REPÚBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
UNIVERSIDAD DE POSGRADO DEL ESTADO

Trabajo de titulación para obtener la Maestría de Investigación en Seguridad y Defensa

TESIS

TÍTULO DEL TRABAJO

"CIBERSEGURIDAD Y MEDIDAS DE PROTECCIÓN DE LA INFORMACIÓN ADOPTADAS POR EL ESTADO ECUATORIANO"

Autor: Lauro Pozo Acosta
Director: Dr. Diego Pérez

Quito, febrero 2022

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

No.522 - 2022.

ACTA DE GRADO

En el Distrito Metopolitano de Quito, hoy 09 de agosto de 2022, **LAURO PATRICIO POZO ACOSTA,** portador del número de cédula: 1707767875, **EGRESADO DE LA MAESTRÍA EN SEGURIDAD Y DEFENSA (2017-2019),** se presentó a la exposición y defensa oral de su tesis, con el tema, **"CIBERSEGURIDAD Y MEDIDAS DE PROTECCIÓN DE LA INFORMACIÓN ADOPTADAS POR EL ESTADO ECUATORIANO",** dando así cumplimiento al requisito, previo a la obtención del título de **MAGÍSTER EN SEGURIDAD Y DEFENSA.**

Habiendo obtenido las siguientes notas:

Promedio Académico:	8.95
Tesis Escrita:	8.33
Defensa Oral Tesis:	8.83
Nota Final Promedio:	**8.76**

En consecuencia, **LAURO PATRICIO POZO ACOSTA,** se ha hecho acreedor al título mencionado.

Para constancia firman:

Dr. Diego Pérez
PRESIDENTE

Dr. Daniel Ponton
MIEMBRO

Dra. Johanna Espín
MIEMBRO

Abg. Juan Maldonado.
DIRECTOR DE SECRETARÍA GENERAL

AUTORÍA

Yo, **Lauro Patricio Pozo Acosta**, máster, con **CC: 170776787-5,** declaro que las ideas, juicios, valoraciones, interpretaciones, consultas bibliográficas, definiciones y conceptualizaciones expuestas en el presente trabajo, así como los procedimientos y herramientas utilizadas en la investigación, son de absoluta responsabilidad de el/la autor/a del trabajo de titulación. Asimismo, me acojo a los reglamentos internos de la universidad correspondientes a los temas de honestidad académica.

Firma
C.I. 170776787-5

AUTORIZACIÓN DE PUBLICACIÓN

"Yo, **Lauro Patricio Pozo Acosta**, cedo al IAEN, los derechos de publicación de la presente obra por un plazo máximo de cinco años, sin que deba haber un reconocimiento económico por este concepto. Declaro además que el texto del presente trabajo de titulación no podrá ser cedido a ninguna empresa editorial para su publicación u otros fines, sin contar previamente con la autorización escrita de la universidad"

Quito, agosto de 2022

LAURO PATRICIO POZO ACOSTA

CI: 170776787-5

Índice

Índice de Figuras

Índice de ilustraciones

Índice de Tablas

INTRODUCCION

La existencia del internet ha tenido gran relevancia en el mundo, puesto que se clasifican generaciones de acuerdo a su existencia, convirtiéndose en una revolución tecnológica muy importante. En la actualidad, la sociedad se maneja en una forma virtual con uso de internet, desde actividades más sencillas hasta actividades más complejas y relevantes para un país o nación como el mundo industrial, social, político y de seguridad.

Debido a este uso, también se puede aumentar la seguridad de los espacios cibernéticos, ya que el espionaje ha acompañado a la sociedad desde la antigüedad cuando se enviaban personas espías para vigilar el movimiento del pueblo vecino con un fin específico.

En vista del mundo digital con el que se encuentra la sociedad en la actualidad, el espionaje no pasa desapercibido, encontrando términos como ciberseguridad o ciberdefensa que es la práctica de defensa de los servidores electrónicos, redes y datos que se encuentran en este medio electrónico.

El cuidado de los servicios cibernéticos es un tema que se hace gran mención debido a las formas de espionaje cibernéticos, por ello varios países del mundo han adoptado estrategias de protección de sus sistemas, evitando situaciones desfavorables del mismo, en Ecuador se logra apreciar un sistema de ciberdefensa inferior en comparación a países desarrollados.

El Gobierno ecuatoriano, en su esfuerzo por minimizar estos problemas, tomó algunas decisiones de tipo político-coyuntural que son necesarias analizarlas para confirmar su efectividad al garantizar la seguridad cibernética de los ecuatorianos.

Además, el actual gobierno establece, en el plan de creación de oportunidades 2021-2025, que se deberá garantizar la soberanía nacional, integridad territorial y seguridad del estado. Desde este plan nacional se propone entender a la seguridad desde una nueva concepción que tendrá un alcance multidimensional, pues el mundo ha estado sujeto a varios cambios en diversos ámbitos: por ejemplo, el tecnológico. Algunas amenazas, como los ciberataques, podrían afectar la defensa y seguridad de un estado, por lo que el estado tiene derecho soberano de establecer estrategias, planes y acciones para enfrentar lo que amenaza su propia seguridad (Secretaría Nacional, 2021).

En este momento, en Ecuador existen pocos trabajos de investigación sobre la inseguridad de la información en el ciberespacio y los ataques a los que constantemente se encuentran organizaciones tanto de los organismos públicos como privados.

En el presente trabajo se centró en conocer las estrategias que utiliza el gobierno ecuatoriano para el cuidado y protección de los sistemas cibernéticos; también, se pretendió entender la forma de efectuar estas medidas de protección en las instituciones privadas como bancos, entre otros, para ofrecer protección a sus socios. Esto se realizó mediante técnicas de recolección de información, mediante la lectura científica, con fuentes bibliográficas de alto impacto para fundamentar correctamente la información obtenida, esto permitió conocer estrategias mundiales adoptadas mundialmente.

Con las revelaciones hechas por Julián Assange y posteriormente por Edward Snowden, se evidenció el espionaje por parte de los Estados Unidos a países de todo el mundo incluso los de Latinoamérica.

Se pretende utilizar técnicas de investigación cualitativas, que ofrecen la posibilidad de explorar aspectos complejos de los problemas de ciberdefensa y

comprender el cómo y porqué de los fenómenos observados en el contexto real. Como fuentes primarias se utilizará diferentes bases de datos como revistas científicas y repositorios digitales, donde accederemos a revistas y tesis que nos brindará un sustento científico – teórico.

Las técnicas cualitativas usadas para desarrollar la investigación fueron la revisión bibliográfica y análisis reflexivo, con el que se explora el tema usando pensamientos y experiencias personales que permiten al escritor reflexionar sobre los acontecimientos mundiales, la historia personal, la experiencia emocional o sobre algún hecho objetivo, permitiendo a la larga, tejer reflexiones de manera que le transmitan un nuevo pensamiento al lector.

Para el análisis reflexivo, mediante esta técnica fenomenológica se puede llegar a explorar, describir, analizar, proponer y explicar hechos o fenómenos que determinan el desarrollo de la investigación en el campo de la ciberdefensa en el estado ecuatoriano (Badii, Castillo, Landeros, & Cortez, 2007).

Para el desarrollo de la presente investigación, en el primer capítulo se revisarán las terminologías necesarias, los principales conceptos, elementos teóricos de ciberseguridad y las estrategias de ciberdefensa que permitirán compenetrarse al tema y al planteamiento del problema para desarrolla los contenidos teóricos centrales de la investigación que permitirán una buena comprensión de la temática.

En el segundo capítulo se revisarán las amenazas de los ciberataques que suceden o acontecen a nivel mundial, específicamente en países caracterizados por un alto grado de ciberataques, los quen se han motivado a trabajar para salvaguardar la seguridad que ocupan el ciberespacio como una nueva forma de vida o manera de

interactuar diaria. Se revisarán también ciberataques sucedidos a nivel regional y de forma particular en el Ecuador.

En el tercer capítulo se aborda las estrategias de ciberdefensa internacional y de los países suramericanos y como parte de estos, el estado ecuatoriano, además se ha tomado en cuenta textos e investigaciones en las cuales se abordan temas como: las estrategias de defensa a nivel internacional, en dónde se presenta las estrategias de varios países europeos y la misma línea se aborda las estrategias de defensa por parte de los países de américa del sur.

En el cuarto capítulo se revisa las medidas utilizadas por el estado ecuatoriano basándonos en normas, leyes, decretos, acuerdos, acciones y presupuestos, cuya finalidad es proteger la información, ante posibles ciberataques, lo que ha convocado la necesidad de crear diferentes estrategias de ciberdefensa y ciberseguridad, que acontecen de la información digital de manera continua durante la interacción de las computadoras con el internet, por lo que su estudio en materia político-estratégica es fundamental a la hora de pensar en la defensa de las naciones.

CAPITULO I: MARCO TEÓRICO Y REFERENCIAL

Si bien el presente estudio gira en torno a la ciberseguridad, no debemos dejar de lado elementos como antecedentes y el contexto donde se desarrolla esta nueva temática ya que hoy en día existe un nuevo escenario, en donde la seguridad evoluciona para cumplir su función, la cual es proteger al individuo de posibles amenazas. Asimismo, es importante conocer las nuevas amenazas que surgen en estos nuevos escenarios.

A lo largo de este capítulo se revisarán las terminologías y los conceptos que se le da a los constructos teóricos centrales de la investigación que permitirán una buena comprensión de la temática.

Antes que nada, es necesario empezar con la descripción de la corriente realista, pues esta servirá como marco de referencia para comprender el origen los conflictos dentro de la sociedad, es decir, cómo surgen el conflicto entre la interacción cotidiana de los humanos, específicamente cuando un conjunto de individuos pertenece a un estado y los intereses de este chocan con los de otros estados.

El Realismo

Esta corriente es tomada por el presente trabajo como punto de referencia para el análisis de los nuevos conflictos sucedidos en el ciberespacio, por lo que será de vital importancia revisar algunos postulados de sus representantes.

Para Roberte O. Keohane:

> El realismo suministra un buen punto de arranque para el análisis de la cooperación y la discordia, otro enfoque las teorías socio psicológicas del comportamiento internacional se han centrado en estudio del poder y como contribución a la teoría de las relaciones internacionales, el realismo suministra

> un gran número de propuestas acerca del comportamiento del Estado, sirven como barreras contra el optimismo infundado. (1984, p. 245)

Por su parte, para Morgenthau (1972), uno de los exponentes del realismo, afirmaba que la búsqueda del interés nacional es el principal móvil de los Estados, por eso el conflicto es un rasgo característico de la política externa; sin embargo, sostenía que para lograr los objetivos del estado no se debe permanecer aislados de los demás, por lo que las alianzas y la concurrencia entre naciones también son inherentes a las relaciones internacionales.

Para los miembros de la corriente realista, la condición que hace posible la estabilidad de las relaciones entre Estados es el equilibrio de los distintos poderes que coexisten y luchan por satisfacer sus intereses. Contra la visión liberal de las relaciones internacionales sostenían que, la búsqueda de poder es el principio que alienta las acciones de los Estados, por ello la competencia y el conflicto son fenómenos inherentes a las relaciones exteriores (Cabrera, 2014).

Por lo tanto, podemos decir que en las relaciones internacionales cada estado lucha por satisfacer sus propios intereses, siendo este un escenario ideal para la aparición de conflictos. Para los realistas los conflictos son parte de la naturaleza humana, por lo que no es algo de lo que se pueda prescindir.

En este sentido, y en la línea de actual de la problemática parece ser que la naturaleza malvada del ser humano ha traspasado a un nuevo escenario denominado ciberespacio, por lo que es necesario estudiar tanto los ciberataques como la ciberseguridad para entender la dinámica de lo que sucede actualmente.

Antecedentes de la investigación

Con el avance de la tecnología, la sociedad se ha visto en la necesidad de incorporar a su vida cotidiana, herramientas tecnológicas, que les permita avanzar junto con la tecnología. Al darse el avance tecnológico se incrementa con ello el cuidado a la información que se maneja en el ciberespacio, por lo que es de vital importancia la intervención del estado salvaguardar mediante normativas, leyes y organismos rectores esta información proporcionada por cada usuario del ciberespacio asegurando su respectiva protección en la información (Del Catillo , Sanjuan, & Gomez, 2018).

Hay que tener presente que los programas desarrollados para enfrentar o evitar la ciberguerra necesitan conocer las capacidades, debilidades, niveles de sensibilidad y vulnerabilidad, a las que un Estado está expuesto en el momento de defender o atacar en el ciberespacio.

Hay que incentivar la investigación científica para proteger los flujos de información de ataques cibernéticos además que tenemos que conocer las capacidades de potenciales enemigos para estar preparados y defender tanto redes estatales, como infraestructura crítica que pueda vulnerar el bienestar de la población civil (Rodriguez, 2020).

Antes de pasar a revisar los constructos teóricos centrales de la presente investigación, es importante contextualizar la época en la que aparece la problemática planteada, pues debemos conocer con exactitud desde dónde parte la problemática y el entorno dónde se desarrolla esta para comprender las nuevas terminologías y conceptos usados para referirse a los nuevos escenarios donde aparecen este nuevo tipo de conflictos.

Contexto postmoderno

En Modernidad Líquida Zygmunt, Bauman[1] explora cuáles son los atributos de la sociedad capitalista que han permanecido en el tiempo y cuáles las características que han cambiado. El autor busca remarcar los trazos que eran levemente visibles en las etapas tempranas de la acumulación pero que se vuelven centrales en la fase tardía de la modernidad. Una de esas características es el individualismo que marca nuestras relaciones y las torna precarias, transitorias y volátiles (Bauman, 2004, p. 2).

La modernidad liquida es una figura del cambio y de la transitoriedad: "los sólidos conservan su forma y persisten en el tiempo: duran, mientras que los líquidos son informes y se transforman constantemente: fluyen. Como la desregulación, la flexibilización o la liberalización de los mercados" (Bauman, 2004, p. 2).

En lenguaje simple, todas estas características de los fluidos implican que los líquidos, a diferencia de los sólidos, no conservan fácilmente su forma. Los fluidos, por así decirlo, no se fijan al espacio ni se atan al tiempo, (Bauman 1999, 1), no conservan una forma durante mucho tiempo y están constantemente dispuestos (y proclives) a cambiarla; por consiguiente, para ellos lo que cuenta es el flujo del tiempo más que el espacio que puedan ocupar: ese espacio que, después de todo, sólo llenan "por un momento".

"Derretir los sólidos" significaba, primordialmente, desprenderse de las obligaciones "irrelevantes" que se interponían en el camino de un cálculo racional de los efectos; tal como lo expresara Max Weber, liberar la iniciativa comercial de los

[1] BAUMAN, Zygmunt, *Modernidad líquida,* Profesor emérito por la Universidad de Leeds, ciudad inglesa en la que vive desde hace más de treinta años, Zygmunt Bauman natal de Polonia

grilletes de las obligaciones domésticas y de la densa trama de los deberes éticos (Bauman, 1999).

O, según Thomas Carlyle, de todos los vínculos que condicionan la reciprocidad humana y la mutua responsabilidad, conservar tan sólo el "nexo del dinero". A la vez, esa clase de "disolución de los sólidos" destrababa toda la compleja trama de las relaciones sociales, dejándola desnuda, desprotegida, desarmada y expuesta, incapaz de resistirse a las reglas del juego y a los criterios de racionalidad inspirados y moldeados por el comercio, y menos capaz aun de competir con ellos de manera efectiva. (Bauman, 1999).

La "disolución de los sólidos", el rasgo permanente de la modernidad, ha adquirido por lo tanto un nuevo significado, y sobre todo ha sido redirigida hacia un nuevo blanco: uno de los efectos más importantes de ese cambio de dirección ha sido la disolución de las fuerzas que podrían mantener el tema del orden y del sistema dentro de la agenda política.

En la actualidad, las pautas y configuraciones ya no están "determinadas", y no resultan "autoevidentes" de ningún modo; hay demasiadas, chocan entre sí y sus mandatos se contradicen, de manera que cada una de esas pautas y configuraciones ha sido despojada de su poder coercitivo o estimulante. (Bauman 1999, 5-6)

La licuefacción debe aplicarse ahora a las pautas de dependencia e interacción, porque les ha tocado el turno. Esas pautas son maleables hasta un punto jamás experimentado ni imaginado por las generaciones anteriores, ya que, como todos los fluidos, no conservan mucho tiempo su forma.

Darles forma es más fácil que mantenerlas en forma. Los sólidos son moldeados una sola vez. Mantener la forma de los fluidos requiere muchísima atención,

vigilancia constante y un esfuerzo perpetuo… e incluso en ese caso el éxito no es, ni mucho menos, previsible (Bauman 1999, 7).

El poder puede moverse con la velocidad de la señal electrónica; así, el tiempo requerido para el movimiento de sus ingredientes esenciales se ha reducido a la instantaneidad. En la práctica, el poder se ha vuelto verdaderamente extraterritorial, y ya no está atado, ni siquiera detenido, por la resistencia del espacio (Bauman 1999, 10).

La fuerza militar y su estrategia bélica de "golpear y huir" prefiguraron, anunciaron y encarnaron aquello que realmente estaba en juego en el nuevo tipo de guerra de la época de la modernidad líquida: ya no la conquista de un nuevo territorio, sino la demolición de los muros que impedían el flujo de los nuevos poderes globales fluidos; sacarle de la cabeza al enemigo todo deseo de establecer sus propias reglas para abrir de ese modo un espacio –hasta entonces amurallado e inaccesible– para la operación de otras armas (no militares) del poder (Bauman 1999, 10).

Se podría decir (parafraseando la fórmula clásica de Clausewitz) que la guerra de hoy se parece cada vez más a "la promoción del libre comercio mundial por otros medios" (Bauman 1999, 10).

Aferrarse al suelo no es tan importante si ese suelo puede ser alcanzado y abandonado a voluntad, en poco o en casi ningún tiempo, puede resultar positivamente perjudicial, mientras las nuevas oportunidades aparecen en cualquier otra parte. (Bauman 1999, 12).

Cualquier trama densa de nexos sociales, y particularmente una red estrecha con base territorial, implica un obstáculo que debe ser eliminado. Los poderes globales están abocados al desmantelamiento de esas redes, en nombre de una mayor y constante fluidez, que es la fuente principal de su fuerza y la garantía de su invencibilidad. Y el

derrumbe, la fragilidad, la vulnerabilidad, la transitoriedad y la precariedad de los vínculos y redes humanos permiten que esos poderes puedan actuar. (Bauman 1999, 12)

La oposición entre globalización e identidad está dando forma a nuestro mundo y a nuestras vidas. La revolución de las tecnologías de la información y la reestructuración del capitalismo han inducido una nueva forma de sociedad, la sociedad red.

La sociedad red se caracteriza por la globalización de las actividades económicas decisivas desde el punto de vista estratégico, por su forma de organización en redes, por la flexibilidad e inestabilidad del trabajo y su individualización.

Asimismo, se caracteriza por una cultura de la virtualidad real construida mediante un sistema de medios de comunicación omnipresentes, interconectados y diversificados, y por la transformación de los cimientos materiales de la vida, el espacio y el tiempo, mediante la constitución de un espacio de flujos y del tiempo atemporal, como expresiones de las actividades dominantes y de las elites gobernantes (Castells, 1998).

Esta dimensión tecnológica interactúa con las tendencias más amplias características de la sociedad red y con las reacciones comunales a los procesos dominantes que surgen de esta estructura social.

Sostengo que este medio tecnológico induce nuevas reglas de juego que, en el contexto de las transformaciones sociales, culturales y políticas presentadas en este libro, afectan de forma importante a la sustancia de la política.

El punto clave es que los medios electrónicos (incluidas no sólo la televisión y la radio, sino todas las formas de comunicación, como los periódicos e Internet) se han convertido en el espacio privilegiado de la política. No es que toda la política pueda

reducirse a imágenes, sonidos o manipulación simbólica, pero, sin ellos, no hay posibilidad de obtener o ejercer el poder. Así pues, todos acaban jugando al mismo juego, aunque no del mismo modo ni con el mismo propósito (Castells, 1998).

Una vez descrito y comprendido el contexto actual desde donde parte la problemática actual de ciberseguridad y sus componentes o actores implicados, pasaremos a abordar el mundo de la información, debido a que, es necesario tener claros algunos conceptos que nos permitan comprender la problemática de investigación y a su vez, identificar las distintas amenazas latentes en el ciberespacio, los cuales se detallan en el marco teórico.

