación de lineamientos de seguridad informática, a pesar de existir desde el 2004 la Ley de Orgánica de Transparencia y Acceso a la Información Pública. Con la creación de estas instituciones se establecieron diferentes reglamentos que cambiaron las políticas públicas en este ámbito.

Así mismo esta investigación se apoyará en el cambio de las diferentes políticas que las instituciones públicas en materia de seguridad informática manejaban antes del gobierno de Correa. Es por ello que, para poder medir el desarrollo del Ecuador en este campo el análisis se enfocará en tres indicadores fundamentales; 1) Alineación de acciones para trabajar de manera armoniosa; 2) Coordinación de la cooperación de los sectores públicos y privados; 3) Transmisión de responsabilidades, directivas y establecer relaciones entre todas las partes involucradas (Leiva, 2015, p. 163).

El primer indicador se analizará comparando los diferentes reglamentos y leyes de las instituciones públicas para verificar la armonía entre sí. Para el segundo indicador se verificará si existe cooperación de las empresas privadas con las entidades públicas. Por último, el tercer indicador se medirá teniendo en cuenta no solo a las instituciones públicas, funcionarios, empresas sino también la vinculación que ha tenido la ciudadanía en este tema.

5. ANÁLISIS DE CASO

Se ha escogido la Teoría de securitización para explicar el cambio de las políticas en la seguridad informática ya que este tema no era de mucha relevancia para el país; sin embargo, con la creación de nuevas instituciones, estas comienzan a adoptar medidas que integran temas de seguridad informática. Uno de los elementos fundamentales de esta teoría es el discurso, y cómo este fue tomando forma en función de los diversos acontecimientos.

A pesar de que en la Ley Orgánica Penal se establecen artículos sobre el tema, los ciberataques no configuraron una amenaza para el Ecuador hasta el surgimiento de eventos que dejaron en manifiesto la poca seguridad informática que tenía el gobierno. En mayo de 2007 salió a la luz en un video que mostraba una conversación del entonces ministro de Economía Ricardo Patiño con delegados de Abadi & Co, una reconocida banca de inversión, en la que el gobierno se veía implicado en una manipulación del mercado de bonos (Neira, 2015). En ese mismo año, Correa expidió el decreto ejecutivo Nº 468, el cual agregaba un literales al artículo 80 del Reglamento a la Ley de Radiodifusión y Televisión, en el apartado de sanciones, donde se prohibía la libre difusión de grabaciones no autorizadas (El Comercio, 2009, párr. 2). Si bien Álvaro Gómez Vieites menciona que la seguridad informática busca proteger la integridad de los usuarios en internet, no obstante, este decreto no buscó defender el bienestar informático de los ciudadanos, sino más bien limitar a los medios y activistas a que difundan información que pudiesen dañar la imagen de él o su gabinete.

Con lo mencionado, se puede decir que, si bien los cibercrímenes no eran una amenaza de gran magnitud para el Ecuador para Rafael Correa la divulgación de cierta información configuraba una amenaza para el gobierno y sus autoridades, por lo que empezó a construir su discurso en torno a este tema tal y como lo fue en el caso de la filtración de los “Pativideos” cuando a finales del 2014. Para entonces, el exmandatario en sus discursos empezó a manifestar que los ciberataques atentan contra la seguridad del estado. En este sentido, haciendo uso del speech act, en uno de sus discursos mencionó que el país había sido blanco de ataques cibernéticos provenientes de Colombia (El Universo, 2014, párr. 2).

De la misma manera, en una de sus sabatinas denunció que el Ecuador habría sufrido ataques cibernéticos provenientes de Estados Unidos. Uno de los argumentos que uso Rafael Correa para justificar los ataques, fue el de que intentaban hackerlo para conseguir información y hacer espionaje de las conversaciones, recalcando que el país debe estar preparado para una “guerra cibernética”. En su discurso destacó que estos ataques significan un gran peligro debido a que puede causar daños graves como dejar sin energía al país, causar accidentes de aviación y que se debe estar preparado para esa clase de ataques (El Comercio, 2014, párr. 8). Por lo tanto, el tema de la seguridad informática se fue configurando en el speech act como una amenaza que requería medidas urgentes. Y en efecto se empezó a prestar más atención a este tema y la sociedad civil ecuatoriana aceptó tácitamente las medidas que el gobierno estaba tomando.

Una de las limitantes de esta teoría es que no ofrece herramientas conceptuales para observar el cuál es el trasfondo de esta, centrándose solamente en la función del discurso como una construcción bajo la presencia del establecimiento de identidades de las partes. Es por esto que la teoría de securitización rechaza la genealogía de los significados donde se podrían encontrar el estímulo por diferentes temas (Revelo, 2018).

La información personal se ha convertido en la moneda más codiciada de todas las naciones. Si globalizamos esta situación podemos ver cómo han salido a la luz varios secretos publicados por WikiLeaks y por Edward Snowden, ex colaborador de la Agencia de Seguridad Nacional (NSA por sus siglas en inglés), sobre el espionaje masivo de Estados Unidos a nivel mundial, con el pretexto de querer vigilar a los terroristas y los supuestos ataques que podían perpetrar al resto de personas (CNN, 2013, párr. 12). En 2008 el expresidente Rafael Correa decretó la creación de la "Secretaria Nacional de Inteligencia" (SENAIN), entidad que más tarde sería disuelta por el gobierno de Lenin Moreno y acusada por realizar espionaje y persecución política. También en la página de WikiLeaks se filtró información en la que la Institución fue acusada de estar involucrada en un contrato con una empresa italiana especializada en equipos de espionaje (La Hora, 2017, párr. 3).

Durante el período del expresidente del Ecuador, Rafael Correa en agosto de 2012, el Estado ecuatoriano le otorgó asilo político a Assange, bajo el argumento de ser perseguido político, ya que las acusaciones de violación en su propio país (Suecia) eran solo para camuflar la persecución por los datos publicados en su portal web "WikiLeaks" (BBC, 2018). Esta situación será analizada en una sección posterior de este trabajo.

A finales de 2014 se popularizó un portal web llamado "Ecuador Transparente" que viene a ser una página parecida a la de WikiLeaks, donde sus creadores buscan publicar filtraciones de información del estado a la ciudadanía. El caso que llevó a esta página a su fama fueron las conversaciones que mantuvo el Ecuador con la Unión Europea, en donde Ecuador se veía amenazado en materia arancelaria sino firma el acuerdo de Tratado de Libre Comercio (Delgado, 2014, párr. 1). En efecto, estos sucesos dieron paso a un escenario hostil, en el cual las autoridades del Ecuador se veían amenazadas ante las posibles infiltraciones.

