UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA

UNAN - MANAGUA

RECINTO UNIVERSITARIO "RUBÉN DARÍO"

FACULTAD DE HUMANIDADES Y CIENCIAS JURÍDICAS

DEPARTAMENTO DE FILOSOFÍA

TESIS MONOGRÁFICA PARA OPTAR AL TÍTULO DE LICENCIADO EN CIENCIAS POLÍTICAS Y RELACIONES INTERNACIONALES

TEMA:

CIBERSEGURIDAD: IMPORTANCIA DE UNA ESTRATEGIA CENTROAMERICANA HOMOLOGADA PARA CONTRARRESTAR LA CIBERDELINCUENCIA COMO UNA AMENAZA EMERGENTE.

AUTOR:

BR. JOSÉ DANIEL DESAYES HERRERA

DOCENTE TUTOR:

MSC. RICARDO ALFONSO ESTRADA FLORES

MANAGUA, NICARAGUA 03 FEBRERO 2022

"A LA LIBERTAD POR LA UNIVERSIDAD"

Dedicatoria

A Dios en primer lugar por darme sabiduría y fortaleza lo cual me ha permitido llegar a esta etapa de mi vida que es de suma importancia para mí a pesar de las adversidades que se me presentaron en el camino. En cada obstáculo él estuvo a mi lado guiándome e iluminando mi senda a pesar de mis errores, cumpliendo lo que dice en su santa palabra, La Biblia, que él es nuestro pastor y nada nos faltará.

A mi madre quien me dio la vida y a pesar de no tenerla físicamente presente, la llevo siempre en mi corazón junto con sus invaluables enseñanzas y consejos teniendo mucho por honrarla.

A mis tías, Martha Lorena Agurcia, Martha Eudomilia Albir, Maritza Desayes Albir, Karla Yahaira Albir, quienes han realizado el papel de padre y madre para mí, apoyándome incondicionalmente en todas mis metas, especialmente en esta etapa de mi vida.

Agradecimientos

A Dios por darme sabiduría y ser mi guía para poder cumplir mis objetivos. A él sea toda honra y gloria por siempre.

A mi madre que, a pesar de no tenerla presente, mantengo sus enseñanzas conmigo las cuales me han permitido ser una persona mejor.

A mis tías y demás familiares que me brindaron sus consejos, apoyo y cariño durante los años de mi carrera.

A cada uno de los docentes que nos impartieron clases, demostrando su alta dedicación y esmero por darnos el pan de saber.

A mi Tutor, Msc. Ricardo Estrada Flores quien brindo sus máximos conocimientos para realizar esta tesis, también por haber sido paciente y una excelente persona conmigo.

A su vez, al Msc. Álvaro Padilla Lacayo por haber aportado en gran medida a la formación y desarrollo de esta tesis.

Carta Aval del Tutor

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA
UNAN - MANAGUA

"2021: Año del Bicentenario de la Independencia de Centroamérica"

Facultad de Humanidades y Ciencias Jurídicas

Departamento de Filosofía

Martes 19 de octubre del 2021

El suscrito Docente Tutor de Monografía para optar al título de Licenciatura en Ciencia Política y Relaciones Internacionales de la Facultad de Humanidades y Ciencias Jurídicas de la Universidad Nacional Autónoma de Nicaragua, UNAN-Managua, por este medio extiende:

CARTA AVAL

Al Br. José Daniel Desayes Herrera, carné número 17-18-31-40 dado que la presente tesis titulada "*La Ciberseguridad y Ciberdefensa: Importancia de una Estrategia Centroamericana para contrarrestar la Ciberdelincuencia como una amenaza emergente*", cumple los requisitos establecidos para su respectiva pre-defensa y defensa ante el Tribunal Examinador.

MSc. Ricardo Alfonso Estrada Flores
Docente
Departamento de Filosofía

Cc: Archivo Personal

¡A la Libertad por la Universidad!

Resumen

En la actualidad nuestro mundo experimenta diversos cambios sobre todo en los factores tecnológicos por el avance de la globalización, sin embargo, esto resulta un desafío ya que, por medio del avance tecnológico, también surgen nuevas amenazas que pueden llegar a perjudicar las capacidades de los Estados y degradar su estabilidad interna, especialmente aquellos que no poseen mecanismos de ciberseguridad en sus recursos estratégicos para enfrentar la ciberdelincuencia, como el caso de la región centroamericana.

La presente investigación expone el desafío que poseen los Estados centroamericanos para formular y homologar una estrategia regional en ciberseguridad, teniendo en cuenta que los mecanismos de seguridad regional existentes, no contemplan explícitamente el tema de la ciberdelincuencia como una amenaza real latente y emergente para Centroamérica, o bien una iniciativa de concretar de manera unánime una seguridad cibernética regional. Lo que representa un problema para la región al no contar con un sistema de prevención, protección y respuesta inmediata ante ataques o interferencias por parte de la ciberdelincuencia.

Centroamérica viene adaptándose a los nuevos desarrollos tecnológicos, especialmente los que están dirigidos a las áreas indispensables de una sociedad, como son los servicios básicos, la economía, infraestructura, institucionalidad gubernamental y seguridad. Por lo tanto, los Estados de la región necesitan brindar protección a sus capacidades o recursos estratégicos y mantener constantemente sus mecanismos de prevención, puesto que las amenazas como la ciberdelincuencia gozan de un constante cambio que les permite adaptarse y obtener mejores capacidades para ejercer daño, sobre todo cuando las Tecnologías de la Información y Comunicación (TIC) forma parte de una capacidad crítica.

Lo que conlleva a un asunto estratégico debido que, si ocurre algún detrimento en las capacidades críticas de la región, las consecuencias no solamente afectarán a cada Estado centroamericano, también se verán perjudicadas los Estados vecinos, la región e incluso tendría posibles efectos en el área internacional. Es por ello, que resulta indispensable que Centroamérica alcance mediante el diálogo y la cooperación técnica una Estrategia Regional de Seguridad Cibernética, la cual beneficie integralmente a toda la región y proteja constantemente sus áreas indispensables para el desarrollo propio de los Estados.

Palabras clave: Ciberseguridad, Ciberdelincuencia, Estados, Tecnología, Centroamérica.

Abreviaturas

1.	APT	Amenaza Persistente Avanzada
2.	BCIE	Banco Centroamericano de Integración Económica
3.	CSIRT	Equipo de Repuesta a Incidentes de Seguridad
4.	CCDCOE	Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN
5.	CISA	Agencia de Seguridad e Infraestructura de Estados Unidos
6.	CEPAL	Comisión Económica para América Latina y el Caribe
7.	CFAC	Conferencia de las Fuerzas Armadas de Centroamérica
8.	CNLS	Comisión Nacional de Seguridad en Línea
9.	CICTE	Comité Interamericano Contra el Terrorismo
10.	COCATRAM	Comisión Centroamericana de Transporte Marítimo
11.	COMITRAN	Consejo Sectorial de Ministros de Transporte de Centroamérica
12.	COMTELCA	Comisión Técnica regional de Telecomunicaciones
13.	CRIE	Comisión Regional de Interconexión Eléctrica
14.	CREI	Centro de Repuesta a Emergencia Informática
15.	DNII	Dirección Nacional de Investigación e Inteligencia
16.	ESCA	Estrategia de Seguridad de Centroamérica
17.	EOR	Ente Operador Regional
18.	EPR	Empresa Propietaria de la Red
19.	JID	Junta Interamericana de Defensa
20.	NSA-CSS	Agencia de Seguridad Nacional-Servicio de Seguridad Central
21.	OTAN	Organización del Tratado del Atlántico Norte
22.	OEA	Organización de Estados Americanos
23.	REDCA	Comisión Centroamericana de Telecomunicaciones
24.	UNDP-PNUD	Programa de las Naciones Unidas para el Desarrollo
25.	SIEPAC	Sistema de Interconexión Eléctrica de los Países de América Central
26.	SIECA	Secretaria de Integración Económica Centroamericana
27.	SICA	Sistema de la Integración Centroamericana
28.	TIC	Tecnologías de la Información y Comunicación
29.	UE	Unión Europea
30.	UIT	Unión Internacional de Telecomunicaciones de las Naciones Unidas
31.	UNODC	Oficina de Naciones Unidas contra la Droga y el Delito

Índice de Contenido

Tabla de Ilustraciones

CAPÍTULO I

Introducción

La humanidad en sus diferentes etapas históricas ha utilizado medios como las herramientas las cuales han permitido desarrollar mejores condiciones de vida para los individuos y sus necesidades. Los ejemplos más notables de esto ocurrieron a través de las tres revoluciones industriales, sin embargo, la tercera revolución industrial tiene su mayor importancia debido que contiene las bases que moldearon y rigen la actualidad como la globalización, el internet, la informática y las Tecnologías de la Información y Comunicación (TIC) y otros semejantes como la llamada Sociedad de la Información.

A su vez por el avance tecnológico ha contribuido a plantear nuevos términos como la revolución industrial 4.0, teniendo por objetivo transformar el uso habitual de la tecnología por nuevos conceptos como la tecnología inteligente, la nanotecnología, los sistemas cuánticos y una mayor amplitud del ciberespacio. Este último juega un rol vital en cuanto a las interconexiones otorgándole al estilo de vida del ser humano mejores capacidades de interactuar. De acuerdo con el Departamento de Defensa de EEUU (DOD) el ciberespacio es "Un dominio global dentro del entorno de la información que consiste en la red interdependiente de infraestructuras de tecnología de la información y datos residentes, incluidos internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados" (P.1)

Teniendo en cuenta lo anterior, podemos deducir que el ciberespacio se consolida como un nuevo eje de poder que tiene su teatro de operaciones en lo virtual pero sus efectos logran tener un alcance en la realidad. En este sentido representa un campo donde surgan peligros potenciales como la ciberdelincuencia, la cual tiene la capacidad para perjudicar los recursos estratégicos de un Estado degradando su estabilidad interna y con repecursiones a su población.

De manera que esto representa un reto en materia de seguridad, sobre todo para aquellos Estados o regiones que, de acuerdo a sus demandas internas, se modernizan mediante la adquisición de nuevas tecnologías como el caso de la región centroamericana en base al estudio de la CEPAL de Estado de la Banda Ancha de América Latina y el Caribe (2016) estimando que más de 12 millones de centroamericanos tienen acceso a internet y nuevas tecnologías, representando como un desafío para los mecanismos de seguridad cibernética que posea la región.

La región centroamericana de manera unánime, no cuenta con una iniciativa de seguridad cibernética, los Estados de la región solamente poseen sus propios mecanismos de seguridad y defensa mediante la articulación de acciones institucionales, programas y principalmente sus mecanismos jurídicos. Por tanto, Centroamérica se encuentra inerme para brindar una mejor seguridad cibernética regional, a pesar de algunos esfuerzos de los organismos de integración regional como el Sistema de Integración Centroamericana (SICA) al reforzar la importancia de tomar acciones en materia de ciberseguridad, y el peligro que representaría para toda la región un ciberataque a los recursos estratégicos que dependen los Estados para su funcionamiento lo que repercutiría gravemente en los niveles de seguridad interna de los países y de la región en general.

Sin embargo, los Estados que conforman la región centroamericana, poseen mecanismos que pueden ayudar a impulsar o concretar una iniciativa de ciberseguridad centroamericana de manera homologada, partiendo desde el Protocolo de Tegucigalpa, el Tratado Marco de Seguridad Democrática en Centroamérica, Estrategia de Seguridad de Centroamérica y la Estrategia regional Digital del SICA, los cuales resultarían ser las principales bases para realizar un consenso mutuo entre los Estados centroamericanos. Asimismo, esto permitiría armonizar los estándares jurídicos que poseen los Estados en materia de ciberseguridad, ciberdefensa y crear espacios de cooperación con las instituciones gubernamentales encargadas de estas áreas específicas.

Del mismo modo los Estados de la región tienen la posibilidad de implementar una ciberdefensa mediante el mecanismo de integración militar como es la Conferencia de las Fuerzas Armadas Centroamericanas (CFAC), debido que al haber un ciberataque hacia una capacidad estatal, se estaría produciendo una violación a la soberanía de ese Estado, lo cual entraría en concordancia con el rol que juegan las fuerzas armadas de los países centroamericanos al ser estas las encargadas de velar por la estabilidad nacional. Lo único que se requiere una mayor voluntad política por parte de los Estados para profundizar multilateralmente una iniciativa que ayude a la armonización de intereses, la cooperación y coordinación de acciones para proteger los recursos vitales de la región y de los Estados ante las amenazas emergentes como la ciberdelincuencia.

1.1 Planteamiento del Problema

La región centroamericana se ha caracterizado por mantener la paz, la estabilidad y afrontar todo tipo de amenaza que socave la seguridad de los Estados por medio de los principios establecidos en el marco normativo de integración como es el Protocolo de Tegucigalpa. A pesar de los esfuerzos para mantener una armonización en la región, Centroamérica no se encuentra exenta de tensiones políticas internas que prevalecen en ella actualmente, con el posicionamiento de directrices ideológicas tradicionales como las vertientes ideológicas de izquierda o derecha sumando conflictos externos, como la guerra de las 5G entre EEUU y China, la cual tiene importancia en el desarrollo de nuevas redes móviles de quinta generación y su impacto en la configuración de la internacionalización del internet de las cosas.

Por lo tanto, Centroamérica esta propensa a diversos desafíos especialmente en las nuevas amenazas que surgen con el desarrollo de la tecnología al nivel global, como es el caso de la ciberdelincuencia. La ciberdelincuencia en base a la definición que ofrece la Agencia de Seguridad e Infraestructura de EEUU (CISA) es una nueva modalidad de delitos internacionales que puede proceder de individuos con intereses y altamente capacitados, organizaciones criminales, terrorismo y Estados, los cuales operan por medio del ciberespacio para perjudicar objetivos estratégicamente importantes. Asimismo, el accionar de la ciberdelincuencia permite diferenciarse de los delitos cibernéticos comunes los cuales se limitan a un impacto temporal en pequeños sectores colectivos o individuales, mientras que la ciberdelincuencia posee una mayor velocidad, alcance y perjuicio en los recursos o capacidades de un Estado.

En este sentido ¿Qué mecanismos de ciberseguridad regional poseen los Estados centroamericanos para adaptarse y hacer frente a la problemática de la ciberdelincuencia en la actualidad y en el futuro? de manera propia los Estados disponen de algunos instrumentos en materia de seguridad cibernética, sin embargo, como región centroamericana no cuentan con un mecanismo homologado que los dirija en una sola estrategia en común, en consecuencia, Centroamérica tiene una brecha desigual en protección y defensa cibernética, sumando su vulnerabilidad como región ante un ciberataque dirigido a las capacidades de los propios Estados.

Las capacidades que poseen los Estados centroamericanos representan un objetivo vital puesto que garantizan su propio funcionamiento, tomando ejemplo en las redes de interconexión eléctrica y sus centrales desde Guatemala hasta Panamá, con 300MW, otorgando un masivo suministro de energía para todos sus fines. Seguidamente de los puertos marítimos de carga en donde se ejecutan las importaciones y exportaciones, sobre todo en el canal de Panamá, representando una parte principal para las economías de los Estados centroamericanos al administrar más de 150 mil toneladas de carga según el resumen estadístico portuario de la región 2017.

También se encuentran los 20 aeropuertos regionales de estándar internacional que son una base esencial para la interconectividad aérea con otros países y continentes aportando al transporte de carga y la movilidad de personas. El sector de salud y el suministro de agua potable o recursos de material dispensable para el consumo y utilización, junto con los sistemas financieros, los cuales representan el desarrollo de la economía moderna y la estabilidad monetaria en sus factores macroeconómico y microeconómico, destacando su adaptación hacia las nuevas demandas tecnológicas para actualizar el sistema financiero regional.

Por tanto, si algunas de estas capacidades llegasen a sufrir un ciberataque, los Estados, así como la región en general, se verían gravemente afectados, degradando los niveles de seguridad interna y externa de Centroamérica, afectando a su vez las regiones cercanas, sus capacidades y la propia población, debido a la posición geográfica y la interconexión transoceánica que posee esta misma. De tal modo que la región necesita consolidar una iniciativa que permita armonizar los intereses de los Estados, así como los mecanismos de seguridad cibernética que estos poseen, principalmente los de carácter jurídico e institucional por su mayor adaptabilidad a los mecanismos regionales ya existentes, lo que facilitaría a los Estados centroamericanos homologar un solo mecanismo de protección y defensa.

1.2 Justificación

El uso de nuevas tecnologías, ha introducido grandes avances a la humanidad, hoy en día tanto los Estados, empresas y la propia ciudadanía están altamente interconectados, lo cual significa no solamente un mayor impulso positivo para el desarrollo de las actividades humanas, también representa un alto índice para que las amenazas cibernéticas de alto peligro como la ciberdelincuencia, tengan un mayor influencia e impacto negativo por medio del ciberespacio. Generando consecuencias considerables como daños a dispositivos informáticos o provocando fallas a las capacidades de un Estado lo que incide directamente en la estabilidad y seguridad nacional de un país, región o continente.

Teniendo en cuenta las repercusiones que pueda tener la incidencia de la ciberdelincuencia en un Estado, la ciberseguridad se ha convertido en un tema de alto valor estratégico, debido a la importancia que tienen al de otorgar seguridad a los factores tecnológicos que ayudan al funcionamiento de un Estado y el desarrollo de su población. Sobre todo, para aquellos países que vienen adaptándose a las nuevas demandas tecnológicas actuales, y que estos necesitan asegurar sus capacidades como es el caso de la región centroamericana.

La presente investigación, tiene como fundamento resaltar la necesidad de una estrategia homologada al nivel centroamericano en materia de ciberseguridad, también la posibilidad de conformar una estrategia en ciberdefensa para hacer frente a los nuevos desafíos que representan las amenazas emergentes como la ciberdelincuencia, la cual no solamente está presente en los grandes países industrializados como las tradicionales costumbres o creencias lo presentan, también las amenazas cibernéticas afectan a los países en vías de desarrollo con alta demanda tecnológica en sus áreas económicas, políticas y sociales, más aún cuando estos no poseen una iniciativa sólida en protección y defensa contra este peligro.

De igual forma, en esta investigación se aborda los principales mecanismos de integración centroamericana y sus debidos principios y propósitos los cuales ayudarían a la implementación de una política en materia de ciberseguridad, que tenga por objetivo crear niveles óptimos de resiliencia en el ciberespacio centroamericano. Además, que representa una necesidad en auge debido a los nuevos avances tecnológicos que además de sus impactos positivos, también trae consigo consecuencias graves por el nivel de dependencia que poseen los estados de ella.

1.3 Objetivos

1.3.1 Objetivo General:

Determinar el reto que representa una ciberseguridad homologada para los Estados centroamericanos ante su vulnerabilidad frente a la ciberdelincuencia.

1.3.2 Objetivo Específicos:

1. Identificar los mecanismos de ciberseguridad que poseen los Estados centroamericanos.
2. Describir los riesgos que representa la ciberdelincuencia para los Estados centroamericanos.
3. Explicar la importancia de un mecanismo centroamericano homologado en materia de ciberseguridad y la conformación de una ciberdefensa armoniosa.

CAPÍTULO II

Marco Referencial

2.1 Antecedentes de Investigación.

2.1.1 Antecedentes Internacionales

Nicolás Alfredo; Arias Torres, (2015) en su investigación titulada*: Modelo Experimental de Ciberseguridad y Ciberdefensa para Colombia* (Tesis de Ingeniería) -Universidad Libre de Bogotá, tuvo como objetivos generales: la construcción de un modelo de referenciación que garantizase al Estado colombiano parametrizar las condiciones de protección en el ciberespacio como repuesta a los ataques producidos por alguna guerra informática, además de la valorización de estudios sobre esquemas de defensa y minimización de riesgos en el ámbito informático de dicho país. Algunas de las conclusiones que se presentaron y poseen relación con la presente investigación, se estructuran en la necesidad de evaluar acciones de logística e interpretación analítica de los ejes organizacionales, para el control y formulación de procedimientos en la ciberseguridad y la ciberdefensa, cuyo resultado es el refuerzo de los sistemas internos de una nación para combatir amenazas de categoría cibernética.

Del mismo modo que enfatiza y proyecta la adaptabilidad y función de esquemas que se adecuen a las necesidades internas y externas de un país especialmente en el factor internacional, el cual está sumergido a constantes cambios, especialmente en el área de los ciberdelitos y la propia cibercriminalidad. Por lo que el estudio interno y externo siempre tiene que poseer alto valor estratégico para la ciberseguridad y ciberdefensa.

Adair & Julian, (2014) en su tesis titulada: *Ciberdelito* (tesis de ingeniería)-Universidad Autónoma de México, tuvo como prioridad el estudio de las políticas de seguridad informática, elaborando un análisis de la evolución, utilización y resultados de los medios de comunicación computarizados y el ciberespacio, tanto de sus primeros desarrollos como el panorama actual.

Un énfasis especial de esta tesis es sobre los tipos de delitos que imperan en la red ya sea bajo la definición de sistemas informáticos, bajo relación de contenido multimedia, y de factor económico, agregando los mecanismos que pueden intervenir para enfrentar este tipo de amenaza. Las conclusiones que presenta esta tesis aportan a un mayor análisis para la presente investigación, destacando los términos que conlleva el área del ciberdelito y la propia ciberdelincuencia y el

comportamiento que este posee en los medios informáticos, sobre todo el uso o el papel que estos tienen en las actividades delictivas actuales.

2.1.2 Antecedentes Nacionales

Rugama; Rodriguez, (2019) en su investigación titulada*: Las Ciberamenazas: El desafío que enfrentan los países del SICA en el nuevo escenario Internacional* (Tesis de Licenciatura)-UNAN-Managua, tuvo como objetivo general, analizar los tipos de medidas, políticas públicas y estrategias que han tomado los países que conforman el SICA hacia las ciberamenazas de este nuevo escenario internacional, ádemas de señalar las ciberamenazas a las que estan expuestas las infraestructuras críticas e institucionales de los países del SICA.

En sus conclusiones presentan los retos que tienen los países del SICA para asegurar sus infraestructuras críticas, y lo expuesto que se encuentran estas ante la ciberdelincuencia. Asimismo se resalta la disparidad que existe en la región con respecto a una iniciativa que ayude convalidar un solo objetivo en materia de ciberseguridad, añadiendo a su vez que Centroamerica posee diferencias tecnológicas, acceso a internet y en la armonización jurídica para establecer una política de cooperación común.

El aporte que realiza esta tesis a la presente investigación es de vital importancia ya que expone las vulnerabilidades que tiene la región centroamericana ante las ciberamenazas, más aún cuando refiere a que los países que conforman el SICA no poseen un marco normativo que delimite la protección efectiva de las infraestructuras críticas y la seguridad de la región, especialmente la de cada país. De igual manera, presenta algunos de los principales antecedentes en los cuales lo países que integran el SICA han sido objetivos de ciberataques.

Chavarría, Jirón, & Miranda, (2016) en su investigación titulada: *La ciberdelincuencia y su regulación jurídica en Centroamerica con énfaisis en Costa Rica, El Salvador y Nicaragua* (Tesis de Licenciatura)-UNAN-León, Nicaragua, tuvo como objetivo un análisis general de la ciberdelincuencia en los países de la región centroamericana, resaltando los mecanismos jurídicos y los retos que impiden la regulación de este fenómeno, a la misma vez que se indica la incidencia que posee la cooperación internacional en esta materia.

Algunas de las conclusiones que se presentaron en este estudio hacen referencia al continuo avance tecnológico y las nuevas formas de desarrollo e impacto que poseen los delitos en el mundo, especialmente los que ocurren a través del ciberespacio, por lo se presenta la necesidad de crear mecanismos adaptables, especialmente los de marco jurídico para que los Estados y los propios individuos puedan tener opciones y medios para protegerse ante cualquier actividad delictiva que afecte por medio del uso del ciberespacio.

El aporte que otorga este estudio a la presente investigación se resalta en la parte de los mecanismos jurídicos que poseen los Estados de la región centroamericana para hacer frente a los ciberdelitos, lo cual es un factor fundamental para la creación o articulación de mecanismos que permitan aumentar los niveles de seguridad en un país o en una región. También es vital para la orientación de iniciativas que permitan la cooperación y la complementariedad de los intereses regionales.

Espinoza, (2014) en su investigación títulada: *El nuevo delito de acceso y uso no autorizado de registros, datos o archivos informáticos introducido por la Ley número 641, Código Penal* (tesis de licenciatura)-Universidad Centroamericana-Managua, Nicaragua, tuvo como objetivos generales la definición de los efectos de caracter jurídico de los delitos de acceso y uso no autorizado de datos o archivos informáticos. Asimismo la determinacion de los bienes e intereses jurídicos tangibles y no tangibles contemplados en al artículo 198 del código penal nicaragüense.