Ciberespacio

Con el aparecimiento del Internet, a partir de la década de los 60, se crea un nuevo espacio considerado como un sinónimo del Internet. A partir de 1985 se menciona como "Ciberespacio"; un lugar en el espacio virtual[2], en donde se han dado un sinnúmero de intromisiones en los archivos de información que poseen los países y las instituciones privadas, para así sacar ventaja en las diferentes transacciones y convenios comerciales o internacionales, como de la seguridad militar y estatal.

El ciberespacio es un concepto que se emplea dentro de la comunidad de informática, que refiere sobre el conjunto de medios físicos, virtuales y lógicos; que conforman las estructuras del sistema de comunicaciones informáticos (Santiago & Allende, 2017).

[2] Según (Clarke y Knake, 2011, pág. 104), el ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan desde redes de ordenadores a las que, se supone, no es posible acceder desde internet porque son privadas y se encuentran separadas de ella.

Es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos y las telecomunicaciones que los vinculan.

Lévy (2007) propone de forma optimista que, a través del internet (ciberespacio) se pueda transformar a la sociedad como más colaboradora, cooperativa e informativa, en el siguiente párrafo se describe su visión del internet.

> Un sistema cuasi social donde tiene cabida toda clase de conocimiento, sin imponerse de manera totalitaria. En tal sentido, su universalidad creciente convierte a la Internet en el ciberespacio propicio para la creación de una "inteligencia colectiva", donde una comunidad de usuarios no solamente recopila información, sino que, de manera innovadora, construye, crea, comparte, opina, debate, sugiere, donde sus miembros se interconectan formando así el universo ciber cultural que conforma la actual sociedad digital (Levy, 2007, p. 387).

Podemos definirlo un conjunto de medios y procedimientos basados en las TICs que pueden ser aplicados a la prestación de servicios, convirtiéndose actualmente en parte importante de nuestra sociedad, siendo un factor diferencial de la evolución cultural (Santiago & Allende, 2017).

El ciberespacio es conformado por todas las redes informáticas en el mundo de modo que conectan y controlan todo, no es solo el internet, es el internet más otras redes de ordenadores a los que no se puede acceder; estas redes tienen similitud con el internet, pero se encuentran separadas (Santiago & Allende, 2017).

Los ciberespacios se encuentran en las actividades cotidianas de la sociedad, es por ello que un ataque cibernético puede cambiar el estilo de vida de una nación, es el

caso de ser atacados los servidores públicos, clientes de una institución financiera, esto puedo colocar en riesgo la seguridad del estado (Vargas, 2014).

Con base en la información presentada en este apartado, el trabajo actual entiende al ciberespacio como un nuevo lugar, en dónde su espacio es de tipo virtual. Este nuevo espacio virtual hace referencia a un conjunto de redes informáticas que se encuentran interconectadas en distintas partes del mundo de tal forma que conectan y controlan todo desde las redes informáticas. Para acceder a esta dimensión es necesario contar con ordenadores que contengan redes de similitud con el internet.

Hoy en día el ciberespacio se ha convertido en la nueva cotidianeidad del ser humano. De modo que pueden interactuar desde sus ordenadores con distintas partes del mundo, este nuevo tipo de interacción virtual ha permitido facilitar mucho el estilo de vida de un individuo, mejorando y evolucionando aspectos de la vida del hombre como el trabajo, educación, comunicación, comercio, etc. En este sentido, un ataque al ciberespacio de estos individuos implicaría un impacto de gran medida de la normalidad y seguridad de una persona.

Ahora que comprendemos el ciberespacio, pasaremos a revisar como este puede ser un lugar con predisposición para la aparición de conflictos, recordemos que en el ciberespacio los individuos se encuentran en una constante interacción con sus semejantes en distintas partes del mundo, pues en esta interacción pueden surgir algunos conflictos en función de sus intereses.

Ciberespacio como escenario de guerra o conflicto

A raíz de la revolución industrial, se desarrolla en la economía un progreso y bienestar, esto abre puertas a espacios para la tecnología y metodología. Todo esto ha permitido el desarrollo de la formación del talento humano, el avance en el

conocimiento científico y tecnológico, dando como consecuencia la autonomía de los países, además la creación de instituciones que permiten la innovación con la finalidad de impulsar la economía en campos como el comercio internacional (Cujabante , Bahamón , Prieto, & Quiroga, 2020).

Desde el siglo XX y parte del siglo XXI, lo internacional se basa en la hiper-globalización que es impulsada gracias a la tecnología digital, lo que ha transformado socialmente, políticamente y económicamente a la sociedad, a esta era se le llama la cuarta revolución misma que se identifica con millones de personas conectadas a través de dispositivos móviles.

La revolución mencionada anteriormente, da lugar al poder de procesamiento y capacidad de almacenamiento; todo esto gracias al incremento masivo de tecnologías como: robótica, internet de las cosas, inteligencia artificial, big data, vehículos automáticos, impresión 3D, otros (Cujabante , Bahamón , Prieto, & Quiroga, 2020).

La cuarta revolución trae consigo cambios trascendentales gracias al acceso y manejo adecuado de la información generada al instante, sin embargo, esta revolución trae consigo cambios negativos como los múltiples espacios delictivos (internet profundo), el caos disfuncional e inclusive las brechas tecnológicas y acceso a la información. El ciberespacio es un espacio artificial (Cujabante , Bahamón , Prieto, & Quiroga, 2020).

El ciberespacio como nuevo escenario para ejercer soberanía en Ecuador

El desarrollo actual de la tecnología ha permitido que la población en general tenga acceso a la información, que sin importar la distancia a la que se encuentre en cualquier parte del mundo, en pocos segundos la tecnología actual permite que una cantidad significativa de información este a nuestra disposición, inclusive tomando en

cuenta que tan solo al contar con un computador nos da acceso a la tecnificación de los bienes y servicio personalizado. Adicionalmente, el acceso a la información nos permite tener contacto con una sociedad globalizada en el ciberespacio.

El ser humano convive cotidianamente en diferentes escenarios a largo y ancho del mundo, es así que, cuando conquista un lugar, busca la supremacía y el control absoluto de este espacio, de esta forma las Fuerzas Armadas de todos los países del mundo, incluido el nuestro, consideran los sistemas del campo de batalla para emplearlos en un conflicto o una guerra; al aire, mar, tierra y hasta en el mismo espacio.

El aparecimiento de este espacio virtual nos ha llevado al análisis del surgimiento de un nuevo campo de batalla, que debe tener en cuenta la repercusiones en materia de seguridad y defensa de un Estado, en donde cualquier país que en una guerra tradicional es considerado de poder blando (Llongueras, 2013) o Estado más débil, el manejo apropiado del ciberespacio puede marcar una ventaja identificando las vulnerabilidades de los Estado más fuerte o de poder duro, aventajándose en el dominio de este espacio virtual con respecto a los países más fuertes en la guerra tradicional.

Otro aspecto de análisis es entender cómo se interpreta la soberanía en el ciberespacio y el internet, al observar que individuos como Edward Snowden o Julián Assange, afectan a la información de los listados sin siquiera estar en ellos, es decir, lo hacen empleando la tecnología y más allá de sus fronteras, materializando una de las características del llamado conflicto híbrido, también conocida como la "revolución de los colores" como parte de la ejecución de la doctrina de Valery Gerasimov[3].

[3] General Valery Gerasimov, jefe del Estado Mayor Ruso, publicó el 23/02/2013. "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations" in Voyenno-Promyshlennyy Kuricr (VPK) (Military-Industrial Courier). En este artículo se describe una perspectiva futura de como Rusia ve los conflictos y la guerra. Esta doctrina fue empleada en Crimea y Ucrania.

Para Gerasimov, la esencia de un conflicto híbrido es que trata conseguir los fines políticos aplicando una presión militar mínima sobre el enemigo. Principalmente, se debe debilitar su potencial militar y económico, la presión informativa y psicológica, el apoyo activo a la oposición interna, del uso de acciones guerrilleras y de operaciones especiales. Se utilizan las 'revoluciones de colores como medio principal para conducir a un cambio no violento de gobierno en el país oponente (Palacios, 2016). En conclusión, cualquier revolución de color es un golpe de estado organizado desde el exterior.

Bauman indica que "Ya no existen fronteras naturales ni lugares evidentes que uno debe ocupar. Donde quiera que nos encontremos en un momento dado, no es posible ignorar que podríamos estar en otra parte de manera que hay cada vez menos razones para hallarnos en un lugar en particular" (2003, p. 103).

Vargas, Recalde y Reyes (2017) analizan que el organismo encargado de Ciberdefensa se constituirá como una entidad que se encargará de la planificación estratégica y de la aplicación de una política de investigación, prevención y reacción de defensa contra amenazas cibernéticas, para lo cual deberá cumplir principalmente 5 aspectos:

1. Proponer la organización y funcionamiento de la ciberdefensa, en las siguientes áreas: protección de las infraestructuras críticas, manejo de crisis, ciberterrorismo, ciberdefensa militar, inteligencia y contrainteligencia, y gobernanza en internet y ciberdelitos (Klimburg 2013).
2. Disponer de una red de expertos conformando "observatorios de seguridad de la información" tanto públicos como privados de manera coordinada con cada sector estratégico.

3. Coordinar las actividades de ciberdefensa entre el sector gubernamental, los sectores privados y la población en general, articulando un sistema de intercambio de información y comunicación de incidentes (ISO/IEC27032 2012).
4. Coordinar actividades de ciberdefensa con otros países, y entidades regionales mediante acuerdos y creando estructuras de información de ciberseguridad para propósitos de intercambio (establecido en la Agenda Política de la Defensa).
5. Orientar el desarrollo de políticas del COSEPE, basado en el levantamiento de las "debilidades, vulnerabilidades y riesgos actuales, y sobre los dilemas" (Klimburg 2012) existentes en cada ámbito, como son: estimular la economía versus mejorar la seguridad nacional, modernizar la infraestructura crítica o proteger la infraestructura crítica y protección de los datos o compartir información.

El análisis y la resolución de estos dilemas permitirá establecer los objetivos de seguridad derivados de las necesidades nacionales mediante un balance entre los significativos de libre flujo de información y las necesidades de seguridad del sector público, sector privado y los ciudadanos en general. Como resultados del accionar de esta Secretaría de Ciberdefensa, se dictarán políticas y objetivos, alineados con el Plan Nacional del Buen Vivir y que deberán estar plasmadas en el PNSI y en las Agendas Sectoriales.

Ciberguerra

La ciberguerra (en inglés cyberwar) es un tipo de netwar consistente con objetivos militares de Internet y otras redes de comunicación, los ataques se clasifican como ataques de alta y baja intensidad.

Para Ureña (2015) la ciberguerra:

> Es aquel conflicto bélico que utiliza como campo de operaciones, en vez de los campos de batalla convencionales, el ciberespacio y las tecnologías de la información y como armas las aplicaciones, comandos y herramientas diversas que proporcionan la informática y las telecomunicaciones. Los objetivos más comunes son la inhabilitación de los sistemas informáticos del enemigo o la obtención de la información (p. 3).

El ataque de alta intensidad es el que tiene como objetivos equipamiento militares o infraestructuras críticas, en este tipo de ataques es más fácil reconocer al agresor. El ataque de baja intensidad es el más común, representa delitos como robo de identidad o suplantaciones, ataques a páginas webs y en la información bancaria, robo de dinero vía electrónica (Vargas, 2014).

Ciberguerrero

Son los individuos que pueden diseñar programas y ciberarmas capaces de infiltrar el sistema de una organización, con esto tienen acceso a la información confidencial, “colocar bombas lógicas y sabotear el correcto funcionamiento de los flujos de información” tanto de una página de internet, así como el de una red eléctrica de un país (Villamil, Bahamon, Prieto, & Quiroga, 2020).

Generalmente los ciberguerreros están ligados a la fuerza militar de un Estado, sin embargo, existen “geeks” personas interesadas en el estudio de software y hardware

para propósitos académicos, otros para el perjuicio a empresas y gobiernos (Villamil, Bahamon, Prieto, & Quiroga, 2020).

Ciberataque

Entre los delitos tipificados como ciberdelincuencia encontramos: el fraude, el robo, el chantaje, la falsificación y la malversación de caudales públicos.

> Se han introducido otros delitos que emplean las tecnologías de la información y la comunicación, tales como el acoso electrónico contra la libertad de personas, el descubrimiento y revelación de secretos, la interferencia ilegal de información o datos, los delitos contra la propiedad intelectual y los abusos con fines sexuales a través de internet u otros medios de telecomunicación a menores. (Pons, 2017, p. 82)

De acuerdo con Ureña (2015) la ejecución de un ciberataque depende del objetivo que se quiera alcanzar o en medida del daño que se quiere ocasionar. Para alcanzar estos objetivos el ciberdelincuente considera algunas técnicas que se presentan a continuación que pueden ser aplicadas de forma combinadas o individualmente.

Los virus informáticos: Por lo general los virus informáticos constituyen programas con aspecto malicioso, cuya intención es infectar los archivos que contiene un ordenador, de manera que pueda causar algún tipo de daño o cambios en el sistema del ordenador que ya ha sido infectado, en este sentido al archivo que ha sido contaminado se llama víctima. El virus incrusta "en los archivos infectados una secuencia de código malicioso, dirigida fundamentalmente a los archivos ejecutables del sistema atacado. A cada ejecución de estos archivos, se produce una propagación del virus, infectando a nuevos archivos y multiplicando sus efectos" (Ureña, 2015, p. 4).

El envío masivo de correos no deseados o SPAM: El término spam se refiere a aquellos correos no deseados o de remitente desconocido (mensaje anónimo), por lo general, estos aparecen en comerciales publicitarios que son enviados en gran cantidad para perjudicar al usuario. “La acción de enviar de enviar dichos mensajes se denominan spamming. Aunque se puede hacer spam por distintas vías, las más utilizada entre el público en general es la basada en el correo electrónico” (Ureña, 2015, p. 4).

La suplantación de remitentes de mensajes mediante Spoofing: Este es un tipo de ataque que consiste en lo siguiente: desde un ordenador, “un atacante simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado” (Ureña, 2015, p.4). Hoy en día, este tipo de ataque es peligroso y sencillo de realizar en contra de cualquier organización.

El envío o instalación de archivos espías o Keyloggers: Este es “un programa que registra y graba la pulsación de teclas y, algunos, también los clicks del ratón. La información recolectada será utilizada luego por la persona que lo haya instalado” (Ureña, 2015, p.4). En la actualidad, podemos encontrar dispositivos o programas que realizan esta actividad.

El uso de Troyanos para el control remoto de los sistemas o la sustracción de información: Estos caballos de troya “son una clase de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos habituales – fotos, archivos de música, archivos de correo, etc.-, con el objeto de infectar o causar daño” (Ureña, 2015, p.4). Pero, el objetivo primordial de un caballo de troya es dejar abierta una puerta trasera que permita manejar de manera remota el ordenador infectado, lógicamente con la intención de adueñarse de información personal y confidencial.

El uso de archivos BOT del IRC (Internet Relay Chat): Este es un tipo de programa que permite controlar un ordenador de forma remota sin que el usuario tenga algún conocimiento acerca de este control. En las páginas webs de "conversación online, como por ejemplo los chats o programas IRC, algunos bots son utilizados son utilizados para simular una persona y hacer un uso maligno, intentando hacer creer a los demás usuarios del servicio que hablaban con una persona real" (Ureña, 2015, p.4).

El uso de Rootkits: Este hace referencia a "un conjunto de herramientas que consiguen ocultar un acceso ilícito a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos" (Ureña, 2015, p.4).

Estos son algunos ejemplos de ciberataque que se pueden dar en el ciberespacio, pero hoy en día existen muchos más, estos son realizados con el fin de acceder ilegalmente a espacios virtuales para perjudicar o hacer algún daño a los ordenadores para satisfacer intereses personales.

Hasta aquí hemos revisado el nuevo espacio virtual, en donde cotidianamente el ser humano se desenvuelve. Asimismo, hemos observado los personajes involucrados en este nuevo ciberespacio que podría ser un escenario más para desatar conflictos o ciberataques. Ahora bien, pasaremos a revisar la contraparte de los ciberataques, lo que denominaremos como la ciberdefensa.

Ciberseguridad

Los ciberataques se han convertido en una fuente de amenazas en el mundo globalizado en que vivimos. Así ya lo contemplan algunos países del mundo y distintas organizaciones internacionales, algunos de estos ya han elaborado estrategias de

ciberseguridad o ciberdefensa (Bejarano, 2011). Tanto la ciberdefensa como la ciberseguridad son los nuevos términos acuñados por los gobiernos y organizaciones internacionales para referirse a la forma de hacer frente a estas nuevas amenazas que han surgido con el acelerado avance de la tecnología.

La Organización del Tratado del Atlántico Norte (OTAN) es de los principales organismos internacionales que se han preocupado por esta nueva temática y ha orientado sus esfuerzos para combatirla. Para esto, la OTAN realiza actividades de: coordinación y asesoramiento en ciberdefensa; asistencia a las Naciones; investigación y formación; y cooperación con los socios.

La OTAN ha sido consciente del riesgo emergente y como tal lo ha tratado en la agenda de sus cumbres: la Cumbre de Riga de 2006, tras haber elaborado un concepto de ciberdefensa y una política de ciberdefensa, y haber establecido una estructura de gestión dentro de la estructura global de la OTAN; y, la Cumbre de Lisboa en 2010 que marcó una hoja de ruta cuyo primer fue la definición de un nuevo concepto de ciberdefensa y el segundo hito consistente en la elaboración de una nueva política de ciberdefensa (Bejarano, 2011).

Tras estos sucesos, cada país comenzó a interesarse por la defensa nacional. Principalmente cada país atribuyó las funciones de defensa a las fuerzas militares de su país, para lo cual requirió ser analizada y repensada en el contexto del "nuevo rostro de la guerra", de una confrontación que enfrenta lo mejor de los entrenados en el arte de la inseguridad de la información, con lo mejor de los entrenados para controlar y mantener la paz de una nación.

Por tanto, animar una revisión de las estrategias de seguridad nacional ante posibles y factibles escenarios de confrontación tecnológica y de guerra de la

información, prepara a los Estados para defender sus sistemas de gobernabilidad y asegurar su resiliencia en condiciones de falla parcial o total (Cano, 2008).

En esta línea, se debe considerar que la ciberseguridad es la acción básica que es favorable para proteger una nación de forma sistemática. Otro que se suma a esta mirada es Candau (2019), quien concibe a la ciberseguridad como la aplicación de un proceso analítico y de gestión de riesgos, por lo que obedece a un enfoque de protección de la información, de accesos, usos, revelaciones y modificaciones no permitidas por la institución. Es decir, es el conjunto de acciones de carácter preventivo, que tienen por objetivo, asegurar el uso de las redes propia y negarlo a terceros.

La ciberseguridad consta de tres elementos fundamentales, que forman parte de los objetivos que intentan afectar los potenciales atacantes. Estos son la confidencialidad, la integridad y la disponibilidad de los recursos, conocido como la tríada CIA (INFOSEC, 2018). Por otra parte, Candau (2019) define tres categorías basado en los objetivos de la ciberseguridad. Estas son la ciberseguridad preventiva, ciberseguridad de detección y ciberseguridad de recuperación.

Para alcanzar la ciberseguridad debemos ejercerla correctamente, debido a que:

> La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad - que puede incluir la autenticidad y el no repudio -, y confidencialidad (Ribagorda, 2018, p. 14).

El término de ciberdefensa es acuñado como una nueva connotación sistémica y sistemática que deben desarrollar los gobiernos, para comprender ahora sus

responsabilidades de Estado, en el contexto de un ciudadano y las fronteras nacionales electrónicas o digitales.

Un concepto estratégico de los gobiernos que requiere la comprensión de variables como, las vulnerabilidades en la infraestructura crítica de una nación; las garantías y derechos de los ciudadanos en el mundo online; la renovación de la administración de justicia en el entorno digital; y, la evolución de la inseguridad de la información en el contexto tecnológico y operacional (Cano, 2008).

Para Ribagorda (2018) 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. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. (p. 14)

Si analizamos la ciberdefensa, podemos afirmar que es un conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición; ambos se complementan entre sí, ya que son un conjunto de variables claves, en la cuál es necesario el desarrollo de la práctica que le dan sentido a este contexto (Santiago & Allende, 2017).