En 2015 el famoso portal web BuzzFeed, una compañía estadounidense de medios de comunicación virtual publicó que la SENAIN habría contratado por más de 4 millones de dólares a la empresa Emerging MC para que ésta se encargara de eliminar contenidos “nocivos “para la Rafael Correa (La Hora, 2017, párr. 5). A pesar de que el gobierno negara tal información, se cree que tales contratos eran reales debido a la mala relación que llevó Correa con los medios de comunicación, por lo que no sería una sorpresa que quisiera eliminar cualquier tipo de información que dañara su imagen, dado su carácter y tipo de personalidad que mostró tener en su mandato. En consecuencia, se puede decir que el uso a esta institución fue para satisfacer fines políticos y ayudar a perpetuar su estancia en el poder, ya que como lo muestran los papeles oficiales de esta entidad, el gasto público se concentró en mas 310 millones de dólares desde el 2012 (El Comercio, 2018, párr. 8), entre la adquisición de aparatos altamente tecnológicos para operaciones de inteligencia, remodelaciones etc.

Se puede decir que este caso contrasta con lo mencionado por George F. Kennan sobre la defensa del interés nacional, ya que claramente hubo una defensa de intereses particulares sobre los nacionales. La SENAIN juntamente con las leyes que el gobierno de Correa promulgó, fueron parte de su estrategia política intimidatoria para mantenerse en el poder. Si bien el país alcanzó un gran posicionamiento en cuanto a políticas de seguridad informática, la principal razón no fue la inseguridad informática, sino que se trató de una estrategia de poder para poder controlar a la disidencia y a la oposición.

Se puede afirmar que por este motivo el gobierno de Correa si bien tomó medidas para que la información del Estado no caiga en manos equivocadas, también implementó medidas para que el Estado posea mayor control en la información de los ciudadanos. Pero a Rafael Correa lo que le preocupaba mayormente más que los ataques cibernéticos como amenaza era que la ciudadanía se entere de asuntos que el gobierno no quería que supiese. Fue a partir de estas circunstancias que se empezó a implementar medidas de

seguridad con la creación de nuevas instituciones, así como la adopción de reglamentos para salvaguardar la información de las entidades públicas.

Lo que sí se debe saber es que simplemente con el hecho de conectar el móvil a una antena de telecomunicaciones estamos compartiendo nuestra ubicación (Esteve, 2016, párr. 2), al conectarse a internet estamos compartiendo la región de procedencia mediante nuestra dirección IP. No obstante, se puede asegurar que Ecuador mantendrá en privado toda información personal, sin hacer uso de ello para sacar ventaja frente a situaciones del país precisamente por las medidas de securitización que se han ido tomando paulatinamente, según las circunstancias.

Sin embargo, en este mundo globalizado es difícil tener control total sobre la información personal, ya que desde las redes sociales se le está otorgando permisos de acceso a información privada, de igual manera al postear fotos, videos, información, los dueños de aquello, es la red social. No obstante, cuando se habla de que el gobierno es el que va a ser el que maneje esa información las personas entran en pánico, pero ¿Qué tanto poder tienen las personas sobre su información?

5.1 Alineación de acciones para trabajar de manera armoniosa

Se puede decir que los delitos informáticos antes de estar tipificados como tales, podrían haber sido interpretados en el Código Civil, ya que existe la denominación de delitos y cuasidelitos, donde refiere que “si la norma dice que, si el hecho es ilícito y cometido con intención de dañar, constituye un delito. Si el hecho es culpable, pero cometido sin intención de dañar, constituye un cuasidelito” (Código Civil, 2005, art. 2184). Por lo que, si se quería tomar acciones de algún delito de seguridad informática, se podía comprobar el daño e interpretar las leyes en base a ellos, obviamente las medidas a tomar no iban a estar tan claras como en la actualidad. A continuación, se mencionará alguna de las leyes e instrumentos legales que nacieron entorno a este contexto.

En 2009 el gobierno puso en marcha un sistema denominado “Quipux” mediante el Acuerdo Ministerial 718, que disponía que los servidores de las entidades de la Administración Pública Central de la Función Ejecutiva utilicen la plataforma en donde se “almacenará y clasificará la información documental de las entidades o instituciones registradas y que utilicen el Sistema, bajo estrictas normas y estándares de seguridad, confidencialidad, privacidad, disponibilidad y conservación de la información ” (Acuerdo Ministerial No. 718, 2009, art. 4). Por lo que con esto se puede observar que se buscó integrar a las instituciones entre sí mediante este sistema.

El 2010 la Asamblea Nacional del Ecuador aprobó la Ley de Registro de Datos Públicos a través de la cual se obliga a entidades del Estado a almacenar información pública mediante la creación del Sistema Nacional de Registro de Datos que unifica, interconecta y organiza dicha información. Esta ley contempla registros civiles, mercantiles, societarios etc., para que luego todos los registros se puedan cambiar tanto pública como privadamente. De esta manera gran parte de la información de los ciudadanos pasó de papeles a estar completamente digitalizada y de conocimiento público, por lo que la toma de esta decisión generó controversia y debates acerca de esta medida. La ex asambleísta Betty Amores del partido de Alianza País, partido que pertenecía el presidente Rafael Correa, proponía que en la ley se establezcan tres niveles limitantes, “los datos personales que son confidenciales; los patrimoniales, que son de libre acceso, y los datos constantes en los registros, que actualmente ya son públicos, de libre y gratuita difusión” (El Universo, 2009, párr. 6) . Así mismo uno de los argumentos de la oposición era la posibilidad de que esta ley vulnere la privacidad de las personas, debido a que la ley promueve medidas para conseguir información. La promulgación de esta ley mantiene concordancia con lo establecido por Lawrence Lessing, quien el siglo pasado afirmó que el mundo cibernético se iba a transformar en uno de los sitios más regulados del mundo (Domínguez, 2013, p. 166). Sin embargo, los hackers siguen encontrando formas para pasar por alto dichas regulaciones. Esto fue otro de los factores, que junto a la implementación del sistema “Quipux”, que ayudaron a configurar

Estado pesquisa pues más que para proteger al gobierno electrónico de un ataque cibernético, lo hacía como un mecanismo de persecución y manipulación de la información.

En 2013 se creó el Acuerdo Ministerial 166, teniendo como precedente los Acuerdos Ministeriales 804 y 837 de 2011, de los cuales la Secretaría Nacional de la Administración Pública fundó una Comisión dedicada a la Seguridad informática y Tecnologías de la Información y Comunicación, la cual estaría obligada a fijar parámetros de esta rama, protegiendo así la infraestructura computacional y abarcando la información que maneja las diferentes entidades del Estado. Estos acuerdos ministeriales tienen en consideración la Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000:2012 para la Gestión de Seguridad de la Información, que no fue más que la transcripción de la norma internacional, ISO/IEC 27006 de 2007. Cabe destacar que esta norma estaría en constante cambio ya que, dependiendo de los nuevos parámetros internacionales, la normas ISO ecuatorianas tendrían diferentes ediciones, como por ejemplo en la actualidad la norma vigente es la NTE INEN-ISO/IEC 27000:2016, basada en los nuevos lineamientos internacionales.

