UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

ESCUELA DE CIENCIA POLÍTICA

ANÁLISIS DE LOS BENEFICIOS PARA EL ESTADO DE GUATEMALA AL ADHERIRSE AL CONVENIO DE CIBERDELINCUENCIA FIRMADO EN LA CIUDAD DE BUDAPEST

TESIS

Presentada al Consejo Directivo

de la

Escuela de Ciencia Política

de la

Universidad de San Carlos de Guatemala

por

EMELY PAOLA QUIXTAN VELASQUEZ

Previo a conferírsele el grado académico de

LICENCIADA EN RELACIONES INTERNACIONALES

y el título profesional de

INTERNACIONALISTA

Guatemala, abril de 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLÍTICA

RECTOR EN FUNCIONES
M.A. Pablo Ernesto Oliva Soto

SECRETARIO GENERAL
Dr. Gustavo Enrique Taracena Gil

CONSEJO DIRECTIVO DE LA ESCUELA DE CIENCIA POLÍTICA

DIRECTOR:	Maestro Mike Hangelo Rivera Contreras
VOCAL I	Licenciado Juan Carlos Guzmán Morán
VOCAL II:	Maestra Beatriz Eugenia Bolaños Sagastume
VOCAL III:	Licenciado José Rolando Samayoa Lara
VOCAL IV:	Bachiller Héctor Raúl del Valle Muñoz
VOCAL V:	Bachiller Hellen Herrera Vásquez
SECRETARIA:	Maestra Ana Nineth Burgos Méndez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL DE CONOCIMEINTOS -PRIVADO-

COORDINADOR:	Doctor Pablo Daniel Rangel Romero
EXAMINADORA:	Licenciada Nidia Eunice Díaz Morales
EXAMINADOR:	Maestro Aldo Nery Bonilla Vicente
EXAMINADORA:	Maestra Alma Consuelo Coguox Perez
EXAMINADOR:	Maestro Rubén Corado Cartagena
EXAMINADOR:	Licenciado Guido Armando Barillas Quezada

TRIBUNAL QUE PRACTICÓ EL EXAMEN PÚBLICO DE TESIS

DIRECTOR:	Maestro Mike Hangelo Rivera Contreras
SECRETARIA:	Maestra Ana Nineth Burgos Méndez
COORDINADORA:	Maestra Beatriz Eugenia Bolaños Sagastume
EXAMINADOR:	Licenciado José Gilberto Cortez Chacón
EXAMINADORA:	Maestra Alma Consuelo Coguox Perez

Nota: Únicamente el autor es responsable de las doctrinas sustentadas en la tesis. (Artículo 73 del Normativo de Evaluación y Promoción de Estudiantes de la Escuela de Ciencia Política)

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, diez de marzo de dos mil veintidós. ----------

Con vista en los dictámenes que anteceden y luego de verificar la autenticidad de la certificación de Examen de Suficiencia y/o cursos aprobados por la Escuela de Ciencias Lingüísticas, se autoriza la impresión de la Tesis titulada **"ANÁLISIS DE LOS BENEFICIOS PARA EL ESTADO DE GUATEMALA AL ADHERIRSE AL CONVENIO DE CIBERDELINCUENCIA FIRMADO EN LA CIUDAD DE BUDAPEST",** presentada por el (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** registro académico No. **201409994.**

Atentamente,

"ID Y ENSEÑAD A TODOS"

Msc. Mike Hangelo Rivera Contreras
Director Escuela de Ciencia Política

Se envía el expediente
c.c.: Archivo
10/javt

ACTA DE DEFENSA DE TESIS

En la ciudad de Guatemala, el día dos de marzo de dos mil veintidós, se efectuó el proceso de verificar la incorporación de observaciones hechas por el Tribunal Examinador, conformado por: Licenciada Beatriz Eugenia Bolaños Sagastume, Licenciado José Gilberto Cortez Chacón y el Maestro Rubén Corado Cartagena, Coordinador de la Carrera de Relaciones Internacionales, el trabajo de tesis: **"ANÁLISIS DE LOS BENEFICIOS PARA EL ESTADO DE GUATEMALA AL ADHERIRSE AL CONVENIO DE CIBERDELINCUENCIA FIRMADO EN LA CIUDAD DE BUDAPEST"** Presentado por el (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** registro académico No. **201409994,** razón por la que se da por **APROBADO** para que continúe con su trámite.

"ID Y ENSEÑAD A TODOS"

Maestro Rubén Corado Cartagena
Coordinador de Carrera

c.c.: Archivo
9/ javt

ECP
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLÍTICA

ACTA DE DEFENSA DE TESIS

En la ciudad de Guatemala, el día veinticuatro de noviembre de dos mil veinte, se realizó la defensa de tesis presentada por el (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** Carnet No. **201409994**, para optar al grado de Licenciado (a) en **RELACIONES INTERNACIONALES** titulada **"ANÁLISIS DE LOS BENEFICIOS PARA EL ESTADO DE GUATEMALA AL ADHERIRSE AL CONVENIO DE CIBERDELINCUENCIA FIRMADO EN LA CIUDAD DE BUDAPEST"** ante el Tribunal Examinador integrado por: Lic. José Gilberto Cortez Chacón, Maestra Alma Consuelo Coguox Perez y la Maestra Beatriz Eugenia Bolaños Sagastume, Coordinadora de la Carrera de Relaciones Internacionales. Los infrascritos miembros del Tribunal Examinador desarrollaron dicha evaluación y consideraron que para su aprobación deben incorporarse algunas correcciones a la misma.