Los términos de ciberseguridad y ciberdefensa son empleados para referirse a lo mismo. Con base en la revisión realizada en párrafos anteriores, podemos verificar

que los términos son usados para referirse a la acción de hacer frente a las nuevas amenazas cibernéticas. La existencia de estos dos términos puede deberse a lo reciente de la temática ya que cada investigador podría proponer sus propios términos para abordar la problemática.

Para finalizar este capítulo, se rescatan los elementos teóricos más importantes que guían el presente estudio:

Primero, se adopta una mirada realista para comprender los conflictos surgidos en el nuevo medio virtual denominado ciberespacio, pues cada nación actúa y vela por sus interese propios, a su vez estos entran en conflicto con los intereses de los demás, entonces empieza un nuevo tipo de ataque (ciberataque).

Segundo, se conceptualiza a el nuevo lugar virtual como ciberespacio, que se trata de una nueva dimensión de tipo virtual, dónde los seres humanos interactúan a tal punto que se ha convertido en su cotidianeidad, en este sentido, una afectación o ataque a este ciberespacio significaría un tipo de vulneración a la seguridad del individuo (usuario).

Tercero, ya contextualizado la problemática del uso del ciberespacio hoy en día y su vulnerabilidad a ser afectado por algún ciberataque, se plantea la ciberseguridad como medio o estrategia para actuar en favor de garantizar la seguridad de los usuarios que interactúan y se desenvuelven diariamente en el ciberespacio.

Por último, se ha descrito a los actores implicados en este nuevo tipo de guerra virtual, pues, esto permitirá en capítulos posteriores comprender la dinámica de la misma y desde dónde se puede abordar la ciberseguridad para alcanzar su objetivo, que es garantizar la seguridad a sus usuarios.

CAPITULO II. AMENAZAS DE CIBERATAQUES

En este capítulo se presentarán los ciberataques que suceden o acontecen a nivel mundial, específicamente se describirá casos de ciberataques sucedidos en países incluso que son caracterizados por un alto grado de ciberataques, pues estos han motivado a los países a trabajar arduamente para salvaguardar la seguridad de los usuarios que ocupan el ciberespacio como una nueva forma de vida o manera de interactuar con los demás y sus actividades diarias. En esta misma línea, se describirá los ciberataques sucedidos a nivel de Latinoamérica con casos particulares de países correspondientes a esta región. Por último, se describirá el caso particular que se presenta en el Ecuador en relación a los ciberataques ocurridos en el mismo.

Ciberataques en el ámbito internacional

Para contrarrestar los ciberataques desde la perspectiva internacional, es fundamental consolidar acuerdos de "colaboración entre estados, organizaciones o alianzas militares internacionales, el sector privado, la industria y el sector académico". Para hacer frente a estos ataques es necesario trabajar en forma conjunta y "multidisciplinar en los campos científico, tecnológico, político, diplomático, económico, jurídico, militar y de inteligencia (Madrigal, 2020).

El ámbito legal en el que se desenvuelve el mundo cibernético solo favorece los intereses de ciertos países, grupos criminales y terroristas en ventaja hacia los países democráticos, ya que en ellos las "libertades públicas y derechos de expresión y privacidad" no permite que las fuerzas armadas, de orden y seguridad ya que están muy restringidos al uso de ciber espacios.

"El uso legal de equipos de penetración (red team), la monitorización de redes, uso legal de datos personales para investigaciones forenses de ciberataques,

competencias policiales y militares" (Ministerio de defensa, 2010, p. 172), todo lo antes mencionado beneficia a potenciales enemigos y adversarios que utilizan las armas cibernéticas y atacar en sociedades democráticas (Madrigal, 2020).

Organizaciones que se relacionan con el área educativa y ejercicios en la OTAN que se desenvuelven con el ciberespacio son de ciberdefensa, por lo que estas organizaciones se cuestionan si se debe entrenar a militares en el uso de herramientas para ciberataque y que luego les permita utilizar estos conocimientos para cometer delitos sin el control de los propios ejércitos, sin embargo parte de la formación de los militares de ciberguerra es adaptar sus funciones a las tecnologías del momento para contrarrestar una guerra electrónica (Izaguirre & León, 2018).

La ciberseguridad en el ámbito militar sirve para actuar como un punto estratégico en contra de ataques en la política de un estado, causando conflicto entre países que miden sus fuerzas, basados en los múltiples ataques como ejemplo la base de datos Nacional de vulnerabilidades de EEUU misma que registra aproximadamente 43.800 de amenazas al mes de septiembre del 2010, de igual forma las alertas a estas que son como 13 al día (Izaguirre & León, 2018).

En vista a las múltiples amenazas a las TICS de los usuarios demandan seguridad, estos ataques pueden proceder de hackers informáticos al igual que terroristas, "organizaciones criminales y extremistas políticos, movimientos fanáticos religiosos, servicios de inteligencia y fuerzas militares adversarias".

En el ámbito de las operaciones militares, los ciberataques son considerados una amenaza porque es probable que estas se combinen con ataques informáticos con el fin de dejar fuera de servicio las redes y sistema del atacante. Un ejemplo dado de ciberataque en el área militar se dio en Georgia en el conflicto con Rusia en Ossetia del Sur y Abkhazia, en donde fue la primera vez que una operación militar estuvo

acompañada por ciberataques a los sitios web del gobierno georgiano y otras páginas comerciales, dejándolas fuera de servicio (Durán, 2011).

Uno de los tipos de atentados cibernéticos también se produce en el ámbito militar, un ejemplo de estos ataques los encontramos en Nueva York, Madrid o Beslán, terrorismo de ciberataques en Estonia, Georgia dejan en evidencia que, frente a los nuevos riesgos y amenazas, las formas de persuadir los militares no son eficaz no garantiza la seguridad. La Unión Europea se ha dotado de una estrategia de seguridad propia, misma que demanda recursos suficientes, uso eficaz y coherente de los instrumentos que dispone para prevenir conflictos, pero ningún país europeo incluso EEUU está en condiciones de hacer frente a estos recursos. (Durán, 2011)

Estados Unidos recibe miles de ataques, que han afectado y robado información secreta de vital importancia como lo fue el caso de Joint Strike Fighter F-35, (NTD Spanish, 15 de marzo 2013). Han logrado ingresar a páginas de instituciones de gran valor para la nación como Departamento del Tesoro y de Estado, el Pentágono y de la Casa Blanca (Sandra, 2014). A continuación, se hacemos mención a renombrados ciberataques que ha sufrido los Estados Unidos de América:

- **MafiBoy (año 2000):** Michael Calce alias MafiaBoy, causó daños en el ciberespacio, era un estudiante de instituto canadiense quien "Atacó a un sistema de computadoras causando que el servicio o recurso sea inaccesible a los usuarios legítimos en varios sitios web comerciales de alto perfil como Amazon, CNN, eBay y Yahoo, este ataque no permitió el acceso a los usuarios a los centros comerciales causando pérdidas económicas a la empresa y a los usuarios.
- **Google China:** Las sedes chinas de Google sufrieron una violación de seguridad, por medio de hackers que abrieron una lata de worms en el sistema

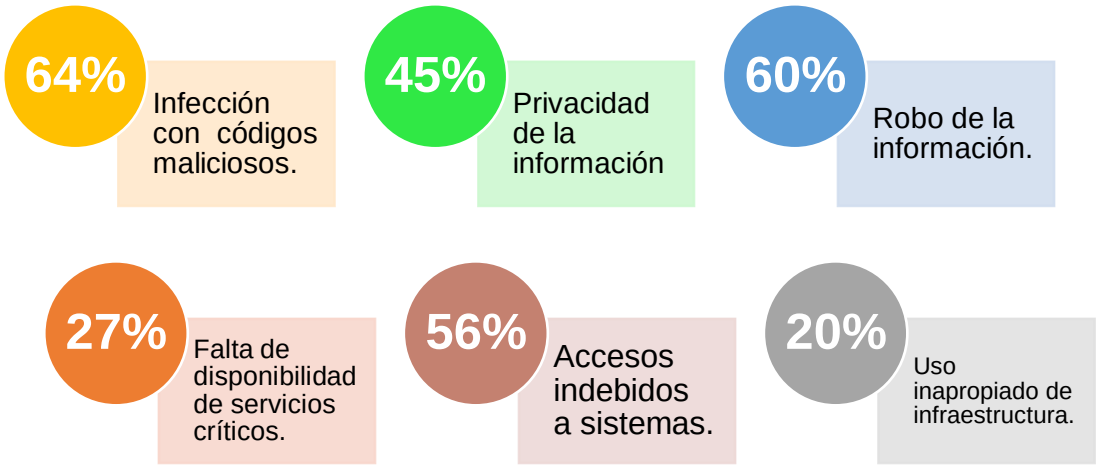
operativo, permitiendo que los hackers tengan acceso a servidores corporativos de Google y puedan apropiarse de la propiedad intelectual de los mismos.

- **Adolescente hackeo Departamento de Defensa de Estados Unidos y la NASA (1999):** Jonathan James de 15 años había logrado ingresar en los ordenadores de una División del Departamento de Defensa e instalado una puerta para interceptar miles de correos electrónicos de diferentes organizaciones gubernamentales, incluidos los de diferentes equipos militares.

Caso de ciberataque en américa latina

El grupo "hacktivista" autodenominado Anonymous en el primer semestre del 2011 atacó los portales de la presidencia de Colombia, el Senado de la república, gobierno en línea y los ministerios del Interior y justicia, Cultura y defensa. Este ataque se da por causa del proyecto de ley que "regula la responsabilidad en las infracciones al derecho de autor y los derechos conexos en Internet" este grupo ha atacado a entidades públicas y privadas entre las cuales tenemos: PayPal, banco suizo Post Finance, MasterCard, Visa y páginas web del gobierno suizo (Caceres, 2017).

Figura 1. Preocupaciones de seguridad digital en las empresas de América Latina

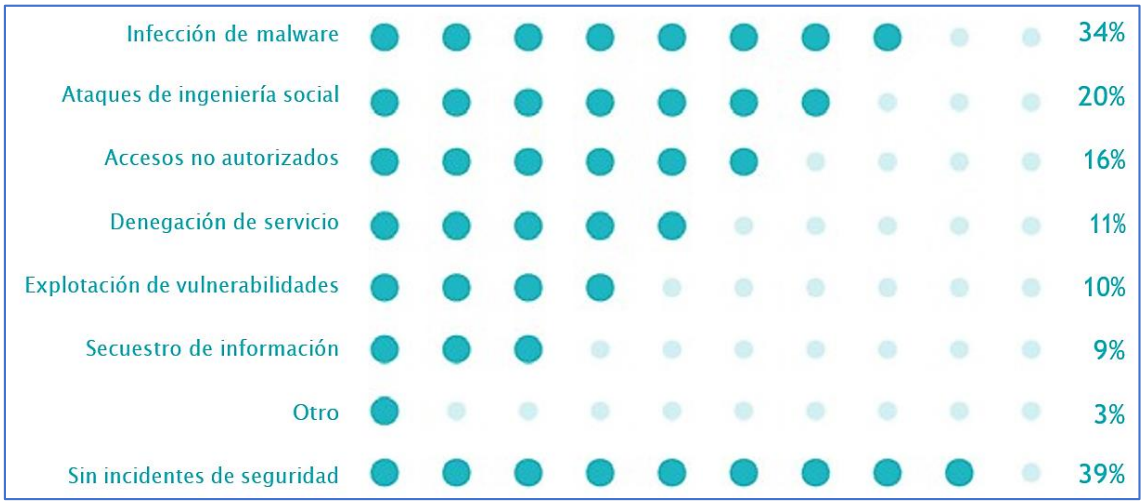


Adaptado de: ESET, Security Report (2021).

La gente común usa el internet para comunicarse entre sí por lo que la mayoría de personas no tienen tanto conocimiento sobre los ataques cibernéticos siendo vulnerables a amenazas o robos de identidad. Por otro lado, tenemos los ataques de mayor magnitud a empresas o gobiernos provocando grandes problemas económicos y de seguridad informática por lo que cada país debe ser consiente y tener conocimiento de los riesgos en el que pueden estar (GONZALEZ LONDOÑO, 2020).

Queda entendido que este es un problema que afecta países y regiones del planeta por eso Latinoamérica no es la excepción ya que es mayormente afectada debido al bajo nivel de protección debido a la falta de conocimiento e interés dando acceso fácil a los cibercriminales para atacar y hacer lo que ellos quieran dentro del país convirtiendo a Latinoamérica el sitio más popular para los ciberataques (Caceres, 2017). Para entrar en contexto, se conoce varias maneras de ataques cibernéticos en América latina entre las más mencionadas tenemos a los virus informáticos, Spam, Spoofing, Pishing, etc.

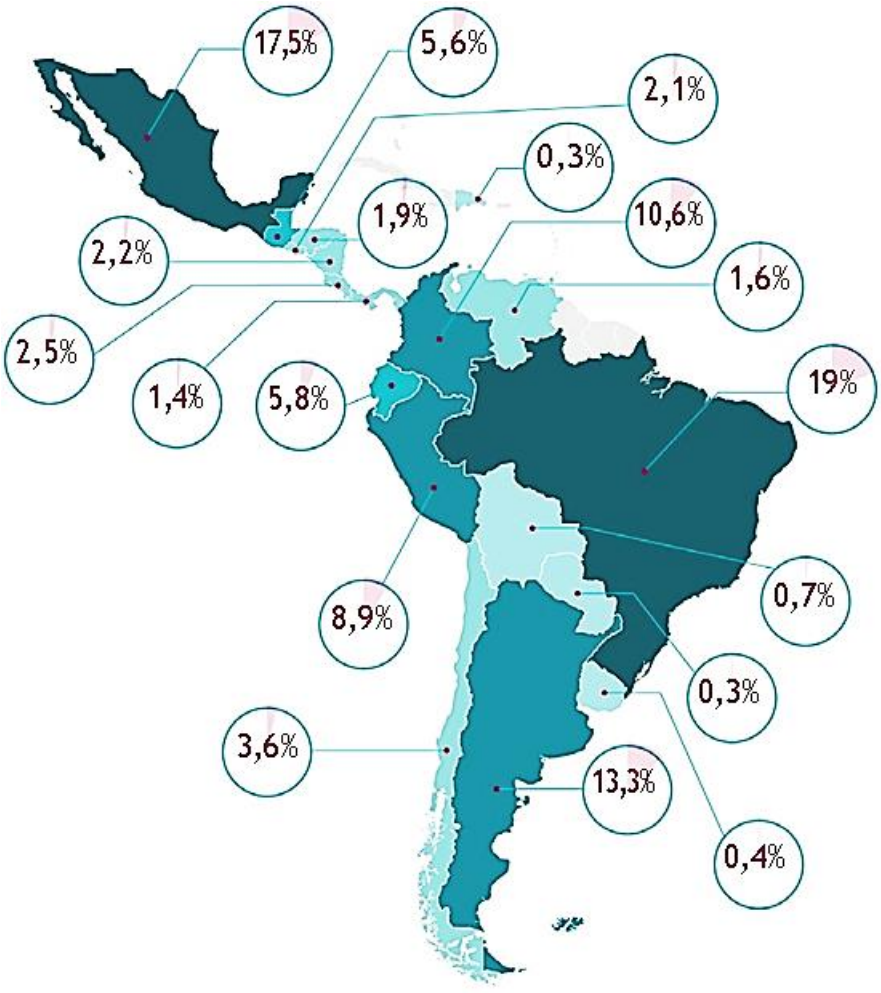
Ilustración 1. Incidentes de Seguridad de la Información en las empresas de Latinoamérica.



Fuente: ESET, Security Report (2021).

Ahora podemos tener conocimiento y los objetivos específicos de cada ataque y podemos analizar que cada uno de ellos tiene como finalidad la obtención de información sensible bien sea para amenazar y sacar beneficio de ellos o usarlo en contra de la empresa o país al cual se lo esté atacando y podemos confirmar que tanto como organizaciones públicas como privadas son las más afectadas con respecto a la vulnerabilidad de sus sistemas. Al referirnos dentro de Latinoamérica, debemos saber que no todos los países tienen la misma igualdad de conexión a la red, por ende, algunos países tendrán mayor riesgo que otros.

Ilustración 2. Detección de malware en empresas de Latinoamérica en 2020



Fuente: ESET, Security Report (2021).

Si apelamos a un ejemplo de estos casos, la empresa Symantec destaca que el 4,2% de los ataques en américa latina y Caribe en 2013, fueron en Venezuela, teniendo un contagio del 23% de malware y 5% de spear phishing dentro de la región. Según la revista Forbes México los países que encabezan las listas con más ataques cibernéticos en la región son Brasil seguido por México, ambos figuran en el top 20 de países más afectados por malware en el mundo (Hernández Armenta, 2019).

En el año 2018 al 2019 la empresa Kaspersky evito 45 intentos de infecciones a causa de la descarga ilegal de Windows 64 bits y el adware que presenta anuncios invasivos entre la navegación (Hernández Armenta, 2019).

La revista Forbes también nos comenta que dentro de la clasificación mundial de ataques por phishing esta Brasil en primer lugar, seguido por Venezuela. Dentro del top 20 también encontramos a Chile, Ecuador, Guatemala, Panamá, Honduras, México y Argentina siendo estas dos, una de las más bajas en posición.

Por esta razón hay varios casos de hackeos dentro de sistemas del gobierno como en el caso de México que sufrió un ataque en marzo del 2016 en el Servicio de Administración Tributaria, donde el grupo Anonnymous México provoco plantar la página web oficial por dos horas con el objetivo de mostrar su poder dentro de la red, Lo mismo ocurrió en Brasil y Colombia. En el caso de Colombia, la mayoría de ataques son en las páginas presidenciales de la Republica y Ministerio de Defensa Nacional dejándolas sin funcionamiento por horas (Izaguirre & León, 2018).

Otro caso muy sonado de ataques fue en 2009 que ocurrieron varios robos de cuentas bancarias haciendo un monto de 50 millones provenientes de 8000 tarjetas de créditos clonadas y 9 millones de dólares que fueron divididos en 5 países de Latinoamérica.

Así como podemos entender que América Latina necesita mejorar su seguridad informática debido a que en la mayoría de países no hay un conocimiento completo sobre la seguridad cibernética, debido a eso falta reforzar la protección de los países con el desarrollo de herramientas tecnológicas para la defensa de los intereses locales y regionales (Acuña Lopez , Villa Motato, 2018).

La creación de leyes para el sector público y privado en las actividades cibernéticas y formar una discusión referente a los delitos de cibernéticos y una solución para ellas.

De esta manera concluimos que, la gran parte del problema de los ciberataques radica en la desinformación y poca educación de los usuarios por lo que se recomienda la implementación de herramientas que resguarden moderadamente la protección de las maquinas.

Por ejemplo, tenemos Panda Protection, Avast free antivirus, entre otros que son gratuitos y ayuda a su protección conectados a la red, también se recomienda su constante limpieza del sistema para mejorar el rendimiento de las aplicaciones y buscar programas que ayuden a eliminar softwares maliciosos (Acuña Lopez , Villa Motato, 2018).

Seguridad y ciberataques en Ecuador

En el intervalo de tiempo, comprendido de 1979 a 2016, el Ecuador, ha atravesado por diferentes formas de organización política, en donde las diferentes formas de institucionalidad del Estado han contribuido en el desarrollo de la sociedad en general. Cabe resaltar que con el pasar de los años, en períodos anteriores al 2007 se ha evidenciado la influencia militar (López, 2016).

Por otra parte, López destaca que a lo largo de la historia se han evidenciado una constante renovación de las concepciones de seguridad por lo que para los entes gubernamentales del Ecuador también han sufrido transformaciones en cuanto a sus lineamientos de seguridad para la protección civil.

Es por eso que, en el año 2008, tras la nueva creación de la Constitución ecuatoriana, el nuevo planteamiento de la concepción de la seguridad, viene denominada por el término ‘‘seguridad integral’’.

La seguridad integral que propone la constitución ecuatoriana posee una visión multidimensional, incluyendo aspectos generales de protección para el hombre, el estado y naturaleza (Sánchez, 2015).