Las conclusiones presentadas por el autor, se adecuan en primera instancia al estudio general sobre los delitos informáticos y sus caracteristicas principales destacando que estos suelen ser mayormente operantes, variados, novedosos, complejos y fluctuantes, por lo tanto no es fácil adecuar un concepto sólido de los mismos ya que estos hoy en dia se desarrollan continuamente por el avance tecnólogico. Por otro lado el bien jurídico resalta su esquema de importancia sobre todo cuando este posee carácter de proteger los sistemas de información, no obstante el autor expone que este tiene un vacio jurídico por corregir.

El aporte que se presenta es sumamente significativo debido al ánalisis jurídico como una herramienta mas para frenar los actos del ciberdelito, a su vez ofrece los tipos de clase en la que estos se comprende y los sujetos activos y pasivos, siendo de mucha utilidad para una mayor compresion y adaptabilidad con los escenarios modernos.

2.2 Marco Conceptual

2.2.1 Amenaza

El concepto de amenaza comúnmente se conoce como todo factor perjudicial, relacionado con algún hecho o acción, en este caso la Ley No. 919 de Seguridad Soberana de la República de Nicaragua, en su Art. 5, inciso 11, define amenaza a todo elemento que se caracteriza por factores naturales y aquellos que son inequívocos, los cuales tienen un impacto real y capacidad ejercer algún daño hacia alguna vulnerabilidad de cualquier índole.

Según Barón, (2008) se pueden clasificar distintas acciones del hombre como amenazas, como la amenaza condicional la cual consiste en la prevalencia de un interés por medio de un soborno, la amenaza formal que tiene relación con una consecuencia al no ejecutarse bien una acción debida, y la amenaza de alta peligrosidad consistiendo en toda acción que perjudique tanto a individuos, sociedad y el propio Estado, agravando su condición física, material y de estabilidad interna. Asimismo, las amenazas de alto peligro pueden reflejarse en los conceptos de seguridad y defensa de un Estado según lo expresa Saint, (2016) al identificar toda actividad o acción que tenga por finalidad dañar o alterar el orden de una nación.

Por lo tanto, podemos asumir que el termino de amenaza representa toda acción destinada a causar un impacto negativo, sobre todo cuando estas acciones están encaminadas a afectar recursos u objetivos estratégicos, tomando ejemplo en las estructuras de un Estado las cuales están compuestas por diversas áreas de intereses como la económica, política, áreas sociales, instituciones gubernamentales, entre otros factores importantes para el desarrollo humano. De igual forma, este planteamiento es reforzado en la Conferencia Especial sobre Seguridad de la OEA (2003) la cual se plantea un nuevo esquema de amenazas desde un enfoque multidimensional y partiendo desde dos ángulos, como son la amenaza tradicional compuesta por acciones de un Estado hacia otro Estado, y las nuevas amenazas o nuevos desafíos los cuales se constituyen en todas aquellas que no necesariamente vienen de un Estado, y que poseen un carácter de organización y vinculación con actividades delictivas que afecten las normas, leyes o estabilidad de un país y su propia ciudadanía.

2.2.2 Amenazas Tradicionales

En base al Libro de la Defensa Nacional de la República de Nicaragua, Capítulo II, inciso B, las amenazas tradicionales están vinculadas a toda relación o conflicto interestatal o de agenda convencional que incluya todo lo relacionado a intereses nacionales, disputas territoriales y defensa de la soberanía ante cualquier amenaza o injerencia proveniente de un Estado.

Teniendo en cuenta lo expuesto por el Libro de la Defensa Nacional de la República de Nicaragua, podemos manifestar que las amenazas tradicionales pueden concebirse como toda acción de carácter agresiva o disuasoria que ejecuta un Estado hacia otro, con el fin de hacer prevalecer su interés. Las amenazas tradicionales a lo largo de la historia se han destacado por la confrontación militar, ya sea entre dos o más Estados, conociéndose como amenazas externas en lo tradicional, las cuales anteriormente eran impulsadas por intereses ideológicos, dominio de recursos y posesión de un territorio el cual represente un eje clave.

Mediante esto, se desarrollaron eventos de gran magnitud que cambiaron la historia de la humanidad y el propio orden internacional, como fue el caso de la Primera Guerra Mundial y la Segunda Guerra Mundial, resultando ser los conflictos modernos donde se demostró las capacidades de las amenazas tradicionales, sumando a su vez, el periodo de la guerra fría donde las potencias dominantes EEUU y URSS llegaron a implementar nuevas doctrinas y mecanismos dirigidos a afectar directa o indirectamente la estructura del Estado adversario, teniendo en cuenta siempre el desarrollo de un conflicto convencional a gran escala.

De igual forma según Spielman, (2009) las amenazas tradicionales, además de su característica externa, poseen otras variantes como las internas las cuales estas pueden estar sujetas a las problemáticas de orden común de un Estado como las áreas sociales, políticas y económicas, las cuales se pueden convertirse en una alteración al orden mediante situaciones de conflicto sociopolítico, subversiones de carácter ideológico, religioso o de disputa entre ejes o centros de poder económico. En resumen, las amenazas tradicionales son aquellas en donde se producen conflictos de alto grado de violencia y específicamente de orden militar, actualmente esto se puede ver reflejado en disputas limítrofes causadas por circunstancias complejas, sumado a la problemática de escasez y demandas de recursos, lo que incentiva ambiciones expansionistas de buscar y obtener bajo cualquier medio una solución factible.

2.2.3 Amenazas no Tradicionales

Las amenazas no tradicionales o conocidas también como amenazas emergentes, según lo explica Linares, (2003) son aquellas de carácter multidimensional y transnacional, constituyéndose como un peligro grave que afecta el orden y desarrollo de un Estado en sus áreas políticas, económicas y sociales. Causando la perdida de la capacidad de gobernanza y gobernabilidad, puesto que a falta de la presencia del Estado como ente superior de orden y repuesta, se generaría malestares sociales con posibilidad de socavar internamente un país.

Cabe destacar que las amenazas no tradicionales o emergentes actualmente han creado una relación directa con la globalización y sus resultados, como el avance tecnológico principalmente, el cual ha creado medios de interconexión o intercambio de información a través de equipos informáticos lo cuales tienen un elevado alcance hacia las personas y los países. Representando un nuevo campo en donde las amenazas o peligros se extiendan y fortalezcan sus capacidades de impacto e influencia lo que podría repercutir en consecuencias graves para los Estados, y un nuevo desafío para las políticas de seguridad nacional, regional e internacional.

La nueva modalidad de utilizar recursos modernos y adaptarlos para el desarrollo de técnicas para cometer actos delictivos de alta peligrosidad, ha sido una de las principales características que mantienen las amenazas emergentes según lo expone Torres, (2020), tomando ejemplo de lo ocurrido en el año 2002 con el atentado a las torres gemelas, lo cual significo un gran cambio para todo el panorama internacional en base a seguridad nacional y el replanteamiento de la selección de amenazas o quienes realmente representan un riesgo grave a los intereses de los Estados.

Por lo tanto, se asume que las amenazas no tradicionales resultan ser objeto de preocupación para los Estados, ya que estas obstaculizan el avance de un país y contribuyen a la proliferación de estructuras delictivas o bien logran adherirse a otras de mayor estándar de peligrosidad. Estas son conocidas actualmente como el terrorismo, crimen organizado y los ciberataques, del mismo modo se suman otras como el cambio climático el cual ha mostrado tener severas consecuencias para el entorno del ser humano, reorientando las políticas de los Estados y su forma de actuar con respecto a los recursos naturales.

2.2.4 Seguridad Regional

La seguridad regional según Snedden, (2018) es un sistema donde los Estados articulan normas, relaciones y prácticas con el fin de garantizar su seguridad. De este modo, seguridad regional es toda aquella iniciativa que contiene una agenda en común para la estabilidad y desarrollo de sus países como la región en general, optando mecanismos como la homologación de sus intereses en materia de seguridad y defensa. Permitiendo identificar a su vez, los riesgos o amenazas de alto peligro que afecte de manera sistemática a todos los Estados que geográficamente están delimitados en esa región.

Las principales caracteristicas que posee la seguridad regional según Evans, (2013) se destaca por ser un mecanismo de prevención, gestión y reducción de conflictos o amenazas que puedan incidir o perjudicar la seguridad interna de los Estados y la región. Asimismo, el mismo autor plantea que la seguridad regional, es un reto en materia de integración, durabilidad y eficiencia ya que al momento de plantear una estrategia común para beneficiar a los Estados, surge un conflicto de intereses, que de no tener una mediación o un diálogo constante, la iniciativa no logrará concretarse. Por ende, la seguridad regional debe llevarse a cabo mediante la armonización de mecanismos que ayuden no solamenete a obtener los ejes de seguridad deseados, también que los Estados que forman parte de ello se mantengan bajo los lineamienetos establecidos.

En cuanto a ejemplos de seguridad regional mediante mecanismos de integración, se opta por el Sistema de Integración Centroamericano (SICA) el cual mediante el Tratado Marco de Seguridad Democrática en Centroamérica y la Estrategia de Seguridad de Centroamérica, han realizado coordinación, elaboración e implementación de iniciativas y planes preventivos y de seguridad regional. Otro ejemplo de ello, son los organos especializados en materia militar como las Fuerzas Armadas de la Conferencia de Fuerzas Armadas Centroamericanas (FAM-CFAC) y la Junta Interamericana de Defensa (JID), los cuales por su rol en la seguridad soberana de los Estados, se encuentran mejor desarrollados en capacidades y mecanismos de seguridad regional, como estrategías, planes y políticas de defensa.

Además de poseer mayor capacitacion institucional lo que ha permitido la creación de centros especializados contra amenazas, especialmentes las no tradicionales o bien conocidas como las amenazas emergentes, como el crimen organizado, terrorismo entre otros, en concreto cada iniciativa de estos organismos es realizada en base al lineamiento de una seguridad regional.

2.2.5 Ciberespacio

El ciberespacio inicialmente tuvo sus etapas como concepto, el cual procedio inicialmente como cibernética acuñado por Nobert Wiener durante la década de 1940 mediante un estudio sobre los sistemas de comunicación y máquinas. Sin embargo el el término de ciberespacio fue empleado hasta 1984 por el escritor William Gibson en su obra "Nauromante" la cual consistía en presentar de manera ficticia diversos elementos tecnológicos que lograban tener una conección común, mediante un sistema único, el cual los usuarios por medio de una tecnología apropiada, podían interactuar en ese espacio

De igual forma, Romero, (2004) define ciberespacio como un campo relacional en donde ese produce la mayor interactividad entre distintos agentes, lo cual también define la realidad de su estructura, debido a que esta se basa en el mayor intercambio de información. Asi pues, podemos determinar que el ciberespacio se destaca por su naturaleza de origen permanente mediante la comunicación, representanto ser el espacio y medio para realizar una sola acción, añadiendo a su vez otras caracteristicas en base a lo que expone Bernal, (2015) cuando el ciberespacico se desarrolla como un medio inmaterial, sin fronteras físicas, la cohexistencia entre Estados, ciudadanos, organizaciones y conductas aceptables y no aceptables.

Por lo tanto, se presenta una constante dependencia de ciberespacio mediante medios tecnológicos como las Tecnologías de la Información y la Comunicación (TIC) y los medios de carácter digital, creando una nueva forma de interactuar para las sociedades y los Estados al interconectar áreas importantes como los ambitos comerciales, energéticos, transporte, banca y finanzas, comunicación, sistemas de defensa y seguridad nacional, entre otros. Lo cual ha marcado un antes y después en las acciones del ser humano y su entorno, identificandose de acuerdo a la doctrina militar del Ejercito de Estados Unidos y países europeos, como los dominios o dimensiones para la realización de las demoninadas operaciones multidimensionales (tierra, mar, aire, espacio y ciberespacio) de tal modo que representa un nivel estratégico ya que facilita por su medio digital, generar efectos tangibles sobre objetivos físicos.

Cabe destacar que según los autores Martinez, Ceceñas, & Ontiveros, (2014), el ciberespacio no puede ser interpretado con el internet, debido que el ciberespacio es un espacio que posibilita la mayor interaccion e intercambios de comunicación, mientras que el internet es todo aquello relacionado a servicios mediante la delimitación de redes y aplicaciones.

2.2.6 Ciberseguridad

La conceptualización del término de ciberseguridad ha variado de acuerdo a los avances tecnológicos y los riesgos que esta presenta al ser vulnerable ante ciberamenazas o ataques a través del ciberespacio. La Unión Internacional de Telecomunicaciones (ITU) define ciberseguridad como el conjunto de herramientas, políticas, métodos de gestión de riesgos y de seguridad tecnológica que puedan utilizarse para proteger los medios informáticos y los usuarios en el ciberentorno.

Del mismo modo, la Junta Interamericana de Defensa (JID) adjudica que la ciberseguridad es todo fundamento que tiene por objetivo la aplicación de medidas de seguridad para la protección y la libertad de acción en el ciberespacio, agregando a su vez que todo medio informático o bien que forma parte de las Tecnologías de la Información y Comunicación (TIC) tenga condiciones efectivas en su aseguramiento para evitar afectaciones o ataques a sus componentes. Las principales características que posee la ciberseguridad según el Ministerio de Defensa de España, en la Estrategia de la Información y Seguridad en el Espacio (2014) se contemplan en la preparación de las condiciones en materia prevención y detección, seguridad, resiliencia y capacitación lo cual permite dismunir las vulnerabilidades tecnológicas.

En relación con lo expuesto anteriormente, se puede plantear que la ciberseguridad es un conjunto de herramientas para proteger y asegurar una entidad o componentes tecnológicos de vital importancia, ante una amenaza o un ciberataque que surja por medio del ciberespacio permitiendo brindar un nivel de seguridad informática factible. Los autores Chamorro, Fernández, López, & Fernández, (2016) señalan que la ciberseguridad en sus inicios solamente se trataba de proteger la información de accesos ilegales, interrupciones, modificaciones de red entre otras acciones comunes de menor impacto, por lo que solamente estaba dirigida hacia un solo enfoque común sin abarcar un proceso más desarrollado en sus capacidades.

En cambio, en la actualidad con las nuevas transformaciones tecnológicas a causa del avance de la globalización y otros factores como la llamada revolución industrial 4.0, se ha reflejado una nueva visión e implementación del concepto de ciberseguridad, refiriéndose al desarrollo continuo de capacidades preventivas que aporten a la creación de niveles de resiliencia que beneficien con una sólida protección a los medios como las TIC y a los propios usuarios de amenazas cibernéticas de alta peligrosidad como la ciberdelincuencia.

2.2.7 Ciberdefensa

En base a la Junta Interamericana de Defensa, en su Guía de Ciberdefensa (2020) delimita el termino ciberdefensa a toda capacidad de proteger y defender los intereses nacionales frente a ciberamenazas de gran magnitud, destacando elementos fundamentales o sus principales características que definen su modo de operación, como la defensiva y ofensiva, manteniendo lazos de cooperación con otras instituciones, principalmente aquellas que poseen carácter de seguridad nacional. A su vez, el Ministerio de Defensa de Chile enfatiza que la ciberdefensa está delimitada para brindar una repuesta eficiente hacia aquellas áreas que son de vital importancia para el funcionamiento y existencia de un Estado, principalmente aquellas relacionadas a infraestructuras críticas, componentes logísticos y la propia ciudadanía.

Por consiguiente, se considera que el término de ciberdefensa se define por su vinculación en la seguridad y defensa de un Estado y sus componentes, además que tradicionalmente este concepto ha sido acogido por organizaciones de carácter militar o dedicado a la seguridad interna de un Estado estrechando su vinculación directa en asuntos de seguridad nacional. La ciberdefensa en su fundamentación suele ser parte de una política de defensa, por lo tanto, debe de caracterizarse por ser un instrumento de constante adaptabilidad hacia nuevos desafíos y gozar de una capacidad eficiente en su cobertura hacia los ejes vulnerables de un país ante cualquier peligro que surja o quiera afectar utilizando medios tecnológicos o bien por medio del ciberespacio.

De igual forma la Organización del Tratado del Atlántico Norte (OTAN) mediante El Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE) hace relevancia al modo de operación que debe de tener una ciberdefensa eficaz resaltando la tecnología, operaciones, estrategia y el marco de la ley. Añadiendo a su vez que las amenazas cibernéticas hacia la seguridad nacional de los Estados representan uno de los principales desafíos en el panorama actual en un mundo cada vez más interconectado y dependiente de la tecnología.

De tal modo que la ciberdefensa debe de estar altamente preparada para defender, neutralizar y adaptarse ante cualquier hecho perjudicial que atente contra la estabilidad y la seguridad de un Estado, haciendo énfasis a la ciberamenazas las cuales son cada vez más persistentes y peligrosas para cualquier capacidad o recursos importante que no posea una seguridad eficiente.

2.2.8 Ciberresiliencia

Según Carrasco, (2015) la ciberresiliencia puede llegar a tener un carácter complejo en cuanto a su relación con las infraestructuras digitales o TIC, debido que la ciberesiliencia no solamente es un trazo más de un método de seguridad como comunmente se menciona. Esto requiere o implica más de una gestión de seguridad que lleva a aplicar otras acciones como tranformaciones o mejoramiento de una infraestructura crítica en riesgo, para alcanzar una mejor resiliencia tanto en su protección externa como interna, completanto asi una estrategía de ciberseguridad eficiente.

Las principales caracteristicas que posee la ciberesiliencia se destacan en la creación de metodos dedicados a la prevensión, detección y gestión de incidentes de seguridad, asímimo promueve la armonización entre las instituciones gubernamentales de un Estado y los marcos jurídicos para el desarrollo de una política integral y coordinada. La cual permita crear niveles de cooperación eficaces para la consolidación de una seguridad cibernetica factible, dibido que la ciberresiliencia es constante, permanente y abarca los campos necesarios para una mayor efectividad ya que no puede haber un Estado con una infraestructura tecnólogica segura sin un principio de resiliencia.

De acuerdo con Pinilla, (2019) la resiliencia en las infraestructura crítica, trata de aumentar la calidad en la gestión de riesgos y amenazas, ampliando esta modalidad a todo el centro operacional de la misma, como son los Estados, mediante sus instituciones y las propias personas. La ciberresiliencia es un proceso continuo que requiere de muchas capacidades de apatación a los nuevos riesgos y amenazas, los cuales surgen y se fortalecen mediante un avance tecnólogico poco seguro.

Tomando ejemplo en la ciberdeliencuencia, cuya modalidad tiene alcance efectivo en sus daños, ademas de poder adaptarse y unirse a otros formas de delitos, conviertiendose en una amenaza grave para la seguridad de un Estado, y sus componentes esenciales como la economía, sus infraestructuras críticas o recursos que le permiten desarrollarse, los propias instituciones y la población en general. En efecto, la ciberresiliencia es necesaria para fortalecer y dirigir acciones que permitan la seguridad de recursos estrategicos de un Estado asi como preservar la eficiencia de sus propios mecanismos.

2.2.9 Infraestructura Crítica

Si bien el concepto de infraestructura crítica se puede adecuar en base a los recursos que cada nación posee, este termino se aborda desde un punto de vista estratégico y vital, debido a la importancia que representa para el funcionamiento de un país, como expresa Giraldo, (2015) cuando compara una infraestructura crítica con un sistema nervioso central el cual es indispensable para el desarrollo y sostenimiento de cualquier acción, más aún cuando se trata de un Estado, el cual necesita de objetivos vitales para que un pais logre avanzar y existir, ya sea en factores económicos, material, político, de seguridad, entre otros.

De igual forma con lo que implica el avance tecnólogico de la globalización, las infraestructuras críticas han tomado un papel cada vez mas fundamental para los países, especialmente en materia de telecomunicaciones, adecuando los conceptos, estrategias y seguridad de acuerdo al valor que estas tienen, tal como lo expone Miranzo & Río,(2014) al determinar que las infraestructuras críticas representan en la modernidad toda instalación, redes, servicios y equipos físicos que mantengan una relación directa tanto con estructuras gubernamentales como para el desarrollo y beneficio de los ciudadanos.

Por otra parte, los autores anteriormente mencionados, señalan si una o el conjunto de las infraestructuras críticas de un pais llega a tener alguna alteración, interrupción o destrucción, ocasionaria un severo impacto negativo, tanto a la sociedad en general como las bases gubernamentales de un Estado, obteniendo como resultado una inestabilidad interna y un detrimento en los niveles de seguridad en sus sectores primordiales.

De este modo, resulta importante que las infraestructuras críticas de un Estado gozen de altos niveles de seguridad, tanto de aspecto fisico como sus componenetes tecnólogicos-dígitales internos. Esto se puede lograr mediante una capacidad de resiliencia la cual según Pinilla, (2019) es toda capacidad que ayuda a identificar un riesgo y crear un entorno seguro hacia un objetivo vital el cual se vea amenazado fuera de su enorno, ádemas de tomar medidas contra esa amenaza lo cual resulta un punto estrategico para la protección y aseguramiento de las infraestructuras críticas.

2.2.10 Tecnologías de la Información y Comunicación

En base al Informe sobre Desarrollo en Venezuela del Programa de las Naciones Unidas para el Desarrollo PNUD (2002), las Tecnologias de la Informacion y Comunicaccion (TIC) se concibe como el universo o el espacio donde se integran medios tecnológicos de comunicación y equipos audiovisuales, los cuales permiten la creación y el registro de contenidos digitales, en los cuales los usuarios pueden acceder a ellos por medio de equipos iguales o que estos posean el nivel de conección hacia el internet.

El autor Duarte, (2008) hace referencia que las TIC se comprenden principalmente por el uso de equipos como ordenadores y computadoras, lo cual ha definido comunmente su identificación y particularmente su uso en el quehacer del ser humano, aumentando cada vez mas el desarrollo o la evolución de las TIC. De igual forma, Belloch, (2012) presenta algunas de las principales caracteristicas que poseen las Tecnologias de la Información y Comunicación (TIC) de acuerdo a los diversos ambitos en los cuales se destaquen o se utilizen, definiendo algunas como la interactividad, interconexión, digitalización, innovación, diversidad y automatización, concretandose igualmente en dos factores esenciales que determinan su composición, como son la máxima penetración en todos los sectores humanos y su influencia en los diferentes procesos de producción.

Asimismo, a causa del factor de la globalización y los avances en el desarrollo de nuevas áreas tecnólogicas, las TIC se han conformado o bien, forman parte de sectores exclusivos de carácter importante o estratégico, como lo expresa Martínez, (2006) al relacionar el papel que desempeñan los equipos de comunicación, interconección en los sistemas de seguridad y defensa del siglo XXI. Además que estos deben enfrentar a nuevas modalidades, capacidades e impactos de amenazas que hacen uso de las TIC como herramienta para lograr su objetivo, llegando a conocerce como guerras electrónicas y amenazas híbridas, las cuales hacen uso de las TIC y medios como el ciberespacio para cometer acciones de gran peligro y daño hacia un recurso estratégico, en este caso los actores se pueden contemplar en organizaciones y los Estados.

2.2.11 Amenaza Persistente Avanzada

El autor Cortés, (2017) hace énfasis a los diversas amenazas o tipos de ataques que perjudican a la seguridad cibernetica de un sistema, especialmente aquellos que tienen como blanco a un Estado y sus estructuras tecnólogicas de mayor importancia. Los cuales resultan ser los de mayor peligrosidad, debido a que estos poseen una planificación dirigida hacia recursos específicos, además de poseer una capacidad de adaptación y técnicas que le permitan fortalecer sus alcances e impactos, este tipo de accionar delictivo se conoce como Amenaza Persistente Avanzada (APT) por sus siglas en inglés.

Las Amenazas Persistentes Avanzadas (ATP) de acuerdo con Parra, (2019) son el conjunto de tácticas, técnicas y procedimientos los cuales estan diseñados para persistir en su ataque hacia los recursos vitales de una estructura de gran valor como son las empresas, organizaciones y Estados. Sumando que las ATP logran aprovecharse de las vulnerabilidades para mantener un alzamiento constante en su afectación, además que le permite que pase desapercibido. Las ATP estan compuestas por individuos, organizaciones incluso pueden estar formadas por Estados los cuales matienen un perfil sigiloso o desconocido para beneficiar su manera operativa, reflejada en el ciberespionaje o ciberinteligencia. El cual ambas acciones para las ATP consisten, según Cabello, (2021), en estudiar y evaluar los componentes y el desarrollo un objetivo determinado para obtener la mejor información y ejecutar con mayor presición

De igual forma la Junta Interamericana de Defensa, en su Guía de Ciberdefensa (2020) presenta las principales caracteristicas que poseen las Amenazas Persistentes Avanzadas (ATP) comenzado que estas tienen objetivos claros y especificos, un potencial nivel de planeación y participación, añadiendo sus técnicas evasivas con una extensa duración en sus acciones con intentos repetitivos. También su forma operativa consta de 5 fases, la preparación, acceso, persistencia, ejecución y anonimización, las cuales se pueden reflejar en los ejemplos que menciona Parra, (2019) en base a los impactos de las APT en latinoamérica, destacando que la región al tener un aumento considerable en los conflictos geopolíticos y económicos, se ha convertido en un blanco fácil para atacar a los Estados y perjudicar sus sistemas internos o componetes informáticos que se sitúan en áreas sencibles, conviertiendose en un alto peligro tanto para organizaciones importantes como a los propios Estados, debido que estos poseen un alto valor en sus componentes tecnólogicos.