Del Acuerdo Ministerial 166 nace el Esquema Gubernamental de Seguridad de la Información (EGSI), en el cual las entidades de forma mandatoria tendrían que realizar evaluaciones de riesgos y diseñar planes de cómo operar riesgos, todo esto basada en las normas ISO mencionadas con anterioridad (Esquema Gubernamental de Seguridad de la Información, 2013). Y no es sino hasta el año 2016, tres años después de haber sido creado el EGSI, que se promulga la política de seguridad de información en el Ministerio de Telecomunicaciones la cual manifiesta que la autoridad máxima de la institución tendrá que establecer el EGSI, a pesar de que “la implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información” (Esquema Gubernamental de Seguridad de la Información, 2013, art. 2).,poniendo como límite máximo de 18 meses . Básicamente esta ley busca que el Ministerio de

Telecomunicaciones aplique parámetros en términos de seguridad informática, evidenciando una vez más que el Ecuador no posee una ley para las instituciones públicas, menos aún para las privadas y que solo se maneja un esquema que da ciertos parámetros y el resto queda a juicio de cada institución.

En el año 2015, un grupo de hackers vulneró la seguridad de la página del Servicio de Contratación Pública, para beneficiar a empresas o personas, lo que dejó en evidencia el alto índice de vulnerabilidad que tenían ciertas páginas del Estado y empresas privadas. El Ecuador en 2015 habría recibido ciberataques en más de 15 compañías y entidades públicas de las principales ciudades del país (Bravo, 2015, párr. 3). Por lo que se puede afirmar que hasta esa fecha si bien el Ecuador expidió varias leyes y destinó grandes cantidades de dinero en materia de seguridad informática, no fueron suficientes como para que el gobierno enfrente y responda efectivamente a estos ataques y poder contrarrestarlos

En este contexto es imprescindible hablar sobre los delitos informáticos, pero primero se debe establecer lo que es un delito. Según el Código Orgánico Integral Penal del Ecuador (COIP) en el art 18 se establece que una infracción penal es “la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código” (2014, art. 18). Según la página oficial de la Policía Nacional los delitos informáticos son las “actividades ilícitas que se las comete a través de medios y dispositivos tecnológicos y de comunicación, cuyo objetivo es causar algún daño, provocar pérdidas o impedir el uso de sistemas informáticos” (Policía Nacional del Ecuador, 2017, párr. 1). Sin embargo, en el COIP si bien identifica ciertos tipos de delitos informáticos como la pornografía infantil, fraude informático, ataque a la integridad de los sistemas informáticos, entre otros, no se establece en la definición de lo que es un delito informático en sí mismo.

En el artículo 232 del Código Orgánico Integral Penal ecuatoriano aquella persona que altere dañe u ocasione un mal funcionamiento de datos informáticos

será sancionado con prisión de cinco a ocho años (2014). También en el art 234 del mismo Código, se establece que el acceso a todo o parte de un sistema informático, telemático o de telecomunicaciones por parte de una persona sin consentimiento será sancionado con la privación de libertad de tres a cinco años (Código Orgánico Integral Penal, 2014). Y así demás artículos contenidos en el Código Orgánico Integral Penal hacen referencia a la seguridad informática del país. Sin embargo, no existe una ley unificada que determine lineamientos y procedimientos a seguir por parte de cada una de las Instituciones que conforman el Estado ecuatoriano. Es por ello que ni en la propuesta de reforma a la Ley de Seguridad Pública y del Estado se establecieron parámetros que encaminen las buenas prácticas de seguridad informática.

5.2 Coordinación de la cooperación de los sectores públicos y privados

En el 2013 se creó la norma de digitalización de documentos de la Dirección Nacional de Registro de Datos Públicos (DINARDAP), en donde el objetivo primordial es la “protección integral y optimización de la guarda de los datos asentados en archivos, registros y documentos físicos, los mismos que pudieran ser alterados o modificados de alguna forma; prevaleciendo la veracidad, autenticidad y debida conservación y custodia de los registros”(Norma de Digitalización de Documentos de la DINARDAP, 2013, art. 1)

Siendo esta una norma de gran importancia para el registro digital de datos públicos y privados, esto no se debe referir únicamente a un ingreso seguro de datos sino también a que la plataforma o lugar donde se vayan a almacenar sean seguros y se pueda tener un respaldo, así como también contar con mecanismos que posibiliten la identificación de anomalías dentro del sistema. Es por ello que crearon un Manual para Inspección de Adaptadores de Registros de Datos Público, en donde se plasmaban lineamientos para la seguridad informática en los procesos de adaptadores, que es un software que tiene como objetivo “obtener, transforma y estandarizar la información” (2012, art. 7)

A principios de 2015 se expidió la Ley Orgánica de Telecomunicaciones en la que se resuelve la creación de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), vinculada al Ministerio de Telecomunicaciones y de la Sociedad de la Información. Las funciones de esta institución, como se cita en su página oficial, es el de “administrar, regular y controlar las telecomunicaciones” (Agencia de Regulación y Control de las Telecomunicaciones, 2018, párr. 1). Con la creación de esta institución, se comenzó a desarrollar un proyecto denominado “Norma Técnica para Coordinar la Gestión de Incidentes y Vulnerabilidades que Afecten a la Seguridad de las Redes y Servicios de Telecomunicaciones”, el cual fue socializado con una parte de la ciudadanía, e incluso se abrió un canal electrónico y físico para recibir comentarios y sugerencias para esta norma. El objetivo principal de esta norma fue: “establecer criterios, medidas técnicas y de gestión, procedimientos; y, mecanismos de coordinación para que los prestadores de servicios del régimen general de telecomunicaciones, adopten las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar, con un nivel de seguridad adecuado al riesgo existente, el secreto de las comunicaciones y de la información transmitida por sus redes” (Agencia de Regulación y Control de las Telecomunicaciones, 2017, párr. 3)
ARCOTEL recibió observaciones por diferentes instituciones públicas y privadas como CNT, CONECEL, NETLIFE, TELCONET, PUNTONET, etc. Posteriormente ARCOTEL realizó un informe público para dar a conocer cómo se manejaron las recomendaciones y las modificaciones que se dieron al proyecto.