En el período reconocido como el regreso a la democracia en el Ecuador, (1979-2001) hubo un impacto perceptible para la sociedad ecuatoriana en diferentes momentos, en donde se vivieron acontecimientos que afectaron de manera directa la seguridad y defensa del estado ecuatoriano, al año 1978, luego de reconocer un Triunvirato Militar como forma de gobierno, e l país estaba totalmente influenciado por la comunidad militar, por lo que la seguridad atendía únicamente a la estabilidad territorial de la nación (Sánchez, 2015).

Tras la institucionalización militar, en el año de 1979 se reforma la Ley de Seguridad Nacional en el registro oficial N° 887, manifestando en su artículo 2 que:

> El Estado garantiza la supervivencia de la colectividad, la defensa del patrimonio nacional y la consecución y mantenimiento de los Objetivos Nacionales; y, tiene la función primordial de fortalecer la unidad nacional, asegurar la vigencia de los derechos fundamentales del hombre y promover el progreso económico, social y cultura de sus habitantes, contrarrestando

> los factores adversos internos y externos, por medio de previsiones y acciones políticas económicas, sociales y militares. (Ley de Seguridad Nacional N° 275, 1979).

En este sentido, la seguridad nacional sería regida por la autoridad máxima, en este caso, el presidente de la República, siendo capaz de tomar decisiones bajo el propósito de fortalecer los diferentes ejes fundamentales para el desarrollo socioeconómico. Sánchez (2015), certifica que, para esta época, el área de la defensa hace responsable al Estado frente al planteamiento y cumplimiento de objetivos predominando la defensa para la integridad territorial y la soberanía mediante organismos superiores como el Consejo de Seguridad Nacional (COSENA) y al Comando Conjunto de las Fuerzas Armadas.

Ya en el año de 1981, en la guerra de Paquisha, se vuelve a replantear las ideas relacionadas con la defensa orientada en la soberanía, el enfrentamiento bélico para la defensa de intereses y la militarización de las zonas para la protección del estado frente a las amenazas de invasión, no obstante, si bien se adoptaron medidas relacionadas con la defensa civil, la tregua se pudo dar gracias a los convenios bilaterales (Torres, 2000).

Para el período 1984-1998 la seguridad estaba sustentada en la Doctrina de Seguridad Nacional, es decir una visión geopolítica tradicional estancando nuevamente el conflicto bélico con Perú (Sánchez, 2015), sin embargo, el problema pudo resolverse tras una firma de paz en el año de 1998, sin embargo, la participación militar aún era latente debido a que la comunidad militar se vio involucrada en el escenario político.

En el año 2001, el Ecuador vive uno de sus peores escenarios, tras un proceso de dolarización, y un suceso de impacto mundial, como fue el atentado que

vivieron los Estados Unidos de América, los diferentes países cambiaron nuevamente su visión acerca de la seguridad, redireccionando su preocupación en aspectos como el terrorismo, el narcotráfico y el crimen organizado (Benalcázar, 2008).

Con el fin de un conflicto fronterizo, la influencia de la política de seguridad de EE. UU y el origen de nuevas controversias, en el año 2002 nuevamente se ve definido un nuevo panorama e incorporación de la política de defensa en el año 2002, como un proceso de restructuración de la seguridad y defensa. El jefe de gobierno del año 2002, expuso el Libro Blanco de la Defensa Nacional, identificándolo como una agenda que mantiene el modelo de Estado, pero que cubre temas económicos, políticos, sociales y ambientales, además de la participación de organizaciones no estatales. También incluye una serie de aspectos que nunca antes se habían abordado, como: la pobreza extrema, la guerra contra el terror, la escasez de recursos y la migración (López N. , 2011).

En el (Libro Blanco de la Defensa Nacional, 2002) muestra no solamente los objetivos que tiene la nación ecuatoriana al defender la población y recursos, sino que expone de manera concreta la visión de los gobernantes frente al nuevo concepto de seguridad adoptado al momento, abandonando el concepto de seguridad que se había tenido previamente debido al deseo del Estado en relación a la preservación de los intereses nacionales. (López N. , 2011).

Según (Jarrín, 2008), debido a la inestabilidad política posterior al año 2003 por la destitución del presidente (Lucio Gutiérrez), desencadenó la necesidad de reestructurar las instituciones con el propósito de ejecutar diversos cambios para la despolitización institucional para fortalecer la defensa nacional.

Él Libro Blanco (2005) es reescrito con una nueva visión, basado nuevamente en el conflicto limítrofe ecuatoriano con Colombia, estudiando las amenazas recibidas por la situación ya que se desencadenó una con oleada con el tráfico de droga, la violencia organizada, afecciones de los desplazados y refugiados, el libro expone en esta actualización la necesidad de paz regional y una reestructuración de las Fuerzas Armadas ecuatorianas, por lo que en el período 2005-2006 se trabaja en la creación de una nueva "Agenda de Defensa Nacional".

> El territorio ecuatoriano, para los años 2008-2013 logra conseguir una ''estabilidad política'' en relación a la estancia fija del gobernante en el poder (Rafael Correa), se destaca en este período la creación de una nueva Constitución (2008) que se deslindó por completo de la visión tradicional de la milicia, planteando un enfoque integral para la seguridad y defensa, dando al Estado la responsabilidad de conceptualizar, crear y regular políticas, leyes y crear instituciones encargadas de cumplir las actividades de seguridad y defensa del territorio ecuatoriano. En esta nueva constitución, se describe como un deber del Estado ''Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción'' (Constitución de la República del Ecuador, 2008, Art. 3 numeral 8).

En los años 2009-2013, la (Secretaria Nacional de Planificación y Desarrollo, 2009) articula el Plan Nacional del Buen Vivir, misma que encierra en conjunto el Estado (estadocéntrico), el ser humano (antropocéntrico) y la naturaleza (Biocéntrico), por lo que hablar de seguridad incluye aspectos como los derechos humanos, la protección del individuo, preocupándose también por la calidad de vida bajo una visión soberana además de las capacidades estratégicas de la seguridad integral. Por otra parte, se plantea la Ley de seguridad Pública y del Estado (2009).

Adicionalmente, se logra diseñar el Plan Nacional de Seguridad Integral (2011-2013) que incluye y comprende la actuación de la sociedad y el Estado ecuatoriano mediante temas de gobernabilidad, derechos humanos, democracia, la integración latinoamericana, y la seguridad global.

En base a la nueva ley creada, el gobierno entiende necesario la creación del Consejo de Seguridad Pública y el Estado (COSEPE), que será el nuevo encargado del área de seguridad. Por otra parte, quien se encargaría de diseñar y ejecutar las políticas de seguridad (Plan de Seguridad Integral), el nuevo ministerio creado a la fecha, el Ministerio Coordinador de Seguridad, en este nuevo documento legislativo se logran designar a los nuevos encargados de la defensa, posicionando a:

- Ministerio de Defensa
- Ministerio de Relaciones Exteriores
- Secretaria Nacional de Inteligencia

Además, también se plantearon las agendas a cumplir por los ministerios destinados a direccionar el desarrollo de la seguridad, siendo las siguientes:

1. Agenda Estratégica de Política Exterior.
2. Agenda Política de Defensa.
3. Agenda de Seguridad Ciudadana y Gobernabilidad.
4. Agenda de Justicia, Derechos Humanos y Cultos.
5. Agenda Política de Gestión de Riesgos.
6. Agenda Nacional de Inteligencia.
7. Agenda de Plan Ecuador.
8. Agenda de Estrategias de Seguridad Vial (Plan Nacional del Buen Vivir 2009-2013).

El plan Nacional de Seguridad Integral sufre una nueva actualización en el período 2014-2017 debido a los vacíos conceptuales, una situación compleja para el gobernante en curso debido a que atravesaba su tercer período consecutivo y debía ‘‘sostener’’ un mismo pensamiento para contemplar el nuevo planteamiento del plan de seguridad integral. Para esta actualización se consideraron ejes enfocados de manera directa con su definición e implementación, ampliando su operatividad a través de los ámbitos:

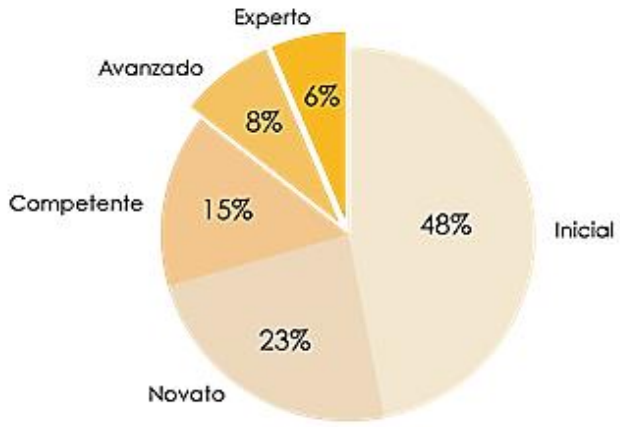
- Defensa y Relaciones Internacionales.
- Seguridad Ciudadana y Justicia.
- Gestión de Riesgos y Ambiente.
- Soberanía Tecnológica.
- Ciencia e Inteligencia Estratégica para el fortalecimiento democrático.

Si bien los casos de ciberataques a nivel mundial han tenido un crecimiento evidente en función de la evolución tecnológica, el Ecuador no había reportado un alto nivel de ataques cibernéticos hasta la captura y retiro de asilo político a Julian Assange. Según el reporte de P. Real viceministro de Tecnologías de la Información y Comunicación (TIC) del gobierno de Lenin Moreno (2017-2021), se registraron más de 40 millones de ciberataques al escenario digital del Ecuador en menos de dos días. Estos ataques provenían mayormente del continente europeo (Rumanía, Francia, Austria, Holanda, Alemania), y en porcentajes menores los registros manifestaron ataques provenientes de Brasil, Estados Unidos y de Ecuador mismo (Diario El Comercio, 2019).

El Ecuador a manera de crear medidas para la ciberseguridad de las empresas, ha adoptado la iniciativa del BID (Banco Interamericano de Desarrollo) que consiste en

realizar un chequeo gratuito de los niveles de madures digital, esta herramienta sirve de base para mejorar la gestión de seguridad digital de cada empresa además de medir y comparar los avances a lo largo del tiempo. Este estudio se aplicó a 617 empresas en donde se evidenció que la madurez digital tiene niveles deficientes (Reporte Chequeo Digital Ecuador, 2021).

Ilustración 3. Porcentajes de madurez digital de las empresas en el Ecuador



Fuente: (Reporte Chequeo Digital Ecuador, 2021).

En este sentido, se puede reconocer la sensibilidad del ciberespacio ecuatoriano, siendo un escenario perfecto para recibir ciberataques con mayor facilidad. A continuación, se detallan algunos de los ataques más sonados durante la última década en el Ecuador.

Julian Assange

En el año 2006 fue fundada por Julian Assange la organización WikiLeaks, un website encargado de poner en evidencia, filtrar y divulgar la información más sensible de diferentes países, de los más controversiales se citan (Forn, 2015):

- Manual de procedimiento militar en el campamento Guantánamo (7 de noviembre del 2007).
- Publicación de video de muerte a 11 iraquíes por soldados estadounidenses. (5 de abril del 2010).
- Publicación de alrededor de noventa mil documentos de reportes de la guerra de Afganistán (25 de julio del 2010).
- Publicación de trescientos noventa mil documentos clasificados del Pentágono relacionados a ataques en Irak (octubre del 2010).
- Publicación de doscientos cincuenta mil documentos que revelaron la disposición de que diplomáticos estadounidenses hagan espionaje a políticos extranjeros y altos funcionarios de la ONU (28 de noviembre del 2010).

Los temas expuestos tuvieron tanta repercusión a nivel mundial debido a la gran afección política que presentaron los países atacados, por lo que en el año 2010 (agosto) se abre una investigación en contra del fundador del sitio web de WikiLeaks por el delito de acoso sexual en Suecia y posteriormente se emitió la orden de arresto (diciembre). En este contexto, fue dado de baja WikiLeaks.org y entregado al Partido Pirata Helvético. Durante este mismo año, Assange fue detenido por los cargos formulados en su contra: acoso sexual y violación, no obstante, salió en libertad por hacer uso de su derecho a fianza.

Luego de declarar que dejará de publicar los secretos de estado por la falta de financiación pues PayPal canceló la cuenta de WikiLeaks en el mes de diciembre del año 2010, Assange, manifiesta ser un perseguido por los medios de comunicación por haber filtrado información confidencial de EE. UU (Pulido, 2021).

De manera confidencial, un tribunal secreto de los Estados Unidos levantó cargos en contra de Assange, con el propósito de conseguir su extradición, su proceso inició en febrero del 2011 y en noviembre del mismo año el Tribunal Supremo de Londres da por aprobada su extradición, para evitar su extradición, el fundador de WikiLeaks apeló la sentencia, misma que fue rechazada, por lo que Assange busca refugio en la embajada de Ecuador (Londres).

El 5 de julio del 2012, el portal WikiLeaks no solo reaparece, sino que nuevamente empieza a compartir información de políticos del régimen Sirio en más de dos millones de correos electrónicos. Ante este evento las autoridades Británicas solicitan efectuar el arresto para Assange en la embajada del Ecuador, de lo contrario entrarían de manera forzosa. Ante este evento el gobierno ecuatoriano enfatiza nuevamente el asilo político para el informático manifestando un peligro eminente debido a que Assange era sujeto de interés contra EE. UU, por lo que, se da inicio un proceso de negociación entre los ex cancilleres Ricardo Patiño (Ecuador) y Williann Hague (Reino Unido) para dar solución al caso. En el mes de noviembre, los Estados Unidos notifican que no se presentarán los cargos anteriormente citados, no obstante, en el año 2014 nuevamente se levantan presunciones a cerca de nuevos cargos contra Julian Assange, vinculando al informático con cargos de Espionaje y Terrorismo (Pulido, 2021).

Pese a la zozobra, el sitio web de Assange, nuevamente arremete contra los Estados Unidos y expone cerca de veinte mil correos electrónicos en contra de la campaña de Clinton, lo que desestabilizó su carrera política, haciendo que de alguna manera Trump, triunfará en la contienda electoral. Por el asunto suscitado, el ex presidente del Ecuador (Rafael Correa) solicita a Assange no intervenir en los asuntos

de carácter político, por lo que también, ordenó el retiro del servicio de internet para el informático.

En mayo de 2017 se cierran las investigaciones del caso WikiLeaks, no obstante, en meses posteriores tras la contienda abierta para las elecciones presidenciales de Francia, el portal vuelve a poner en evidencia correos de Macron, lo que avecinaba nuevamente una persecución para Assange, frente a esto, el gobierno del Ecuador ahora dirigido por Lenin Moreno, otorga la nacionalidad ecuatoriana al informático, con el propósito de facilitar su salida de Reino Unido y asumir el cargo diplomático, algo totalmente rechazado por el gobierno Británico. Posteriormente, Moreno, reconoce a Assange como un ‘‘problema’’ para su gobierno, por lo que, durante un período corto emite medidas estrictas de para regular el comportamiento del informático en su portal web para posteriormente quitar el asilo dado a Assange. Sin embargo, en el año 2019, nuevamente se expone información en WikiLeaks, lo que provocó su detención, a través del Departamento de Justicia de los Estados Unidos por varios delitos informáticos en contra del Estado. En abril del mismo año, debido a que Assange no contaba con ningún tipo de asilo, se confirmó y cumplió un proceso de extradición a los Estados Unidos, en donde al informático le fueron formulados 18 cargos que sumaron ciento setenta y cinco años de condena (BBC News, 2019).

Ante este proceso judicial, en Ecuador, se vincula de manera arbitraria al Ola Bini, quien había trabajado en el área de la seguridad informática del Ecuador. El presidente Moreno justifico a CNN, que la detención de Bini, había intervenido en la política ecuatoriana y la de otros países. La situación tanto de Assange como de Bini, desencadenó una serie de ciberataques al Ecuador afectando la información personal de los ciudadanos (La Posta, 2019).

La base de datos del Ecuador fue expuesta de manera pública por informáticos israelíes, lo que llevó al gobierno ecuatoriano a alertar a la ciudadanía. La información personal de casi 17 millones de ciudadanos del Ecuador, estuvo disponible en un servidor administrado por NOVAESTRAT (empresa ecuatoriana) y se podía encontrar información como montos de seguros privados, sueldos del mes de agosto y otro tipo de información reservada. Ante este evento, el exministro A. Michelena, reconoció que solamente el 26% de las Instituciones Públicas almacena la información más sensible en sitios seguros, por lo que cualquiera pudiera atacar y acceder a la información de manera fácil, en este sentido, Michelena propone intervenir de manera emergente la situación para investigar a los posibles implicados y sumado a esto bloquear el portal que divulgó la información sensible de la sociedad ecuatoriana (El Comercio, 2019).

Caso ANT

El sistema de la ANT (Agencia Nacional de Tránsito) se vio vulnerado desde el año 2017 por 99 usuarios externos que lograron emitir aproximadamente 15.970 licencias de conducir, se modificaron 14.583 multas y se dio la devolución de 26.801 puntos a las licencias de conductores que cometieron diferentes infracciones dentro de la seguridad vial. Ante este evento se levantó la denuncia en contra de los representantes de la ANT, ya que, si bien el delito fue perpetrado por expertos en informática, se pretende descartar o corroborar la participación de los miembros internos de la Agencia Nacional de Tránsito del Ecuador. Por otro lado, cabe destacar que, si bien el sistema fue atacado, la duración de este ciberataque fue tan extensa que hace suponer que los portales de la ANT no cuentan con ningún tipo de protección que hubiese permitido hacer una detección temprana sobre el asunto.

Las medidas de solución fueron de carácter civil, se revocarán las licencias y actividades realizadas por los hackers, pero aún no se ha planteado o al menos no se ha expuesto cual es el plan de ciberseguridad que se le dará a la Agencia Nacional de Tránsito (El Comercio, 2019).

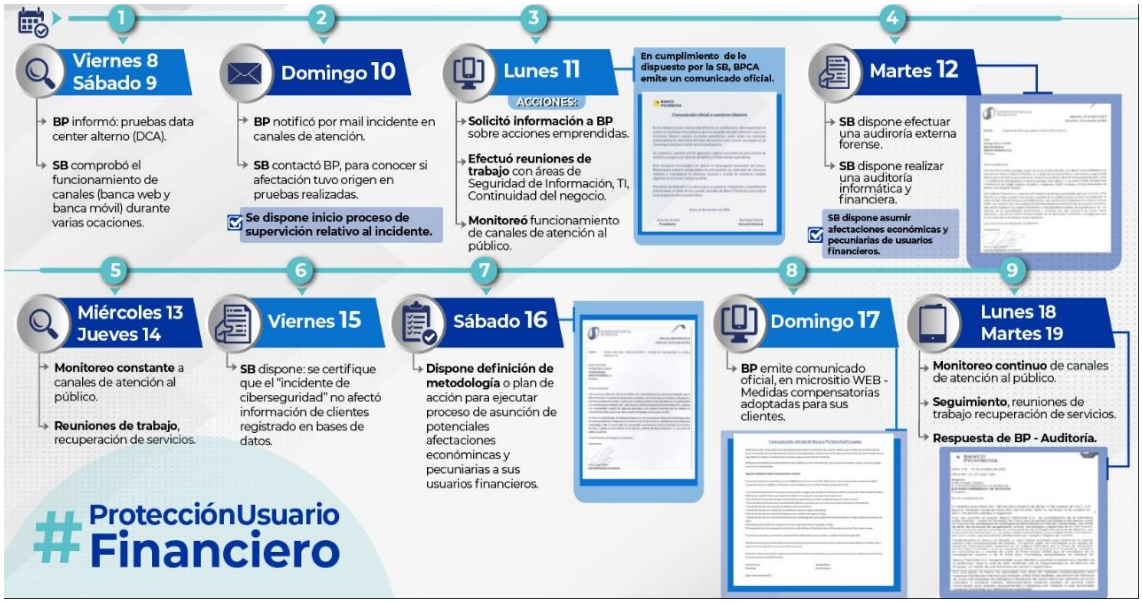
Sistema Financiero

Banco de Pichincha presentó en sus servicios durante el 09 de octubre en donde los usuarios manifestaron a través de diferentes canales, la dificultad de realizar transacciones por los canales electrónicos del Banco. Las autoridades tanto internas como externas reconocieron este caso como un ataque cibernético, y tras un proceso investigativo se detectó que fue hecho por atacantes internacionales que obstruyeron la web de la banca móvil y los corresponsales no bancarios, para regular la situación, Banco Pichincha manifestó contar con niveles de seguridad estandarizados por lo que reconoció tener la capacidad para el manejo de crisis. Si bien, por un lado, se reguló la inestabilidad de la crisis, por otro lado, las intermitencias continuaron e incluso se presentaron nuevos ataques en fechas posteriores, esto debido a que en el país no se cuenta con las herramientas que faciliten la investigación del caso ya que existe una única Unidad de Investigación de Ciberdelitos (Pichincha). La Superintendencia aportó al caso, recomendando al Banco una auditoría de carácter interno y otra forense además de que el Banco facilité la información oportuna y transparente a la ciudadanía y a esto se añadan medidas compensatorias para los afectados tras el ataque e inhabilitación de los servicios de Banco Pichincha, esta compensación consistía en devoluciones de: cobro e intereses, postergaciones y reconocimientos (El Universo, 2021).