2.2.12 Ciberdelincuencia

Aunque no se encuentre una definición concreta en cuanto al término de ciberdelincuencia, podemos partir de acuerdo a la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) que la ciberdelincuencia es aquella acción que ataca principalmente los sistemas, datos y redes, ya sea mediante el uso o contra las Tecnologías de la Información y Comunicación, conocidas como (TIC); del mismo modo, la Comisión Europea desde la Dirección General de Migración y Asuntos de Interior, agrega que la ciberdelincuencia se relaciona con otros delitos como el terrorismo y el crimen organizado, por lo que sus acciones pueden estar comprendidas no solo por un individuo, también por grupos, Estados u organizaciones de alto perfil delictivo.

Cabe destacar que la ciberdelincuencia al ser un delito informático con alta capacidad de delimitar, penetrar y perjudicar recursos estratégicamente importantes, logra establecer un contraste con los ciberdelitos comunes, los cuales en su mayoría se ejecutan a través de una red o propiamente del internet con un menor grado de afectación si se compara con las consecuencias que puede generar un ciberataque dirigido a un recurso de vital importancia para un Estado, sobre todo cuando este forma parte de su desarrollo y seguridad nacional tal como lo afirma el Servicio de Seguridad Central de la Agencia de Seguridad Nacional Norteamericana (NSA-CSS) al evaluar su alcance y gravedad de impacto.

Según Antonio, (2020) existen dos eventos que reflejaron el modo de operación y alcance que pueda tener la ciberdelincuencia, especialmente en vulnerar la seguridad nacional de un Estado, tomando ejemplo en Tallin, Estonia 2007, durante una situación de tensión política la cual conllevó a un ciberataque hacia las redes de organismos financieros y gubernamentales de dicho Estado, el otro ejemplo concreto fue durante la invasión a Osetia del Sur 2008, al demostrar las vulnerabilidades de los sistemas de red y telecomunicaciones que tienen un Estado ante las capacidades estratégicas que posee el ciberespacio.

Tomando en cuenta los dos ejemplos anteriormente mencionados, podemos asumir que las capacidades de la ciberdelincuencia pueden convalidarse o utilizar el entorno o situación momentánea para colocarse en una posición de mayor incidencia o ataque por lo que la mayor característica que posee actualmente es la adaptación con otras amenazas que debiliten la seguridad o estabilidad de un Estado, llegando a un solo objetivo común de provocar daños severos hacia los recursos esenciales de país, lo cual también repercute en afectaciones directas a la ciudadanía.

2.2.13 Ciberamenaza

Las ciberamenazas han tenido su desarrollo o evolución, de acuerdo a los intereses de quienes la provocan, sobre todo en el contexto de la globalización. Según Fernández, (2017) anteriormente las ciberamenazas eran conocidas solamente por actos o acciones de violación a la privacidad, robo de información personal, acceso no autorizado a tarjetas de crédito, dirección empresarial entre otros, los cuales son tomados como delitos comunes. Sin embargo, con el avance de la tecnología se ha introducido nuevas dimensiones que han transformado las actividades humanas, sobre todo aquellas que se relacionan con elementos delictivos que perjudiquen la estabilidad de una sociedad o Estado como el caso de las ciberamenazas.

Las ciberamenazas con base a Díaz, (2016) se define como toda actividad delictiva que se desarrolla a través del ciberespacio, utilizandolo como medio para cometer acciones que perjudiquen un objetivo. Estas se caracterizan por estar relacionadas con individuos, organizaciones, grupos criminales, incluso Estados los cuales tienen un alto grado de capacidad para afectar o degradar la seguridad cibernetica de un objetivo de alto valor, lo cual también la delimitación de su objetivo, les permite categorizarse ya sea por tener intereses estrategícos, economícos, sociales y políticos.

De este modo, las ciberamenazas han multiplicado su capacidad de ejercer daño sobre cualquier área, esto se debe a la acelerada expansión del ciberespacio con el avance tecnológico, más aún cuando las empresas, organizaciones o los Estados no tengan una protección o defensa contra estos peligros. El ciberespacio en este caso representa un factor de suma importancia ya que este es una herramienta o medio que permite concretar el ciberataque dirigido por la ciberamenaza.

El ciberataque según Gazapo & Nieva, (2016) es una acción directa encaminada a afectar sistemas de información, los cuales forman parte de un eje esencial ya sea para un individuo, empresa o institución gubernamental, teniendo como consecuencia afectaciones graves para los medios que operan mediante redes, servicios almacenamientos de información y sumado a un degradamiendo en la estabilidad interna de un Estado. Por tanto las ciberamenazas son un elemento de alto peligro en el ciberespacio con capacidad de provocar daños a gran escala, más si esta logra penetrar sin alguna defensa efectiva que la contrarreste, sumado a las capacidades tecnólogicas que posea el area afectada.

2.2.14 Política de Defensa y Estrategia de Seguridad

La Ley No. 919, Ley de Seguridad Soberana de la República de Nicaragua, en su Art.5, inciso 12, define como política de defensa a todo el conjunto de acciones, líneas y directrices que son dirigidas y responden ante un marco constitucional. Asimismo, según el Ministerio de Defensa del Gobierno de España, la política de defensa es el conjunto donde se estipulan los objetivos de la defensa nacional y los recursos y acciones, los cuales representan las herramientas para lograr o cumplir una misión dentro de esta materia.

De igual forma, el Ministerio de las Fuerzas Armadas de Francia, plantea que las principales características de una política de defensa se destacan principalmente en que están sujetas a un marco normativo supremo que la dirige, en este caso se refiere a las constituciones de un Estado, una ley de seguridad o programación militar, el libro blanco y cuenta con las capacidades necesarias de órganos de seguridad y defensa de una nación.

En cuanto al concepto de estrategia, según Contreras, (2013) se conoce o se basa en la coordinación de acciones para cumplir un objetivo, por lo tanto, se entiende como una toma de decisiones competitiva la cual a su vez requiere de una planeación. Bajo el concepto militar la estrategia se convierte en el arte de cooperar, y dirigir las operaciones militares ya sea para un uso determinado o en la guerra mediante la identificación de un objetivo de alto valor, de la misma manera la seguridad se entiende como toda medida empleada para crear una condición de estabilidad y control.

En este sentido, el autor Francesch, (2015) presenta que una estrategia de seguridad es toda aquella en donde se evalúan amenazas o desafíos los cuales presenten un grave peligro para un sector de suma importancia o de mayor relevancia como el caso de organizaciones y los Estados. Las principales características que posee una estrategia de seguridad se determinan en la alta capacidad de analizar o estudiar áreas vitales como los factores económicos, políticos, sociales los cuales actualmente representan el entorno humano y su vivencia, también donde convergen cada una de sus acciones. En concreto, el concepto de estrategia es un elemento muy dinámico, que responde a un área en específico como puede ser la seguridad nacional de un Estado-nación los cuales precisa de nuevos lineamientos o políticas que responde ante dificultades o necesidades de una mejor amplitud, superando objetivos trazados y capacidades ya empleadas.

2.3 Marco Teórico

A pesar que actualmente tanto la ciberseguridad y ciberdefensa no contemplan una visión meramente teórica que permita un mayor análisis o estudio de su estructura, se puede tomar de referencia, algunos aportes los cuales se relacionan directamente en el accionar y en los resultados de esta temática, tomando ejemplo en los mecanismos que poseen los Estados para abordar la ciberseguridad y ciberdefensa tanto interno como externo, sobre todo en el con texto del desarrollo tecnológico y de seguridad. Por tanto, en el presente marco teórico, se abordarán los siguientes planteamientos teóricos:

2.3.1 Teoría de la Globalización

La teoría de la globalización según Flores, (2016) en su estructura se puede entender como todo lo relacionado a los sistemas de interconexión o comunicación global en los cuales los Estados, organizaciones, grupos sociales y los propios individuos interactúan en un esquema más fluido, sumado al auge y fortalecimiento de otras áreas de interés como el desarrollo económico y el avance tecnológico. Por tanto, al nivel internacional surgen diversos actores los cuales tienen un nivel de incidencia importante, destacándose en las empresas transnacionales, organizaciones internacionales y los propios Estados los cuales forman parte de las grandes tendencias que configuran el escenario internacional moderno.

Para la presente tesis, la teoría de la globalización resultada factible debido que, por medio de esta, se resaltan los principales espacios que contribuyen al desarrollo y avance de la interconexión global como son el factor tecnológico, la modernización de la sociedad y las propias instituciones estatales lo que delimita el campo de acción de los esquemas cibernéticos. De igual forma, la globalización es el campo principal donde surgen las acciones que moldean el entorno del ser humano ya sea para su propio beneficio o perjuicio, destacando las amenazas cibernéticas como la ciberdelincuencia que a su vez, por la transformación tecnológica que implica el nuevo desarrollo global de la tecnología, se necesita de repuesta eficaces y factibles como son en este caso la ciberseguridad y ciberdefensa, por lo tanto la teoría de la globalización representa ser el espacio principal donde surgen estos esquemas los cuales son parte esencial de la actualidad.

2.3.2 Teoría de Seguridad Nacional

De acuerdo con Villarreal, (2009) la seguridad nacional es un conjunto que se constituye en una esencia y deber del Estado teniendo como base el arte de gobernar y garantizar que los individuos tengan las menores vulnerabilidades posibles ante cualquier amenaza, este tipo de concepto logro concretarse en los términos de seguridad nacional. La seguridad nacional es una macroteoría militar del Estado, compuesta por una sistematización de conceptos o acciones relacionadas a la geopolítica y la estrategia de intereses con la finalidad de alcanzar un objetivo que tenga por resultado la estabilidad y el fortalecimiento de interno o externo de un Estado que ayude a su vez, crear las condiciones propias para el desprestigio y erradicación de alguna amenaza o algún enemigo que desee perjudicar la estabilidad de una nación y su ciudadanía.

Este concepto tuvo su mayor auge a finales de la Segunda Guerra Mundial, adoptado principalmente por países occidentales en el marco de la guerra fría la cual asentó los postulados esenciales como la conceptualización de una guerra generalizada y un conflicto bipolar. En la actualidad con el auge de las nuevas tecnologías y los nuevos escenarios de la globalización, la seguridad nacional se ha adaptado hacia los nuevos desafíos que implican una mayor adaptación de sus términos ante un mundo cada vez más interconectado, a su vez el rol que desempeñan los Estados a través de sus distintos mecanismos para salvaguardar su estabilidad y sus intereses.

Para la presente tesis, la seguridad nacional resulta factible por su rol en mantener la estabilidad y el desarrollo interno de un Estado, puesto que las medidas de ciberseguridad y ciberdefensa forman parte de una acción encaminada a proteger y defender a un objetivo estratégico ante cualquier amenaza, lo que representa el accionar común de una seguridad nacional. De igual forma la conceptualización de seguridad nacional aporta a comprender mejor los impactos que esta puede tener al nivel externo cuando uno o más Estados tienen un grado de seguridad, contribuyendo a generar un entorno con mayor confianza y reducir las vulnerabilidades ante cualquier injerencia.

2.3.3 Teoría sobre Cibercriminología

La cibercriminología es un área que forma parte de la criminología la cual tiene por objetivo el estudio y análisis de la delincuencia en el ciberespacio y sus repercusiones de acuerdo a lo establecido por el Dr. Kyung Shick. De igual forma la cibercriminología forma parte de las criminologías especificas la cual permite clasificar los tipos de hechos, en este caso la cibercriminología hace un contraste con el delito cometido a través de medios informáticos y el propio ciberdelito, el cual el primero se refiere a toda acción delictiva que se ejecute con o contra equipos informáticos o medios TIC y el segundo hace énfasis a toda actividad ilegal que es ejecutada a través de un ordenador y que pueden estar sujetas a penalización en marcos legales o códigos específicos.

Para la presente tesis la definición de cibercriminología fortalece el termino y la identificación de los delitos cometidos a través de medios tecnológicos y su especificación, en este caso se puede identificar el accionar de la ciberdelincuencia como un delito internacional que utiliza y a su vez perjudica medios relacionados a las TIC, que se sitúan en áreas estratégicas, lo cual repercute en una alteración grave a la estabilidad de un ente importante, en este caso los Estados de la región centroamericana.

2.3.4 Realismo en las Relaciones Internacionales

El Realismo en las Relaciones Internacionales por parte de uno de sus principales teóricos como Hans Morgenthau, sostiene que los Estados son los principales actores en el área internacional por medio de su característico predominio del poder, actuando mediante sus intereses, colocando objetivos estratégicos que permitan alcanzar su desarrollo, estabilidad y existencia, además de garantizar su propia seguridad.

Para la presente tesis, el Realismo en las Relaciones Internacionales de Hans Morgenthau, es una base la cual se puede partir en diferentes aspectos, desde la aceptación del Estado como el primer ente que desarrolla el sistema internacional y la estructuración de sus objetivos los cuales están trazados para lograr la existencia del mismo En el caso de la ciberseguridad y ciberdefensa por medio de esta teoría, representaría un valor estratégico para el Estado no solamente en la parte de salvaguardar sus componentes internos, basados en la seguridad, también porque esta temática puede ser abordada desde los aspectos de homologación de intereses que permita la búsqueda de un bien común para todas las partes.

2.4 Marco Legal

El presente marco legal se estructura primeramente de acuerdo a los mecanismos internacionales en materia de desarrollo tecnológico y ciberseguridad, los cuales representan a través de convenios, la voluntad y la armonización de los Estados al nivel internacional para cooperar en áreas tecnológicas y ciberseguridad, abordando a su vez la problemática de la ciberdelincuencia como una amenaza a la seguridad nacional de las naciones. De igual forma este marco legal está compuesto por los mecanismos de integración centroamericana como los tratados y estrategias en materia de seguridad regional y cooperación tecnológica, permitiendo convalidación de los intereses de los Estados centroamericanos para un beneficio común.

Por lo tanto, el presente marco legal se estructura de la siguiente manera, Convenio Internacional de Telecomunicaciones en Ginebra, Convenio de Budapest sobre Delitos Cibernéticos, Protocolo de Tegucigalpa a la Carta de la Organización de Estados Centroamericanos (ODECA), Tratado Marco de Seguridad Democrática en Centroamericana, Estrategia de Seguridad de Centroamérica (ESCA), Estrategia Regional Digital para el Desarrollo de la Sociedad de la Información y el Conocimiento SICA**,** y las respectivas cartas magnas, leyes, códigos, decretos e instituciones gubernamentales que abordan o logran contribuir a la formulación de iniciativas en ciberseguridad y ciberdefensa.

2.4.1 Convenio Internacional de Telecomunicaciones en Ginebra

El convenio Internacional de Telecomunicaciones suscripto en Ginebra el 21 de diciembre de 1959, tiene por objetivo “mantener y ampliar la cooperación internacional para el mejoramiento y el empleo racional de toda clase de telecomunicaciones, asimismo favorecer el desarrollo de los medios técnicos y su más eficaz explotación, a fin de aumentar el rendimiento de los servicios de telecomunicación, acrecentar su empleo y generalizar lo más posible su autorización por su público, armonizar los esfuerzos de las naciones para la consecución de estos fines comunes, de igual forma este convenio coordinará los esfuerzos para eliminar toda interferencia perjudicial entre las estaciones de radiocomunicaciones de los diferentes países y mejorar la utilización del espectro de frecuencias radioeléctricas” (Objeto de la Unión, Art.3, Convenio Internacional de Telecomunicaciones 1959).

2.4.2 Convenio de Budapest sobre Delitos Cibernéticos

En el marco internacional se toma como ejemplo concreto el primer convenio multilateral en materia de ciberdelitos como es el Convenio de Budapest sobre Delitos Cibernéticos el cual representa uno de los principales ejes que conducen a la elaboración de una política de ciberseguridad o ciberdefensa. Esta iniciativa fue llevada a cabo por el Consejo de Europa, Japón, Canadá entre otros los cuales firmaron el 23 de noviembre del 2001, entrando en vigor en el año 2004. Actualmente más de 60 países han rectificado este convenio, de los cuales 4 (Costa Rica, República Dominicana, Panamá y Guatemala) pertenecen a la región centroamericana y 2 (Honduras y El Salvador) se encuentran en proceso de firma.

El Convenio de Budapest tiene por objetivo "prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen contra dichos delitos, facilitando su detección, investigación y sanción, tanto al nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable".

2.4.3 Protocolo de Tegucigalpa a la Carta de la Organización de Estados Centroamericanos (ODECA)

El Protocolo de Tegucigalpa constituye la máxima estructura orgánica regional que refleja la voluntad de los Estados centroamericanos con el fin de alcanzar la integración, la paz, la libertad y el desarrollo regional. El protocolo de Tegucigalpa fue suscrito el 13 de diciembre de 1991, el cual logró la conformación del Sistema de la Integración Centroamericana, conformado por Belice, Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panamá y República Dominicana,

El Protocolo de Tegucigalpa tiene por objetivos principales "consolidar la democracia y fortalecer sus instituciones sobre la base de la existencia de Gobiernos electos por sufragio universal, libre y secreto, y del irrestricto respeto a los Derechos Humanos, concretar un nuevo modelo de seguridad regional sustentado en un balance razonable de fuerzas, el fortalecimiento del poder civil, la superación de la pobreza extrema, la promoción del desarrollo sostenido, la protección del medio ambiente, la erradicación de la violencia, la corrupción, el terrorismo, el narcotráfico y el tráfico de armas" (Naturaleza, Propósitos, Principios y Fines, Protocolo de Tegucigalpa 1991)

2.4.3 Tratado Marco de Seguridad Democrática en Centroamérica

El Tratado Marco de Seguridad Democrática en Centroamérica fue impulsado para concretar un modelo de seguridad regional sustentado, fortaleciendo el desarrollo democrático de los Estados firmantes. Este tratado entro en vigor el 15 de diciembre de 1995 en San Pedro Sula, siendo sus firmantes Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá. Este tratado tiene por objetivo "el fortalecimiento y perfeccionamiento constante de las instituciones democráticas en cada uno de los Estados, para su consolidación mutua dentro de su propia esfera de acción y responsabilidad, por medio de un proceso continuo y sostenido de consolidación y fortalecimiento del poder civil, la limitación del papel de las fuerzas armadas y de seguridad pública a sus competencias constitucionales y la promoción de una cultura de paz, diálogo, entendimiento y tolerancia basada en los valores democráticos que les son comunes, el mantenimiento de un diálogo flexible y la colaboración mutua sobre los aspectos de la seguridad" (Título I, Estado de Derecho, Art.1, inciso a y c, 1995).

2.4.5 Estrategia de Seguridad de Centroamérica (ESCA)

La Estrategia de Seguridad de Centroamérica fue creada el 12 de diciembre del 2007 durante la XXXI Reunión Ordinaria de Jefes de Estado y de gobierno del SICA, en Guatemala, la cual fue motivada para preservar e impulsar acciones de seguridad regional, el desarrollo sostenible y el fortalecimiento institucional. De igual forma el ESCA tuvo diferentes etapas para fortalecer su contenido, adaptándolas a las nuevas demandas de seguridad en la región, ejemplo de ello fue la Conferencia Internacional de Seguridad de apoyo a la ESCA, ejecutada del 20 al 23 de junio del 2011, con la presencia de más de 50 delegaciones, declarando apoyo absoluto para la búsqueda de mejores soluciones y abordar los problemas de Centroamérica de manera común.

Los países firmantes de esta estrategia, son Belice, Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panamá y República Dominicana, los cuales, mediante la ESCA, coordinan, fortalecen y gestionan políticas de seguridad que permitan crear mejores niveles de seguridad en la región, así como mejorar las condiciones internas de cada Estado, para obtener altos índices de estabilidad y orden.

La ESCA tiene por misión el “establecer los componentes y actividades necesarias para fortalecer, la seguridad de las personas y sus bienes en la región centroamericana permitiendo a nuestros pueblos alcanzar los objetivos del desarrollo humano sostenible, integrar los diferentes esfuerzos que realiza la región en materia de seguridad a fin de armonizarlos y obtener mejores resultados, facilitar la coordinación e intercambio de información y experiencias entre las diversas instancias y agencias operativas de la región para combatir más eficazmente las actividades delictivas regionales, identificar y gestionar las necesidades financieras, de recursos y de formación que demandan las instituciones encargadas de velar por la seguridad; desarrollar políticas, programas, estrategias y acciones que permitan la prevención en los siguientes temas: violencia juvenil, violencia armada, violencia de género, tráfico ilícito y trata de personas, prevención desde lo local, y los efectos de los desastres naturales en especial los provocados por el cambio climático” (Objeto General y específicos, Estrategia de Seguridad de Centroamérica, 2007).

2.4.6 Estrategia Regional Digital para el Desarrollo de la Sociedad de la Información y el Conocimiento SICA

La Estrategia Regional Digital del SICA es producto de los compromisos en la Cumbre Mundial de la Sociedad de la Información (CMSI) celebrada en Ginebra en el año 2003, la cual consistió en orientar acciones comunes a construir una sociedad más desarrollada y actualizada en los medios tecnológicos, lo cual aporte a su propio beneficio, contribuyendo a su vez al desarrollo sostenible y los principios de la Carta de las Naciones Unidas.

La presente estrategia tiene por objeto “Proporcionar a los países miembros del SICA un entorno facilitador para que avancen de manera coordinada y armonizada, en la implementación de iniciativas regionales públicas y privadas, donde el diálogo y el intercambio de experiencias promuevan el desarrollo de la sociedad de la información y el conocimiento en la región; contribuyendo al desarrollo económico, político y social en beneficio de la población centroamericana”. De igual forma se añade sus prioridades las cuales son establecidas en la Cumbre Extraordinaria de Jefes de Estado y de Gobierno de los países miembros del SICA para el relanzamiento del proceso de la integración centroamericana, celebrada en la ciudad de San Salvador el 20 de julio de 2010, las cuales se agrupan en los cinco grandes pilares cuyos objetivos se describen a continuación: Seguridad Democrática, Cambio Climático y Prensión de Desastres,

Integración Social y Lucha contra la pobreza, Integración Económica, y Fortalecimiento Institucional.

2.4.7 Belice

El Estado de Belice hasta la fecha no posee en su carta magna o bien un decreto bajo ley que establezca alguna iniciativa de ciberseguridad y ciberdefensa, solamente posee leyes reguladoras como la Ley No 229, Ley de transacciones electrónicas/ art.9 que define la movilización de capitales y la Ley No 95, Ley de pruebas electrónicas/ art.12 en cuanto a la autoría de las firmas y la Ley de telecomunicaciones parte VIII art.47 a 55 en la formalidad de establecimientos de equipos de comunicación.

2.4.8 República de Guatemala

En la República de Guatemala se encuentra la iniciativa que dispone aprobar la Ley de Prevención y Protección contra la Ciberdelincuencia, la cual tiene por objetivo "la creación de figuras delictivas, y la adecuación de normas penales existentes, para hacer frente a la ciberdelincuencia. Así mismo, se estipulan reglas procesales necesarias para incorporar los medios de prueba digitales que permitan la obtención de evidencias y pruebas electrónicas en el proceso penal y la creación de órganos competentes para una investigación eficaz y la cooperación internacional en la materia" (Iniciativa No.5601, Título I, Disposiciones Generales y Elementos Conceptuales, Capítulo I, Objeto, Bienes Jurídicos Tutelados y Ámbito de Aplicación, Art. 1, 2019).

De la misma manera se comprenden otros mecanismos jurídicos como el Código penal de Guatemala, decreto N0. 17-73, Capitulo VII De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos los cuales ayudan al fortalecimiento de la integridad tanto del Estado como del propio ciudadano, así como la Estrategia Nacional de Seguridad Cibernética aprobada en el 2018. Sumando en la parte de ciberdefensa el Comando de Informática y Tecnología, del Ministerio de la Defensa Nacional de Guatemala, teniendo como misión la administración de los sistemas electrónicos de información, además de facilitar la toma de decisiones tanto del Ejército como del Estado Guatemalteco.

2.4.9 República de El Salvador

En la Constitución de la Republica de El Salvador se resalta protección y privacidad de los medios TIC, cuando expresa que "la correspondencia de toda clase es inviolable, interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los casos de concurso y quiebra. Se prohíbe la interferencia y la intervención de las comunicaciones telefónicas" (Titulo II Los Derechos y Garantías Fundamentales de la Persona, Capítulo I Derechos Individuales y su Régimen de Excepción, Art. 24, 1983).

De la misma forma, la Republica de El Salvador posee una Ley Especial contra los delitos Informáticos y Conexos la cual tiene por objeto "proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación(TIC), así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley" (Decreto No.260, Título I, Disposiciones Generales, Art. 1, 2016).