En 2017 uno de los retos para la banca fue el acceso al servicio por medio de internet de una forma rápida y segura desde un dispositivo inteligente. Otro de los retos fue educar a los usuarios para la utilización de las plataformas de dicha índole. Se implementaron otras medidas como la One Time Password, que es un código que se produce aleatoriamente el que hacen llegar al usuario ya sea por correo o por mensaje de texto (Tapia, 2017, párr. 8). Para la seguridad

informática, el avance tecnológico es un desafío permanente, así como también la inversión en medidas securitizadoras.

Luego de la socialización, el 26 de julio de 2018 se expidió esta norma. Durante ese año se efectuaron 23 acciones regulatorias entre las que se destaca dicha norma y otras más como la “Norma técnica que regula las condiciones generales de los contratos de adhesión, del contrato negociado con clientes, y del empadronamiento de abonados y clientes”, “Norma técnica de calidad para la prestación del Servicio Móvil Avanzado”, “Norma técnica de portabilidad móvil”, entre otras (ARCOTEL Ecuador, 2019). ARCOTEL no solo expide normas, sino que también efectúa misiones técnicas para verificar el adecuado funcionamiento y aplicación de las normas y jugó un papel más preponderante y monopólica. Se encargó de dar más de 159 charlas a instituciones educativas sobre la seguridad en redes sociales y ciberbullying y también creó su propio programa de televisión para informar sobre las medidas usadas y los compromisos de la empresa.

Si bien el sector privado deja a criterio propio ciertos aspectos de la seguridad informática, se ha evidenciado la cooperación de las instituciones privadas en esta materia, sin embargo, en cuanto a coordinación se presencia falencias, ya que con los ataques que sufrió el Ecuador en 2017, cada institución actuó de manera separada en sus esfuerzos por intentar contrarrestar los efectos de este incidente mundial.

5.3 Transmisión de responsabilidades, directivas y establecer relaciones entre todas las partes involucradas

Durante el mandato del expresidente Rafael Correa invirtió en el sector de telecomunicaciones, ya que este campo estaba poco desarrollado en el país. Es así que para el año 2013 las conexiones de Internet aumentaron significativamente: se multiplicó el 21 por ciento desde el 2006, debido a que la dinamización de este factor es clave para el desarrollo en el ámbito económico,

educativo y tecnológico. Las escuelas fiscales se vieron beneficiadas por estas medidas, puesto que se instalaron conexiones de internet en la gran mayoría de aulas escolares, lo que sin duda ayudó al desarrollo educativo del país. Tal y como lo dice Carolina Sancho, que el crecimiento de usuarios en internet supone nuevos desafíos, como lo es el buen uso de este recurso (Hirare, 2017, p. 8). En este sentido, por el desarrollo tecnológico y de telecomunicaciones, el gobierno se vio obligado a pensar en medidas de seguridad informática. Es así que se emitieron diferentes acuerdos ministeriales y leyes que dieron nacimiento a un conjunto de instituciones públicas y privadas que más tarde jugarían un rol importante en las políticas de este campo (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2013)

ARCOTEL posibilitó la integración de partes involucradas como se mencionó con anterioridad, por lo que en cierta medida se puede percibir cierta relación con las partes involucradas en este tema, ya que las empresas privadas, públicas y ciudadanos participaron de la creación de “Norma Técnica para Coordinar la Gestión de Incidentes y Vulnerabilidades que Afecten a la Seguridad de las Redes y Servicios de Telecomunicaciones”.

Otra de las instituciones que ha desempeñado un papel crucial en este ámbito es EcuCERT, que nació en 2014 del seno de SUPERTEL, ahora conocida como ARCOTEL. Esta plataforma trabaja conjunto con ARCOTEL, pues la misión de esta institución es el de “brindar a su comunidad objetivo el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, sensibilización y soporte técnico” (EcuCERT, 2017, párr. 4). Básicamente lo que hace esta plataforma es receptar incidentes informáticos que los ciudadanos o instituciones públicas o privadas reportan. Como se mencionó con anterioridad, esta institución trabaja de la mano con la Agencia de Regulación y Control de las Telecomunicaciones y también con las máximas autoridades de instituciones que demanden sus servicios. Uno de los propósitos de EcuCERT es promocionar la conformación de un Comité de Ciberseguridad el cual fomente las buenas prácticas de las instituciones en este campo.

Cabe destacar que esta plataforma posee lineamientos internacionales reconocidas en este campo como lo son el Computer Emergency Response Team (CERT), que es un grupo de expertos en seguridad informática que responden a delitos informáticos denunciados, buscando darle una solución inmediata a esa situación. También posee la Forum of Incident Response and Security Teams (FIRST). Por ello esta institución es reconocida como un CIRT (Critical Incident Response Team) nacional oficial de acuerdo con el índice mundial de ciberseguridad y perfiles de ciberbienestar. De igual manera trabaja de la mano de otras instituciones de Estados Unidos, Europa, Latinoamérica etc., pero en especial con la Unión Internacional de Telecomunicaciones de las Naciones Unidas.

En 2014 se expidió el acuerdo 034-CG-2014 en el que se estableció un “Reglamento de Seguridad de la Información, buen uso del internet, correo electrónico, Control de los Recursos Informáticos y Telecomunicaciones de la Contraloría General del Estado”. Dicho reglamento tuvo por objetivo la creación de un marco normativo que regule la protección de la información digital que maneje esta institución. El órgano encargado de brindar soluciones y mantenimiento a la plataforma informática de la Contraloría es la Dirección de Tecnología de Información y Telecomunicaciones. Esta ley es muy importante ya que la función de la Contraloría General del Estado es velar por los recursos públicos que sean bien utilizados además de que estos reglamentos sean seguidos por las demás instituciones públicas. No obstante, en el 2017 se la deroga y se da paso a un nuevo reglamento, en el que se incorpora que los servidores públicos deberán pedir autorización para el almacenamiento de información digital, también se contempla más control por parte de servidores en la utilización de dispositivos tecnológicos dentro de la Institución. Tal y como lo dice Ricardo M. Mata y Martin la existencia de un departamento especializado para este tema es importante para el manejo de posibles incidentes informáticos

Se podría decir que todas las políticas implementadas en las diferentes instituciones han dado frutos, en vista de que en el último reporte en el que se evaluó el compromiso de los Estados frente a la seguridad informática, realizado en julio de 2017, teniendo en cuenta que son 19 países que conforman América Latina, la República del Ecuador obtuvo el sexto puesto (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2017, párr. 1). Este estudio del índice global de ciberseguridad lo realiza la Unión Internacional de Telecomunicaciones.