Frente a este evento, una de las entidades gubernamentales del Ecuador, trabajó de manera rápida en la intervención del ataque para garantizar la ciberseguridad del

Banco y sobre todo la protección de derechos de todos los usuarios mediante el cumplimiento de diferentes actividades planificadas (post-ataque).

Ilustración 4. Supervisión incidente Banco Pichincha C.A – Octubre 2021



Fuente: Superintendencia de Bancos (2021).

Tabla 1. Ecuador: Indicadores de Medición del índice de ciberseguridad de la OEA

Dimensiones	Niveles de madurez de capacidad en
Política y estrategia	
Estrategia nacional de seguridad cibernética oficial o documentada	Inicial: No hay evidencia de la existencia de una estrategia nacional de seguridad cibernética; si existe un componente cibernético, puede ser responsabilidad de uno o más departamentos del gobierno.
Defensa cibernética	En cuanto a organización, su indicador mantiene un estado formativo, evidenciando que la defensa cibernética se incorpora a las diferentes ramas de las fuerzas armadas, pero no existe una estructura.
Cultura y sociedad	
Mentalidad de seguridad cibernética	Solamente en el sector privado se mantiene un nivel de madurez formativo, que han comenzado a darle prioridad a la seguridad cibernética.

Conciencia de seguridad cibernética	Formativo: Empresas líderes han comenzado a darle prioridad a una mentalidad de seguridad cibernética mediante la identificación de prácticas de alto riesgo.
Confianza en el uso de Internet	Formativo: La confianza en los servicios en línea se identifica como una preocupación; los operadores de infraestructuras toman en consideración medidas para fomentar la confianza en los servicios en línea; sin embargo, no se han establecido medidas.
Privacidad en línea	Inicial: La discusión con grupos de interés sobre asuntos de privacidad ha comenzado a nivel gubernamental.
Educación	
Disponibilidad nacional de la educación y formación cibernéticas.	Formativo: existe mercado para la educación y la formación en seguridad de la información, así como dirigidas a profesionales para incrementar el atractivo de las carreras en ciberseguridad.
Desarrollo nacional de la educación de seguridad cibernética	Formativo: Existen incentivos para la formación y la educación
Formación e iniciativas educativas públicas y privadas	Formativo: No hay transferencia de conocimientos por parte de los empleados de seguridad cibernética capacitados; debido a una formación limitada, solo hay uso informal de herramientas, modelos o plantillas.
Gobernanza corporativa, conocimiento y normas	Formativo: Las juntas directivas tienen algún conocimiento de cuestiones de seguridad cibernética, pero no de la forma en que estas podrían afectar a la organización.
Marcos legales	
Marcos jurídicos de seguridad cibernética	Formativo: Los socios experimentados han sido consultados para apoyar el establecimiento de marcos jurídicos y reglamentarios; se han identificado prioridades clave para la creación de marcos legales de seguridad cibernética pero aún no se han evidenciado.
Investigación jurídica	Formativo: Existe una capacidad mínima de investigación para indagar delitos que involucren pruebas electrónicas.

Divulgación responsable de la información	Inicial: No se reconoce la necesidad de una política de divulgación responsable en las organizaciones del sector público y privado.
Tecnologías	
Organizaciones de coordinación de seguridad informática	Formativo: La función de mando y control está en manos, de manera informal, del mismo modo existe un equipo o personal de respuesta a incidentes en el país, con roles y responsabilidades identificadas.
Respuesta a incidentes	Formativo: en cuanto a coordinación, se han identificado y publicitado directores de incidentes en cada agencia y ministerio a nivel nacional; pero los canales de comunicación entre estos directores siguen siendo ad hoc e incoherentes.
Protección de la Infraestructura Crítica Nacional (ICN)	Inicial: en todos sus indicadores marcan el estado inicial, pero el que destaca es la de coordinación donde se destaca que hay poca o ninguna interacción entre los ministerios gubernamentales y los propietarios de los activos críticos.
Gestión de crisis	Inicial: No hay entendimiento, o es mínimo, de que la gestión de crisis es necesaria para la seguridad nacional.
Mercado de la ciberseguridad	Inicial: Poca o ninguna tecnología se produce en el país; pueden estar restringidas las ofertas internacionales o son vendidas con un sobreprecio. tampoco se ha identificado la necesidad de un mercado de seguros ante delitos informáticos.

Tomado de: *Desafíos globales del cibercrimen.* Ochoa, 2021.

CAPITULO III. ESTRATEGIAS DE CIBERDEFENSA

Para la elaboración de la presente investigación de ciberdefensa en el estado ecuatoriano, se ha tomado en cuenta como referencia entre otros textos e investigaciones en las cuales se abordan temas como: las estrategias de defensa a nivel internacional, en dónde se presenta las estrategias de varios países europeos; seguido, en la misma línea de presentación se aborda las estrategias de defensa por parte de los países de América del sur.

Estrategias de defensa a nivel internacional

A continuación, se describen las estrategias utilizadas por los países de talla mundial que destacan por su ciberseguridad, esta descripción tiene la intención de presentar las estrategias clave usadas por estos países y que les han permitido tener un alto grado de seguridad para sus pobladores (usuario).

Cubeiro (2021), indica que mundialmente los ciberataques son el principal riesgo global de origen humano, con diversas consecuencias que casi siempre se traducen en interrupción de servicios, pérdidas económicas o daños a la reputación de la víctima. La gran mayoría persigue un fin económico, pero también hay algunas que se realizan con fines activistas para obtener información sobre un adversario, otras como acciones integradas en un plan militar.

En el mismo artículo Cubeiro (2021), indica que la superioridad en el ciberespacio desnivela la contienda a su favor, incluso en casos que el adversario sea superior en otros ámbitos operacionales. Esto ha dado lugar al surgimiento de nuevos actores en este medio cibernético, a los que se los conoce actualmente como Actores-Estado, quienes se mantienen al margen del mundo real, sea esto en tiempo de paz,

crisis o conflicto, ejecutando en el anonimato, campañas de ciberespionaje durante seis, siete y hasta ocho años antes de ser detectadas.

En este ecosistema heterogéneo, se han conformado unidades de ciberespionaje y ciberguerra que trabajan al servicio de los Estados, especialmente para las superpotencias, sin embargo se han unido a estos grupos algunos Estados de menor peso (Irán, Israel, Corea del Norte) que se presentan fuertes por dotarse de estas capacidades (Cubeiro, 2021).

Cubeiro (2021), nos hace conocer que estas unidades están integradas por grupos multidisciplinares y con importantes recursos, vinculados a las grandes agencias gubernamentales de inteligencia y organizaciones militares. Se les denomina Amenazas Persistentes Avanzadas (APT). Estos grupos analizan sus objetivos y llevan a cabo ataques extraordinariamente sigilosos y muy dirigidos.

Algunas de las principales APT descritas en Cubeiro (2021), que actualmente operan en el mundo con denominaciones atribuidas a diferentes empresas dedicadas a la inteligencia de ciberamenazas son las siguientes:

Ciberseguridad China

Como APT1, una de las más activas, con muchas agencias vinculan desde hace años con la **Unidad 61398** del Ejército chino. Se le atribuyen ataques en su mayoría al espionaje industrial a más de un millar de organizaciones y empresas de más de cien países. En el año 2013 en un informe elaborado por la empresa Mandiant, se especifica la localización geográfica de sus operaciones, encuadrándola orgánicamente dentro del Ejército Popular de Liberación.

Corea del Norte

Uno de los grupos que más notoriedad han alcanzado en los últimos años es el **Lazarus Group**, que se presume opera desde Corea del Norte. Se conoció de ellos en el año 2014 con el ataque contra la empresa Sony.

Sus primeros años iniciaron especializándose con ataques contra la banca y el sector financiero. Posiblemente iniciaron como un grupo criminal que buscaba beneficio económico, actualmente se observa que sus objetivos coinciden con los del gobierno de Corea del Norte.

Segú algunos analistas se presumen que crearon el virus WannaCry que en el año 2017 causó afectaciones por todo el mundo, sin haberse identificado aun claramente sus intenciones en diferentes procesos, de los cuales algunos de sus miembros resultado ser fichados para su busca y captura por el FBI.

Ciberseguridad Rusia

Uno de los grupos rusos más activos y conocidos es **Fancy Bear**, también conocido como **APT 28 y Sofacy**, Se presume que su base principal opera desde Moscú realizando ciberespionaje. Según algunos analistas se ha integrado o vinculado al Servicio de Inteligencia ruso (GRU).

Sus operaciones se centran contra agencias gubernamentales, empresas de los sectores aeroespacial, defensa, energía y administraciones públicas de un gran número de países, especialmente contra los estados miembros de la OTAN o transcaucásicos.

En varios informes se los ha vinculado en actividad a los grupos Fancy Bear con la de **APT 29** otro grupo de los más conocidos grupos rusos. Se ha indicado en

estos informes que estos dos grupos coordinarían su actividad en función de sus capacidades técnicas.

Ciberseguridad Estados Unidos

En el medio de ciberdefensa mundial se considera al **Equation Group** como el grupo APT más sofisticado y poderoso del mundo. Se lo encuentra vinculado a la Agencia de Seguridad Nacional de los Estados Unidos, la NSA.

Su principal especialidad es el ciberespionaje, dentro de este medio se atribuyen acciones contra infraestructuras críticas, además se los considera como los creadores de algunos malwares más sofisticados que se han conocido, como Stuxnet y Flame. Se cree que las ciber-armas puestas a subasta en el 2016 fueron robadas a la NSA por el grupo autodenominado **Shadow Brokers**.

Del análisis desarrollado se deduce que las operaciones efectuadas por el **Equation Group** son pocas en una comparación con las efectuada por las APT rusas, iraníes o norcoreanas y las APT chinas. Antonio Villalón, analista y director de seguridad de la empresa valenciana S2 Grupo, explica los motivos por lo que se da esta circunstancia, primero, la calidad de las campañas llevadas por Estado Unidos, las que no permiten su fácil detección; segundo por el monopolio mundial que ejercen las empresas americanas (Microsoft, Apple, Google, Oracle, Cisco…), en lo que se refiere a software de base, sistemas operativos, componentes de comunicación y servicios de internet, lo que le permite no estar preocupado en desarrollar malware, puesto que ya tiene acceso a los drivers.

Ciberseguridad Irán

Un grupo iraní con escaso recorrido, el APT, Rocket Kitten., se lo identifica como el autor de algunas acciones de ciberespionaje, contra los EE. UU, Israel y algunos estados vecinos, como el desarrollo de operaciones al interior del país contra organizaciones y ciudadanos notables contrarios al gobierno.

Ciberseguridad Alemania

Para el año 2017, en Alemania se creó un equipo inicialmente constituido por 260 personas con la intención de abarcar a 13500 integrantes entre civiles y militares para armar el denominado ciberejército. (Segura, 2019, p. 43).

Ha señalado Segura (2019), que la nación alemana creó dos instituciones para contener, repeler o prevenir cualquier tipo de ataque cibernético. La primera es el centro Nacional de Ciberdefensa, el cual se encarga de detectar y analizar las posibles amenazas con el fin de poder coordinar las estrategias necesarias para resolver dichas amenazas. La segunda es el Consejo Nacional de Ciberseguridad, la cual está controlada por la oficina federal para la seguridad de la información que a su vez laboran con otras oficinas federales. Desde estas oficinas se intenta prevenir los posibles ataques cibernéticos ya que en Alemania es un país con mucha incidencia tecnológica en su cotidianeidad, pues, en este país se "controla y manejan desde sistemas computacionales el abastecimiento de agua, electricidad, energía nuclear, así como también el sistema bancario y de transporte ferroviario" (p. 43).

Con la creación de este ciberejército, Alemania adquiere estrategias de ciberseguridad concretas, en donde establece de manera específica los entes que se encargarán de cumplir con las funciones y acciones determinadas para garantizar la

ciberseguridad, lo cual esto se convierte en unos de los puntos más fuerte de ciberseguridad en Alemania.

A continuación, en el siguiente fragmento se puede conocer la noción que sigue y mantiene Alemania con respecto a la aplicación de ciberseguridad:

> La ciberseguridad debe basarse en un enfoque integral. Esto requiere intercambio de información y coordinación más intensivos. La estrategia de ciberseguridad se centra principalmente en los enfoques y medidas civiles. Se complementan con medidas tomadas por la Bundeswehrp para proteger sus capacidades y medidas basadas sobre los mandatos para hacer de la seguridad cibernética una parte de la seguridad preventiva de la estrategia alemana. Dada la naturaleza global de la tecnología de la información y las comunicaciones, coordinación internacional y redes apropiadas centradas en el extranjero y la seguridad los aspectos de política son indispensables. (European Union Agency for Network and Information Security [UNISA], 2011, p. 3)

Ciberseguridad España

El gobierno español mantiene una clara política de ciberseguridad planteada en base a objetivos. Para garantizar la ciberseguridad a sus ciudadanos el estado español ha creado varias oficinas especializadas en ciberseguridad y cada una de estas cumple con determinados objetivos, esto implica que dentro de España se maneja una ordenada política y línea de acción para proteger el ciberespacio.

Segura (2019), indica que los objetivos que persigue el estado español son los siguientes:

Objetivo 1: “Para las Administraciones Públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el adecuado nivel de seguridad y resiliencia”.

Objetivo 2: “Para las empresas y las infraestructuras críticas, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular”.

Objetivo 3: “En el ámbito judicial y policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio”.

Objetivo 4: “En materia de sensibilización, concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio”.

Objetivo 5: “En capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad”.

Objetivo 6: “En lo que se refiere a la colaboración internacional, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales”.

Además, de acuerdo con Segura (2019), el gobierno español pone en ejecución las siguientes líneas de acción para alcanzar sus objetivos:

Primero, la capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas. Segundo, Seguridad de los Sistemas de Información y

> Telecomunicaciones que soportan las Administraciones Públicas. Tercero, seguridad en los sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas. Cuarto, Capacidad de investigación y persecución del ciberterrorismo y la ciberdelicnuencia. Quinto, seguridad y resiliencia de las TIC en el sector privado. Sexto, Conocimientos, competencias e I+D+i. Séptimo, la cultura de ciberseguridad. Octavo, el compromiso internacional. (p. 45)

Por lo tanto, como lo vemos en el caso alemán y español, hoy en día no basta que las fuerzas armadas se encarguen de construir las estrategias en ciberseguridad, "sino que se involucran inclusive los actores privados para poder tener una política estatal más acorde a las amenazas que representa el inadecuado manejo del ciberespacio y el desconocimiento de los potenciales riesgos y vulnerabilidades" (Segura, 2019, p. 46).

Estrategias de ciberdefensa en américa del sur

Ciberseguridad en Colombia

El organismo que se encarga de la ciberseguridad y ciberdefensa en Colombia es el Ministerios de Defensa Nacional, por otro lado, desde el 2009 se crea el ColCERT (Equipo de Respuesta a Emergencias Informáticas de Colombia) mismo que tiene como función "coordinar las acciones necesarias para la protección de la infraestructura critica del Estado colombiano" haciendo frente a emergencias cibernéticas que comprometan a la Seguridad y Defensa Nacional (Caceres, 2017).

Para salvaguardar la seguridad se requiere en primera instancia del fortalecimiento jurídico e institucional, mismo que se trata de la adopción y adaptación del sistema del legislativo y judicial para la ciberseguridad, además propone que los

asuntos internacionales deben ser de vital importancia para los intereses colombianos, observando los casos internacionales y las tendencias que se marcan en el ámbito de la ciberseguridad y ciberdefensa en cuanto a medidas preventivas que minimicen el riesgo de ataques cibernéticos, así como los acuerdos que pueda asumir el estado sea este bilateral o multilateral (Vargas V. , 2014) .

También se estudia las medidas contra el delito cibernético, se refiere a las capacidades de defensa que se pueden brindar por medio del ColCERT, demás se hace énfasis del trabajo mancomunado con las entidades privadas para la obtención de financiación y poder evolucionar el fortalecimiento de esta entidad. Actualmente esta entidad desde su página web www.cplcert.gov.co, brinda información en foros mundiales sobre seguridad informática, de igual manera asesora sobre actualizaciones de seguridad para sistemas operativos y así reducir la vulnerabilidad de los ordenadores (Vargas, 2014).

EL gobierno colombiano en el año 2011, crea el CONPES 3701(Consejo Nacional de Política Economía Social), organismo máximo de coordinación de la política económica, esta no dicta decretos solo da orientación de una política macro, sobre el tema de Ciberseguridad y Ciberdefensa, este organismo está dirigido por el primer mandatario y la secretaria técnica la ejerce el jefe de Departamento Nacional de Planeación misma que elabora la documentación a tratar en cada sesión (Caceres, 2017).

Este organismo nació el 14 de julio del 2011, la misma trata de “Lineamientos de Política para Ciberseguridad y Ciberdefensa” en Colombia, cuyo objetivo es crear lineamientos de política en ciberseguridad y ciberdefensa para el desarrollo de una estrategia nacional para contrarrestar el crecimiento de amenazas informáticas que afecten profundamente al país (Caceres, 2017).

La información es un bien necesario para las organizaciones y países ya que influyen de manera social y económica debido al intercambio internacional y local de la información por medio del ciberespacio que es la forma más rápida de comunicación social, por esta razón, la dependencia al ciberespacio nos fuerza a integrar todos los medios para aumentar la capacidad del desarrollo de herramientas y técnicas que beneficien a la ciberseguridad.

Cada país ha integrado las ENCS (Estrategias nacionales de ciberseguridad) que se la puede definir como "el marco de referencia de un modelo integrado basado en la implicación, coordinación y armonización de todos los actores y recursos del Estado, en la colaboración público-privada, y en la participación de la ciudadanía." (Carlini, 2016).

De la misma forma, según la OECD nos resalta que los objetivos de la ENCS son "aumentar la coordinación gubernamental al nivel de políticas y operaciones, así como clarificar los roles y responsabilidades de cada institución" (OECD, 2012). Como podemos observar, ambas definiciones destacan la importancia de la participación estatal, privada y de la sociedad civil ya que la cooperación y la coordinación son esenciales en una gestión efectiva de ciberseguridad.

Ciberseguridad en Brasil y Chile

En los últimos años los países latinoamericanos como Chile y Brasil han desarrollado políticas para combatir esta amenaza moderna, en Brasil en el año 2015 se publicó la estrategia nacional de seguridad de las comunicaciones de información y seguridad cibernética de la administración pública federal 2015 – 2018 donde se plantea principios que guiaran las acciones con respecto a la ciberseguridad a nivel nacional.

Para eso se estableció la gobernanza en los sistemas ciberseguridad para contribuir con las reglas de la Policía Nacional de la Seguridad Informática y Comunicación de Seguridad Cibernética. También se considera la alianza de los sectores públicos, privados, nacionales e internacionales para el apoyo de los temas cibernéticos y la retroalimentación tecnológica (Carlini, 2016). Finalmente, se le da importancia de resiliencia que contribuye en la suma de infraestructuras destinadas a la seguridad cibernética (Carlini, 2016).

En Chile, en los años 2014 al 2018 se necesitó la implementación de una Política Nacional de Ciberseguridad (PNCS) la cual protegerá a todos los usuarios de posibles amenazas en contra de su privacidad. A causa de esto, en 2015 se creó el Comité Interministerial sobre ciberseguridad que se encargaba de instruir al presidente de la República en todo lo referente a la seguridad cibernética, así mismo, presenta una política nacional que identifica amenazas en el ciberespacio y además coordina planes y acciones de distintos participantes (Alvarez, 2017).