Entre otras regulaciones o marcos jurídicos, se encuentra el Código penal de El Salvador, art. 172, 173 y 346 los cuales otorgan acciones contra delitos comunes que se cometan a través de medios electrónicos o estos sean utilizados para provocar algún daño hacia las personas y el propio Estado salvadoreño. A su vez en materia de ciberdefensa posee una Unidad de informática la cual responde directamente al Ministerio de la Defensa Nacional de El Salvador, la cual tiene por objetivo aportar a una mayor seguridad tanto del Estado de dicho país como a sus fuerzas armadas.

2.4.10 República de Honduras

La Republica de Honduras, para comenzar solamente posee un breve énfasis en su Constitución en cuanto a los derechos básicos de los individuos en sus áreas privadas, entre estas las comunicaciones, cuando presenta que "toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial" (Titulo III, De las Declaraciones, Derechos y Garantías Capitulo II De los Derechos Individuales, Art.100, 1982). A su vez, se agrega una Iniciativa de Ley Nacional de Ciberseguridad y Medidas de Protección Ante los Actos de Odio y Discriminación en Internet y

Redes Sociales, iniciada el 08 de febrero del 2018, la cual tiene por objetivo brindar una mayor seguridad a los ciudadanos en su uso del internet y evitar que estos sean víctimas por parte de contenidos o acciones ilegales afectando tanto su dignidad como su estado físico.

Cabe mencionar que esta iniciativa de Ley, solamente se aprobó una primera discusión quedando pendiente dos discusiones para que pueda aprobarse formalmente y entrar en vigor. Asimismo, se destacan otros mecanismos o herramientas jurídicas como el Código penal de Honduras, art. 143 y 271, capitulo III, art.214. los cuales establecen acciones de penalización a cualquier acto que por medios tecnológicos como las TIC perjudiquen a ciudadanos y su integridad, a su vez mediante el decreto No. 139 en el año 2016, en materia de ciberdefensa, Honduras cuenta con la Dirección Nacional de Investigación e Inteligencia y el Centro de Repuesta a Emergencia Informática los cuales brindan protección a los sistemas informáticos del Estado hondureño, además de mantener una capacitación constante del personal o especialista y crear una repuesta factible ante incidentes de seguridad tecnológica.

2.4.11 República de Nicaragua

La Republica de Nicaragua en su Constitución Política, presenta normas sobre la seguridad de sus sistemas electrónicos y de comunicación, destacando que "para los efectos de la seguridad nacional: a) En ningún caso es permisible el establecimiento de sistemas que alteren o afecten los sistemas de comunicación nacional. b) Los puntos de comunicación para fines de la defensa nacional en el territorio nacional deberán ser propiedad del Estado. c) El espectro radioeléctrico y satelital es propiedad del Estado nicaragüense y debe ser regulado por el ente regulador, la ley regulará la materia" (Título V Defensa y Seguridad Nacional. Seguridad Ciudadana, Capítulo Único, Art. 92, 1987).

Del mismo modo, Nicaragua cuenta con una Ley Especial de Ciberdelitos la cual tiene por objeto "la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes, en los términos previstos en esta Ley" (Ley No.1042, Capítulo I, disposiciones Generales, Art. 1, 2020). Asimismo, la Republica de Nicaragua, posee una Estrategia Nacional de Ciberseguridad, teniendo como objetivos "Garantizar el uso soberano, seguro y confiable del ciberespacio, que permita el aprovechamiento de las TIC como herramienta

que contribuya a la paz, la estabilidad, la seguridad y el desarrollo sostenible del país" (Decreto No. 24-2020 Capítulo IV Estrategia Nacional de Ciberseguridad, inciso b, 2020).

Cabe resaltar que Nicaragua, hasta el momento no cuenta con un órgano especializado en materia de ciberdefensa como tal, sin embargo, posee algunos mecanismos de aspecto jurídico como leyes las cuales son utilizadas como base o iniciativas en materia ciberdefensa, como el caso del Código de Jurisdicción y Previsión social Militar del Ejercito del Nicaragua, el cual expone que el Ejercito puede "participar, en coordinación con las instituciones competentes, en la protección a los sistemas de datos, registros informáticos, espectro radioeléctrico y satelital, para evitar alteraciones o afectaciones a los sistemas de comunicación nacional y lo dispuesto para los fines de defensa nacional" (Ley 181, Título I Organización Militar, Capítulo I Disposiciones Generales, Naturaleza y Funciones del Ejército, Art.2 inciso 15, 2014).

También bajo está misma lógica, se encuentra la Ley de Seguridad Soberana, la cual establece como uno de sus objetivos, "la preservación y protección de la vida de la persona, la familia y la comunidad nicaragüense, los bienes, la democracia directa, participativa y representativa, fundada en el desarrollo económico, político, cultural, social, alimentario, ambiental, tecnológico de la nación nicaragüense" asimismo entre las definiciones o tipos de amenazas se establecen los "ataques externos a la seguridad cibernética que alteren o afecten los sistemas de comunicación nacional"(Ley No. 919, Capítulo I Disposiciones Generales, Art.6, inciso 1 y Art.8, inciso 9, 2015) añadiendo a su vez el Código Penal de la Republica de Nicaragua el cual en sus Art. 249, 250 y 327 hacen relevancia a medidas que se optan contra aquellos delitos que atenten a la estabilidad de los sistemas informáticos o infraestructuras relacionadas a ello.

2.4.12 República de Costa Rica

La Constitución de la República de Costa Rica en su Título IV Derechos y Garantías Individuales, Capitulo Único, hace referencia sobre la inviolabilidad de los documentos privados y las comunicaciones escritas y orales de sus habitantes, pero no especifica algún énfasis en cuanto las telecomunicaciones o tecnología, sin embargo, este país posee una reforma a su Código Penal nacional, lo cual posibilito la implementación de la Ley de Delitos Informáticos y Conexos, Ley N^0 9048, aprobada el 06 de noviembre del 2012, la cual establece medidas o acciones a tomar contra aquellos actos que perjudiquen tanto al Estado costarricense como a sus ciudadanos, con el uso de medios tecnológicos.

Asimismo, dicho país centroamericano posee en su Código Penal, los art.196, 217 y 229 los cuales hacen relevancia a todo delito común que se cometa con el uso de medios TIC, sumando que este país posee una Estrategia Nacional de Ciberseguridad bajo el Ministerio de Ciencia, Tecnología y Telecomunicaciones aprobada en el 2017, el cual tiene por objetivo mejorar las capacidades de seguridad cibernética de dicho país, además de coordinar con diversos sectores para crear un sector que tenga cooperación con otros en esta materia. En materia de ciberdefensa se puede tomar en cuenta los esfuerzos realizados por el Organismo de Investigación Judicial, Sección Especial Contra Cibercrimen, desempeñándose como "una sección que utilizan técnicas de Computación Forense, en la recolección, preservación y análisis de indicios para garantizar la cadena de custodia de los indicios en computadoras, discos duros, llaves USB, dispositivos móviles, entre otros dispositivos de procesamiento y almacenamiento de datos".

Del mismo modo se destacan otros esfuerzos como la Comisión Nacional de Seguridad en Línea (CNSL) la cual "se encargará de diseñar las políticas necesarias sobre el buen uso de Internet y las Tecnologías Digitales contribuyendo a generar una cultura de comprensión, análisis y responsabilidad personal, que les permita beneficiarse de las ventajas de su utilización, y tener una actitud consciente y proactiva frente a los riesgos inherentes al uso de estos recursos" (Decreto No. 36274, Art.1, 2020).

A su vez se presenta el Centro de Repuesta de Seguridad Informática de Costa Rica (CSIRT-CR) teniendo por objetivo "Coordinar, a nivel nacional acciones que permitan el mejoramiento general de la seguridad cibernética e informática, apoyar a las autoridades administrativas y judiciales en los casos que corresponda para la investigación y procesamiento de perpetradores de delitos cibernéticos e informáticos y Coordinar con el Comité Interamericano contra el terrorismo (CICTE), y otras entidades nacionales e internacionales sobre el diseño y aplicación de políticas, estrategias y lineamientos en la adquisición de bienes y servicios en materia de la seguridad de las tecnologías de la información y la comunicación, con los estándares que observen las normativas vigentes internacionales para la implementación y/o aplicación en el sector público" (Decreto No. 37052-MICIT, Art.2, 2012).

2.4.13 República de Panamá

La Constitución de la República de Panamá, hace referencia a la privacidad y aseguramiento de todo medio que pueda transportar o tener información, "La correspondencia y demás documentos privados son inviolables y no pueden ser examinados ni retenidos, sino por mandato de autoridad competente y para fines específicos, de acuerdo con las formalidades legales. En todo caso, se guardará absoluta reserva sobre los asuntos ajenos al objeto del examen o de la retención. El registro de cartas y demás documentos o papeles se practicará siempre en presencia del interesado o de una persona de su familia o, en su defecto, de dos vecinos honorables del mismo lugar. Todas las comunicaciones privadas son inviolables y no podrán ser interceptadas o grabadas, sino por mandato de autoridad judicial. El incumplimiento de esta disposición impedirá la utilización de sus resultados como pruebas, sin perjuicio de las responsabilidades penales en que incurran los autores" (Titulo III Derechos y Deberes Individuales y Sociales, Capitulo 1 Garantías Fundamentales, Art. No 29, 1972).

A su vez, Panamá cuenta con la Ley que dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones, No. 51, aprobada el 23 de septiembre del 2009, la cual consiste en establecer normas y protección a los suministros de datos por medio de las comunicaciones, protegiendo tanto al servicio de la propia telecomunicación como a los usuarios. Otros mecanismos que posee la República de Panamá, se conforman mediante el Código penal de Panamá Titulo VIII, Capítulo I, art.289-292 los cuales presentan medidas a tomar contra toda acción ilegal o que perjudique a las personas como al propio Estado Panameño, mediante medios tecnológicos.

De igual forma, este país cuenta con una Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Criticas aprobada en el 2013, teniendo como fundamento "el desarrollo de acciones orientadas a mejorar la seguridad cibernética nacional y hace especial énfasis en la protección de aquellas infraestructuras que son vitales para el bienestar de la población, los servicios básicos, el buen funcionamiento del gobierno y las organizaciones privadas, el bienestar económico y la calidad de vida de las personas" (Resolución No.21, Seguridad Cibernética y Protección de Infraestructuras Criticas, 2013).

En materia de ciberdefensa, Panamá cuenta con el Ministerio Seguridad Pública el cual ha realizado esfuerzos para reforzar la protección nacional de dicho país ante ataques o incidencias de ciberamenazas que lleguen a afectan tanto a sus ciudadanos como las infraestructuras vitales del Estado panameño. Otros mecanismos que aportan al desarrollo y mantenimiento de una seguridad cibernética, se destaca el Centro de Repuesta de Seguridad Informática de Panamá (CSIRT-RP) el cual tiene por objetivo "la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos que conforman la infraestructura critica del país y el acceso a la información de parte de los ciudadanos de Panamá", sumado también los esfuerzos de "coordinar, colaborar, y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los niveles de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas y de comunicaciones de las entidades gubernamentales", representando ser ejes primordiales del CSIRT panameño.

2.4.14 República Dominicana

La Constitución de República Dominicana establece que "se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente, de conformidad con la ley" (Título II De los Derechos, Garantías y Deberes Fundamentales, Capítulo I De los Derechos Fundamentales, Sección I De los Derechos Civiles y Políticos, Art. 44, inciso 3, 2010).

De la misma manera Republica Dominicana cuenta con la Ley sobre crímenes y delitos de alta tecnología, la cual tiene por objeto "la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales, en los términos previstos en esta ley. La integridad de los sistemas de información y sus componentes, la información o los datos, que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o

de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos". (Ley No.53-07, Título I, Disposiciones Generales y Conceptuales, Sección I, Objeto, Ámbito y Principios Art.1, 2001)

Asimismo, se agrega la Ley de Protección de Datos Personales teniendo por objeto "la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean éstos públicos o privados, así como garantizar que no se lesione el derecho al honor y a la intimidad de las personas, y también facilitar el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el Artículo 44 de la Constitución de la República Dominicana" (Ley No.172-13, Capítulo I Disposiciones Iniciales, Sección I Del Objeto, Alcance, Ámbito de Aplicación, Restricciones y Principios, Art.1, 2013).

Cabe destacar que Republica Dominicana también posee otros mecanismos de carácter jurídico como el Código penal en sus artículos 330 y 333, los cuales hacen énfasis en medidas a tomar cuando se presenta la violación al derecho de intimidad y cuando se utilicen medios digitales o tecnológicos para causar algún daño a la integridad de la persona. Sumado a esto se encuentra la Estrategia de ciberseguridad de Republica dominicana la cual tiene por misión "establecer los mecanismos de ciberseguridad adecuados para la protección del Estado, sus habitantes y, en general, del desarrollo y la seguridad" (Decreto No. 230-18, Art.2, 2018).

A su vez en materia de ciberdefensa se encuentra el Centro de Comando, Control, Comunicaciones, Computadoras, Ciberseguridad e Inteligencia (C5I) de las Fuerzas Armadas de Republica dominicana, el cual tiene por objeto la conducción de operaciones conjuntas, combinadas e interagenciales que se ejecuten en los diversos órganos o instituciones del Estado, as du vez es responsable de evaluar amenazas que puedan afectar la estabilidad interna de dicho país. Teniendo como capacidad una plataforma tecnológica y otros medios tecnológicos que permitan proteger recursos vitales para el Estado dominicano.

2.5 Preguntas Directrices

1. ¿Cuáles son los mecanismos de ciberseguridad y ciberdefensa que poseen los Estados centroamericanos?
2. ¿Qué tan eficaces son los mecanismos o iniciativas de ciberseguridad y ciberdefensa en Centroamérica?
3. ¿Cuáles son las capacidades que poseen los Estados de Centroamérica, y como pueden ser vulnerables ante un ciberataque?
4. ¿Cuáles son los riesgos que representa la ciberdelincuencia para los Estados centroamericanos?
5. ¿Qué desafíos tienen los Estados en materia de ciberseguridad o ciberdefensa para combatir las ciberamenazas en Centroamérica?
6. ¿Cómo se podría consolidad una estrategia homologada centroamericana en materia de ciberseguridad y ciberdefensa, a fin de proteger a los Estados contra la ciberdelincuencia especialmente bajo los nuevos avances tecnológicos?

CAPÍTULO III

Diseño Metodológico

3.1 Tipo de investigación

La presente tesis fue elaborada bajo el tipo documental-explicativo. La investigación documental según Tancara, (1993) "Es una serie de métodos y técnicas de búsqueda, procesamiento y almacenamiento de la información contenida en los documentos, en primera instancia, y la presentación sistemática, coherente y suficientemente argumentada de nueva información en un documento científico" (P.4). En este sentido el tipo de investigación documental permite estudiar con mayor amplitud un hecho o acción de interés mediante fuentes de información para plantear o mejorar un nuevo esquema de estudio, tomando como énfasis la presente tesis, la cual se abordaron los diferentes medios que contenían información relacionada a la situación de ciberseguridad en la región centroamericana.

En cuanto a la investigación de tipo explicativa, según Sampieri, (2003) "Esta dirigida a responder a las causas de los eventos, sucesos y fenómenos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar porqué ocurre un fenómeno y en qué condiciones se da" (P.15). Partiendo bajo esta lógica, la investigación explicativa posibilita analizar y comprender un tema de importancia, conociendo el origen de sus causas y el porqué de su proceso, obteniendo una información adecuada de la temática de interes, que pueda usarse para nuevos planteamientos. Para esta tesis, el esquema explicativo delimito su importancia en cuanto a comprender y delimitar de una manera general a una forma especifica y ordenada de los hechos, en este caso la necesidad de una ciberseguridad homologada al nivel de toda la región centroamericana.

3.2 Enfoque de investigación

La presente tesis se llevó a cabo en base al enfoque cualitativo, según el autor Sánchez, (2019) "El enfoque cualitativo se sustenta en evidencias que se orientan más hacia la descripción profunda del fenómeno con la finalidad de comprenderlo y explicarlo a través de la aplicación de métodos y técnicas derivadas de sus concepciones y fundamentos epistémicos" (P.3). De acuerdo a este planteamiento, el enfoque cualitativo ayuda a desarrollar de forma amplia y ordenada un tema, permitiendo a su vez la comprensión del mismo, para la presente temática de ciberseguridad, se abarco todo lo relacionado tanto al concepto propio como su composición en Centroamérica.

3.3 Método de investigación

El método que se utilizó en esta tesis es el inductivo, según el autor Rodríguez, (2007) el método inductivo "Se inicia con un estudio individual de los hechos y se formulan conclusiones universales que se postulan como leyes, principios o fundamentos de una teoría" (P.6). Por tanto, podemos asumir que el método inductivo consiste en obtener una evidencia singular que sugiera la posibilidad de una conclusión en términos de probabilidades o posibilidades. En la presente temática se tomó en cuenta el análisis del contexto que ocasionaría la no implementación o desarrollo de una ciberseguridad homologada en Centroamérica, teniendo en cuenta unas consecuencias generalizadas para los Estados de la región.

3.4 Paradigma de investigación

De acuerdo con Uzcategui, (2018) el paradigma interpretativo "Su finalidad es profundizar nuestro conocimiento, en comprender la conducta de las personas estudiadas, lo cual se logra cuando se interpreta los significados, actos y pensamientos" (P.3). En base a lo expuesto por el autor, se asume que el paradigma interpretativo tiene por objetivo el estudio del comportamiento y las acciones del ser humano junto con su entorno por medio de herramientas básicas de información. Para la presente tesis el paradigma interpretativo ayuda a entender de cierta forma el actuar del ser humano mediante los medios tecnológicos, sobre todo en el ámbito de la ciberseguridad y el propio actuar de los Estados de Centroamérica en este campo.

3.5 Fuentes de investigación

Las fuentes de investigación en base a Jervis (2017) "Son elegidas de acuerdo al énfasis propuesto para la investigación y pueden ser tanto primarias (entrevistas, noticias, documentos originales, etc.), como secundarias (enciclopedias, revisión de resúmenes, bibliografías, etc.)". En este sentido las fuentes de investigación representan todo medio que contenga información de interés de acuerdo a un objeto de estudio, clasificándose en primarias y secundarias. Para el caso de esta tesis las fuentes de investigación se relacionaron a todo medio de información disponible en materia de ciberseguridad al nivel centroamericano, abarcando desde los conceptos generales de esta temática hasta los objetivos planteados en esta tesis. Del mismo modo las fuentes primarias y secundarias se clasificaron de acuerdo al interés del tema abordando el mejor contenido disponible.

3.6 Técnicas de análisis de información

Para la elaboración de la presente tesis se aplicó principalmente la técnica del análisis documental de acuerdo al autor Iglesias, (2004) "El análisis documental es una forma de investigación técnica, un conjunto de operaciones intelectuales, que buscan describir y representar los documentos de forma unificada sistemática para facilitar su recuperación" (P.2). Por consiguiente, el análisis documental resulto factible al momento de procesar la información y sintetizarla de acuerdo al interés de la presente tesis.

De igual forma se destaca la revisión de documentos relacionados a la presente temática como son los informes, resúmenes, conferencias y guías de organismos regionales como el SICA, CFAC y otros organismos que abordan la presente temática como son la Junta Interamericana de Defensa, Organizaciones de los Estados Americanos, Banco Interamericano de Desarrollo, CEPAL, entre otros. Asimismo, se visitó mediante un cronograma de trabajo las páginas web de las organizaciones regionales, sumado al estudio y análisis de esquemas de seguridad y defensa y cibernética conteniendo datos cualitativos y cuantitativos, que conduzcan objetivos relacionados a esta tesis.

3.7 Técnica de recolección de información

La técnica de recolección de información, en base a Hernández, (2020) "Está orientado a crear las condiciones para la medición. Los datos son conceptos que expresan una abstracción del mundo real, de lo sensorial, susceptible de ser percibido por los sentidos de manera directa o indirecta, donde todo lo empírico es medible" (P.1). De acuerdo a este planteamiento la recolección de datos es una medición para facilitar la obtención de nuevo conocimiento que permita fortalecer o ampliar un tema de interés. En este caso, para la elaboración de la presente tesis se utilizaron técnicas de recopilación y selección de documentos especializados en el tema de seguridad regional centroamericana, ciberseguridad, ciberdefensa y ciberdelincuencia. De igual forma técnicas de registro, análisis y sistematización de la información para adecuarla primeramente lineamiento investigativo de la carrera de Ciencia Política y Relaciones Internacionales, como es Estado, Gobernabilidad y Políticas Publicas.

Asimismo, se aplicó la entrevista como un mecanismo prioritario para recopilar información por parte de individuos o personas capacitadas que tengan relación con el tema investigativo fortaleciendo el contenido del mismo. Es necesario mencionar que a causa de la situación actual de la pandemia del COVID-19, dichas entrevistas se realizaron de manera digital conteniendo una estructura puntual de preguntas, obteniendo la información necesaria que aporte a la presente tesis, las entrevistas se realizaron a las siguientes personas:

Entrevista realizada al Msc. Álvaro Miguel Padilla Lacayo, Abogado y Notario de la República de Nicaragua, Catedrático Universitario desde año 2004, quien se ha desempeñado laboralmente como Asesor Técnico para Asuntos de Integración del Despacho del Ministro de Relaciones Exteriores de Nicaragua (2017), realizando coordinación y seguimiento de temas regionales trabajados en el marco del SICA, entre otros. Especialista en Asuntos de Justicia y Seguridad de la Secretaria General del Sistema de la Integración Centroamericana, realizando la coordinación del Proceso de Armonización de la Legislación en materia penal en los países del SICA, procesos de revisión y actualización de Tratados y Convenios Regionales, Seguimiento, implementación y ejecución de la temática de la Agenda de Seguridad Regional y Planes de Trabajo de la Comisión de Seguridad de Centroamérica.

La segunda entrevista se realizó al Msc. Arturo Danilo Barberena, el cual tiene su perfil profesional en ser Abogado y Notario, Lic. En Comunicación Social. Él fue coordinador de comunicación y prensa del Ministerio de Defensa de la republica de Nicaragua, asimismo se desempeñó como asistente ejecutivo del despacho del Ministerio de Defensa. La entrevista realizada al Msc. Arturo Barberena tuvieron como resultado la afirmación que desde el ámbito regional del SICA o fuerzas armadas, no se cuenta con planes regionales conjuntos sobre el tema, el trabajo regional realizado a la fecha se enmarca únicamente en el ámbito jurídico.

CAPÍTULO IV

Análisis y Discusión de Resultados

4.1 Mecanismos de ciberseguridad que poseen los Estados centroamericanos

Para obtener una mejor explicación en cuanto a que mecanismos de seguridad cibernética dispone Centroamérica, comenzaremos primeramente analizando desde la perspectiva como región abarcando 2 de sus importantes sistemas de integración y cooperación como es el Sistema de Integración Centroamericana (SICA) y la Fuerzas Armadas de la Conferencia de Fuerzas Armadas Centroamericanas (FAM-CFAC), además como se encuentran dichos organismos en materia de ciberseguridad y ciberdefensa o bien si disponen de un mecanismo como tal para la región. Continuamente se abordará a los Estados de la región y como se encuentran estos en cuanto a mecanismos de seguridad cibernética desde su perspectiva interna como nación.

Actualmente la región cuenta con un Sistema de Integración Centroamericana (SICA) el cual según sus estatutos plasmados en el Protocolo de Tegucigalpa hace referencia a la seguridad regional, pero dado a la época en que se dio la creación de dicho protocolo, no se aborda directamente la temática de ciberseguridad de manera homologada entre los Estados miembros del SICA, debido a las prioridades que tenía la situación de ese periodo, incluso podemos resaltar en tu Art.3 en modelos de seguridad que no expresa explícitamente una propuesta para consensuar una seguridad cibernética. Por lo tanto, el Protocolo de Tegucigalpa como mecanismo principal de la integración regional, no cuenta con una base sólida que permita tomar como dirección o bien un lineamiento que ayude a la elaboración de una iniciativa regional en materia de ciberseguridad.

De igual forma, el SICA dispone de un Tratado Marco de Seguridad Democrática que también hace énfasis en concretar un modelo de seguridad regional, combatiendo toda amenaza regional o internacional que pueda afectar a los Estados centroamericanos, mediante el establecimiento de mecanismos de coordinación operativa con las instituciones correspondientes, fortaleciendo a su vez la armonización y convergencia de las políticas de seguridad. Resultando de mucha importancia puesto que este tratado aborda todo lo referente a la seguridad regional y teniendo relación directa a la seguridad nacional de los Estados centroamericanos, que por medio lo consensuado en este tratado los Estados llegan a abordar y desarrollar sus políticas de seguridad interna.