5.4 Las consecuencias de haber dado el asilo a Julian Assange y las consecuencias de haberlo retirado

En la actualidad la seguridad informática empezó a tener más importancia en el Ecuador, a raíz del discurso de los hackeos del 2014, del asilo otorgado a Assange y con mucho énfasis, cuando la página de la Corte Constitucional del Ecuador fue hackeada luego de que el país le retiró el asilo (abril de 2019).

Ecuador pasa por una crisis económica delicada por lo que se empiezan a realizar ajustes en los gastos del país, siendo así cuando el canciller José Valencia frente a la Asamblea Nacional declara que se gasta aproximadamente un millón de dólares por año en mantener a Assange en temas de seguridad, alimentación, medicina, etc. (El Universo, 2019, párr. 2). Incluso el presidente Lenin Moreno lo declaró como “una piedra en el zapato” (Vistazo, 2019, párr. 1), agregando detalles como su comportamiento inaceptable en la embajada, supuesta filtración de datos privados de Lenin Moreno, intención de participar en política de otros países, etc.

El 29 de marzo el presidente de Ecuador, Lenin Moreno, denunció de un hackeo a sus dispositivos móviles personales incluyendo a los miembros de su familia con la consecuencia de un robo de información privada y su respectiva divulgación por la web como conversaciones con funcionarios públicos y fotos

intimas. Lenin Moreno acuso a Julián Assange de los ataques informáticos realizados hacia él y su familia.

Ecuador tomó la decisión el 11 de abril del 2019 de expulsar a Julián Assange de la embajada ecuatoriana en Londres (Romo, 2019). El Ecuador vivió un ambiente de conmoción cibernética, debido al retiro del asilo de Julián Assange ya que hasta el jueves 11 de abril del 2019 Ecuador ocupo la posición número 50 de los países más atacados en el espacio cibernético (García, 2019, párr. 2), y luego fue aumentando progresivamente, esto pone al Ecuador en una situación de alerta frente a estos ataques, sin embargo si bien existe la legislación en materia de seguridad informática en la práctica no es así, ya que al no poseer un cuerpo normativo que regule todas las instituciones del Estado, hace que los activos informativos sean vulnerables. Este mismo día en la ciudad de Quito se detuvo a un ciudadano sueco, que presumiblemente estaría relacionado con WikiLeaks, al encontrarse con libros de hackeo electrónico (La Hora, 2019, párr. 5).

El presidente Lenin Moreno explicó los motivos por los cuales se ha retirado el asilo político a Julián Assange, catalogando el asilo como insostenible e inviable. Ecuador garantizó la protección de los derechos humanos durante todo el proceso, además de cubrir todas las necesidades presentadas por Assange en la embajada en Londres. Sin embargo, el asilado infringió en repetidas ocasiones disposiciones de la convención sobre asilo diplomático de la Habana y Caracas. En enero del 2019 WikiLeaks filtró documentos del Vaticano. Autoridades visitaron a Assange antes y después del suceso, por lo que las investigaciones confirman que Assange aún está vinculado con WikiLeaks siendo partícipe en problemas de otros Estados. Adicionalmente, su comportamiento en la embajada era reprochable. Instaló dispositivos electrónicos de distorsión no permitidos, bloqueó cámaras de seguridad, accedió a archivos de la embajada ecuatoriana sin permiso. Ecuador a pesar de ello, continuó observando los derechos de Assange e inclusive solicitó al gobierno británico que no se lo extraditara a un país donde sufriera daño físico o pena de muerte. Gran Bretaña accedió al

pedido, y entonces se realizó la entrega de Julián Assange al estado británico (El Comercio, 2019).

CNN informa también que la página web del cantón La Maná fue hackeado mostrando una imagen de Julián Assange además de un mensaje; sin embargo, la misma cadena CNN reveló que hasta la fecha de publicación 13 de abril del 2019 desconocía si los autores del ataque tenían vinculación con el fundador de WikiLeaks (CNN, 2019, párr. 1).

Los ataques realizados tienen fechas muy cercanas a la salida de Assange de la embajada ecuatoriana por lo que se presumen que los ataques están relacionados con una represalia por su parte. El enlace a la página web de la corte constitucional de ecuador presentaba el siguiente mensaje: “Owned For Julian Assange”. Según un boletín presentado por la misma corte menciona que los ataques recibidos desde aproximadamente las 6 horas del jueves 18 de abril (El Comercio, 2019, párr. 2).

A raíz del retiro del asilo político a Julián Assange surgieron una infinidad de ataques cibernéticos a Ecuador con orígenes en diferentes partes del mundo como Estados Unidos, Alemania, Rumania, Francia, Brasil e incluso desde el territorio ecuatoriano. Durante los días siguientes al 11 de abril, (fecha del retiro del asilo) el país sufrió más de 40 millones de ataques de vulneración, pasando del puesto 51 al 31 en la lista de las naciones más atacadas cibernéticamente. Patricio Real, viceministro de Telecomunicaciones ecuatoriano, también mencionó que los ataques mencionados fueron intermitentes y que en ningún momento se dio algún robo de información (Rodríguez, 2019). Por otro lado, Juan Sebastián Roldán, secretario particular de la presidencia de la República, afirmó que Ecuador se preparó para una muy posible ola de ataques cibernéticos por la inminente decisión de entregar a Assange a la policía británica (El Comercio, 2019).

Con todo lo ocurrido, entidades del gobierno de Ecuador activaron los debidos protocolos de seguridad informática, ya que, si bien los ataques no han tenido un impacto muy alto, era necesario tomar medidas preventivas, ya que los sistemas del Estado se encuentran en una situación de vulnerabilidad. No obstante, al no existir un protocolo para todas las instituciones y que cada una tenga sus propias reglas a seguir, hace que esta situación se complique y no exista coordinación entre ellas.

6. CONCLUSIONES

Se puede afirmar que el cambio de las políticas de seguridad informática se evidencia con la creación de nuevas instituciones como ARCOTEL, Dirección Nacional de Registro de Datos Público, EcuCert, etc y por la promulgación de leyes, acuerdos y reglamentos en este tema. No obstante, la motivación para que se de este cambio en la legislación ecuatoriana, no fue ningún tipo de amenaza dentro del espacio cibernético, o que el país se haya visto afectado a gran escala por los ciberataques. Lo que sí está claro es que Rafael Correa quiso proteger la información del Estado y todo su aparato de espionaje y corrupción, valiéndose del establecimiento de nuevas políticas de seguridad cibernética pública y de la creación de instituciones. Es por ello que se ordenó el registro de los datos públicos en una sola plataforma para ejercer mayor control. Al realizar esta acción se tenía que pensar en la manera de protegerla, por ello se da el auge de políticas de seguridad informática.