En 2017 la PNCS otorgó la seguridad de las personas en el ciberespacio a partir de un nivel de seguridad que permita la ejecución de actividades de manera normal y de esa forma protege el país desde los habitantes. Finalmente busca la colaboración y alianzas entre organizaciones, instituciones gubernamentales y organismos privamos así también la cooperación internacional de países y organismos para el control y análisis de las ciberamenazas (Alvarez, 2017).

Por lo anterior, los objetivos de la PNCS se dividen en 2 agencias, la primera llamada Agencia de medidas 2017 – 2018 y la otra de largo plazo que se extiende hasta 2022 que constara de 5 objetivos:

- La obtención de una infraestructura de información preparada

- El cuidado de los derechos de las personas dentro del ciberespacio
- Educar y enseñar buenas prácticas en el manejo de las tecnologías digitales
- Relacionarse con otros actores y participantes políticos
- Promover el desarrollo de una industria de ciberseguridad que ayude a los objetivos estratégicos.

En ambos países, dentro de su ENCS incorporan la seguridad del gobierno, en el caso de Brasil, cuenta con la Agencia Brasileña de Inteligencia, que se encarga de brindar a los integrantes del gobierno la información estratégica para la toma de decisiones, de igual manera tienen el Centro de Investigación y Desarrollo para la Seguridad de las Comunicaciones que brindara herramientas de emisión segura de la información para el Gobierno Federal.

Por otra parte, Chile dentro del Decreto Supremo N°1 del año 2015, estableció normas para los sitios webs y servidores de la Administración del Estado que estuvieron vigentes desde 2018 por el INN (Instituto de Normalización) (Alvarez D. , 2018).

Cada país cuenta con su estrategia de protección de infraestructura crítica que tiene un equipo que lidia con la ciberamenaza enlazados a los órganos de seguridad principal del estado. En el caso de Brasil, cuenta con el CTIR Gov (Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo) integrado por la policía federal, gendarmería Nacional, la Policía de Seguridad Aeroportuaria y la Prefectura Naval que tiene como objetivo la cooperación en conjunto para dar respuesta inmediata al manejo de incidentes de seguridad computacional en órganos gubernamentales (Ministerio del interior y seguridad pública, 2018).

De igual manera aconsejara al Departamento de Seguridad de la Información del Gabinete de la Seguridad Institucional de la Presidencia de la República para la creación de normas metodológicas para la solución de este asunto (CTIR, 2019).

Por el contrario, Chile solo cuenta con el Ministerio del Interior y Seguridad Pública que manejan un equipo de respuesta ante problemas de seguridad informática dentro del estado, ya que tienen como prioridad responder las ciberamenazas que altera la infraestructura de información crítica (Ministerio del interior y seguridad pública, 2018).

Chile también cuenta con un centro de investigación de crimen cibernético de la policía de investigación junto con el OS-9 de carabineros de Chile, el indicador de resiliencia es clave para ver resultados de la ciberseguridad de un país como Brasil, que tiene como objetivo el seguimiento sistemático de daños de infraestructuras para tener en mano las respuestas de cada problema sin alterar de as las estructuras, por su parte, Chile cuenta con la Ley 20.478 que habla de un plan de respaldo y recuperación de las infraestructuras en incidentes a partir de las resoluciones de la Subsecretaria de Telecomunicaciones (Alvarez V. , 2017).

En este caso, Chile trabaja con un marco de identidad digital el cual trata de la identidad en línea que permite libre navegación a documentos personales y servicios del gobierno por medio de cualquier dispositivo, el servicio es por medio del programa de Gobierno Digital que mediante a una “Clave única” da acceso a servicios públicos vía web. Aparte del programa de identidad única (Ministerio de la secretaria general de la presidencia, 2019).

Con respecto a los derechos de los ciudadanos, Chile plantea que sus medidas ya propuestas de ejecución y diseño, tiene un enfoque de respeto a los derechos para los

ciudadanos en el ciberespacio igualando los derechos de manera física. El Ministerio de Justicia y Derechos Humanos es el encargado de inspeccionar los cumplimientos de la legislación en el entorno tecnológico. Analizando las relaciones y la cooperación tanto internacional, gubernamental y cooperación pública-privada, es necesario para que un país tenga conocimiento de la seguridad cibernética y logre cumplir los objetivos de las ENCS (Ministerio de la secretaria general de la presidencia, 2019).

El ciberespacio y la comunicación social rompen fronteras exponiendo a los usuarios a las ciberamenazas. Chile en el año 2017 ratificó el Convenio de Budapest, elaborado por el Consejo de Europa que tiene el objetivo de unir los estados respecto a delitos informáticos. Chile también estableció dos acuerdos con España e Israel en el 2018 para el intercambio de sus prácticas en estrategias nacionales de seguridad cibernética y los beneficios de conocimiento en tecnología de la quinta generación (5G) por parte de Israel (Herrera, 2020).

En cuanto a Brasil, estableció acuerdo con España en el 2015 y con Suecia en el 2018 con el fin de resguardar su infraestructura de información crítica y así enfrentar con mayor conocimiento los ciberataques de grandes potencias (Amaral, 2014).

Dentro de las relaciones gubernamentales, para un enfoque interinstitucional, los dos países establecen una coordinación entre organismos gubernamentales como en Brasil con el ya mencionado CTIR Gov, de igual manera Chile con el CSIRT que se encarga de la colaboración de los órganos del estado para la eficiencia y orientación para las tomas de decisiones (CTIR, 2019).

Ciberseguridad en Argentina

En la República Argentina la ciberdefensa es parte de la institucionalidad, cuenta con un sistema de defensa en caso de agresiones. El estado argentino en materia

de defensa funda su reconocimiento basado en la cooperación interestatal y dimensión multilateral como instrumentos complementarios de la política de defensa propia (Caceres, 2017).

El estado argentino en su sistema de defensa tiene a cargo la protección del mismo en relación a ataques que afecten la soberanía, su "independencia e integridad territorial", por lo que este sistema exige que los elementos afectados sean de origen externo y que el agresor sea un actor estatal. Las organizaciones que se destacan en el cuidado de la seguridad estatal son: El ministerio de defensa, Jefatura de Gabinete de ministros, otras normas vinculadas a la regulación de internet (Cornaglia & Vercelli, 2017).

a) Comité de Seguridad de la Información

Mediante resolución del Ministerio de Defensa N°364, del 12 de abril del 2006, se crea el comité de seguridad de la información del ministerio de defensa, mismo que integro competencias en "política, planes y programas, presupuesto, tecnología, asuntos jurídicos, recursos humanos, administración y despacho" (Cornaglia & Vercelli, 2017).

b) Ciberespacio para el sistema de defensa nacional

La secretaria de Estrategia y Asuntos militares de los ministerios de defensa en el año 2010, crea un grupo de análisis desde el punto de vista técnico y normativo cuales son las implicaciones del ciberespacio con la expansión de las redes informáticas en el mundo para determinar una estrategia doctrinaria y normativa en materia de defensa nacional (Cornaglia & Vercelli, 2017).

c) Unidad de coordinación y ciberdefensa

Esta unidad fue creada por la existencia de las Fuerzas Armadas del proceso de generación de capacidades y unidades especializadas para emergencias teleinformáticas, el estado en concepto de ciberdefensa requiere la participación de los miembros del sistema de defensa e innovación tecnológica del país como: levantamiento exhaustivo de infraestructuras, redes, recursos humanos, procesos y actividades relativas, el diseño y planificación estratégica e implementación de políticas, impulsar el desarrollo doctrinario, analizar cómo ha evolucionado la normativa (Cornaglia & Vercelli, 2017).

d) Comando Conjunto Ciberdefensa

Las operaciones militares según decreto son conducidas por el Estado mayor conjunto de las Fuerzas Armadas a través del comando operacional quien tiene la capacidad para conjugar y repeler ciberataques contra infraestructuras críticas de la información y activos del sistema de Defensa Nacional y su Instrumento Militar. Argentina adoptado un modelo de defensa de carácter defensivo mismo que esta conducido por el Comando está a cargo del oficial superior y conducción de ciberdefensa.

e) Actualización de Directiva de Política Defensa Nacional

Aunque los ciberataques tienen un origen virtual afectan al espacio físico y a diversas infraestructuras críticas como: agua potable, medios de comunicación o sistemas bancarios; por ende, se plantea necesidad del desarrollo operaciones de dimensión ciberespacial a desenvolverse en ambientes terrestres, naval y aéreo, así como incremento de ciberseguridad en redes del sistema de defensa nacional.

Operación "Machete" en América Latina

El grupo especializado de cibersoldados detrás de la campaña de ciberespionaje MACHETE, que fue reconocido inicialmente en el 2014, continúa teniendo como objetivos entidades e instituciones de países latinoamericanos. La campaña MACHETE fue descubierta inicialmente por investigadores de Kaspersky en agosto del 2014 y según sus estudios, indican que estuvo llevándose a cabo por lo menos desde el año 2010.

La infección se realizaba en ese entonces a través de archivos java que se cargaban durante la navegación por internet, atacando el navegador y vulnerabilidades de sistema operativo, con el objetivo de lograr control en la máquina víctima.

Por su parte, los ciberespías orientaron sus campañas a servicios de inteligencia, embajadas, instituciones gubernamentales y militares. La mayoría de sus víctimas se encuentran en países latinoamericanos y de habla hispana como: Ecuador, Colombia, Perú, Venezuela, Argentina, Cuba y España. Se han encontrado casos con menores incidencias en: República Dominicana, Bolivia, Guatemala, Nicaragua y México.

En la actualidad estas mismas campañas han evolucionado en técnicas, utilizando phishing especializado y focalizado para objetivos específicos y blogs o webs de distintas temáticas que ejecutan el software malicioso infectando el sistema (enHacke, 2017).

La mayoría de los cerca de 780 objetivos están en Venezuela (42%), Ecuador (36%) y Colombia (11%) – pero hay otros países afectados, entre ellos Rusia, Perú, Cuba y España. El objetivo de los espías es secuestrar información confidencial, como documentos militares y diplomáticos de las organizaciones comprometidas – hasta

ahora los hackers consiguieron gigabytes de datos confidenciales, “tal vez incluso más”, dice Dmitry Bestuzhev, director del Centro de Investigación y Análisis Global del Team de Kaspersky Lab en América Latina. El experto comenzó a investigar la operación para examinar un archivo sospechoso en el cuaderno de un general, a petición de uno de los países afectados. (Eset Research, 2019)

Señala Rodríguez (2014), “A pesar de la simplicidad de las herramientas utilizadas en esta campaña, fueron muy eficaces, dados los resultados. Parece que los autores de las amenazas en América Latina están adoptando técnicas de campañas similares a nivel mundial”, agregó. “Nuestro pronóstico es que el nivel tecnológico de las operaciones de espionaje cibernético locales va a aumentar mucho. Así que probablemente haya un nuevo tipo de campañas muy similares, desde el punto de vista técnico, a las que se hacen a nivel mundial” (Rodríguez, 2014)

Se ha señalado en enHacke (2017), que el código malicioso encontrado dentro de las computadoras analizadas es capaz de proveer a una central de control las siguientes características y acciones sobre el sistema comprometido:

- Registro de tipeo o de escritura: Todo lo que el usuario escribe, incluyendo CONTRASEÑAS y texto altamente SENSIBLE es registrado y enviado a la central de procesamiento de datos
- Captura de audio: El malware da acceso al micrófono de modo que se puede escuchar en forma remota todo lo que sucede alrededor de la computadora infectada
- Información de geolocalización: El malware intenta recabar información en el sistema para tratar de definir la ubicación donde se encuentra la computadora
- Pantallazos: En cualquier momento la central puede pedir pantallazos de las máquinas victimas

- Captura de video/fotos de webcam: Videos o fotos capturadas a través de la webcam de la computadora
- Exfiltración de documentos: Obtener información sensible o definida como importante en forma remota y transparente de la máquina victima
- Infiltración de documentos: Envenenamiento de la información o incluso incriminación de algún delito o falta para alguna institución.

Según análisis realizados por la firma antivirus, en esta campaña de ciberespionaje, aproximadamente ya ha sido extraído cerca de 100GB de información de las victimas analizadas (enHacke, 2017).

La mejor protección contra campaña de ciberespionaje tales como Machete es aprender cómo el spear phishing y otros ataques funcionan y no caer en sus trampas, así como contar con una solución de seguridad funcional y actualizada.

El Machete muestra que hay muchos jugadores regionales en el mundo de los ataques selectivos y que tales ataques se han vuelto parte del arsenal de ciberataques de muchos delincuentes y países en todo el mundo. “Podemos estar seguros que existen ataques selectivos paralelos en América Latina y otras regiones”, concluye Kaspersky Lab. (Carrasco, 2014).

CAPITULO IV. ANÁLISIS DE LAS POLÍTICAS DE CIBERSEGURIDAD EN ECUADOR

En la actualidad, el ciberespacio ha convocado la necesidad de crear diferentes estrategias de ciberdefensa y ciberseguridad, incluyendo los fenómenos que actúan en el advenimiento de la información digital, en el escenario cotidiano se desarrollan diferentes actividades del mundo global, y en estas se visualiza de manera continua la intervención tanto de las computadoras como del internet, por esto que, su estudio en materia político-estratégica es fundamental a la hora de pensar en la defensa de las naciones.

En el caso del Ecuador, el estudio de la defensa cibernética tiene una dimensión poco pragmática, el estado propone la configuración de un modelo local de gobernanza en ciberdefensa en el ciberespacio inscrito en la normativa vigente. Esta norma ha sido planteada desde el ámbito político dentro de los sectores estratégicos del estado ecuatoriano.

El Gobierno del Ecuador, ha planificado un sistema de protección en beneficio de la defensa del ciberespacio en favor de los sectores estratégicos más relevantes del estado, defendiendo el concepto de la defensa de la infraestructura digital ante las amenazas de origen antrópico y natural con el fin de precautelar y garantizar el desarrollo de las actividades esenciales de la sociedad relacionadas con las TIC.

Con el propósito de mantener una visión holística la política de seguridad cibernética se sustenta en un proceso de origen técnico mediante la dirección de diferentes instituciones estatales ligadas a la seguridad, bienestar y tecnología como el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), el Ministerio de Gobierno (MDG), el Ministerio de Defensa (MDN), el Centro de

Inteligencia Estratégica (CIES) y el Ministerio de Relaciones Exteriores y Movilidad Humana (MREMH), estos actores conforman la mesa de defensa para la elaboración de los lineamientos de la ciberseguridad ecuatoriana.

Esta mesa fue creada y dirigida por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). La disposición del Gabinete sectorial de Seguridad tras la resolución N° GSS-509 encarga al MINTEL, la batuta para la elaboración de la Política Nacional de Ciberseguridad.

No obstante, al considerar la amplitud del tema de seguridad, el Ministerio de Telecomunicaciones tras el Memorando Nro. MINTEL-SGERC-2021-0134-M, establece un ‘‘Grupo Interinstitucional de Ciberseguridad’’ (mesa de defensa) con el propósito de crear políticas desde los enfoques visionarios de cada sector estratégico (MINTEL, MDG, MDN, CIES, MREMH) de manera que se pueda fortalecer y asegurar el entorno digital en el Ecuador.

Las políticas de este plan buscan cubrir las temáticas descritas a continuación:

1. Promover una cultura e instaurar conocimientos sobre la ciberseguridad en la sociedad.
2. Instituir marcos: normativos y legales para una ciberseguridad responsable en la sociedad.
3. Diseñar estrategias y políticas para la seguridad del ciberespacio mediante un marco legal y regulatorio que controle los riesgos tanto tecnológicos y organizacionales como de la infraestructura crítica.
4. Fomentar el conocimiento de la ciberseguridad para controlar los posibles riesgos a través de organizaciones, estándares y tecnologías.

5. Mejorar la resiliencia de la ciberseguridad a través de marcos legales y reglamentarios para la respuesta a incidentes, gestión de crisis, redundancia y protección de la infraestructura crítica.
6. Diseñar políticas de ciberseguridad para controlar los posibles riesgos a través de organizaciones, estándares y tecnologías.

La política de seguridad establecida por la mesa de defensa de la ciberseguridad, se extiende hasta el año 2023, en el que, tras líneas de seguimiento capaces de medir la eficiencia del mismo contemplarán la posibilidad de mantener, mejorar o reestructurar el plan vigente.

No obstante, a la fecha, esta política se sustenta en un marco normativo amparado en las diferentes leyes del Ecuador descritas en: La Constitución de la República del Ecuador; Código Orgánico Integral Penal; Ley Orgánica de Identidad y Datos Civiles; Ley de Seguridad Pública y del Estado; Ley Orgánica de Telecomunicaciones; Ley Orgánica para prevenir y erradicar la violencia contra las mujeres; Código Orgánico de la Economía Social de los conocimientos.

Tabla 2. Constitución de la República del Ecuador, Registro Oficial 449 de 20-oct.-2008

Artículo 3. Son deberes primordiales del estado:	**1.** Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución. **2.** Garantizar y defender la soberanía nacional. **3.** Fortalecer la unidad nacional en la diversidad. **4.** Garantizar la ética laica (…). **5.** Planificar el desarrollo nacional, (…) promover el desarrollo sustentable (…), para acceder al buen vivir. **6.** Promover el desarrollo equitativo (…). **7.** Proteger el patrimonio natural y cultural del país. **8.** Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral (…).

Artículo 16. Todas las personas, en forma individual o colectiva, tienen derecho a:	**1.** Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos (…). **2.** El acceso universal a las tecnologías de información y comunicación. **3.** La creación de medios de comunicación social, y al acceso en igualdad de condiciones (…). **4.** El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial (…). **5.** Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación;
Artículo 66. Se reconoce y garantiza a las personas:	**1.** La protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter (…). **2.** La inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley (...).
Artículo 158. Las Fuerzas Armadas y la Policía Nacional son instituciones de protección de los derechos, libertades y garantías de los ciudadanos. Tienen como misión fundamental la defensa de la soberanía y la integridad territorial:	La protección interna y el mantenimiento del orden público son funciones privativas del Estado y responsabilidad de la Policía Nacional.
Artículo 313.	El Estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficiencia. Los sectores estratégicos, (…) son aquellos que por su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental, (…).
Artículo 393.	El Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas (…).

Elaboración propia.

En la Constitución Ecuatoriana se citan artículos que contemplan el vínculo de la sociedad, la seguridad y la información, bajo la visión de la protección y el cumplimiento de los derechos de los ciudadanos frente a estos elementos.

Tabla 3. Código Orgánico Integral Penal

Artículo 103. Pornografía con utilización de niñas, niños o adolescentes.	La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos (…) será sancionada con pena privativa de libertad de trece a dieciséis años, y en un caso de abuso de veintidós a veintiséis años.
Artículo 104. Comercialización de pornografía con utilización de niñas, niños o adolescentes.	La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, (…) será sancionada con pena privativa de libertad de diez a trece años.
Artículo 178. Violación a la intimidad.	La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, (…) será sancionada con pena privativa de libertad de uno a tres años.
Artículo 190. Apropiación fraudulenta por medios electrónicos.	La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, (…) será sancionada con pena privativa de libertad de uno a tres años.
Artículo 194. Comercialización ilícita de terminales móviles.	La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.
Artículo 229. Revelación ilegal de base de	La persona que, en provecho propio o de un tercero, revele información registrada,

datos.	contenida en ficheros, archivos, bases de datos o medios semejantes, (…), será sancionada con pena privativa de libertad de uno a tres años (…).
Artículo 230. Interceptación ilegal de datos.	Será sancionado con pena privativa de libertad de tres a cinco años (…).
Artículo 231. Transferencia electrónica de activo patrimonial.	La persona que, con ánimo de lucro, altere, manipule (…) será sancionada con pena privativa de libertad de tres a cinco años.
Artículo 232. Ataque a la integridad de sistemas informáticos.	La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, (…) será sancionada con pena privativa de libertad de tres a cinco años (…).
Artículo 233. Delitos contra la información pública reservada legalmente.	La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.
Artículo 234. Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	La persona que sin autorización acceda en todo o en parte a un sistema informático (…) para explotar ilegítimamente el acceso logrado, modificar un portal web, (…) será sancionada con la pena privativa de la libertad de tres a cinco años.
Artículo 472. Información de circulación restringida. No podrá circular libremente la siguiente información:	**1.** Aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la ley. **2.** La información acerca de datos de carácter personal (...). **3.** La información producida por la o el fiscal en el marco de una investigación previa y aquella originada en la orden judicial relacionada con las técnicas especiales de investigación. **4.** La información acerca de niñas, niños y adolescentes (...). **5.** La información calificada por los organismos que conforman el Sistema nacional de inteligencia.