No obstante, al igual que el protocolo de Tegucigalpa, el Tratado Marco de seguridad Democrático Centroamericano no posee una sección especial que aborde el tema de ciberseguridad, o bien un acercamiento a estos términos que permitan seleccionar una dirección para la elaboración de una estrategia armonizada en dicha materia, sobre todo en el Titulo III de su seguridad regional. Solamente contiene los lineamientos importantes que puedan llevar al desarrollo de la misma, como el factor de fortalecer la cooperación, coordinación, armonización y convergencia de las políticas de seguridad, valorando también la gravedad de cualquier actividad delictiva la cual tendría repercusiones regionales en la que los Estados se comprometan a contrarrestarlas.

Asimismo, el SICA posee una Estrategia Regional para el Desarrollo de la Sociedad de la Información y el Conocimiento, teniendo como objetivos dirigir regionalmente políticas públicas y privadas en materia tecnológica y desarrollo socio-económico, pero en sus objetivos y procedimientos no da a conocer o bien no se plantea una iniciativa o mecanismo que haga énfasis a una ciberseguridad regional. Más aún cuando esta estrategia está basada en el ámbito tecnológico y en sus prioridades de resalta una seguridad democrática pero obtiene el mismo resultado en cuanto el vacío de una política de ciberseguridad armonizada para la región que contribuya a proteger el desarrollo tecnológico de la región, presentando las mismas características de los anteriores instrumentos regionales mencionados, destacando que estos solamente disponen de las bases necesarias para que los Estados logren consensuar la delimitación de una sola amenaza y cooperar para contrarrestar sus impactos y fortalecer a la región en su ámbito de seguridad.

De acuerdo a lo presentado anteriormente, Centroamérica a través del Sistema de Integración Centroamericana (SICA) posee instrumentos de cooperación, consenso y armonización que ayudan a los Estados a abordar sus intereses, problemáticas y crear iniciativas que beneficien tanto a los propios Estados como a la región en general. Pero no tienen en sus estructuras una directriz o bien una línea que permita a los Estados abordar concretamente la ciberseguridad y optar por una cooperación tangible en esta materia, sobre todo cuando los Estados por sus intereses y necesidades internas modernizan sus capacidades lo que a su vez incide para toda Centroamérica tomando énfasis en cuanto a los programas y proyectos de carácter económicos y de infraestructura que tienen los Estados para potenciar su funcionamiento.

Cabe resaltar que, a pesar de no contar sólidamente con una iniciativa regional en seguridad cibernética, los Estados en algunas ocasiones han impulsado esfuerzos que aborden la ciberseguridad como un asunto prioritario, incluso bajo la misma perspectiva ha sido impulsada por el SICA de acuerdo a los resultados obtenidos de esta tesis por medio de la entrevista al MSc. Álvaro Padilla al destacar que, durante "El año 2014, el tema comienza a ser parte de la agenda de la Comisión de Seguridad de Centroamérica, especialmente de la Subcomisión de Defensa integrada por funcionarios representantes de los Ministerios de Defensa y Ejércitos Nacionales de los países miembros. A partir de ese momento la ciberamenaza se han convertido en el nuevo desafío que deben de enfrentar los países del SICA en el dinámico escenario internacional, en la medida que estos países van implementando el uso de la tecnología en todas sus actividades y no se toman las precauciones necesarias, se vuelven más propensos a cualquier amenaza procedente del ciberespacio".

Los esfuerzos de los Estados centroamericanos para abordar la ciberseguridad se pueden ver reflejados en conferencias, reunión de representantes de gobiernos, adopción de algunas medidas de entendimiento, capacitaciones entre otros, pero sin obtener un resultado concreto en una estrategia centroamericana o bien que por parte del SICA se establezca una sesión especial que tenga por objetivo la actualización de los tratados o mecanismos regionales que ayuden a establecer una iniciativa completa de ciberseguridad. La ciberseguridad para que obtenga su verdadera funcionalidad requiere de un sólido desempeño y desarrollo para proteger las capacidades que pueden ser blanco de un ciberataque, teniendo como resultado una resiliencia efectiva y una administración del riesgo, lo que significa una seria evaluación de capacidades que permanezcan en constante actualización y desarrollo.

Es necesario mencionar que la falta de una voluntad política concreta en esta materia ha dificultado la toma de un solo consenso que ayude a crear las bases de una estrategia o política regional común en el ámbito de la ciberseguridad, sobre todo que este goce de un carácter eficaz y buena funcionalidad. En consecuencia, los Estados afianzan de manera propia sus propias iniciativas en ciberseguridad representadas principalmente en los mecanismos jurídicos que tienen por finalidad dotar al Estado de instrumentos para hacer frente a un eventual ciberdelito, también para que estos puedan desarrollar o tener una adaptabilidad del campo de seguridad cibernética hacia sus instituciones gubernamentales.

Como resultado los Estados centroamericanos de manera propia cuentan con iniciativas de ciberseguridad, principalmente en sus mecanismos de ámbito jurídico los cuales representan la primera instancia para partir de una dirección que ayude a abordar este campo de manera sostenible. Los mecanismos jurídicos que poseen los Estados centroamericanos, como se planteó en el marco legal de esta tesis, están compuesto de acuerdo al orden de su carga magna o sus constituciones, las leyes que abordan la ciberseguridad como un ámbito de protección nacional, los códigos penales que, si bien estos pueden adecuarse a los delitos cibernéticos comunes, también son parte del esquema de una iniciativa de ciberseguridad, seguidamente de sus decretos e instituciones gubernamentales teniendo como principio las etapas que lleva una ciberseguridad como se muestra en la siguiente imagen:

Figure 1 Etapas de la Ciberseguridad

Fuente: Elaboración propia.[1]

[1] Nota: El presente ciclo refleja las etapas que se llevan a cabo para consolidad una ciberseguridad efectiva desde su planificación hasta su gestión continua.

En cuanto a las Fuerzas Armadas Militares de la Conferencia de Fuerzas Armadas Centroamericanas (FAM-CFAC) tienen sus objetivos delimitados en la protección y defensa regional mediante la cooperación, coordinación y apoyo mutuo de quienes forman parte de esta integración regional militar. La CFAC se destaca por ser un organismo que ayuda a valorar la situación de Centroamérica en temas se seguridad y elaborar propuestas o iniciativas que permitan aumentar los niveles de seguridad en Centroamérica, así como para los propios Estados, lo que representa del mismo modo otro mecanismo de integración regional eficaz para consensuar u homologar intereses.

Pero al igual que el SICA, la CFAC no ha concretado una iniciativa regional en materia de ciberseguridad o bien que la ciberdelincuencia sea contrarrestada de manera unánime en el Eje de Enfrentamiento a las Amenazas Emergentes que posee esta organización, solamente se conocen algunos acercamientos de dicho tema mediante reuniones de directores de enlaces en operaciones e inteligencia, pero dada la escasa información pública sobre ello y el vacío constante de no tener una ciberdefensa disponible, se asume que hasta el momento la CFAC no ha planteado una línea homologada en esta materia.

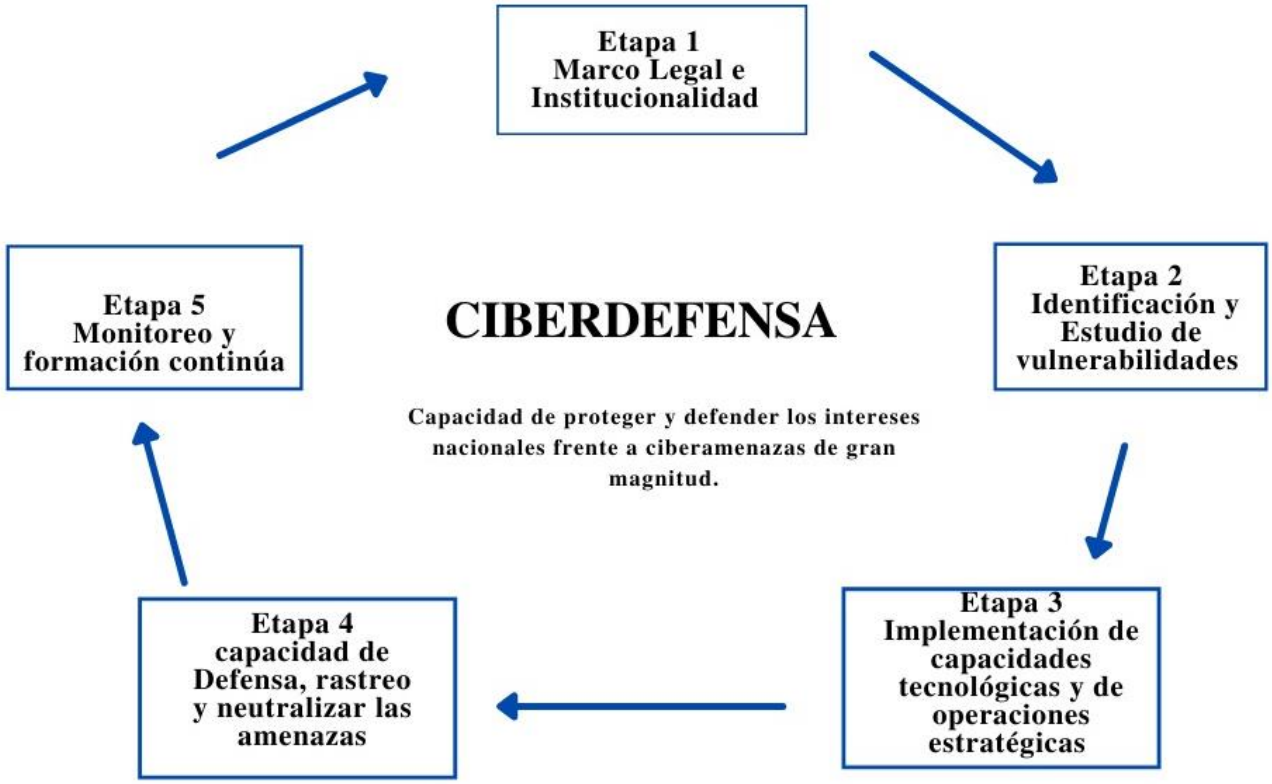
Asimismo, la falta de un mecanismo regional por parte de la CFAC en materia de ciberseguridad o bien una iniciativa de ciberdefensa, es reforzada por los resultados de esta tesis por medio de la entrevista realizada al Msc. Álvaro Padilla, cuando hace énfasis a que “En la actualidad, desde el ámbito regional desde SICA o fuerzas armadas, no se cuenta con planes regionales conjuntos sobre el tema, el trabajo regional realizado a la fecha se enmarca únicamente en el ámbito jurídico….se desconoce la existencia de iniciativas propias generadas en el seno de la Conferencia de Fuerzas Armadas de Centroamérica, es bueno tener en cuenta, que las iniciativas regionales en materia de seguridad nacen en el marco de la Comisión de Seguridad y se trabajan desde los Ministerios de Relaciones Exteriores”.

También en la misma línea, se aborda lo expuesto por el MSc. Arturo Barberena al afirmar que “La CFAC hasta el momento no cuenta con una iniciativa concreta en ciberdefensa, sin embargo, se considera que las ciberamenazas pueden afectar de manera directa o indirecta. Puesto que aún, si un ciberataque es dirigido a un blanco en específico, trae consigo siempre daños colaterales, ya sea como privar de algún servicio o de realizar alguna función…Los países del SICA así como las fuerzas armadas centroamericanas CFAC no son ajenos a esta nueva realidad,

considerando que los Estados miembros han venido empleando herramientas de tecnología digital en diversos aspectos de la sociedad, pero no cuentan con los recursos apropiados o la experiencia necesaria en este ámbito y así tomar las medidas de seguridad correspondientes".

En este sentido la CFAC puede dar alternativa a la formulación de una ciberdefensa homologada al nivel centroamericano teniendo en cuenta su naturaleza de capacidad militar en operar, detectar y neutralizar amenazas, además por su rol de proteger y preservar la soberanía de los Estados de manera que cuenta con todas las capacidades necesarias para implementar una ciberdefensa consensuada con carácter sostenible y amplia, cumpliendo las etapas que esta requiere para consolidarse como se puede ver reflejado en la siguiente ilustración:

Figure 2 Etapas de la Ciberdefensa



Fuente: Elaboración propia.[2]

[2] Nota: El presente ciclo expone los procesos llevados a cabo para efectuar y consolidar una ciberdefensa sostenible y adaptable ante las amenazas cibernéticas.

En concreto tanto CFAC y como el SICA son organismos de integración que poseen estructuras o mecanismos que benefician a la región centroamericana en materia de desarrollo y seguridad, sin embargo a pesar que han empleado ciertas acciones en abordar la seguridad cibernética, no se ha consolidado una ciberseguridad y ciberdefensa homologada, por consiguiente los Estados centroamericanos se han caracterizado por ser realizar esfuerzos de manera individual y no colectiva en esta área, teniendo en cuenta que cada Estado tiene sus propios objetivos e intereses estratégicos dejando como resultado que los únicos mecanismos de ciberseguridad o ciberdefensa en Centroamérica son los que cuentan de manera independiente cada Estado, principalmente los de orden jurídico e institucional.

En cambio, estos esfuerzos pueden abonar la posibilidad de crear una iniciativa que permitan homologar un instrumento en seguridad cibernética, o bien determinar de manera consensuada la ciberdelincuencia como una amenaza para Centroamérica y establecer parámetros de cómo afrontarla protegiendo a su vez las capacidades o recursos estratégicos de cada Estado.

Capacidades de los Estados centroamericanos

Los Estados centroamericanos por sus necesidades internas y las demandas que ejerce la globalización en actualizar todo ámbito tecnológico, se han creado nuevas capacidades que están sujetas directamente a todo recurso que representa o garantiza un óptimo funcionamiento de los servicios otorgados por un organismo, empresa y principalmente los Estados, como son sus infraestructuras críticas. Las cuales al nivel regional están dedicadas a los sectores mayoritariamente económicos como los sistemas financieros, energía y telecomunicaciones, agua y salud, puertos marítimos, transporte y otros sectores productivos, también cabe resaltar las propias instituciones estatales, ya que estas representan un eje clave para que el Estado realice y desarrolle sus acciones.

Al mismo tiempo, en la entrevista hacia el MSc. Barberena, se destacó las capacidades regionales y propias de los Estados centroamericanos cuando refiere que “En la región existe un gran número de infraestructura física e informáticas que conforman las infraestructuras críticas nacionales y regionales dedicadas a distintos sectores; energía y telecomunicaciones, sector productivo; bancaria y de fabricación, sector de defensa, salud y agua en los cuales se emplea la tecnología de la información y comunicación incluso en productos que antes no lo tenía, lo que ha dado paso otro aspecto tecnológico en la vida cotidiana de algunas regiones urbanas, al

denominado Internet de las cosas" por tanto se hace un énfasis especial que la región experimenta un auge de modernización y desarrollo en sus componentes tecnológicos.

De igual forma, las capacidades o bien en este caso se puede mencionar como infraestructuras críticas, en su concepto, el cual fue abordado con anterioridad, se conocen como todo el conjunto de servicios o sistemas los cuales permiten el desarrollo de un área importante, para este caso representaría la funcionalidad de un Estado. Por ende, si estas llegasen a tener alguna interrupción o son severamente incapacitadas por medio de un ataque, ocasionarían un detrimento en la estabilidad y seguridad de un Estado, como de cualquier área de gran valor la cual este compuesta por una infraestructura crítica.

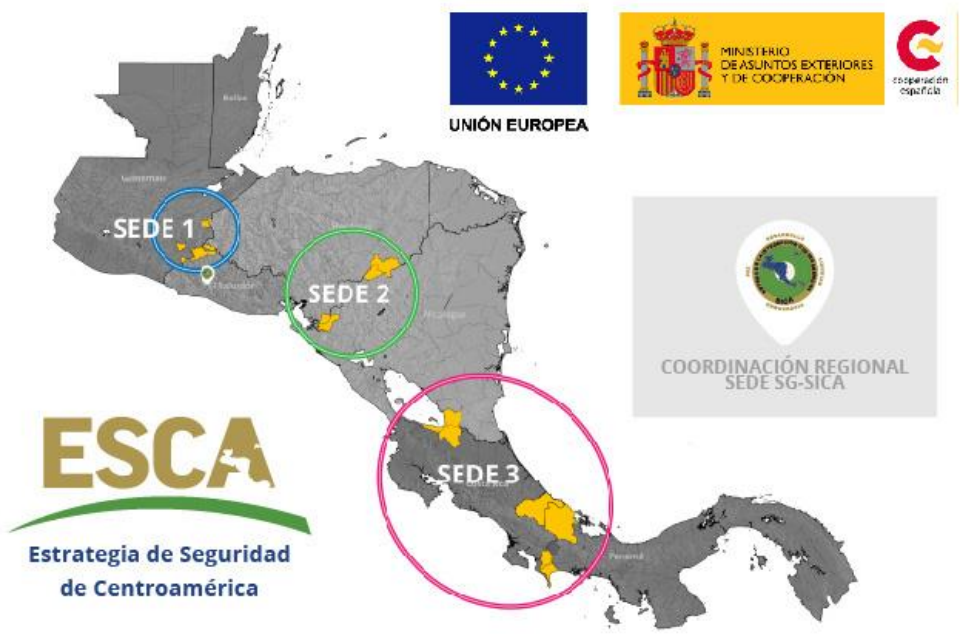
En este caso se abordarán las principales capacidades que posee la región centroamericana que a su vez son las que cada Estado posee internamente y presentan un gran valor para su desarrollo y estabilidad como los sistemas financieros, sector de redes eléctricas, sector de telecomunicaciones, sector de aeropuertos, sector agua potable, plantas de tratamiento, tuberías de gas y petróleo, sector de puertos marítimos y el propio canal de Panamá. Estas capacidades son de alto valor estratégico llegando a valorar si estas llegan a ser amenazas o atacadas por cualquier medio, sobre todo tecnológico, se convertirían en una capacidad crítica, específicamente sus infraestructuras al ser vulneradas ante una incidencia perjudicial.

Instituciones Gubernamentales: Al nivel centroamericano los Estados representan el ente de mayor importancia ya que este es el máximo responsable de proteger y dar orden a una sociedad contribuyendo a su máximo desarrollo. Estas acciones se logran a través de sus instituciones o entes gubernamentales los cuales de acuerdo a sus necesidades de intereses se organizan principalmente en sectores administrativos, económicos, social y de seguridad fortaleciendo los poderes existentes como el ejecutivo, judicial y legislativo.

Con los nuevos avances en la actualidad, las instituciones de los Estados centroamericanos han realizado esfuerzos en la modernización de mecanismos que ayuden a fortalecer el impacto del Estado en la sociedad, tomando ejemplo en la ampliación de las Tecnologías de la Información y Comunicación (TIC) en áreas primordiales. Asimismo, de acuerdo a los resultados obtenidos en la aplicación de instrumentos presentes en esta investigación, podemos asumir que la región centroamericana ha fortalecido sus entes gubernamentales mediante la actualización de equipos tecnológicos que fortalezcan sus capacidades, sobre todo en áreas importantes como la

administración pública, economía, servicios básicos y la seguridad y defensa del propio Estado y sus ciudadanos.

También se evidencia el fortalecimiento institucional interno de los Estados por medio de la cooperación con los organismos regionales como el SICA, mediante sus tratados, con la finalidad de fortalecer la capacitación y el desarrollo de acciones para los Estados en materia económica, social y de seguridad.



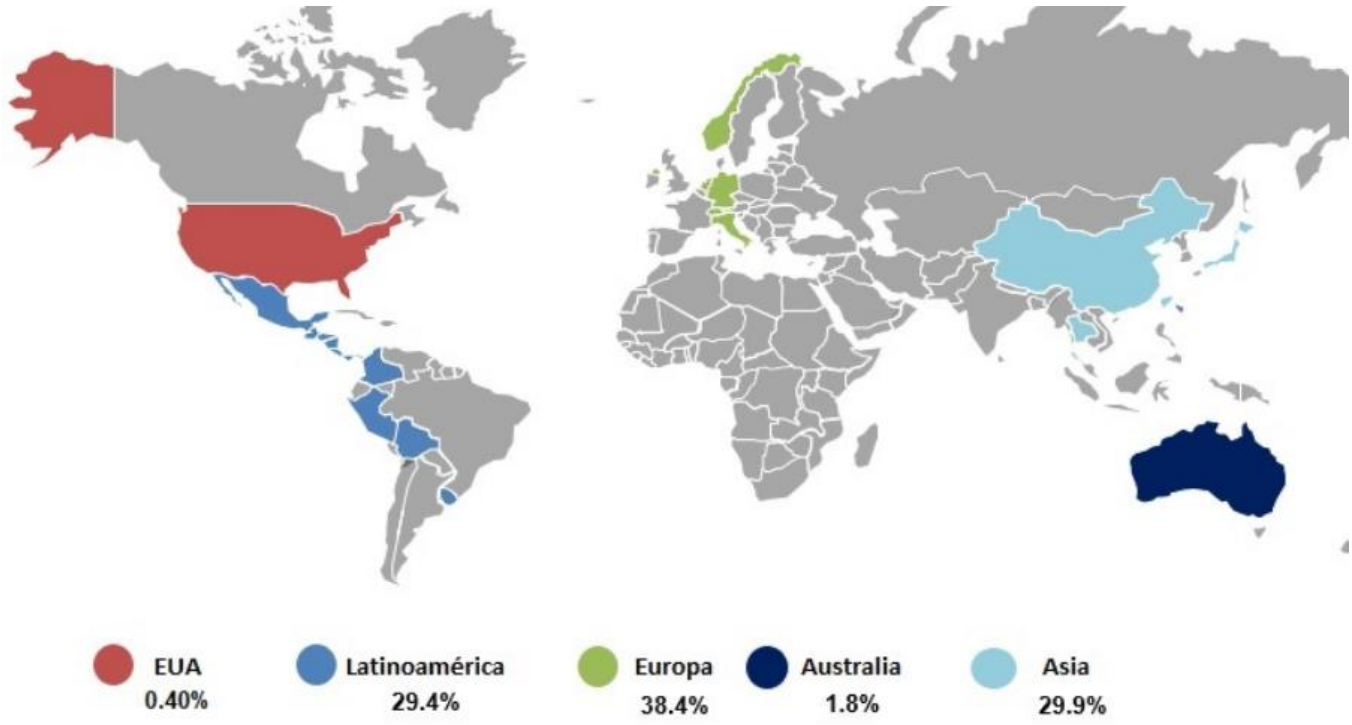
Proyecto de Prevención Social de la Violencia desde los Gobiernos Locales en Centroamérica, parte de la Estrategia de Seguridad de Centroamérica (ESCA) 2015-2017. Fuente: https://www.sica.int/be1/generalidades.aspx

Sistema Financiero: El sistema financiero es otra de las áreas importantes al nivel centroamericano, ya que por medio de este se desarrollan las principales actividades económicas que influyen en las sociedades diariamente, mediante la inversión de capital hacia las actividades productivas de un país aportando al mejoramiento de la calidad de vida de sus ciudadanos como la del Estado. En Centroamérica el sistema financiero se puede clasificar en bancos estatales, financieras y compañías privadas las cuales captan los recursos económicos para que estos se

administren e inviertan de manera eficaz y efectiva para crear una sostenibilidad tanto para los Estados como a la propia región centroamericana.

Los principales bancos en la región tanto privados como estatales se estructuran por su capacidad de abarcar altos niveles financieros en la región como en el Banco de América Central, Banco Promerica, Banco LAFISE Bancentro SA, y el Banco Centroamericano de Integración Económica el cual se destaca por promover la integración económica y el avance económico, social y al otorgar recursos, cooperación técnica a los Estados de la región y sectores privados, siendo el BCIE un ente de suma importancia para Centroamérica, no solamente para el desarrollo socioeconómico también como una forma de fortalecer las iniciativas de cooperación regional en sus distintos campos, abarcando en su impacto la mayoría de la región como podemos observar en las siguientes laminas:

El Banco Centroamericano de Integración Económica (BCIE) tiene su sede en Tegucigalpa, Honduras, y cuenta con oficinas regionales en Guatemala, El Salvador, Nicaragua, Costa Rica, Panamá, República Dominicana y la República de China Taiwán. Fuente: https://www.bcie.org/acerca-del-bcie



Presencia del BCIE en los Mercados de Capitales

La activa participación del BCIE en los mercados de capitales internacionales refleja la buena percepción de su perfil crediticio,

El Banco Centroamericano de Integración Económica (BCIE) tiene más de dos décadas de presencia ininterrumpida en los mercados de capitales internacionales. Fuente: https://www.bcie.org/relacion-con-inversionistas/instrumentos-de-deuda/programas-de-mediano-y-largo-plazo

El patrimonio de los sistemas financieros o bancarios centroamericanos según el informe del sistema bancario de Centroamérica, ha tenido un aumento mayor del 80% en relación al 60% durante el año 2019, lo que representa que la banca centroamericana mantiene una importante línea de activos, los cuales pueden estar sujetos a cualquier incidencia que desea perjudicar a este sector por motivos económico; lo que repercutiría en la perdida de niveles de seguridad y confianza del sector financiero o bancario hasta llegar a una ruina o crisis económica tanto al nivel interno de un Estado como la región en general.