Si bien existen lineamientos en seguridad informática dentro del Ecuador, basándose en los tres indicadores para determinar qué tan preparado está el Estado ecuatoriano en materia de seguridad informática, se puede afirmar que tiene ciertos logros en cada área. No obstante, la gran falencia dentro de este tema es que no se pensó en la seguridad informática de una manera más armonizada, en vista de que el gobierno no posee un programa o ley de acción que posibilite ejecutar medidas que integren a todas instituciones del país; cada una posee sus propios parámetros lo que convierte al Ecuador en un objetivo

vulnerable dentro del ciberespacio. La falta de integración de instituciones públicas provoca que la coordinación con las entidades públicas sea limitada y su eficacia se vea reducida, por lo que se debería pensar en estas instituciones y como la coordinación entre todas instituciones otorgarían una mejor respuesta frente a los ataques informáticos. Así como también a la implementación de medidas de prevención y reparatorias.

Al no existir armonización entre las diferentes entidades del Estado, las relaciones entre las partes involucradas no son óptimas. Sin embargo, si existe una entidad que se encarga de controlar y mitigar los ciberataques, ARCOTEL, que trabaja en conjunto con otras entidades que comparten responsabilidades. Por lo que el tercer indicador si existe una transmisión de responsabilidades y directivas por parte del Estado, pero la no trabajar en conjunto todas las instituciones, este avance no presenta los resultados deseados.

Se puede decir que no fue sino hasta estos sucesos que los ciberataques significaron como tal una amenaza existencial real dentro de la seguridad del Estado; no obstante, para cuando estos ataques ocurrieron, el país ya tenía conocimiento y herramientas para procurar una seguridad informática. Pero instituciones como el Banco Central del Ecuador, SRI, Cancillería, etc. simplemente se limitaron a denegar el servicio, que se traduce en la saturación del sitio web para bloquear el acceso. No obstante, el hackeo de la página de la Corte Constitucional se mantuvo algunos días. Lo que no se dio a conocer es si este grupo de hackers obtuvieron información confidencial del Estado.

A pesar de que las instituciones estatales disponen de mecanismos y múltiples herramientas de seguridad informática, en la práctica se pudo identificar bastantes falencias de coordinación, lo que ocasiona que esas medidas no sean eficientes.

En otro orden de cosas, los diversos escándalos de funcionarios del gabinete de Correa exigieron la protección de la información y la toma de medidas de

seguridad a fin de ocultarlos al país. Sin embargo, el objeto referente dentro del discurso del exmandatario, fueron las amenazas externas, que, si bien se configuraban como una amenaza real, el trasfondo era proteger un sistema de corrupción que hoy está siendo demostrado a través de la prensa libre.

Por otro lado, el asilo otorgado a Julián Assange provocó un gran distanciamiento con el gobierno británico. La diversidad de actores participantes en este hecho, sujetos a diferentes jurisdicciones con marcos legales diferentes, permitieron que surgieran paraísos informáticos en donde no existe control estatal y que permitieron que Assange jugara con la información nacional e internacional en función de sus intereses y de los intereses de gobiernos afines al socialismo.

REFERENCIAS

Acuerdo Ministerial No. 718. (2009). Publicado el 11 de mayo de 2009. Recuperado de: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/06/Acuerdo-Ministerial-No.-718-de-27-de-julio-de-2011.pdf

Agencia de Regulación y Control de las Telecomunicaciones. (2018). *ARCOTEL cumple tres años de vida institucional*. Recuperado de: http://www.arcotel.gob.ec/arcotel-cumple-tres-anos-de-vida-institucional/

Agencia de Regulación y Control de las Telecomunicaciones. (2017). *Se analizará norma para coordinar gestión de incidentes que afecten la seguridad de redes y servicios de telecomunicaciones*. Recuperado de: http://www.arcotel.gob.ec/se-analizara-norma-tecnica-para-coordinar-gestion-de-incidentes-que-afecten-la-seguridad-de-redes-y-servicios-de-telecomunicaciones/

Aguilera, P. (2010). *Seguridad Informática.* Madrid, España: Editex.Obtenido de: https://books.google.com.ec/books?id=jofTAwAAQBAJ&pg=PA8&hl=es&source=gbs_toc_r&cad=3#v=onepage&q&f=false

ARCOTEL Ecuador. (2019). *Acciones destacadas de la Arcotel 2018*. Recuperado de: https://www.youtube.com/watch?v=-HRAbnlY_Eg

BBC. (28 de julio de 2018). *Ecuador discute el asilo de Julian Assange con Reino Unido*. Obtenido de BBC: https://www.bbc.com/mundo/noticias-america-latina-44991115

Bertalanffy, L. V. (1968). *Teoría General de los Sistemas*. México: Fondo de Cultura Económica. Recuperado de: https://cienciasyparadigmas.files.wordpress.com/2012/06/teoria-general-

de-los-sistemas-_-fundamentos-desarrollo-aplicacionesludwig-von-bertalanffy.pdf

Bravo. D. (26 de julio de 2015). *Ecuador se muestra vulnerable a ciberataques.* El Comercio. Sección actualidad. Recuperado de: https://www.elcomercio.com/actualidad/ecuador-muestra-vulnerable-ciberataques.html

Brena, D. E. (24 de noviembre de 2006). Biopoder como elemento de Seguridad Nacional. Puebla, México: Universidad de las Américas de Puebla. Recuperado de: http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/mendez_d_de/capitulo2.pdf

Buendía, J. F. (2013). *Seguridad Informática.* Madrid: McGraw-Hill / Interamericana de España. Recuperado de: https://www.academia.edu/8358689/Seguridad_Informatica_Mc_Graw-Hill_2013_-_www_Free_Libros_me_-_copia

Buzan, Barry, Ole Wæver y Jaap de Wilde. 1998. *A New Framework for Analysis*. Londres: Lynne Rienner Pub.

Cano, J. J. (2004). *Inseguridad Informática: Un Concepto Dual en Seguridad*. Revista de Ingeniería. 40-44. doi: 10.16924/riua.v0i19.437

CNN. (10 de junio de 2013). *¿Quién es Edward Snowden, el hombre que filtró datos secretos de la NSA?*. Sección mundo. Recuperado de: https://cnnespanol.cnn.com/2013/06/10/quien-es-edward-snowden-el-hombre-que-filtro-datos-secretos-de-la-nsa/

CNN. (13 de abril de 2019). *¿Fue el hackeo de sitio en Ecuador una represalia?*. Sección mundo. Recuperado de:

https://cnnespanol.cnn.com/video/hackeo-julian-assange-wikileaks-ecuador/).