Elaboración propia.

Los artículos descritos en el sistema del Código Orgánico Integral Penal describen los delitos que limitan el cumplimiento de los derechos de los ciudadanos para garantizar la seguridad dentro del plan general y dentro del escenario digital. Estos describen normas jurídicas de carácter punitivo que, bajo el enfoque del sistema penal del Ecuador, establece penas para los delitos a manera de promover la cultura de paz y seguridad para la sociedad del ciberespacio.

El Ecuador también considera una ley para el área de Telecomunicaciones, y de manera específica los artículos que se contemplan en el tema de ciberseguridad son los siguientes (Ley Especial de Telecomunicaciones, 2013):

- Artículo 76.- **Medidas técnicas de seguridad e invulnerabilidad. -** Las y los prestadores de servicios (…) deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red (…).
- Artículo 77.- **Interceptaciones. -** únicamente se podrán realizar interceptaciones cuando exista orden expresa de la o el Juez competente (…).
- Artículo 78.- **Derecho a la intimidad. –** (…) garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal. (…) adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad (…).
- Artículo 79.- **Deber de información. -** en caso de que exista un riesgo (…) el prestador de servicios de telecomunicaciones deberá informar a sus abonados.

- Artículo 80.- **Procedimientos de revelación. -** Los prestadores de servicios implementarán procedimientos internos para atender las solicitudes de acceso a los datos personales de sus abonados (…).

- Artículo 82.- **Uso comercial de datos personales. -** Los prestadores de servicios no podrán usar datos personales, información del uso del servicio (…) a menos que el abonado (…) haya dado su consentimiento previo y expreso.

- Artículo 83.- **Control técnico. -** cuando para la realización de las tareas de control técnico, ya sea para verificar el adecuado uso del espectro radioeléctrico, (…) la Agencia de Regulación y Control de las Telecomunicaciones deberá diseñar y establecer procedimientos que reduzcan al mínimo el riesgo de afectar los contenidos de las comunicaciones.

- Artículo 84.- **Entrega de información. -** Los prestadores de servicios, entregarán a las autoridades competentes la información que les sea requerida dentro del debido proceso (…).

- Artículo 140.- **Rectoría del sector. -** El Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones y de la sociedad de la información, informática, tecnologías de la información y las comunicaciones y de la seguridad de la información.

Por lo anteriormente citado se puede destacar que, dentro del tema de la gobernabilidad informática, al menos, en el caso ecuatoriano, la visión no tiene un enfoque digital sino estandarizado, es decir, incluye una visión general de la seguridad

con un enfoque social y económico, por lo que se puede concluir que no tiene un plan de acción que combine las estrategias de protección en una infraestructura de hardware y software.

El Ecuador, hoy en día, solamente cuenta con lineamientos legales que únicamente combaten las amenazas a la seguridad nacional, pero no se centran en trabajar por la seguridad en el ciberespacio y mucho menos prevenir estas amenazas en el contexto digital, por lo que es importante considerar un estudio aplicativo en la política vigente para poder contrastar la seguridad que existe en la actualidad en el escenario digital, de manera que pueda implementarse uno nuevo, que pueda seguir una tendencia capaz de adaptarse a las transformaciones que el internet y las redes tienen actualmente.

Asimismo, sería importante que desde la ciberseguridad del Ecuador se pueda analizar la eficiencia del marco normativo y legal debido a que si bien considera aspectos generales en cuanto a los delitos cibernéticos, no contempla los nuevos delitos cibernéticos que han aparecido hasta la fecha en el contexto internacional de manera que al contemplar un mejoramiento de esta estructura bajo un enfoque no solo holístico sino determinante para así alcanzar la anhelada gobernabilidad dela ciberseguridad no solo en el contexto nacional sino en el contexto internacional.

Dentro de los objetivos que enmarca este plan estratégico para la seguridad cibernética se establece como objetivo general:

> ‘‘Construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio, encaminando acciones para

garantizar un ciberespacio seguro'' (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

Se puede concluir, que el objetivo tiene una visión relacionada con el desarrollo economico, humano y social del Ecuador a través de una confianza digital que permita el intercambio de información, compra y venta de bienes y servicios en las diferentes plataformas virtuales a través de mecanismos de regulación que garanticen el escenario seguro para todos los sectores estrategicos de la sociedad.

Por otro lado, este planteamiento deduce un esquema de objetivos específicos a trabajar para alcanzar el escenario seguro en el espacio digital, estos son:

1. Promover la cooperación entre el sector público y privado a nivel nacional fomentando la confianza y generando respuestas comunes a los riesgos y amenazas del ciberespacio.
2. Potenciar las capacidades de detección, previsión, prevención y gestión de los incidentes cibernéticos, al igual que el manejo de crisis de ciberseguridad de manera oportuna, efectiva, eficiente y coordinada.
3. Proteger la infraestructura crítica digital del Estado ante amenazas y riesgos en el ciberespacio para garantizar su adecuado funcionamiento y la entrega de servicios esenciales.
4. Resguardar la seguridad pública y ciudadana en el ciberespacio, previniendo y contribuyendo a la investigación de delitos cibernéticos, para el normal desarrollo de las actividades públicas y privadas, y el ejercicio de los derechos fundamentales de la ciudadanía, en un entorno de confianza.

5. Potenciar la diplomacia ecuatoriana en el ámbito de la ciberseguridad por medio de los espacios de cooperación a nivel regional e internacional, en línea con el interés nacional y la política exterior del Ecuador.
6. Generar una cultura de ciberseguridad y promover el uso responsable del ciberespacio en el Ecuador (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

El planteamiento y cumplimiento de estos objetivos buscan construir la capacidad sustentable para el ejercicio del derecho de los ecuatorianos, se sustenta bajo el marco inicial del objetivo general con el propósito de hacer sostenible la seguridad en el ciberespacio a mediano y largo plazo.

No obstante, es importante considerar que este planteamiento de objetivos si bien intenta favorecer seguridad en el intercambio de información no avala la posibilidad de medición del cumplimiento de los mismos, sino que delega encargados (Ministerios) para velar por el relativo cumplimiento de estos mediante la supervisión básica de los procesos informáticos,

De manera que, durante la vigencia de esta política, anteriormente indicada, no se han hecho los ajustes correspondientes bajo la visión holística que se plasmó inicialmente, sino que, de manera interna, cada encargado ha trabajado bajo perspectiva de visión sobre la seguridad informática con un alcance nacional alineado a la normativa ecuatoriana y no bajo un modelo de ciberseguridad de alcance global.

Sumado a estos objetivos anteriormente indicados, el Ministerio de Telecomunicaciones y de la Sociedad de la Información plantea siete pilares que bajo la visión de la seguridad ecuatoriana, garantizarán la seguridad en el ciberespacio, estos

tendrán seguimiento mediante instituciones responsables encargadas de dar cumplimiento a los objetivos planteados.

Figura 2. Pilares de la Ciberseguridad en el Ecuador

Elaboración propia, adaptado de (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

Al hablar de la gobernanza de la ciberseguridad en el Ecuador, los precursores de la seguridad digital buscan integrar a la sociedad con la evolución de las nuevas tecnologías además de sus actividades e infraestructuras críticas por lo que su alcance debe trabajar en un modelo con un alcance de intervención, gestión y evaluación de todos los sistemas de información utilizados por la sociedad ecuatoriana.

Actualmente, se puede decir que el tema de Gobernanza de Internet tiene un déficit considerable, debido que, según la Superintendencia de Telecomunicaciones ‘la participación ecuatoriana en los espacios de Gobernanza de Internet tiene el mismo

matiz que la gran mayoría de participaciones de países subdesarrollados o en vías de desarrollo" (SUPERTEL, 2013).

Por lo tanto, se puede decir que el tema digital en el Ecuador no tiene un reconocimiento considerable en el contexto de la gobernabilidad digital, no obstante, se destaca el interés de los sectores estratégicos por alcanzar la trascendencia de la gestión nacional de internet, alcanzando la presencia en el contexto nacional e internacional para contribuir de esta manera con el desarrollo tecnológico del país.

Para poder debatir la eficiencia de la gobernanza en el tema de la ciberseguridad, el análisis no se enfoca en un modelo de cobertura digital como lo hacen los países que han alcanzado una gobernanza optima, sino que en el caso de Ecuador es necesario considerar las bases en las que se cimientan los lineamientos generales de la seguridad digital, tales como la constitución de la República del Ecuador, el Código Orgánico Integral Penal y la Ley Orgánica de Telecomunicaciones.

Los sistemas de Información y gestión de incidentes, buscan en primera instancia proteger los sistemas de datos que facultan el procesamiento de otros para las actividades desarrolladas en los sistemas empresariales y de la ciudadanía en general, es importante trabajar este aspecto ya que este pilar permite trabajar de manera oportuna y directa en aspectos relacionados con la integridad confidencialidad, bases de datos, calidad de servicios, etc., bajo la visión de la política de ciberseguridad los incidentes del escenario digital son los que se exponen en la siguiente tabla.

Tabla 4. Clasificación de Incidentes de Seguridad de la Información y Ciberseguridad

Clasificación	Tipo de incidente
Faltas a la política de seguridad de la información	Incumplimiento a la Norma para la Administración de Seguridad de la Información
Acceso no autorizado a datos	Cuentas de usuario o credenciales vulneradas. Acceso o intrusión física no autorizada a datos Intrusión física Alteración o destrucción no autorizada de información
Contenido malicioso	Spam Ciberacoso Difamatorio o discriminatorio Contenido sexual o violento inadecuado
Contenido dañino	Sistema, aplicación o componente de la infraestructura tecnológica infectado. Modificación, instalación o eliminación no autorizada de software Sabotaje Interrupciones en la disponibilidad del servicio
Filtración de datos	Robo de datos Pérdida de datos Divulgación de datos Mal uso de datos Revelación de información Falla del sistema o aplicación
Falla de componentes tecnológicos	Falla en la red Criptografía débil Sistema o aplicativo vulnerable
Fraude	Uso no autorizado de recursos Derechos de autor Suplantación Phishing
Ciberataque	Compromiso de cuenta con privilegios DoS (Denegación de servicio) DDoS (Denegación distribuida de servicio) Ransomware Malware Caballo de Troya

	Rootkits
	Spear phishing
	Spyware
	Virus
	Gusanos
	Armouring
	Ingeniería Social
	Explotación de vulnerabilidades conocidas
	Explotación de Vulnerabilidades de software
	APT (amenaza persistente avanzada)
	Ciberterrorismo
	Ataque desconocido

Elaboración propia, adaptado de: (Banco Central del Ecuador, 2019).

Los incidentes se catalogan de manera eficiente dentro del contexto internacional, no obstante, bajo la ciberseguridad establecidos por la línea de seguridad del ciberespacio no existe un marco normativo y legal a la hora de contrarrestar estos incidentes en el ciberespacio, sino, solamente los que se citaron previamente en este análisis.

Los incidentes de la tabla N° 1, son analizados y estudiados única y exclusivamente dentro del contexto gubernamental pero no se analizan y trabajan bajo un perfil de la coyuntura de la seguridad nacional ni mucho menos de la seguridad cibernética.

Por lo tanto, si bien se reconoce el delito como tal no tiene un enfoque penal de manera estandarizada para poder contrarrestarlo, de esta manera, se puede concluir que el pilar que estudia los sistemas de información y la gestión de incidentes es un eje positivo a la hora de estudiar la seguridad en el espacio digital, pero estudiarla nunca será suficiente, lo fundamental.

En este sentido, se debe construir una herramienta y un ente que permita combatir y denunciar en todos los escenarios digitales las amenazas presentes a través de

seguimientos, penalizaciones, capacitaciones, etc., y generando a la vez el conocimiento en la ciudadanía sobre la gestión oportuna para la seguridad ante los diferentes ataques.

Tabla 5. Actores, pilares y objetivos de la política de Ciberseguridad en el Ecuador

PILAR	OBJETIVO	INSTITUCIÓN 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. IV. Soberanía y defensa.	OBJETIVO 3	Ministerio de Defensa Nacional (MDN)
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: (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

Para el Ecuador, es primordial manejar un modelo de gobernanza materializado en ciberseguridad y ciberdefensa, sin que este sea tratado únicamente bajo la política de la seguridad, sino bajo una participación holística, teórica y pragmática para así poder abordar cada una de las amenazas informáticas ya que a la fecha el modelo de ciberseguridad ofrecido por los gobiernos de la última década ha diseñado estructuras

aun incipientes ligadas a un modelo de gobierno bajo la línea de un plan de trabajo limitado y no bajo un modelo real de ciberseguridad.

De esta manera, es oportuno resaltar que la defensa también comprende medidas militares encargadas de vigilar y atacar las amenazas además de prevenir los peligros para todos los segmentos de la sociedad mediante estrategias de protección, conservación y una eficiente capacidad de respuesta frente a estos sucesos.

Entonces, se observa que en el Ecuador se aborda la ciberseguridad desde el ámbito político principalmente. Esto no es suficiente para hacer frente a los ciberataques contemporáneos que amenazan la seguridad en el ciberespacio. Pues, en el Ecuador la ciberseguridad es muy difusa debido a que no existe una articulación adecuada entre los entes encargados, sus funciones y las rutas de acción a seguir para alcanzar los objetivos planteados en los planes de gobierno.

Ahora bien, los entes encargados de la ciberseguridad tienen claro, en cierta medida, los objetivos planteados para alcanzar la ciberseguridad. Sin embargo, no existen lineamientos o rutas de acción a seguir para hacer frente a un ciberataque, además, estas rutas deberían ser creadas con base científica al menos en relación a modelos de ciberseguridad que ya han demostrado su eficacia en otros países que destacan en el tema de ciberseguridad.

Trabajar en cada uno de los ejes de la seguridad del ciberespacio no solo garantizan la estabilidad del sector digital, sino que en otra instancia describe una estructura social y política competente en el escenario internacional ya que el desarrollo estatal está ligado con la condición de seguridad que ofrece un país además de su capacidad de defensa frente a las diferentes amenazas que el ser humano hace, aun, en el escenario de las TIC’s, por lo que de esta manera se puede justificar que la necesidad

de crear garantías de seguridad no deben tener estándares generales como en el caso ecuatoriano sino más concretos para atacar las amenazas e incrementar el tema de seguridad y defensa digital.

En el Ecuador es necesario contar con una ley que establezca 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.

El Estado debe defender y proteger la soberanía, seguridad integral, las infraestructuras críticos públicas y privadas, la integridad política, la seguridad económica y la seguridad nacional; así́ también, salvaguardar los sistemas de información digital de los organismos estratégicos, operacionales y tácticos ante ataques, riesgos o amenazas en el ciberespacio.

Se debe aprobar una ley que establezca 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.

El asambleísta Rodrigo Fajardo, presentó el proyecto de Ley, para pedir al Presidente de la República, que se hagan los esfuerzos necesarios para ratificar el

Convenio de Budapest, que es el único en materia de ciberseguridad a nivel internacional", este proyecto crea un subsistema de ciberseguridad, el mismo que estará conformado por los Ministerios de Gobierno y de Telecomunicaciones, así como por la Policía Nacional. También prevé la figura de agentes encubiertos en la red, para investigar, prevenir y mitigar incidentes que afecten la seguridad informática. (Asamble Nacional, 2021)

Con la expedición de Ley Orgánica de Seguridad Digital, Ciberseguridad, Ciberdefensa y Ciberinteligencia por parte de la Asamblea Nacional, se contaría una ley 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 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.

CONCLUSIONES

La ciberseguridad toma gran importancia en esta era digitalizada, dentro de una sociedad que ha dado un salto importante al ciberespacio. Este último es un escenario nuevo que puede ser sujeto de ciberataques, es decir, el crimen cotidiano que lo veíamos con normalidad en nuestro mundo real, ha traspaso a un nuevo mundo de tipo virtual. En este contexto, los organismos internacionales orientan sus esfuerzos por plantear nuevas estrategias para hacer frente a estos nuevos crímenes, pues toman como punto de partida la defensa y seguridad desde el plano militar, ya que estos son los expertos en estrategia para salvaguardar la seguridad de un país.

Con la globalización de la tecnología, se han evidenciado grandes aportes al desarrollo social, económico y político, no obstante, en este proceso también se destacan los problemas que el ciberespacio acarrea, y es que, al no contar con las medidas de ciberseguridad oportunas los países constantemente se ven amenazados y en el peor de los casos atacados mediante el robo de información, dinero, etc. Es por esto que a nivel nacional e internacional se plantea la utilización de diferentes modelos que protejan a todos los elementos que se encuentran en el entorno digital.

Los ciberataques son el principal riesgo global de origen humano, las consecuencias de los ciberataques son muy diversas y casi siempre se traducen en interrupción de servicios, pérdidas económicas o daños a la reputación de la víctima. La gran mayoría persigue un fin económico, el ciberdelito es, desde hace ya unos cuantos años, la forma delictiva que más dinero mueve a nivel mundial, pero también hay otros que se realizan con fines activistas, o para obtener información sobre un adversario, o como acciones integradas en un plan militar para el desarrollo de las operaciones.

La superioridad en el ciberespacio de una de las partes puede desnivelar la contienda a su favor, incluso en el caso de que el adversario sea superior en el resto de ámbitos operacionales, en donde se debe considerar que el derecho internacional de los conflictos armados limita enormemente las acciones que pueden llevarse a cabo contra los servicios esenciales e infraestructuras críticas del adversario.

La enorme imperfección del ciberespacio, plagado de vulnerabilidades físicas, lógicas y humanas que pueden ser explotadas: errores de diseño, fallos de programación, arquitecturas o interconexiones inadecuadas, emanaciones electromagnéticas, políticas imperfectas, carencia o incumplimiento de los procedimientos, desconocimiento, falta de concienciación. Esto ha permitido conocer infinidad de ejemplos de campañas de ciberespionaje que han estado activas durante seis, siete y hasta ocho años antes de ser detectadas, el anonimato, la suplantación de identidad o la utilización de infraestructuras de terceros son relativamente fáciles de conseguir en el ciberespacio.

Los países que presentan mejores características de ciberseguridad, lo han logrado trabajando de manera integral. Se observó que estos países presentan un fuerte fundamento de tipo jurídico e institucional, sumado a esto, se incluye el abordaje desde el ámbito político para proponer políticas en favor de la ciberseguridad. A su vez algunos de ellos toman como referencia organismos internacionales como referentes de la ciberseguridad.

En los países con mayor ciberseguridad se evidencia una clara actuación frente a los ciberataques, en donde existen ministerios que cumplen funciones específicas, claras y delimitadas con rutas o lineamientos de acción para hacer frente a un ciberataque. Estas características permiten tener una claridad para actuar a favor de la ciberseguridad.

En el caso ecuatoriano, no existe un modelo de ciberseguridad específico que pueda dar seguridad al entorno actual, sino que utiliza un conjunto de estrategias, lineamientos y objetivos de carácter político para proteger el ciberespacio, sin embargo, aunque este plan tiene una visión holística, se enmarca en la constitución para garantizar los derechos de los ciudadanos y penaliza los delitos cometidos dentro del entorno digital no se enfoca en garantizar la identificación, protección y detección de los ataques debido a que no se cuenta con un modelo oportuno para la ciberseguridad y se limita al cumplimiento de un plan estratégico de políticas de ciberseguridad.

Es necesario que, en el Ecuador se elabore normativas que permitan actuar y mitigar los delitos que se pretenden ejecutar desde la red. Se deben articular las instituciones de seguridad, defensa, inteligencia, para poder manejar las diferentes crisis de ciberseguridad, ciberdefensa y ciberinteligencia y de esta forma proteger las infraestructuras tecnológicas del Estado y de sus ciudadanos, previniendo, delitos e ilícitos en el ciberespacio.

Actualmente el ordenamiento jurídico ecuatoriano cuenta con varias disposiciones jurídicas enfocadas en la protección de los datos e información como parte de la seguridad digital de las operaciones que se dan en el ciberespacio, pero esta normativa no resulta eficiente para los ataques y amenazas en dicho entorno. Se debe expedir un Sistema de Seguridad Digital que englobe todos los aspectos que intervienen en las operaciones que se realizan empleando la tecnología.