Cabe resaltar, que Centroamérica lleva un proceso de modernización financiera para mejorar el impacto del desarrollo y movilidad económica como las inversiones proyectos, transacciones regionales y proyecciones de moneda según los datos del SIECA 2019, destacando a su vez el empleo de los Estados en nuevas áreas como las criptomonedas en el caso de El Salvador, lo que requiere a su vez un sistema financiero seguro con sus respectivas capacidades.

Consejo Monetario Centroamericano
Secretaría Ejecutiva

REM N° 259, octubre-21

PROYECCIONES/METAS 2021-2022 DE LOS PRINCIPALES INDICADORES MACROECONÓMICOS

Cuadro 1

Inflación (IPC) porcentajes	2018	2019	2020	Proyección inicial 2021	Proyección revisada 2021	Proyección 2022
Costa Rica	2.0	1.5	0.9	3.0 ± 1	3.0 ± 1	3.0 ± 1
El Salvador	0.4	-0.01	-0.1	n.d.		n.d.
Guatemala	2.3	3.4	4.8	4.0 ± 1	4.0 ± 1	4.0 ± 1
Honduras	4.2	4.1	4.0	4.0 ± 1	4.0 ± 1	4.0 ± 1
Nicaragua	3.9	6.1	2.9	3.5 - 4.5	4.5-5.5	n.d.
Rep Dominicana	1.2	3.7	5.6	4.0 ± 1	4.0 ± 1	4.0 ± 1
Promedio región CA	**2.0**	**3.0**	**3.7**	**n.d.**		**n.d.**

Cuadro 2

PIB real variación anual	2018	2019	Preeliminar 2020	Proyección inicial 2021	Proyección revisada 2021	Proyección 2022
Costa Rica	2.6	2.3	-4.1	2.6	5.4	4.5
El Salvador	2.4	2.6	-7.9	9.0	10.3	n.d.
Guatemala	3.3	3.9	-1.5	2.5 - 4.5	4.0 - 6.0	3.5-5.5
Honduras	3.8	2.7	-9.0	3.2 - 5.2	8.0 - 9.0	3.2 - 5.2
Nicaragua	-3.4	-3.7	-2.0	2.5 -3.5	6.0 - 8.0	n.d.
Rep Dominicana	7.0	5.1	-6.7	5.5	10.7	5.5
Promedio región CA	**3.9**	**3.2**	**-5.0**	**4.2 - 5**		**n.d.**

Cuadro 3

Cuenta Corriente/PIB porcentajes	2018	2019	Preelimin ar 2020	Proyección inicial 2021	Proyección revisada	Proyección 2022
Costa Rica	-3.0	-2.1	-2.2	-3.0	-3.8	-2.5
El Salvador	-3.3	-0.6	0.5	n.d.		n.d.
Guatemala	0.9	2.3	5.1	4.7	4.4	4.7
Honduras	-5.45	-1.4	3.8	-2.9	-2.1	-2.0
Nicaragua	-1.8	6.0	7.6	n.d.		n.d.
Rep Dominicana	-1.5	-1.3	-2.0	-1.5 a -2	-1.6	n.d.
Promedio región CA	**-1.7**	**-0.3**	**1.22**	**n.d**		**n.d.**

Cuadro 4

RIN del Banco Central en millones de US$	2018	2019	2020	Proyección inicial 2021	Proyección revisada 2021	Proyección 2022
Costa Rica	7,495	8,912	7,225	9,377		n.d.
El Salvador	3,354	3,936	2,915	n.d.		n.d.
Guatemala	12,756	14,789	18,468	20,468	20,468	20,468
Honduras	4,853	5,809	8,149	n.d.		n.d.
Nicaragua	2,039	2,209	3,074	n.d.		n.d.
Rep Dominicana	7,627	8,781	10,752	n.d.		n.d.
Total región CARD	**38,123**	**44,437**	**50,582**	**n.d.**		**n.d.**

Reporte macroeconómico de los países de Centroamérica, República Dominicana y Panamá, que revelan los principales indicadores bancarios de cada país. Fuente: https://www.secmca.org/periodo_informe/mensual/

Sector de redes eléctricas: Para abordar el sistema de interconexión eléctrica en la región, se aborda en primera instancia el Tratado Marco del Mercado Eléctrico de América Central 1997-1998, el cual tiene por objetivo tiene por objetivo contribuir al desarrollo de un mejor suministro de eléctrico en la región, de manera sostenible y competitivo, a su vez que contribuya a la protección del medio ambiente, los gobiernos firmantes de este tratado son Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá, conformando así un mecanismos de integración eléctrica regional.

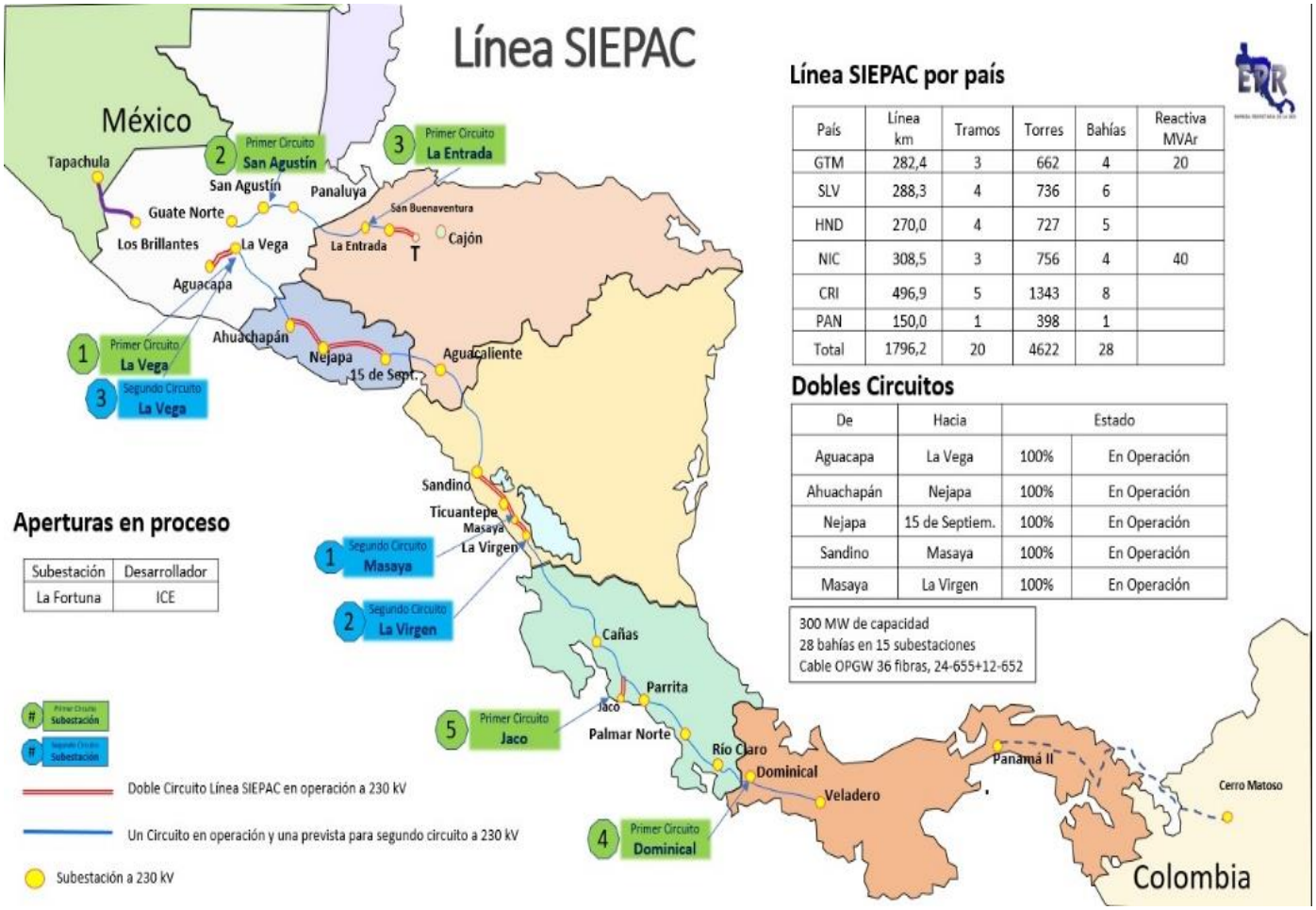
De igual forma por medio del Tratado Marco del Mercado Eléctrico de América Central se conformaron los organismos encargados de la regulación y operación, como son el Ente Operador Regional (EOR), la Comisión Regional de Interconexión Eléctrica (CRIE) y la Empresa Propietaria de la Red (EPR) como base para la implementación de la infraestructura eléctrica centroamericana conocida como el Sistema de Interconexión Eléctrica de los Países de América Central (SIEPAC). Este sistema contribuye al desarrollo de una energía eficaz y sostenible para los Estados centroamericanos, destacando sus principales características como la de otorgar un sistema de transmisión seguro, reducción de costes en generación eléctrica, ampliación de las capacidades de transmisión entre los Estados de la región y la creación de iniciativas para implementar energías renovables.

Mercado Eléctrico Regional (MER) • El MER es el ámbito en el que se realizan las transacciones regionales de electricidad entre los agentes del mercado. Intercambios de corto plazo, derivados de un despacho económico regional de energía.

Fuente: https://publications/spanish/document/Integración-eléctrica-centroamericana

El SIEPAC está compuesto por 1,830 Km de tendido eléctrico de 230Kv, recorriendo los cinco países de la región, desde Guatemala hasta Panamá, conformándose un total de 15 subestaciones, por medio de 28 bahías de acceso, lo cual permite fortalecer los índices de amplitud

y calidad del suministro eléctrico. Asimismo, este sistema eléctrico regional ha permitido la realización de dos grandes proyectos de interconexión, México-Guatemala y Panamá-Colombia, aumentando la calidad y el desarrollo de la interconexión eléctrica, a su vez la generación de nuevas fuentes económicas que beneficien a la región y sus usuarios, como se presenta en las siguientes imágenes:



El componente de infraestructura (SIEPAC), bajo responsabilidad de la EPR, consistió primordialmente en el diseño, ingeniería y construcción de aproximadamente 1.820 kilómetros de líneas de transmisión de 230 kv con previsión en torres para un segundo circuito futuro, las que se conectan a 15 subestaciones de los países de la región, mediante 28 bahías de acceso, y además se incluyen equipos de compensación reactiva.

Fuente: [Descripción: Línea SIEPAC (eprsiepac.com)]

Interconexión Panamá-Colombia

La interconexión eléctrica entre Colombia y Panamá es un complemento fundamental para la consolidación de la visión de integración regional. El desarrollo de este proyecto representa la integración de la Comunidad Andina con Mesoamérica (quien ya cuenta con un mercado organizado a través de la red SIEPAC), y su ejecución posibilitará el acceso a fuentes de generación económicas con beneficios para los usuarios.

Fuente: https://www.eprsiepac.com/contenido/wp-content/uploads/Diagrama-Interconexion-Panama-Colombia.jpg

El proyecto consiste en una línea de transmisión 400 KV de 98.6 Km (27 Km en México y 71.6 Km en Guatemala) con un circuito habilitado y las estructuras preparadas para doble circuito, la ampliación subestaciones Los Brillantes y Tapachula, con una capacidad transformación de 225 MW iniciales.

Fuente: Descripción: Línea SIEPAC (eprsiepac.com)

Los sistemas de interconexión de Centroamérica, así como los internos de cada Estado que conforma la región, son vitales para el quehacer de los ciudadanos, sobre todo para la funcionalidad del Estado y las áreas primordiales como los sectores de salud en hospitales, centros de atención médica, empresas privadas, centros financieros, equipos de información y comunicación, plantas de suministro de agua potable, gas, combustible, así como los sectores transporte y de seguridad.

Por lo tanto, el factor energético se convierte en una de las principales infraestructuras críticas en la región, por su importancia para los ciudadanos, así como para los Estados en general, ya que, si el sistema de interconexión eléctrica centroamericano llegase a tener alguna falla provocada o alguna incidencia negativa, las consecuencias serían altamente perjudiciales para la región, así como para su entorno paralizando la actividad humana y provocando afectaciones serias en las áreas vitales de los Estados y su ciudadanía.

Sector de telecomunicaciones: En cuanto al sector de las telecomunicaciones en Centroamérica, se encuentra la Comisión Técnica Regional de Telecomunicaciones (COMTELCA), la cual surge por medio del Tratado sobre Telecomunicaciones, 1966, conformado actualmente por las Repúblicas de Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panamá, República Dominicana y México. COMTELCA tiene por objetivos coordinar la integración y el desarrollo de las telecomunicaciones regionales, así como las internacionales que se presentan en Centroamérica, mediante un marco jurídico que ayuda a armonizar, administrar y dictar regulaciones o resoluciones de estricto cumplimiento en esta materia.

La Comisión Técnica Regional de Telecomunicaciones (COMTELCA) está conformada por 8 miembros designados por los países de la región, los cuales se clasifican en las principales instituciones de carácter gubernamental, que abordan los asuntos referentes a las telecomunicaciones, por tanto, la representación estatal es de suma importancia debido a que muestra hasta donde han llegado a tener impacto las Tecnológicas de la Información y Comunicación (TIC) al forman parte de un área importante de un Estado.

Asimismo, al nivel regional, se cuenta con la presencia de la Red Centroamericana de Telecomunicaciones (REDCA) la cual es un operador de transporte de banda ancha en base a la línea SIEPAC y dirigidas a un gran parte de las telecomunicaciones. REDCA fortalece a la región centroamericana en materia de interconexiones innovadoras, tomando ejemplo con la presencia de 10 puntos de operaciones desde Guatemala hasta Panamá, 3 conexiones de cable submarino, 12

nudos de amplificación y 9 conexiones de salida internacional. Las telecomunicaciones en Centroamérica, han contribuido al mejoramiento de la calidad de vida de los ciudadanos y el desarrollo de nuevos campos que alcance de la comunicación y el quehacer de los Estados.

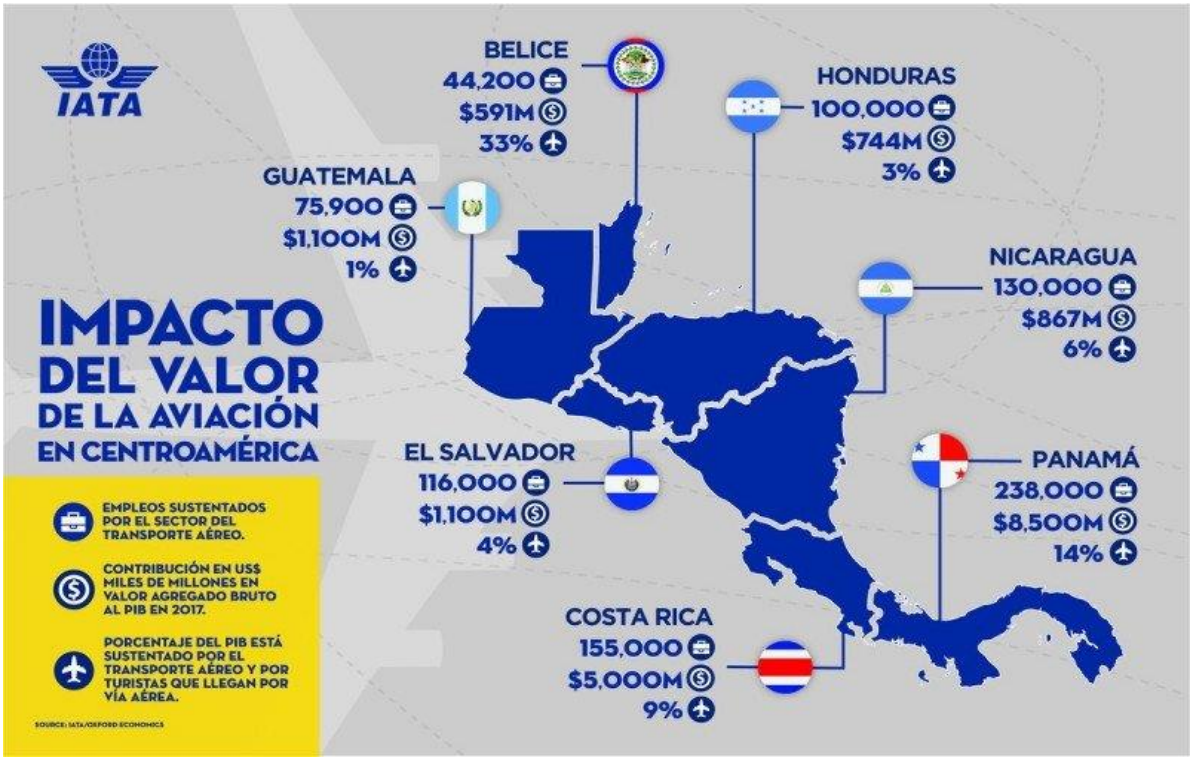
El REDCA tiene por misión ofrecer soluciones de transporte de banca ancha terrestre innovadoras, que apoyen el crecimiento de la región

Fuente: http://www.redcasiepac.com/red/mapa

Sector aeropuertos: El sector aeroportuario al nivel centroamericano, representa una de las infraestructuras críticas más vitales, ya que por medio de este campo se impulsa la innovación en la comunicación al conectar por vía aérea diferentes factores, sobre todo a las personas y los Estados. Para Centroamérica esto se traduce en uno de sus principales objetivos, como es el progreso económico, se aumentan los niveles de acceder a los mercados globales y generar el consumo con la llegada de ciudadanos extranjeros, impulsando a su vez el desarrollo de empleos.

Del mismo modo, la Secretaria de Integración Económica Centroamericana (SIECA), por medio del Consejo Sectorial de Ministros de Centroamérica, (COMITRAN) resalta la importancia que posee el sector aeroportuario, no solamente por las capacidades económicos que este presenta, también por las iniciativas de desarrollo en cuanto a la adquisición de nuevas tecnologías que permiten sus actividades, tomando ejemplo en la composición de radares, sistemas de operaciones y tránsito aéreo, instalaciones de seguridad, navegación y radio ayuda. Según los datos del SIECA

2019, se contemplan entre 20 principales aeropuertos los cuales han transportado más de 422, 510 volúmenes de carga, aumentando la competitividad en Centroamérica y generando mayores oportunidades para los países y sus ciudadanos en mejorar la economía.



La aviación genera 859.000 empleos y aporta US$ 17.900 millones al valor añadido bruto del PIB total de los siete países de América Central.

Fuente: https://www.hosteltur.com/lat/123290_aerolineas-reclaman-mejores-condiciones-gobiernos-centroamerica.html

Asimismo, para los Estados de la región, el sector aeroportuario representa un reto, sobre todo para su seguridad y estabilidad mediante mecanismos que permitan la protección física de sus instalaciones como la de sus componentes tecnológicos internos, mediante iniciativas de seguridad cibernética. Lo cual permita consolidar los niveles de estabilidad interna de los Estados, así como el bienestar de los ciudadanos, ya que por medio del transporte aéreo son los primeros en estar expuestos ante cualquier acción que se ejecute en esta área, sobre todo si en un dado caso ocurre alguna incidencia negativa, lo que repercutiría directamente en la pérdida de vidas humanas.

Sector de agua potable, plantas de tratamiento, tuberías de gas y petróleo: Según los diagnósticos y estudios por parte de la CEPAL en la región, el gas natural y el petróleo en la actualidad son las principales fuentes de energía para Centroamérica, utilizándose para uso doméstico, industrial y de comercio lo cual se puede asumir que este recurso forma parte diaria en el quehacer de los ciudadanos, así como el desarrollo de los Estados que conforman la región. A su vez, el SICA en sus iniciativas de cooperación regional, resaltan la importancia del agua potable y las plantas de tratamiento, para el avance de la sociedad, más aún cuando se trata de modernizar los alcances que tienen estos valiosos recursos, otorgando una mejoría en las condiciones de vida de los ciudadanos, así como el resto de los sectores que necesitan del vital líquido como el agua para cumplir con sus diversas necesidades e intereses.

La modernización de las plantas encargadas de la administración y suministro del agua potable, cuentan con sistemas novedosos como el SCADA (Software de adquisición de datos y control de supervisión) el cual otorga una automatización a los equipos encargados de almacenar y procesar alguna materia, mejorando el rendimiento, el servicio y calidad del mismo. Al nivel centroamericano, en materia de sistemas modernos que administren recursos importantes como el agua, se estima que más de 120 plantas hidroeléctricas y térmicas funcionan bajo esta lógica, logrando un alto avance en la actualización de los servicios básicos, sobre todo aquellos que son indispensables en el quehacer humano.

Agregando a su vez, los que suministran el desarrollo de las industrias como son el petróleo y el gas natural, consolidándose junto con el agua y sus estructuras de las plantas de tratamiento, como los ejes de mayor valor para la región, si alguno de estos llegasen a tener un impacto negativo en sus componentes, se presentaría un serio detrimento en los servicios básicos de un país, afectando directamente a los ciudadanos y todo los sectores que necesiten de estos recursos para cumplir sus labores.

Sector de puertos marítimos: Las demandas en el comercio global y la implementación de nuevas tecnologías a causa del proceso de la globalización, ha requerido que los Estados centroamericanos inviertan en mejorar sus infraestructuras portuarias para desarrollar una mejor competitividad y eficacia en el comercio marítimo mundial. Entre los principales órganos regionales que destacan en esta materia, se resalta La Comisión Centroamericana de Transporte Marítimo (COCATRAM) fundada el 15 de julio de 1980, el cual es un órgano especializado del

Sistema de Integración Centroamericano (SICA), teniendo por objetivo la creación de políticas marítimas portuarias que permitan crear una sostenibilidad y competitividad en la región, mejorando su posicionamiento en el comercio internacional.

Estadísticas Marítimas de los principales puertos (año 2019)

País	Puerto	Carga (TEU)
Guatemala	Quetzal	507,810
	Barrios	420,827
	Santo Tomás	565,389
El Salvador	Acajutla	249,472
Honduras	Cortés	643,856
	Castilla	110,000
	San Lorenzo	36,851
Nicaragua	Corinto	167,798
Costa Rica	Caldera	298,175
	Limón - Moín	218,688
	TCM	1,011,703
Panamá	Balboa	1,762,417
	PSA	873,361
	Colón	784,252
	Manzanillo	2,313,346
	Cristóbal	975,213
	TOTAL	10,939,158

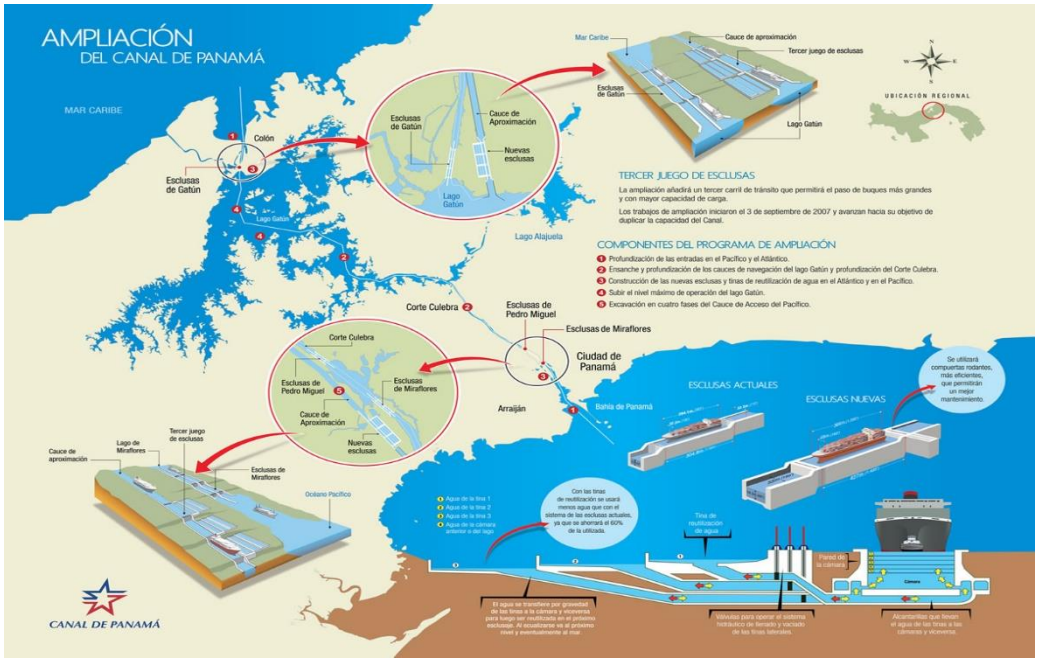
Fuente: SIECA

La Política Marco Regional de Movilidad y Logística de Centroamérica contempla los diversos ejes sectoriales que rigen el funcionamiento de los modos de transporte y determinan el desempeño logístico de la región: marítimo-portuario, aeronáutico-aeroportuario, ferroviario y carretero. Esta también comprende los ejes transversales que impulsan el comercio, la transformación productiva, la operación coordinada en los puestos fronterizos y la movilidad de personas.