Código Civil. (2005). Registro Oficial Suplemento 46 de 24 de junio de 2005. Reformas en Registro Oficial Suplemento 12 de abril 2017. Recuperado en: http://www.lexis.com.ec/wp-content/uploads/2017/09/CODIGO-CIVIL.pdf

Código Orgánico Integral Penal. (2014). Registro Oficial Suplemento 180 de 10 de febrero de 2014. Reformas en Registro Oficial Suplemento 3 de junio de 2019. Recuperado en: http://www.silec.com.ec.bibliotecavirtual.udla.edu.ec/WebTools/LexisFinder/DocumentVisualizer/FullDocumentVisualizerPDF.aspx?id=PENAL-CODIGO_ORGANICO_INTEGRAL_PENAL_COIP

Delgado, Andrés. (2014). *El Wikileaks ecuatoriano*. GkillCity. Recuperado de: https://gk.city/2014/10/20/el-wikileaks-ecuatoriano/

Delgado, J. Andrés. (2014). *Gobernanza de Internet en Ecuador: Infraestructura y acceso*. Recuperado de: repositorio.educacionsuperior.gob.ec/handle/28000/1579

Domínguez, J. (2013). La ciberseguridad: aspectos jurídicos internacionales. *Revista Española de Derecho Militar*.(100), 161-223. Obtenido de: https://www.ehu.eus/documents/10067636/10825000/2014-Jeronimo-Dominguez-Bascoy.pdf/d11521d6-914f-a0a3-e57c-01887d6807a4

Dussan, C. (2006). *Políticas de seguridad informática*. Entramado. 2(1), 86-92 Recuperado de: http://www.redalyc.org/articulo.oa?id=265420388008

Ecuavisa. (16 de mayo de 2017). *Cuáles son los países de América Latina más afectados por WannaCry, el virus protagonista del ciberataque de*

alcance global. Recuperado de: https://www.ecuavisa.com/articulo/tendencias/tecnologia/273821-cuales-son-paises-america-latina-mas-afectados-wannacry-virus

EcuCERT. (2017). *Misión de EcuCERT*. Recuperado de: https://www.ecucert.gob.ec/nosotros.html

El Comercio. (30 de septiembre de 2009). *¿Cómo normar la información clandestina?*. Sección actualidad. Recuperado de: https://www.elcomercio.com/actualidad/normar-informacion-clandestina.html

El Comercio. (22 de marzo de 2018). *La Senain manejó 310 millones en 7 años*. Sección seguridad. Recuperado de: https://www.elcomercio.com/actualidad/senain-presupuesto-gastosespeciales-seguridad-inteligencia.html

El Comercio. (11 de abril de 2019). *Fechas clave en el caso del australiano Julian Assange.* Sección política. Recuperado de El Comercio: https://www.elcomercio.com/actualidad/julian-assange-detenido-wikileaks-embajada.html

El Comercio. (15 de abril de 2019). *Ecuador esperó a 'blindarse' antes de suspender el asilo a Assange.* Sección política. Recuperado de: https://www.elcomercio.com/actualidad/ecuador-blindarse-superder-asilo-assange.html

El Comercio. (19 de abril de 2019).*Corte Constitucional informa que su web fue hackeada desde Turquía*. Sección política. Recuperado de El Comercio: https://www.elcomercio.com/actualidad/hackeo-web-corte-constitucional-ecuador.html

El Universo. (29 de noviembre de 2009). *Ahora el Estado va tras datos*. Sección política. Recuperado de: https://www.eluniverso.com/2009/11/29/1/1355/ahora-estado-tras-datos.html

El Universo. (16 de octubre de 2014). *Rafael Correa denuncia ataques cibernéticos, algunos originados en Colombia*. Sección política. Recuperado de: https://www.eluniverso.com/noticias/2014/10/16/nota/4111566/rafael-correa-denuncia-ataques-ciberneticos-algunos-originados

El Universo. (11 de abril de 2019). *Cuánto dinero gastó Ecuador en Julián Assange durante casi 7 años*. Sección internacional. Recuperado de: https://www.eluniverso.com/noticias/2019/04/11/nota/7280711/cuanto-dinero-gasto-ecuador-julian-assange-durante-casi-7-anos

Esquema Gubernamental de Seguridad de la Información. (2013). Registro Oficial Suplemento 88 de 25 de septiembre de 2013. Recuperado en: https://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-InformaciÃ³n.pdf

Esteve, J. (22 de octubre de 2016). *Datos, antenas y GPS, así se utilizan los móviles para dar caza a un delincuente*. El Confidencial. Sección tecnología. Recuperado de: https://www.elconfidencial.com/tecnologia/2016-10-22/telefono-movil-localizacion-datos-wifi-antenas_1278503/

García, A. (11 de abril de 2019). *Exdirector de Inteligencia advierte de posibles ataques cibernéticos por caso Assange*. El Comercio. Sección política. Recuperado en: https://www.elcomercio.com/actualidad/ataques-inteligencia-ciberneticos-julian-assange.html

Gomez, A. D. (2010). *El Delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*. Universidad de La Rioja, España. 14(5), 169-203. Recuperado en: http://www.cienciared.com.ar/ra/usr/3/1115/hologramatica_n14_v4pp27_86.pdf

Hirare, C. S. (2017). Ciberseguridad. URVIO. *Revista Latinoamericana De Estudios De Seguridad*, 1(20), 8-15. Recuperado de: http://repositorio.flacsoandes.edu.ec/bitstream/10469/12197/1/RFLACSO-01-Sancho.pdf

Idiart, H. P. (2013). *Un aporte sobre los 'Security Studies'*. Seminario de Práctica Pre-Profesional I. Obtenido de: http://www.hugoperezidiart.com.ar/spp-pdf/UAI-Security-Studies-completo.pdf

Instructivo para uso de sistema Quipux en Administración Pública. (2011). Registro Oficial 597 de 25 de mayo de 2009. Reformas en Registro Oficial de 27 de julio de 2011. Recuperado de Lexis: http://www.silec.com.ec.bibliotecavirtual.udla.edu.ec/WebTools/LexisFinder/DocumentVisualizer/FullDocumentVisualizerPDF.aspx?id=GESTION-INSTRUCTIVO_PARA_USO_DE_SISTEMA_QUIPUX_EN_ADMINISTRACION_PUBLICA

Jaimovich, D. (2018). *Cómo surgió y se propagó WannaCry, uno de los ciberataques más grandes de la historia*. Infobae. Recuperado de: https://www.infobae.com/america/tecno/2018/05/12/como-surgio-y-se-propago-wannacry-uno-de-los-ciberataques-mas-grandes-de-la-historia/

Kennan, G. (1985). Morality and Foreign Policy. *Foreign Affairs*, 64(2), 205-218. doi:10.2307/20042569

La Hora. (22 de septiembre de 2017). *La larga historia de una pieza política llamada Senain*. Sección noticias. Recuperado de: https://lahora.com.ec/noticia/1102101691/la-larga-historia-de-una-pieza-politica-llamada-senain