Ecuador requiere de un sistema adecuado de Seguridad Digital con sus respectivos subsistemas, para evitar cualquier vulneración de derechos y asegurar una adecuada protección, su aprobación debe ser priorizada, ya que nos encontramos en una situación de vulnerabilidad con respecto a los países de la región que cuentan con normas adecuadas que previenen el cometimiento de ilícitos.

Simultáneamente se debe desarrollar estrategas que permitan armonizar normas comunes en la región, realizando un análisis de derecho que definan procedimientos, mecanismos de cooperación, acciones conjuntas en función de garantizar la ciberseguridad, ciberdefensa, ciberinteligencia y que no sigamos teniendo incidentes y delitos como se han dado últimamente con los ataques a diferentes instituciones públicas, privadas y los sistemas financieros.

En el caso del Ecuador, el estudio de la defensa cibernética tiene una dimensión poco pragmática, el estado propone la configuración de un modelo local de gobernanza en ciberdefensa en el ciberespacio inscrito en la normativa vigente. Esta norma ha sido planteada desde el ámbito político dentro de los sectores estratégicos del Estado ecuatoriano, 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.

BIBLIOGRAFÍA.

Acuña Lopez , Villa Motato, L. (2018). ESTADO ACTUAL DEL CIBERCRIMEN EN COLOMBIA CON RESPECTO A LATINOAMÉRICA. *Repositorio Institucional Universidad Abierta y a Distancia*. Recuperado el 2021, de https://repository.unad.edu.co/bitstream/handle/10596/25619/%20%09lfacunal.pdf?sequence=1&isAllowed=y

Alvarez Gonzales , S. (Febrero de 2016). Los retos y desafíos de la ciberseguridad y ciberdefensa en el ámbito de la formación y el entrenamiento. *Monográfico El reto de la ciberseguridad*, 7. Recuperado el 2021, de https://www.coit.es/sites/default/files/archivobit/pdf/monografico_samuel_esther.pdf

Alvarez, D. (2018). Agenda legislativa sobre ciberseguridad en Chile. *Revista chilena de derecho y tecnología, 7*(2). doi:http://dx.doi.org/10.5354/0719-2584.2018.51992

Alvarez, V. (2017). Los desafíos de la ciberseguridad en Chile. *Revista Chilena de derecho y tecnología, 6*(2). doi:http://dx.doi.org/10.5354/0719-2584.2017.48027

Amaral, A. (2014). La amenaza cibernética para la seguridad y defensa de Brasil. *Visión conjunta*. Obtenido de http://cefadigital.edu.ar/handle/1847939/32

Artiles, N. G. (2011). Situación de la ciberseguridad en el ámbito internacional y en la OTAN. En N. G. Artiles, & M. d. Estratégico (Ed.), *Cuadernos de estrategia* (Vol. 149, págs. 165-214). España. Obtenido de https://dialnet.unirioja.es/servlet/revista?codigo=7646

Badii, M., Castillo, J., Landeros, L., & Cortez, k. (2007). PAPEL DE LA ESTADÍSTICA EN LA INVESTIGACIÓN CIENTÍFICA. *INOVACIONES*.

Banco Central del Ecuador. (2019). *Manual de Procedimiento para la Gestión de Incidentes de Seguridad de la Información y Ciberseguridad.* Cuenca: Dirección Nacional de Riesgos Operacionales.

Barbe, E. (1987). El papel del realismo en las relaciones internacionales. *Revista de estudios políticos*, 149 - 176. Obtenido de file:///C:/Users/Usuario/Downloads/Dialnet-ElPapelDelRealismoEnLasRelacionesInternacionales-26941.pdf

BAUMAN, Z. (2003). La globalización consecuencias humanas, Editorial Fondo de Cultura Económica, México DF.

Bauman, Z. (2004). Modernidad Líquida. Editorial Fondo de Cultura Económica. México DF.

Bejarano, M. (2011). Documento informativo del IEEE 09/2011; nuevo concepto de ciberdefensa de la OTAN. Ieee.es. Recuperado de: file:///C:/Users/usuario/Downloads/Dialnet-NuevoConceptoDeCiberdefensaDeLaOTAN-7271583.pdf

BBC News Mundo. 2019. "Quién es Julian Assange, el polémico fundador de WikiLeaks arrestado en la embajada de Ecuador y que EE.UU. considera una amenaza". 11 de Abril. https://www.bbc.com/mundo/noticias-internacional-47895702.

Byron. (2016). "Aplicación de la Ciberdefensa en la Seguridad Nacional". Revista Presencia la Asociación de Generales: 59-65.

Cabrera, E. (2014). La invención del realismo político. Un ejercicio de historia conceptual. Signos Filosóficos. 16 (32). 126-149. Recuperado de: http://www.scielo.org.mx/pdf/signosf/v16n32/v16n32a5.pdf

Caceres, J. (2017). Colombia, estrategia nacional en ciberseguridad y ciberdefensa. *Space Power Journal*, 85- 89. Obtenido de https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-1/2017_1_09_caceres_s.pdf

Candau, J. (2011). Estrategias Nacionales de Ciberseguridad. Ciberterrorismo. Para Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado" (2011) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Madrid (Esp.) Ministerio de Defensa Español.

Candau, J. (2019). CIBERSEGURIDAD: HACIA UNA RESPUESTA Y DISUASIÓN EFECTIVA. *Revista científica*(5), 65-69.

Cano, J. (2008) Cibercrimen y ciberterrorismo. Dos amenazas emergentes. [4]ISACA Information Control and Audit Journal. Vol 6. Disponible en: http://www.isaca.org/ Journal/Past-Issues/2008/Volume-6/Pages/ JOnline-Cibercrimen-y-CiberterrorismoDos-Amenazas-Emergentes.aspx

Carlini, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *Opinión*, 950-966.

Carrasco, F. (21 de Agosto de 2014). *The Standar CIO Información 360 Estrategia.* Obtenido de http://www.cioal.com/2014/08/21/machete-una-campana-de-ciberespionaje-centrada-en-america-latina/

Castells, M. (1998). *La era de la información*, vol. 2, Alianza, Madrid

Código Orgánico Integral Penal. (2014). *Registro Oficial Nº 180.* Quito: Asamblea del Ecuador.

Constitución de la República del Ecuador. (2008). *Registro Oficial 449 de 20-oct-2008.* Quito.

Cornaglia, S., & Vercelli, A. (2017). La ciberdefensa y su regulación legal en Argentina (2006 - 2015). *Revista Latinoamericana de Estudios de Seguridad*(20), 46-62. doi:DOI: http://dx.doi.org/10.17141/urvio.20.2017.2601

Clarke, R. & Knake, R. (2011). Guerra en la red, los nuevos campos de batalla. Barcelona. Editorial Planeta.

CTIR. (2019). *Acerca de CTIR Gaov.* Obtenido de https://www.ctir.gov.br/es/

Cujabante , V., Bahamón , J., Prieto, J., & Quiroga, J. (2020). Ciberseguridad y ciberdefensa en Colombia: un posiblemodelo a seguir en las relaciones cívico-militares. *Revista Científica General José María Córdova*, 2500-7645.

Dallanegra, L. (2009). La política exterior en Tucídides. Los países fuertes y débiles. Reflexión Política. 11(22) ,96-117. Recuperado de: https://www.redalyc.org/articulo.oa?id=11012487008

Del Catillo , S., Sanjuan, G., & Gomez, M. (2018). Tecnologías de la Información y las Comunicaciones: desafío que enfrenta la universidad de ciencias médicas. *Edumecentro, 10*(1).

Durán, J. D. (2011). La ciber seguridad en el ambito militar. (I. E. Estudios, Ed.) *ieee.es*, 215-256. Recuperado el 2021, de https://dialnet.unirioja.es/servlet/articulo?codigo=3837348

Ecuador Universitario. 2012. “El contexto de la Ciberseguridad”, http://ecuadoruniversitario.com/ciencia-y-tecnologia/el-contexto-de-la-ciberseguridad/

El Comercio. (2019). Ecuador denuncia 40 millones de ciberataques tras retiro de asilo a Assange.

El Comercio. (2019). ‘Hackers’ lanzaron ofensiva global para atacar webs estatales.

El Comercio. 2014. “Ecuador implementará un Comando de Ciberdefensa”. 09 de septiembre, http://www.elcomercio.com/actualidad/ciberdefensa-ecuador-comando-fuerzasarmadas-ministerioddefensa.html.

El Universo. (2021). Ciberataque a Banco Pichincha fue realizado por atacantes internacionales, se revela en Comisión de Desarrollo Económico.

El Telégrafo (2022). Hackers emitieron 15.970 licencias fraudulentas.

El Universo.2014. “Formación militar prevé ciberdefensa”. 21 de mayo, http://www.eluniverso.com/noticias/2014/05/21/nota/2991356/formacion-militar-preve-ciberdefensa.

EnHacke. (28 de Marzo de 2017). *enhacke.* Obtenido de http://www.enhacke.com/2017/03/28/campana-espionaje-machete-orientada-paises-latinoamerica/

ESET. (2021). Security Report. Latinoamérica 2021.

Eset Research. (6 de Agosto de 2019). *Welivesecurity By Eset.* Obtenido de https://www.welivesecurity.com/la-es/2019/08/06/machete-sigue-activo-ciberespionaje-latinoamerica/

ESPOL. (2022). *Reporte Chequeo Digital del Ecuador.* Pyme Digital.

European Union Agency for Network and Information Security. [UNISA] (2011). Europa, “Ciber Security Strategy for Germany”. *Noticias*. Recuperado de: https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy2011-1

Forn Bosch, Marta. 2015. “El Asilo Político: El caso Assange”. Tesis de Grado en Derecho. Facultad de Ciencias Sociales: Universitat Abat Oliba CEU.

Fula Perilla, P. A. (s.f.). *LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA, DOCUMENTO CONPES 3701.* Universidad Piloto de Colombia. Recuperado el 2021, de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2723/Trabajo%20de%20grado3294.pdf?sequence=1&isAllowed=y

GONZALEZ LONDOÑO, J. (2020). ESTUDIO DEL ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LAS ORGANIZACIONES DE COLOMBIA. *UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA*.

Recuperado el 2021, de https://repository.unad.edu.co/bitstream/handle/10596/36669/jgonzalezlon.pdf?sequence=1

Hernández Armenta, M. (02 de Septiembre de 2019). En América Latina se registran 45 ataques cibernéticos por segundo. *Forbes*. Recuperado el 2021, de https://www.forbes.com.mx/en-america-latina-se-registran-45-ataques-ciberneticos-por-segundo/

Herrera, P. (2020). El enfoque de género en la Política Nacional de Ciberseguridad de Chile. *Rev. chil. derecho tecnol, 9*(1). Obtenido de http://dx.doi.org/10.5354/0719-2584.2020.51577

Inteligencia, Secretaría de. 2014. "Plan Estratégico Institucional 2015-2016", www.inteligencia.gob.ec/wp-content/.../05/PlanEstrategico2015-2017Aprobado.pdf.

Izaguirre, J., & León, F. (2018). Análisis de los ciberataques realizados en América Latina. *INNOVA, 3*(9), 172 - 181. doi:https://doi.org/10.33890/innova.v3.n9.2018.837

Joyanes, L. (2011) Introducción. Estado del arte de la ciberseguridad. Para Instituto Español de Estudios Estratégicos, Instituto Universitario "General Gutiérrez Mellado" (2011) Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Madrid (Esp.) Ministerio de Defensa Español.

Lévy, P. (2007). Cibercultura. La cultura de la sociedad digital. [Informe al Consejo de Europa]. Prólogo: Manuel Medina. Barcelona: Rubí; México: AnthroposUniversidad Autónoma Metropolitana. isbn: 978-84-7658-808-6.

Ley Especial de Telecomunicaciones. (2013). *Ley No. 184.* Quito.

Lissorgues, Y. (2017). El Realismo. Arte y literatura, propuestas técnicas y estímulos ideológicos. *Fundación Biblioteca Virtual Miguel de Cervantes*. Obtenido de http://www.cervantesvirtual.com/obra-visor/el-realismo-arte-y-literatura-propuestas-tecnicas-y-estimulos-ideologicos/html/01fa98aa-82b2-11df-acc7-002185ce6064_2.html

López, P. (2016). *La evolución de la función de inteligencia dentro del contexto de la seguridad integral: análisis y perspectivas en su entendimieno y aplicación*. Obtenido de http://repositorioslatinoamericanos.uchile.cl/handle/2250/1071078

Madrigal, R. (2020). Impacto del ciberataque en la seguridad internacional. *Ecopapers*. Obtenido de https://EconPapers.repec.org/RePEc:erv:rccsrc:y:2020:i:2020-01:05

Ministerio Coordinador de Seguridad. 2014. "Ciberseguridad escenarios y recomendaciones". Revista Digital del Ministerio Coordinador de Seguridad

Ministerio del interior y seguridad publica. (2018). *Leyes, reglamentos, decretos y resoluciones de orden general.* Chile: Diario oficial.

Ministerio Coordinador de Seguridad. (2014). "Ciberseguridad escenarios y recomendaciones". Revista Digital del Ministerio Coordinador de Seguridad.

Ministerio de la secretaria general de la presidencia. (2019). *Transformación Digital del Estado al servicio de las personas.* Obtenido de Gob digital: https://digital.gob.cl/

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (17 de Mayo de 2021). *Acuerdo Ministerial 006-2021*.

Ministerio de Defensa (2010). Ciberseguridad. Retos y amenazas a la ciberseguridad nacional en el ciberespacio. *Cuadernos de Estrategia 149*. 3-368. Recuperado de: https://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Molas, J. (2007) Políticas de I+D de Defensa de varios países europeos y de EE.UU. En Relaciones entre las innovaciones tecnológicas y la Defensa. Madrid (Esp.) Fundación Rogelio Segovia Para el Desarrollo de las Telecomunicaciones.

Molas, J. (2007) Políticas de I+D de Defensa de varios países europeos y de EE.UU. En Relaciones entre las innovaciones tecnológicas y la Defensa. Madrid (Esp.) Fundación Rogelio Segovia Para el Desarrollo de las Telecomunicaciones.

Morgenthau, H. (1972). Politics among Nations. The Struggle for Power and Peace, Nueva York, Alfred A. Knopf

Ochoa, Alexandra. 2021. ''Desafíos globales del cibercrimen''. Tesis de Postgrado en Desafíos globales del cibercrimen. Área de Estudios Sociales y Globales: Universidad Andina Simón Bolívar, Sede Ecuador.

OECD. (2012). Cybersecurity Policy Making at a Turning Point. *OECD Digital Economy Papers*(211).

Oro, L. (2010). Visión de la naturaleza humana desde el realismo político. Revista Coherencia. 7 (13), 113-150. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-58872010000200006

Palacio, J. (2016). La doctrina Gerasimov: Segunda entrega. Editado por: Grupo de Estudios en Seguridad Internacional (GESI). Lugar de edición: Granada (España). ISSN: 2340-8421.

Pastor, O. Pérez, J. Arnaíz, D. & Taboso, P. (2009). Seguridad Nacional y ciberdefensa. Madrid (Esp.). Fundación Rogelio Segovia Para el Desarrollo de las Telecomunicaciones.

PNSI, (2014) Quito. http://revistas.flacsoandes.edu.ec/urvio/article/view/2571/1605

Pons Gamon, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity. *URVIO. Revista Latinoamericana De Estudios De Seguridad*, (20), 80-93. Recuperado de: https://doi.org/10.17141/urvio.20.2017.2563

Pública, S. N. (2014). *Plan Nacional deGobierno Electrónico 2014 - 2017*. Secretaría Nacional de la Administración Pública, Ecuador. Recuperado el 2021, de www.gobiernoelectronico.gob.ec/PlanGobiernoElectronicoV1.pdf

Ribagorda, A. (2018). Panorama actual de la ciberseguridad. *Dialnet.* 1(410), 13-26. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6815097

Robert O. Keohane: After Hegemony: Cooperation and Discard in the World Political Economy (Prínceton, N.J., Prínceton University Press, 1984)

Rodriguez, F. (2020). ATAQUES CIBERNETICOS Y ACCIONES BASICAS PARA CIBERSEGURIDAD. *Universidad mayor de San Simón*. Obtenido de http://hdl.handle.net/123456789/19489

RVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 31-45 RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

Salinas, N. (2018). *Ciberdefensa en el Estado Ecuatoriano*. Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/14792/CIBERDEFENSA%20EN%20EL%20ESTADO%20ECUATORIANO%20PERIODO%202013-2016.pdf?sequence=1&isAl

Sánchez, C. (2015). *De la Doctrina de Seguridad Nacional a la Seguridad Integral en el Ecuador*. Obtenido de ESPE: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/11587/T-ESPE-049558.pdf?sequence=1&isAllowed=y

Sandra, R. (20 de 10 de 2014). Ciberdefensa y ciberseguridad: una nueva prioridad para las naciones. *Repositorio Institucional UMNG*. Recuperado el 2021, de http://hdl.handle.net/10654/12937

Santiago, E., & Allende, S. (2017). Riesgos de ciberseguridad en las empresas. *Ciencia, tecnología y medio ambiente, XV*.

Secretaría Nacional de Planificación (2021). Plan Nacional de Oportunidades 2021-2025. Recuperado de: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf

Segura, H. (2019). Consideraciones para la implementación de un ciberejército en México. *Infotec*. Recuperado de: https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/454/1/INFOTEC_MDTIC_HMSC_02122020.pdf

SEGURIDAD INFORMÁTICA Y REALIDAD JURÍDICA DEL CIBERESPACIO EN EL ECUADOR. *Repositorio Digital Universidad De Las Américas*. Recuperado el 2021, de http://dspace.udla.edu.ec/handle/33000/7974

SUPERTEL. (2013). Ciberseguridad: Incremento del conocimiento acerca de atención de seguridad informática. *Revista Institucional*.

Tates Almeida , Herrera, C. A. (04 de Diciembre de 2018). LA CIBERSEGURIDAD EN EL ECUADOR, UNA PROPUESTA DE ORGANIZACIÓN. *Revista de Ciencias de Seguridad y Defensa, IV*, 156-169. Recuperado el 2021, de http://geo1.espe.edu.ec/wp-content/uploads/2019/03/7art12.pdf

Tokatlian, J. y Pardo, R. (1990). LA TEORIA DE LA INTERDEPENDENCIA: ¿UN PARADIGMA ALTERNATIVO AL REALISMO? Estudios Internacionales, 23(91), 339–382. http://www.jstor.org/stable/41391338

UIT, U. I. (05 de Noviebre de 2019). Nuevos datos de la UIT indican que, pese a la mayor implantación de Internet la brecha de género digital sigue creciendo. *(UIT), Union Internacional de Telecomunicaciones*. Recuperado el 2021, de https://www.itu.int/es/mediacentre/Pages/2019-PR19.aspx

Urbina, E. (2020). INVESTIGACIÓN CUALITATIVA. *Revista ASD, 1*(1).

Ureña, F. (2015). Ciberataques, la mayor amenaza actual. *Ieee.es*. Recuperado de: file:///C:/Users/HP_USER/Downloads/Dialnet-CiberataquesLaMayorAmenazaActual-7684551.pdf

Vargas, E. (2014). Ciberseguridad y ciberdefensa: ¿Qué implicaciones tienen para la Seguridad Nacional? Universidad militar Nueva Granada. Bogotá D.C.

Vargas, V. (2014). CIBERSEGURIDAD Y CIBERDEFENSA: ¿QUÉ IMPLICACIONES TIENEN PARA LA SEGURIDAD NACIONAL? *UNIVERSIDAD MILITAR NUEVA GRANADA*, 38-55.

Vásquez, B. (2008). Modernidad líquida y fragilidad humana, Pontificia universidad católica de Valparaíso, Universidad Complutense de Madrid, Nómadas, Revista Crítica de ciencias sociales y jurídicas 19, Vega, C. E. (2017).

Villamil, C., Bahamon, J., Prieto, V., & Quiroga, A. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo de relaciones cívico-militares. *Rev. Cient. General José María Córdova*, *18*(30), 357-377.

ZYGMUNT BAUMAN Modernidad líquida, http://www.oei.org.ar/edumedia/pdfs/T14_Docu1_Lamodernidadliquida_Bauman.pdf