Fuente: Mapas de infraestructura de Centroamérica – SIECA

Actualmente, COCATRAM está compuesto por Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, y Panamá, del mismo modo que cuenta con la participación de entidades privadas, las cuales trabajen de manera cooperada para lograr un avance socioeconómico productivo en la región. Del mismo modo el SIECA, establece los principales puertos en la región, los cuales se distribuyen desde Guatemala hasta Panamá, consolidándose en un total de 25, que a su vez durante el año 2019 tuvieron un alto porcentaje de carga, valorada en un total de 10,939,158 dólares. Lo que representa su alto valor estratégico para el ámbito económico de los Estados centroamericanos, lo cual, debido a esto, los puertos se han adaptado a las Tecnologías de la Información y Comunicación (TIC) con la finalidad de mejorar sus capacidades y otorgar un mejor desempeño en sus áreas.

Canal de Panamá: El canal de Panamá representa la principal fuente de comercio exterior que influye en la región centroamericana, debido al papel que este ocupa al ser una ruta marítima importante para el comercio global, convirtiéndose en una de las más transitadas por distintas embarcaciones las cuales incrementan el tráfico y venta de productos o recursos que tienen un alto valor para la región, como el suministro de petróleo, recursos industriales, materia prima, tecnología, alimentos entre otros.



El canal de Panamá es un importante eslabón de la SC mundial por su excelente ubicación acortado distancias y como CD de mercancías a diversos países de la región.

Fuente: https://www.eoi.es/blogs/madeon/2015/05/31/influencia-de-la-proxima-ampliacion-del-canal-de-panama-en-las-rutas-de-transporte-de-mercancias-2/

El Canal de Panamá conecta 144 rutas marítimas y 1,700 puertos en 160 países. Estas son las principales rutas que utilizan los buques que transitan por el Canal.

Fuente: https://www.trendsmap.com/twitter/tweet/1304166507652448256

En consecuencia, el canal de Panamá se convierte en una infraestructura importante y compleja debido a las exigencias de la actualidad en materia tecnológica y de modernización, sobre todo cuando hay un nivel de dependencia alto por parte de la región centroamericana y el comercio global, sumado a la incorporación de nuevas tendencias que pueden tener influencia en la región como la búsqueda de nuevas rutas de comercio mundial y la modernización de planes estratégicos para la incrementación de la interconectividad global.

Para Centroamérica esto representa un reto común para todos los Estados en materia de seguridad, sobre todo en ciberseguridad y ciberdefensa, puesto que un ciberataque en los sistemas de interconexión o telecomunicación pertenecientes al canal de Panamá perjudicaría la interconectividad regional a gran escala, afectando también las regiones cercanas y el comercio marítimo internacional, sumando que se presentaría un deterioro en los niveles de seguridad a tal

grado de que el Estado Panameño no pueda responder ante una incidencia como esta. Es por ello que el canal de Panamá representa una de las principales infraestructuras críticas de la región, por su gran capacidad la cual también podría convertirse en un gran impacto negativo.

4.2 Riesgo que representa la ciberdelincuencia para los Estados centroamericanos

La región centroamericana a causa de sus necesidades y demandas internas que poseen los Estados que la conforman, se ha caracterizado por mantener un avance tecnólogico, especificamente en sus áreas esenciales como economía, el sector social, sector financiero, infraestructura, gobernabilidad, institucionalidad, seguridad entre otros. Sin embargo hay otros sectores que más destacan como son el campo de la interconectividad eléctrica y telecomunicaciones, debido que por su posición geógrafica, Centroamérica representa un punto estratégico que une tanto el norte como el sur del continente americano, además de las dos salidas tanto al Oceano Pacifico como el Mar Caribe, lo cual significa un mayor tránsito o movilización de múltiples sectores, por tanto es justificable que la región desarrolle condiciones tecnólogicas para facilitar tanto su progreso interno Estatal como al nivel regional.

No obstante, los países centroamericanos han presentado algunas deficiencias en materia de seguridad cibernética para los avances y modernización tecnológica que han implementado, lo cual representa un punto alto de vulnerabilidad para estos, especialmente si los avances están ligados o dirigidos a la infraestructura crítica de que ayudan al desarrollo de los propios Estados como a la región en general. La discusión sobre dichos avances pueden surgir en diversos puntos, tomando enfasis en la capacidades que poseen los Estados tanto institucionales, ecónomicas, jurídicas y humanas, destacando a su vez la voluntad política, no obstante no deja de ser un tema importante por su magnitud de impacto que pueda representar un ciberataque a las capacidades de los Estados.

De igual manera, se resalta que la región posee una infraestructura interconectada entre los países como lo expuesto en anterioridad con la capacidades de los Estados, lo que permite una mayor vulnerabilidad y peligro ante amenazas como la ciberdelincuencia o la presencia de ciberamenazas inminentes, que no solamente pueden afectar las capacidades materiales, tambien puede colocar una situación de riesgo o peligro a vidas humanas que ese beneficien o utilicen los servicios esenciales para diversas actividades de interes y desarrollo.

Llegando a valorar si se presenta una incidencia maliciosa en las capacidades críticas de los Estados centroamericanos, resultaria en una afectación por igual y constante teniendo en cuenta los niveles de ataque que posee la ciberdelincuencia como se demuestra en la siguiente imagen:

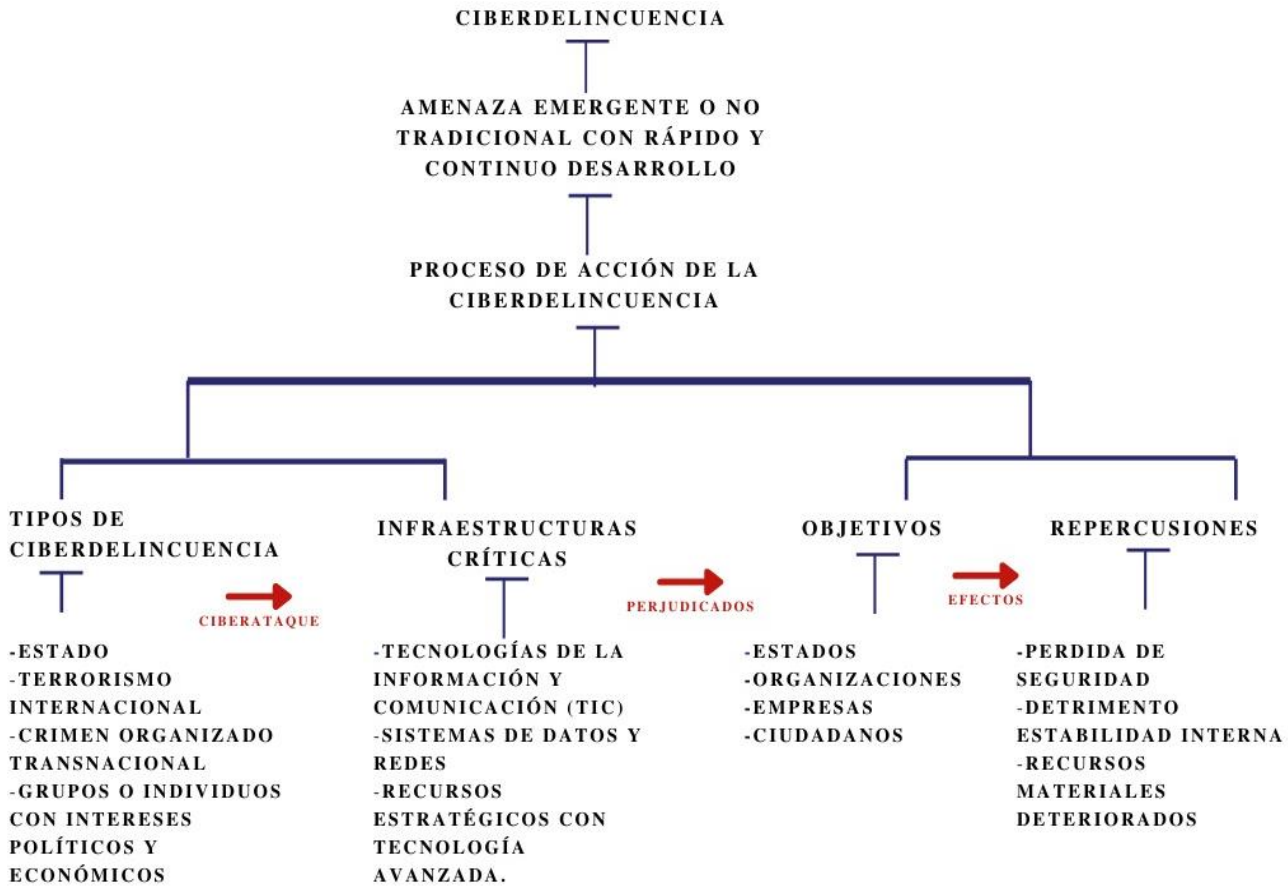
Figure 3 Tipos de amenaza por parte de la Ciberdelincuencia y su nivel de gravedad

Fuente: Elaboración propia.[3]

[3] Nota: El presente esquema refleja las amenazas que ejerce la ciberdelincuencia en sus diferentes modalidades y su impacto en sus diversos objetivos estratégicos.

Cabe destacar que las vulnerabilidades que se presentan en la región, se deben a la falta de un concenso amplio entre los Estados sobre la temática, en otras palabras una voluntad política lo que ha conllevado a que estos mismos, establezcan sus iniciativas de ciberseguridad y ciberdefensa de manera propia , reduciendo las posibilidades de establecer un eje seguro en la región. A su vez,ocasionando una brecha de seguridad cibernética en la región, en otras palabras algunos Estados se encuentran mejor capacitados y desarrollados que otros, creando una región dispareja, cuando deberia de ser lo contrario para prevenir un impacto grave de la ciberdelincuencia, a pesar que ya la región cuenta con algunos antecedentes de ello como son sus mecanismos de orden jurídico, y sus instituciones gubernamentales, que pueden ser parte de la articulación de una sola estrategia regional que permita el desarrollo factible de una ciberseguridad homologada.

Figure 4 Proceso de acción de la Ciberdelincuencia



Fuente: Elaboración propia.[4]

[4] Nota: El presente mapa conceptual muestra el proceso operativo que posee la ciberdelincuencia al delimitar sus objetivos, de acuerdo a sus intereses y tipos de ciberdelincuentes, además de los efectos de sus incidencias en recursos estratégicos

Según los autores Rugama & Rodriguez, (2019), los antecedentes con mayor caracteristica o relevancia sobre la actividad de ciberdelincuencia en la región centroamericana, constan desde el año 2013 hasta 2018, los cuales tres pueden estar cátalogados como alteraciones a la seguridad nacional e incidencia hacia las infraestructuras críticas de un país, tomando ejemplo en la XXVI Cumbre Ibearoamericana en Guatemala, "Kackeo Defacement" de Costa Rica y "Phishing" Banco General de Panamá.

Estos sucesos generados por la ciberdelincuencia representan un alto peligro por su impacto, además que refleja su capacidad operativa al delimitar sus objetivos, en este caso entes gubernamentales, los cuales poseen recursos de gran valor y se encuentran conformados por tecnológias modernas que no poseen una protección y defensa eficaz ante una amenaza o ataque, esto tambien es sustentado a lo expuesto por el MSc. Padilla cuando resalta que "Dentro de las amenazas internacionales podemos contemplar: El Canal de Panamá, así como su Aeropuerto Internacional que es considerado como un punto de Unión de las Américas por sus numerosas conexiones, sus principales aerolíneas son Copa Airlines y Star Alliance para América Latina y el Caribe. A su vez conecta a más de 84 ciudades de América y Europa en 34 países con la que cubre gran parte de Latinoamérica y también tiene vuelos a Asia. Es por ello que el aeropuerto Internacional de Tucumán moviliza alrededor de 12 millones de personas al año, todo ello sumado representa un objetivo vital el cual puede sr blanco de un ciberataque".

Del mismo modo, al nivel regional con los organismos de integración existentes como el Sistema de Integración Centroamericano (SICA), en base a los resultados de las herramientas metodológicas aplicados para esta investigación, podemos resaltar que los sucesos de ciberataques o incidencias de ciberamenazas, son tomados en secreto por cuestiones de seguridad del organismo. Sin embargo, no se descarta la posibilidad de que los organos regionales de integración como el SICA hayan sido blancos de ataques o victimas de la ciberdelincuencia, demostrando el grado de la problemática y los alcances que esta pueda tener.

Asimismo, bajo esta lógíca, se puede plantear que pueda ocurrir algún suceso que afecte considerablemente la región en general, como puede ser la equivalencia a un ciberataque al sistema de interconección centroamericano, el cual también esta sujeto a otros sistemas eléctricos como el Mexicano y Panameño.

Tambien podrían ser blanco los sistemas de radares o tránsito aéreo que poseen los aeropuertos de cada Estado en Centroamérica , lo que causaria un desastre a gran escala en la región como al nivel internacional o mundial, repercutiendo no solamente en daños materiales y de la degradación de los niveles de seguridad, también se contaría con la pérdida de vidas humanas inocentes, valorando incluso este tipo de escenario como producto de un terrorismo cibernetico con fines macabros los cuales hoy en dia estan dentro de diversas probabilidades en terminos de seguridad naciconal.

Del mismo modo, otras infraestructuras críticas o recursos de gran valor pueden estar sujetos a estos impactos, como los sectores portuarios y las bancas y financieras, los cuales ambos constituyen la vertebra de la economía regional y las principales actividades que contribuyen a la interconección global. En este caso se resalta el papel que juega el canal de Panamá como punto estratégico para el comercio global, y los sectores de la banca regional, principalmente aquellos que aportan directamente en el desarrollo financiero regional como el Banco Centroamericano de Integración Económica, el cual si es objetivo de un ciberataque puede tener como resultado la quiebra total en sus activos y la fuga de capitales regionales e inversión extranjera.

Por lo tanto se puede tomar como un ejemplo claro de la capacidades que posee la ciberdelincuencia al penetrar a las estructuras internas tanto de los Estados como otros sectores, mediante el uso del ciberespacio como campo para llevar a cabo sus acciones delictivas. Los riesgos que representa la ciberdelincuencia son altos por sus capacidades y modo de operación, no obstante estos se multiplican y se fortalecen aún más cuando el objetivo de estos no posee un mecanismo de protección y defensa, en este caso asumiremos que la región centroamericana tiene algunos instrumentos que son eficientes para proteger sus recursos ante un incidente cibernético como las medidas internas de los Estados, pero esto no significa que garantice a la totalidad la seguridad de los recursos o las capacidades de un Estado.

Debido que tanto la ciberseguridad como la ciberdefensa requieren de un contínuo desarrollo y actualización, lo que representa un reto para los Estados de la región. Por ende los Estados centroamericanos se acoplan a sus condiciones y capacidades, si fuese de una manera homologada la región podría tener mejores estandares de desarrollo para su seguridad, además que representaria una sólida resiliencia unánime.

4.3 Importancia de un mecanismo centroamericano homologado en materia de ciberseguridad y ciberdefensa.

La región centroamericana como hemos abordado en anterioridad, lleva un proceso de modernización en sus diferentes áreas, especialmente cuando se trata de las propias capacidades que posee un Estado. Sin embargo, estas acciones de actualización tecnológica son llevadas a cabo sin el respaldo de una sólida seguridad cibernética lo que conlleva a crear niveles de vulnerabilidad altos y la región puede estar propensa ante un ciberataque por parte de la ciberdelincuencia lo que causaría la perdida de los niveles de seguridad y estabilidad en la región, así como para los propios Estados.

Para que la región centroamericana evite este tipo de escenario necesita contar con instrumentos eficaces en materia de ciberseguridad y ciberdefensa, especialmente con un mecanismo que sea homologado por los Estados y permita la coordinación, articulación y desarrollo de políticas de seguridad cibernética al nivel centroamericano. Sin embargo, lo único referente a instrumentos de seguridad cibernética son los de orden jurídicos e institucional que posee cada Estado, pero surge el cuestionamiento de que tan eficaces son los instrumentos que tienen los Estados centroamericanos en materia de ciberseguridad o ciberdefensa, sobre todo si estos en realidad son factibles para proteger y neutralizar un ciberataque dirigido hacia un recurso de alto valor estratégico.

Los instrumentos de ciberseguridad o ciberdefensa que posee cada Estado centroamericano se adecua con los recursos que estos disponen para emplearlos, creando como resultado una disparidad en seguridad cibernética lo que en algunos casos resta la efectividad, debido que unos Estados poseen mejores capacidades que otros para contar una ciberseguridad y ciberdefensa más factible y en constante actualización, mientras que otros priorizan áreas esenciales para evitar un desgaste en su capacidad económica e institucional como lo expone el MSc. Barberena al explicar que “Algunos Estados o bien gobiernos delimitan una guía o programa nacional de cómo abordar la ciberseguridad desde diversos puntos, ya sea de seguridad o protección al individuo, de seguridad económica y política, o bien de seguridad en las infraestructuras críticas lo que a veces resulta en parte bien para los países que lo realizan, pero no eficientemente para hablar de una seguridad concreta en la región”.

En general los Estados cuentan con instrumentos de ciberseguridad y ciberdefensa, pero se estructuran en base a las condiciones que estos tienen internamente, y mediante sus propios intereses y no colectivamente. Por ende, Centroamérica no cuenta con un mecanismo homologado que ayude a proteger y defender de manera coordinada y armonizada a la región ante un ciberataque. La falta de un mecanismo homologado al nivel regional se puede abordar en diferentes perspectivas, pero en base a los resultados obtenidos mediante la aplicación de entrevistas, se destaca una variable que constantemente ha permanecido en Centroamérica, sobre todo cuando se trata en temas de integración, y es la falta de una voluntad política.

La falta de una voluntad política entre los Estados desarticula las posibilidades de establecer una ciberresiliencia centroamericana de manera consensuada, la escasa voluntad política se refleja en diferencias ideológicas, económicas y hasta en los conflictos limítrofes lo que repercute en un aumento de los niveles de inseguridad cibernética para la región al no disponer de una iniciativa que ayude a aumentar las capacidades de protección y defensa ante un ciberataque. La voluntad política es la que define el rumbo de la región como lo expresa el MSc. Padilla "Lo primordial es la existencia de una voluntad política y confianza entre los Estados miembros, voluntad que les permita negociar, consensuar y ejecutar estrategias, planes y programas regionales que les permita prevenir y contrarrestar tipo de actividades".

Por lo tanto, la homologación de una ciberseguridad centroamericana representa un reto para los Estados de la región, puesto que se necesita de la voluntad y confianza de todos los Estados para disminuir la brecha de seguridad cibernética, a su vez que permita crear mecanismos eficiente para contrarrestar eficientemente las acciones de la ciberdelincuencia, debido que Centroamérica esta propensa a ataques cibernéticos o bien presentar una mayor vulnerabilidad para aquellos entes que ya han sido víctimas de un ciberataque tal como lo plantea el MSc. Padilla en la entrevista realizada al destacar que "En casos como las organizaciones que se han visto afectadas muchas veces toman la decisión de mantener estos sucesos en secreto; siempre y cuando estos eventos no sean obviados a los usuarios y se mantenga en estricta discreción, y así prevenir repercusiones que comprometan seriamente la organización, es decir el posible flujo de sus usuarios (cuentahabientes) en el caso de bancos; por perder confiabilidad al admitir que sus sistemas fueron burlados y generar desconfianza debido a su exposición a vulnerabilidades de ciberseguridad".

Asimismo, tanto la ciberseguridad como la ciberdefensa requieren de todo un programa completo para lograr sus objetivos de mantener seguro las capacidades tecnológicas de un área estratégica, esto implica el tener condiciones eficientes como los mecanismos institucionales, así como los recursos para sustentar y desarrollar las acciones de respuesta cuando se presente una eventual amenaza cibernética. Puesto que al implementar una ciberseguridad se está creando una espacio o ambiente de resiliencia o dicho de otra manera una administración del riesgo mediante un sistema de prevención. Lo mismo sucede en el caso de la ciberdefensa, para que esta tenga una buena efectividad necesita disponer de capacidades que le permitan actuar, como se menciona en el marco conceptual de esta tesis, la ciberdefensa radica comúnmente en las políticas de defensa y está articulada para defender, neutralizar y adaptarse ante cualquier hecho perjudicial del ciberespacio.

Centroamérica por su actualización tecnológica y las nuevas amenazas que operan en la actualidad por medio del ciberespacio, se presenta la necesidad de homologar un mecanismo de ciberseguridad y ciberdefensa, el cual deba ser articulado con las instituciones correspondientes en materia de seguridad nacional y medios tecnológicos. Esto se puede lograr de manera factible puesto que los Estados de la región cuentan con los instrumentos necesarios para consensuar una estrategia en común, tomando énfasis en los mecanismos de orden jurídico que está presente en el marco legal de esta tesis, conformado por las constituciones, leyes, códigos, decretos e instituciones gubernamentales que abordan el campo de la ciberseguridad y ciberdefensa.

A manera de ejemplo de una convalidación de estos mecanismos podemos tomar primeramente que los Estados definan y consensen la aceptación de una amenaza para Centroamérica como es la ciberdelincuencia, posterior a ello plantear una repuesta hacia esta problemática demostrándolo en un solo programa regional que abarque de manera unánime los instrumentos que tienen los Estados, los cuales en la actualidad no tienen un solo parámetro que homologue una sola acción tal como hace referencia el MSc. Padilla “En los países del SICA solo Panamá, Guatemala, Costa Rica y República Dominicana cuentan con una estrategia de ciberseguridad. En el caso de la Estrategia Nacional de Seguridad Cibernética de Guatemala muestra un panorama global, en el cual evalúa el estado de la seguridad cibernética del país, involucrando a todos los sectores de manera directa o indirectamente”.

De igual forma, haciendo énfasis a la convalidación de instrumentos, podemos resaltar que la mayoría de los Estados de la región centroamericana cuentan con un marco legal que les permite de cierta forma actuar y desarrollar iniciativas en seguridad cibernética, como las disposiciones generales y elementos conceptuales de la constitución, y las leyes de ciberdelito que la mayoría de los Estados de la región poseen los cuales a su vez están presentes en esta tesis. También los Estados estos cuentan con ministerios, comandos, direcciones y unidades especializadas en tecnología y seguridad informática, lo que permitiría la habilitación de una cooperación y coordinación de acciones regionales para fortalecer las capacidades de prevención y repuesta ante un ciberataque por medio del ciberespacio.

Igualmente, Centroamérica cuenta con mecanismos de integración que pueden emplear una mayor cooperación y coordinación, como el SICA, teniendo la capacidad de ampliar iniciativas en materia de acuerdos y adopción de compromisos que beneficien a la región, destacándose áreas económicas, políticas y sociales. Por lo que representaría una base sólida para que los Estados logren acercar una homologación en materia de ciberseguridad, sobre todo lo considerable que pueden ser los protocolos y tratados que este dispone como el Protocolo de Tegucigalpa, el Tratado Marco de Seguridad Democrática y las Estrategias de Seguridad regional y Digital, que, a pesar de no contar tangiblemente con el desarrollo de una ciberseguridad, pueden servir para consensuar una iniciativa nueva o que actualice los anteriores mencionados.

También otro de los organismos que se encuentran constituidos para la coordinación e integración regional es la CFAC, la cual impulsa esfuerzos a fin de proporcionar un nivel óptimo de defensa contra aquellas amenazas que perjudiquen a los Estados, lo que resultaría factible para la constitución de una iniciativa en materia de ciberdefensa mutua. Es necesario que la región centroamericana utilice los mecanismos disponibles para lograr un acercamiento y armonización de sus intereses, debido que la ciberseguridad y ciberdefensa representa un reto no solamente en temas de acuerdo y homologación, también en cuanto a las capacidades de los recursos que poseen los Estados, especialmente en la adquisición de medios materiales tecnológicos y el sostenimiento económico, por lo que si llegase a haber una unanimidad en esta materia, resultaría beneficioso para la ampliación de las capacidades en todos los Estados.

Es considerable mencionar que por la operatividad que tiene la ciberdelincuencia, y sus respectivos impactos altamente perjudiciales, el campo de la ciberseguridad y ciberdefensa se aborda principalmente en términos de seguridad nacional y seguridad regional, en este caso se abarca ambos conforme a los instrumentos que tienen los Estados como son sus áreas jurídicas e institucionales y que estos brindan seguridad a los Estados. No obstante, Centroamérica al no contar con un mecanismo homologado que fortalezca las capacidades de repuesta ante la ciberdelincuencia, se presenta una alta vulnerabilidad o un riesgo ante un ciberataque que degrade los niveles de seguridad y provoque daño a los medios como las comunicaciones interconectadas, los medios digitales o informáticos y los sistemas de servicios básicos.