La Hora. (12 de abril de 2019). *Libros sobre 'hackeo' se encontraron en la casa de Ola Bini*. Sección país. Recuperado de: https://lahora.com.ec/esmeraldas/noticia/1102235925/-libros-sobre-hackeo-se-encontraron-en-la-casa-de-ola-bini

Llorente, G., Muñoz J.,Bravo, A., Rego, M., García, J., Polanco, E., López, P., Carabias, J., Ramos, A., & Larrañeta, J. (2014). Resiliencia, un paso más allá de la convergencia.*VI Ecuentro de Seguridad Integral*. Borrmart. Recuperado de: www.redseguridad.com/content/download/12509/164673/.../CRONICA%20SEG2.pdf

Manual para Inspección de Adaptadores de Registros de Datos Público. (2012). Registro Oficial 778 de 30 de agosto de 2012. Recuperado en: http://www.silec.com.ec.bibliotecavirtual.udla.edu.ec/WebTools/LexisFinder/DocumentVisualizer/FullDocumentVisualizerPDF.aspx?id=PUBLICO-MANUAL_PARA_INSPECCION_DE_ADAPTADORES_DE_REGISTROS_DE_DATOS_PUBLICOS

Martín, R. M. (2003). *Delincuencia Informática y Derecho Penal.* Managua, Nicaragua: Hispamer. doi:99924-57-27-9

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2013). *Logros de la Revolución Tecnológica en Ecuador, se destacan por el Día Nacional de las Telecomunicaciones*. Recuperado de: https://www.telecomunicaciones.gob.ec/logros-de-la-revolucion-

tecnologica-en-ecuador-se-destacan-por-el-dia-nacional-de-las-telecomunicaciones-2/

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (julio de 2017). *Ecuador ocupa sexto lugar en la región, según Índice de Ciberseguridad*. Recuperado de: https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/

Moller, B. (octubre - diciembre de 1996). Conceptos sobre Seguridad:Nuevos Riesgos y Desafíos. *Desarrollo Económico, 36*(143), 769-792. Obtenido de Jstor: https://www-jstor-org.bibliotecavirtual.udla.edu.ec/stable/pdf/3467294.pdf?ab_segments=0%252Fdefault-2%252Fcontrol&refreqid=excelsior%3A35b15ac06bc8a6eeed02bb9c9f481993

Neira, M. (25 de abril de 2015). *Los del círculo son intocables*. Plan V. Sección política. Recuperado de: https://www.planv.com.ec/historias/politica/del-circulo-son-intocables

Norma de Digitalización de Documentos de la DINARDAP. (2013). Registro Oficial Suplemento 22 de 25 de junio de 2013. Reformas en Registro Oficial de 20 de julio de 2016. Recuperada en: https://www.aea.ec/wp-content/uploads/2019/05/Norma-de-Digitalización-de-Documentos-de-la-DINARDAP.pdf

Pino, S. A. (2006). *Delitos Informáticos: Generalidades*.Departamento de Cooperación Jurídica de la OEA. Recuperado de: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Plan Nacional de Seguridad Integral 2014- 2017. (2014). Publicado en enero de 2014. Recuperado de: https://www.resdal.org/caeef-resdal/assets/ecuador---plannacionaldeseguridadintegral2014-2017.pdf

Policía Nacional del Ecuador. (2017). *Delitos informáticos establecidos en el COIP y como prevenirlos*. Recuperado de: https://www.policiaecuador.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Revelo, M. (2018). Securitización como supervivencia, securitización como actos del habla: crítica a la Escuela de Copenhague. URVIO. *Revista Latinoamericana De Estudios De Seguridad*, (22), 58-69. https://doi.org/10.17141/urvio.22.2018.3157

Richero, A & Cerbino, M. (2006). Gobernanza, políticas públicas y aplicaciones de Internet. Flacso. Recuperado de : de https :// www. flacso. org. ec/ docs/ gobernanza. pdf

Rodríguez, R. (15 de abril de 2019). *Ecuador recibió 40 millones de ataques cibernéticos*. El Expreso. Sección actualidad. Recuperado de: https://www.expreso.ec/actualidad/ataquesciberneticos-ecuador-detencionjulianassange-ministeriodetelecomunicaciones-protocolodeseguridad-HB2762494

Romo, R. (13 de abril de 2019). *¿Qué motivó al Gobierno de Ecuador expulsar de su embajada a Assange?*. CNN en español. Sección mundo.Recuperado en: https://cnnespanol.cnn.com/video/gobierno-ecuador-assange-expulsa-razones/

Solarte, F., Rosero, E., & Benavides Ruano, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL*,

28(5), 492-507. Recuperado de: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Tapia. E . (3 de octubre de 2017). *Dos retos para la banca digital* . El Comercio. Sección actualidad. Recuperado de: https://www.elcomercio.com/actualidad/retos-banca-digital-contrasenas-servicios.html

Unión Internacional de Telecomunicaciones. (2007). Guía de ciberseguridad para los países en desarrollo. Recuperado de: https://www.telecomunicaciones.gob.ec/ecuador-ocupa-sexto-lugar-en-la-region-segun-indice-de-ciberseguridad/2

Unión Internacional de Telecomunicaciones. (2018). *Informe sobre Medición de la Sociedad de la Información.*Recuperado de: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR2018-ES-PDF-S.pdf

Vargas Borbúa, R., Recalde Herrera, L., & P. Reyes Ch, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO. *Revista Latinoamericana de Estudios de Seguridad*, (20), 31-45. Recuperado de: http://repositorio.flacsoandes.edu.ec/bitstream/10469/12199/1/RFLACSO-03-Vargas.pdf

Verdes, F. (2014). Seguridad e interregionalismo entre la UE-ALC: Más problemas que política. *Anuario de la Integración Regional de América Latina y el Caribe*. CRIES. (10). 279-316. Recuperado de: http://www.cries.org/wp-content/uploads/2014/11/011a-Montenegro.pdf

Vieites, Á. G. (2011). *Enciclopedia de la Seguridad Informática* (2.a ed.). Madrid, España: Ra-Ma.

Vistazo. (11 de abril de 2019). *Ecuador se saca la "Piedra del Zapato".* Sección país. Recuperado de: https://www.vistazo.com/seccion/pais/actualidad-nacional/ecuador-se-saca-la-piedra-del-zapato

Wæver, Ole. (1998). Securitization and Desecuritzation. *Security*. Nueva York: Columbia University Press. 46–86.

Wolfers, A. (1952) National Security as an Ambigous Symbol. *Political Science Quarterly*, 67(4), 482-483. Recuperado de: https://www.jstor.org/stable/2145138?seq=1#page_scan_tab_contents