En efecto, es fundamental o importante que la región centroamericana disponga de un mecanismo homologado en materia de ciberseguridad y ciberdefensa para brindar resiliencia a las capacidades de los Estados y prevenir cualquier incidente que pueda darse en el ciberespacio, lo que también beneficia a la estabilidad nacional y regional y permita adaptarse y hacer frente a la problemática de la ciberdelincuencia en la actualidad y el futuro. Debido que la tecnología con el tiempo avanza en proporciones altas y es a través de ella que el mundo actual ya sea bajo áreas políticas, económicas, sociales y de seguridad, establecen sus interacciones, lo que conlleva a que Centroamérica acople sus necesidades a estas nuevas formas de desarrollo e interconexión.

Lo cual a mi juicio aportaría beneficiosamente a la región si se poseen los mecanismos adecuados para crear iniciativas en estas materias, pero de lo contrario, solamente se mostrará un aumento de la vulnerabilidad si bien recordamos las capacidades que tiene la región y su rol no solamente para Centroamérica también para el resto del continente y el propio mundo. Por ende, considero que los Estados tienen la viabilidad con sus instrumentos que tienen para lograr establecer una iniciativa que los homologue, ya sea estableciendo un nuevo marco regional o bien actualizar los ya existentes, repercutiendo en una mejoría de las capacidades y estas puedan ser acopladas a los sectores estratégicos.

Estas acciones se pueden llevar a cabo si existe una voluntad política, es importante hacer énfasis en ello, lo cual incide más que las propias diferencias en los recursos o medios que disponga la región, puesto que sin una armonización entre las voluntades de los Estados la región no tendrá un desarrollo factible para su presente y su futuro. Por ende, es necesario que permanezca y se impulse esfuerzos en cooperar políticamente entre los Estados de la región.

CAPÍTULO V

Conclusiones

A manera de conclusión podemos asumir que la región centroamericana posee un alto grado de vulnerabilidad por carecer de una estrategia regional homologada en materia seguridad cibernética, hay que valorar que los Estados de la región han realizado algunos esfuerzos en materia de ciberseguridad y ciberdefensa, pero de manera individual, independiente, por voluntad política nacional pero no ha existido un esfuerzo coordinado al nivel regional que los beneficie mutuamente. Sumado a la creciente demanda en la modernización tecnológica de sectores vitales que contribuyen al desarrollo de los Estados ya sea en materia económica, social, institucional y de seguridad, sin que estos cuenten con un mecanismo de ciberseguridad y ciberdefensa que garantice su bienestar.

Asimismo, Centroamérica no cuenta con un mecanismo homologado que ayude a la coordinación interinstitucional entre los Estados que les permita priorizar, formular y ejecutar una estrategia regional integral en materia de ciberseguridad y ciberdefensa que permita prevenir, proteger y dar respuesta a los ataques cibernéticos, y mejorar los niveles de seguridad y resiliencia en la región ante estas amenazas emergentes no tradicionales de la seguridad regional y nacional. La falta de una estrategia coordinada podría provocar graves daños a las capacidades críticas de los Estados, específicamente a los sistemas tecnológicos que forman parte de sus infraestructuras críticas, cabe resaltar que los ciberataques que podrían ocurrir en la región pueden estar vinculados a diversos motivos, sobre todo los de factor económico, político y de seguridad, lo que representaría una grave degradación de la estabilidad no solamente al nivel interno de los Estados, también para toda Centroamérica, llegando a afectar a otras regiones cercanas.

Por lo tanto, de esta investigación podemos deducir la necesidad real que tienen los Estados centroamericanos en que cuenten con una iniciativa regional integral en materia de ciberseguridad y ciberdefensa que establezca el fortalecimiento de equipamiento tecnológico en los Estados miembros y la creación de mecanismos de coordinación interinstitucional, cooperación técnica, tecnológica y financiera, así como la armonización y homologación de las legislaciones nacionales, que den espacio a un marco legislativo regional, y establezca lineamientos de prevención, protección y repuesta inmediata ante ataques cibernéticos.

Esta Estrategia permitirá a los Estados de la región brindar protección a la infraestructura crítica regional, prevenir y dar respuesta de manera conjunta e integral a las ciberamenazas o ataques provocados por parte de la ciberdelincuencia. De igual forma se resalta la importancia de la presente investigación para evaluar y estudiar a mayor profundidad esta problemática actual, sobre todo en el contexto actual en cual dependemos cada día más de los avances tecnológicos, representando no solamente ámbitos positivos, también repercusiones graves si no se toman las acciones correctas en materia de seguridad.

Recomendaciones

Considerando la importancia que tiene esta investigación y en función de los resultados obtenidos se plantea las siguientes recomendaciones:

Al personal director, docente y alumnos de la UNAN-Managua, especialmente de la Facultad de Humanidades y Ciencias Jurídicas y los estudiantes de la carrera de Ciencia Política y Relaciones Internacionales, que aspiren el tener un profundo interés en esta temática para la elaboración de estudios posteriores que permitan mejores resultados en investigaciones, puesto que este ámbito con el proceso actual de la tecnología y todo su entorno es de continuo desarrollo, y toda norma, acción y resultado hoy en día está regida o bien relacionada a esta área, sobre todo en el campo de las relaciones internacionales, la política, jurisprudencia, seguridad nacional, entre otros ámbitos de vital importancia para los Estados, así como su ciudadanía.

En base a una visión integral para la región centroamericana, se asume que el Protocolo de Tegucigalpa es la base jurídica fundamental que rige cualquier acción coordinada que los Estados de la región centroamericana puedan realizar, por lo tanto, representa un mecanismo que abre la posibilidad de realizar esfuerzos en materia de consenso y entendimiento político entre los mismos por medio de sus representaciones institucionales como sus respectivos Ministerios de Relaciones Exteriores o Cancillerías, Ministerios de Defensa, Ministerios de Gobernación, Ejércitos, Policías, Centros Tecnológicos, entre otros con el fin de homologar una estrategia centroamericana común en materia de ciberseguridad o ciberdefensa.

De igual forma por medio del Sistema de Integración Centroamericano SICA y sus respectivos tratados y estrategias como el Tratado Marco de Seguridad Democrática en Centroamérica, la Estrategia de Seguridad de Centroamérica y la Estrategia Regional Digital para el Desarrollo de la Sociedad de la Información y el Conocimiento, pueden tener la posibilidad de actualizar o consensuar una ciberseguridad homologada que tenga por objetivo el fortalecimiento e implementación de acciones preventivas ante amenazas como la ciberdelincuencia. Articulando una armonización entre los mecanismos jurídicos, que a su vez refuercen las iniciativas ya implementadas por cada Estado en esta materia.

Asimismo, la Conferencia de Fuerzas Armadas Centroamericanas (CFAC) cuenta con la posibilidad de estructurar una iniciativa sólida para la región en materia de ciberdefensa, articulándose primeramente por la voluntad política de los Estados y la coordinación de acciones que permitan a los Estados fortalecer su seguridad cibernética tanto regional como interna, permitiendo a su vez un desarrollo constante en esta materia.

Referencias

Adair, J., & Julian, R. (2011). *CIBERDELITO.* Mexico, D.F: UNAM-Mexico,Facultad de Ingeneria.

Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de amenazas. *Revista de Estudios en Seguridad Internacional, 6*(2). Obtenido de http://dx.doi.org/10.18847/1.12.2

Belloch, C. (2012). Las Tecnologías de la Información y Comunicación en el aprendizaje. *Universidad de Valencia*, 02-09. Obtenido de https://www.uv.es/bellochc/pedagogia/EVA1.pdf

Bernal, A. (2015). El ciberespacio un mundo sin ley. *Managing Partner at Ecix Group*, 02-138. Obtenido de El_ciberespacio_un_mundo_sin_ley

BID. (2016). *Informe anual de Desarrollo de la Banda Ancha en América Latina y el Caribe.* Washington, D.C.: BID. Obtenido de https://publications.iadb.org/publications/spanish/document/Informe-anual-del-%C3%8Dndice-de-Desarrollo-de-la-Banda-Ancha-en-Am%C3%A9rica-Latina-y-el-Caribe-IDBA-2016.pdf

BID. (2020). *Ciberseguridad, riesgos, avances y el camino a seguir en America Latinay el caribe.* Washington D.C: Banco Interamericano de Desarrollo (BID). Obtenido de https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Cabello, E. C. (2021). Unidades de ciberinteligencia y ciberguerra al servicio de Estados. *Instituto Español de Estudios Estratégicos*, 02-27. Obtenido de https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM10_2021_ENRCUB_Ciberinteligencia.pdf

Carrasco, L. d. (2015). Ciberresiliencia. *Instituto Español de Estudios Estrategicos*, 02-15. Obtenido de https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf

Centroamericanas, C. d. (4 de Marzo de 2013). *conferenciafac.org.* Obtenido de conferenciafac.org/ejes-tematicos-de-la-cfac: https://www.conferenciafac.org/ejes-tematicos-de-la-cfac-2/

Chamorro, E. F., Fernández, J. R., López, R. M., & Fernández, S. L. (2016). *La Ciberseguridad Nacional,un compromiso de todos.* Madrid: ISMS Forum Spain,. Obtenido de https://www.ismsforum.es/ficheros/descargas/informe-scsi1348666221.pdf

Chavarría, E., Jirón, M., & Miranda, F. (2016). *"LA CIBERDELINCUENCIA Y SU REGULACIÓN JURÍDICA EN CENTROAMÉRICA CON ÉNFASIS EN COSTA RICA, EL SALVADOR Y NICARAGUA".* León, Nicaragua: FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES, UNAN-Leon.

Chile, M. d. (2021). Ciberdefensa. Obtenido de https://www.defensa.cl/temas-de-contenido/ciberdefensa/

Comisión Europea, D. G. (2021). *ec.europa.eu*. Obtenido de https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

Cortés, A. F. (2017). Amenazas Persistentes Avanzadas (APT): Modelo de Funcionamiento y Análisis al caso de Estudio Projectsauron. *Universidad Piloto de Colombia*, 02-09. Obtenido de http://polux.unipiloto.edu.co:8080/00003618.pdf

Defensa, J. I. (2020). *ORIENTACIONES PARA EL DISEÑO, PLANEAMIENTO,IMPLANTACIÓN Y DESARROLLO DE UNA CIBERDEFENSA MILITAR.* Washington, DC: Junta Interammericana de Defensa. Obtenido de https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf

Delgado Barón, M. (2008). Reconceptualizando la Seguridad: Cambio de Dilemas y Amenazas. *Revista de Relaciones Internacionales,Estrategia y Seguridad*, 02-23. Obtenido de file:///C:/Users/user/Downloads/Dialnet-ReconceptualizandoLaSeguridad-5783738.pdf

Delito, O. d. (Febrero de 2020). *unodc.org*. Obtenido de unodc.org/cybercrime: https://www.unodc.org/e4j/es/tertiary/cybercrime.html

Desarrollo, P. d. (2002). Informe sobre el Desarrollo Humano en Venezuela. *Naciones Unidas*, 02-249. Obtenido de http://hdr.undp.org/sites/default/files/venezuela_2002_es.pdf

Díaz, J. R. (2016). Ciberamenazas: ¿ El terrorismo del Futuro? *Instituto Españo de Estudios Estratégicos*. Obtenido de https://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Dominicana, C. d. (2010). Articulo 44. Obtenido de file:///C:/Users/user/Downloads/constitucion%20de%20la%20republica%202010.pdf

Duarte, E. (2008). Las tecnologías de Información y Comunicacióon (TIC) desde una perspectiva Social. *Educare*, 02-9. Obtenido de https://www.redalyc.org/pdf/1941/194114584020.pdf

Espinoza, L. A. (2014). *El nuevo delito de acceso y suo no autorizado de registros, datos o arhcivos informaticos introducido por la Ley numero 641, codigo penal.* Managua: Facultad de Humanidades, UCA.

Evans, H. G. (28 de Junio de 2013). *gevans.org*. Obtenido de gevans.org: http://www.gevans.org/speeches/speech521.html

Fernández, A. V. (2017). Análisis de las ciberamenazas. *Universidad Nacional de Educación a Distancia*, 02-42. Obtenido de file:///C:/Users/HP/Downloads/Dialnet-AnalisisDeLasCiberamenazas-6115622.pdf

firmantes, E. m. (2001). Convenio sobre la Ciberdelincuencia. 02-30. Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Flores, M. V. (2016). La Globalización como Fenómeno Político, Económico y Social. *Universidad Simón Bolívar*, 17. Obtenido de https://www.redalyc.org/pdf/709/70946593002.pdf

Gazapo, M., & Nieva, M. (2016). La Ciberseguridad como Factor Crítico en la Seguridad de la Unión Europea. *Universidad Complutense de Madrid*, 02-23. Obtenido de https://www.redalyc.org/pdf/767/76747805002.pdf

Giraldo, S. M. (2015). ANÁLISIS DE LAS INFRAESTRUCTURAS CRÍTICAS EN LA ERA DE LAS CIBERGUERRAS EN BÚSQUEDA DEL DELICADO EQUILIBRIO ENTRE LIBERTAD Y SEGURIDAD. *UNIVERSIDAD MILITAR NUEVA GRANADA; FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD*, 02-20. Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/7808/TRABAJO%20GRADO%20SEBASTIAN%20MELAN%20GIRALDO.pdf;jsessionid=8B91869D829A5CB5BC09B3F62487C9B7?sequence=1

Hernández, L. (2020). Técnicas e instrumentos de recolección de datos. *Boletín Científico de las Ciencias Económico Administrativas del ICEA*, 3. Obtenido de file:///C:/Users/user/Downloads/6019-Manuscrito-35678-1-10-20201120.pdf

Honduras, C. d. (1982). Articulo 100. Obtenido de https://www.oas.org/dil/esp/constitucion_de_honduras.pdf

Iglesias, E. (2004). Análisis documental y de información: dos componentes de un mismo proceso. *Scielo*, 4. Obtenido de http://eprints.rclis.org/5013/1/analisis.pdf

Linares, H. (2003). Las Nuevas Amenazas a la Seguridad Nacional. *NACAO DEFESA*, 02-10. Obtenido de https://comum.rcaap.pt/bitstream/10400.26/1771/1/NeD_ExtraAbril03_HelbertLinares.pdf

Martinez, L. M., Ceceñas, P. E., & Ontiveros, v. C. (2014). Virtualidad, Ciberespacio y Comunidades Virtuales. *Universidad Juárez del Estado de Durango*, 02-144. Obtenido de http://www.upd.edu.mx/PDF/Libros/Ciberespacio.pdf

Mejia Jervis, T. (19 de Septiembre de 2017). *¿Qué son las Fuentes de Investigación?* Obtenido de Lifeder: https://www.lifeder.com/fuentes-de-investigacion/

Ministerio de Defensa, C. S. (2014). *Documentos de Seguridad y Defensa-Estrategia de la información y seguridad en el ciberespacio.* Madrid: Ministerio de Defensa. Obtenido de https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF494.pdf

Miranzo, M., & Río, C. d. (2014). LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS. *UNISCI Discussion Papers*(35), 02-15. Obtenido de https://www.redalyc.org/pdf/767/76731410018.pdf

Nicaragua, C. d. (1987). Articulo 92. Obtenido de https://www.oas.org/juridico/spanish/mesicic3_nic_const.pdf

Nicaragua, G. d. (2005). Libro de la Defensa Nacional. *Ministerio de Defensa y Ejérctio de Nicaragua*. Obtenido de https://www.resdal.org/Archivo/nica-libro-blanco.html

Nicolás Alfredo Arias Torres, J. A. (2015). *MODELO EXPERIMENTAL DE CIBERSEGURIDAD Y CIBERDEFENSA PARA COLOMBIA.* BOGOTÁ, D.C: UNIVERSIDAD LIBRE.

Organization, N. A. (02 de Julio de 2021). *nato.int*. Obtenido de https://www.nato.int/cps/en/natohq/topics_78170.htm

Panama, C. d. (1994). Articulo 29. Obtenido de https://pdba.georgetown.edu/Constitutions/Panama/vigente.pdf

Parra, J. (2019). Amenazas Persistentes Avanzadas y su Impacto en Latinoamérica ¿cómo estar preparados? *Universidad Piloto de Colombia*, 02-06. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6285/00005219.pdf?sequence=1&isAllowed=y

Perú, E. (s.f.). *"CIBERDEFENSA Y SU INCIDENCIA EN LA PROTECCIÓN DE LA INFORMACIÓN DEL EJÉRCITO DEL PERÚ. CASO: COPERE 2013 –2014".*

Pinilla, A. (2019). Resiliencia en la Seguridad Informática. *Universidad Piloto de Colombia*, 02-09. Obtenido de http://polux.unipiloto.edu.co:8080/00002215.pdf

Rica, C. d. (1949). Articulo 24. Obtenido de https://www.oas.org/dil/esp/Constitucion_Costa_Rica.pdf

Ricoy Lorenzo, C. (2006). *Contribución sobre los paradigmas de investigación.* Santa Maria, RS, Brasil: Educação. Revista do Centro de Educação, v. Obtenido de https://www.redalyc.org/pdf/1171/117117257002.pdf

Rodríguez, F. (2007). Generalidades acerca de las técnicas de investigación cuantitativa. *Sistema Institucional de Investigación de Unitec (SIIU)*, 31. Obtenido de file:///C:/Users/user/Downloads/Dialnet-GeneralidadesAcercaDeLasTecnicasDeInvestigacionCua-4942053%20(1).pdf

Rojas, L. D. (2018). EL CIBERESPACIO COMO ESCENARIO ESTRATÉGICO DE SEGURIDAD Y DEFENSA EN EL DESARROLLO DE POLÍTICAS EN COLOMBIA. *UNIVERSIDAD MILITAR NUEVA GRANADA*, 02-37. Obtenido de https://repository.unimilitar.edu.co/bitstream/handle/10654/18104/TorresRojasLesdyDaniela2018.pdf?sequence=3&isAllowed=y

Romero, D. J. (2004). Ciberespacio y Comunicación: Nuevas Formas de Vertebración Social en el Siglo XXI. *Revista de Estudios Literarios*, 02-33. Obtenido de https://biblioteca.org.ar/libros/150717.pdf

Rugama, X. G., & Rodriguez, G. d. (2019). *Las Ciberamenazas: El Desafio que enfrentan los paises del SICA en el nuevo escenario Internacional.* Managua. Obtenido de file:///E:/Monografia/MONOGRAFIA%20FINAL.%20CIBERAMENAZA.%20pre-defensa%20(1).pdf

Saint, H. L. (2016). Breve Discusión Conceptual sobre Amenazas. *Revista de Ciencias de Seguridad y Defensa*, 02-10. Obtenido de file:///C:/Users/user/Downloads/2021-7894-2-PB.pdf

Salvador, C. P. (1983). Articulo 24. Obtenido de https://www.oas.org/dil/esp/constitucion_de_la_republica_del_salvador_1983.pdf

Sampieri, R. (2003). Metodología de la Investigación. *Instituto politécnico nacional*, 22. Obtenido de http://www.rlillo.educsalud.cl/Capac_Investigacion_BecadosFOREAPS/Metodologia%20de%20la%20Investigacion.pdf

Sánchez, F. A. (2019). Fundamentos Epistémicos de la Investigación Cualitativa y Cuantitativa: Consensos y Disensos. *Revista Digital de Investigación en Docencia Universitaria*, 21. Obtenido de http://www.scielo.org.pe/pdf/ridu/v13n1/a08v13n1.pdf

Seguridad, A. d. (2021). *nsa.gov*. Obtenido de dni.gov: https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/

Service, C. R. (2021). Defense Primer: Cyberspace Operations. *Informing the legislative debate since 1914*, 3. Obtenido de https://sgp.fas.org/crs/natsec/IF10537.pdf

SICA. (1992). Protocolo de Tegucigalpa. *XI CUMBRE DE PRESIDENTES CENTROAMERICANOS PROTOCOLO DE TEGUCIGALPA A LA CARTA DE LA ORGANIZACION DE ESTADOS CENTROAMERICANOS (ODECA)*, 02-20. Obtenido de https://www.sica.int/documentos/protocolo-de-tegucigalpa-a-la-carta-de-la-organizacion-de-estados-centroamericanos-odeca_1_116823.html

SICA. (1995). Tratado Marco de Seguridad Democrática en Centroamerica. 02-11. Obtenido de https://www.sica.int/documentos/tratado-marco-de-seguridad-democratica-en-centroamerica_1_110795.html

SICA. (2011). *Estrategia de Seguridad en Centroamerica.* Comision Seguridad SICA. Guatemala: SG-SICA. Obtenido de file:///C:/Users/user/Downloads/Estrategia%20de%20Seguridad%20de%20Centroamerica.pdf

Snedden, D. C. (2018). Regional Security Architecture: Some Terms and Organizations. 15. Obtenido de https://apcss.org/wp-content/uploads/2016/12/Regional-organizations-Snedden.pdf

Spielman, J. G. (2009). Chile y los Desafíos Globales de Seguridad. *Unidad de Investigación sobre Seguridad y Cooperación*, 02-13. Obtenido de https://www.ucm.es/data/cont/media/www/pag-72507/UNISCI%20DP%2021%20-%20GRIFFITHS.pdf

Tancara, C. (1993). Investigación Documental. *scielo*, 16. Obtenido de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S0040-29151993000100008&lang=es

Torre, M. G. (2020). Amenazas Emergentes. *Estado Mayor General del Ejército del Perú*, 02-22. Obtenido de https://ceeep.mil.pe/wp-content/uploads/2020/09/2-Gomez-de-la-Torre-CEEEP-26-Ago-20.pdf

UNIDAS, N. (2010). *ESTUDIO SOBRE LAS PERSPECTIVAS DE LA ARMONIZACIÓN DE LA CIBERLEGISLACIÓN EN CENTROAMÉRICA Y EL CARIBE.* New York: United Nations.

Unidas, O. d. (s.f.). *Unión Internacional de Telecomunicaciones (UIT)*. Obtenido de itu.int: https://www.itu.int/es/about/Pages/default.aspx

Uzcategui, S. (2018). Paradigma Interpretativo. *Course Hero*, 66. Obtenido de https://www.coursehero.com/file/96314373/Paradigma-Interpretativopdf/

Villalba, A. (2017). Análisis de las ciberamenazas. Obtenido de file:///C:/Users/ESTUDIANTES/Downloads/Dialnet-AnalisisDeLasCiberamenazas-6115622.pdf

Villarreal, G. M. (2009). Seguridad Nacional: Un concepto ampliado y complejo. *Camara de diputados de Mexico*, 37. Obtenido de http://www.diputados.gob.mx/sedia/sia/spe/SPE-ISS-13-09.pdf

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA
UNAN - MANAGUA

Ciencia Política y Relaciones Internacionales

Modelo de Entrevista

Nombre y apellido: _____

Formación profesional: _____

Ocupación laboral: _____

1. ¿Cómo aborda el SICA y CFAC, la temática de ciberseguridad y ciberdefensa, poseen alguna dirección o lineamiento en esta materia?
2. ¿Cuáles han sido las iniciativas del SICA y la CFAC en materia de ciberdefensa o ciberseguridad?
3. ¿Qué medios que utiliza el SICA y la CFAC para llevar a cabo las iniciativas de ciberseguridad y ciberdefensa?
4. ¿El Sistema de Integración Centroamericano, SICA ha sido víctima de algún ciberataque? ¿Cómo lo han afrontado?
5. ¿La Conferencia de las Fuerzas Armadas Centroamericanas CFAC, ha sido víctima de algún ciberataque? ¿Cómo lo han afrontado?
6. ¿Considera eficiente los mecanismos actualmente que posee el SICA y la CFAC ante la ciberdelincuencia?
7. ¿Cuáles han sido las fortalezas y debilidad del SICA y la CFAC en cuanto a la ciberdefensa y ciberseguridad regional?
8. ¿Cuáles son las infraestructuras críticas que poseen actualmente la Región Centroamericana y cuales representan un alto valor? ¿Estas han sido víctimas de algún ciberataque?

9. ¿Cuáles son los aspectos a tomar para la construcción de una estrategia o política en ciberseguridad o ciberdefensa? ¿Cómo debe mantenerse?
10. ¿Usted considera que los organismos de integración como el SICA y la CFAC, son factibles para la creación de un mecanismo conjunto de ciberseguridad y ciberdefensa?
11. ¿Cuáles son los principales retos en ciberseguridad y ciberdefensa que posee la Región Centroamericana para el futuro?

Anexos

1. Protocolo de Tegucigalpa a la Carta de la Organización de Estados Centroamericanos (ODECA).
2. Tratado Marco de Seguridad Democrática en Centroamericana.
3. Estrategia de Seguridad de Centroamérica (ESCA).
4. Estrategia Regional Digital para el Desarrollo de la Sociedad de la Información y el Conocimiento SICA.
5. Conferencia de Fuerzas Armadas de Centroamérica.