Lic. José Gilberto Cortez Chacón
Examinador

Maestra Alma Consuelo Coguox Perez
Examinadora

Maestra Beatriz Eugenia Bolaños Sagastume
Coordinación de Carrera

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLITICA
COOR REL INT

c.c.: Archivo
8b /javt

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, cinco de noviembre de dos mil veinte.----------

ASUNTO: El (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** Carnet No. **201409994** continúa trámite para la realización de su Tesis.

Habiéndose emitido el dictamen correspondiente por parte del (la) Msc. Aldo Nery Bonilla Vicente en su calidad de Asesor (a), pase al Coordinador (a) de la Carrera de Relaciones Internacionales para que proceda a conformar el Tribunal Examinador que escuchará y evaluará la defensa de tesis, según Artículo Setenta (70) del Normativo de Evaluación y Promoción de Estudiantes de la Escuela de Ciencia Política.

Atentamente,

"ID Y ENSEÑAD A TODOS"

Msc. Mike Hangelo Rivera Contreras
Director Escuela de Ciencia Política

Se envía el expediente
c.c.: Archivo
7/javt

Guatemala,
noviembre 4 de 2020

MSc.
Mike A Rivera
Director
ESCUELA DE CIENCIA POLÍTICA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Respetable señor director:

Tengo el agrado de dirigirme a usted, en ocasión de presentar el trabajo de tesis de la estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ,** con el tema de investigación "*ANÁLISIS DE LOS BENEFICIOS PARA EL ESTADO DE GUATEMALA AL ADHERIRSE AL CONVENIO DE CIBERDELINCUENCIA FIRMADO EN LA CIUDAD DE BUDAPEST*."

El trabajo realizado por la señorita Quixtan, es un estudio analítico con un enfoque eminentemente cualitativo, que responde a las inquietudes alrededor de la importancia que Guatemala pueda firmar su adhesión al Convenio de Budapest sobre ciberdelincuencia lo antes posible, proceso que se encuentra actualmente en el Congreso de la República y que reviste de urgencia para la prevención y protección del país ante la delincuencia virtual.

Debo manifestarle con suma complacencia que la estudiante pudo desarrollar esta investigación fundamentada en su marco metodológico debidamente aprobado y que respetó de manera efectiva los procesos, normas y requisitos académicos exigidos por la Escuela de Ciencia Política, por lo que consecuentemente es para mí un honor dictaminar FAVORABLEMENTE el trabajo desarrollado por la estudiante Quixtan y lo presento a usted para que el proceso continúe su trámite correspondiente para la obtención del grado académico al que aspira.

Al momento de reiterar mi respeto, me permito saludarlo con mis mejores muestras de consideración.

De usted

Lic. Aldo N. Bonilla MSc
Asesor.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLÍTICA

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, quince de noviembre de dos mil diecinueve ----------

ASUNTO: El (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** Carnet No. **201409994** continúa trámite para la realización de su Tesis.

Habiéndose emitido el dictamen correspondiente por parte del (de la) Coordinador (a) de Carrera correspondiente, pase al Asesor (a) de Tesis, Msc. Aldo Nery Bonilla Vicente para que brinde la asesoría correspondiente y emita dictamen.

Atentamente,

"ID Y ENSEÑAD A TODOS"

Msc. Mike Hangelo Rivera Contreras
Director Escuela de Ciencia Política

Escuela de Ciencia Política, Universidad de San Carlos
DIRECCIÓN

Se envía el expediente
c.c.: Archivo
6/javt

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLÍTICA

Guatemala,
15 de noviembre de 2019

Msc. Mike Hangelo Rivera Contreras
Director
Escuela de Ciencia Política
Presente

Respetable Msc. Rivera:

Me permito informarle que tuve a la vista el diseño de tesis titulado **"ANÁLISIS DE LOS BENEFICIOS PARA EL ESTADO DE GUATEMALA AL ADHERIRSE AL CONVENIO DE CIBERDELINCUENCIA FIRMADO EN LA CIUDAD DE BUDAPEST"** presentado por el (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** Carnet No. **201409994** puede autorizarse como Asesor al (la) Msc. Aldo Nery Bonilla Vicente.

Cordialmente,

"ID Y ENSEÑAD A TODOS"

Licda. Beatriz Eugenia Bolaños Sagastume
Coordinador (a) de Carrera

Se envía expediente
c.c.: Archivo
5/javt

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLÍTICA

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, quince de noviembre de dos mil diecinueve ----------

ASUNTO: El (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** Carnet No. **201409994** continúa trámite para la realización de su Tesis.

Habiéndose emitido el dictamen correspondiente por parte del (de la) Coordinador (a) del Área de Metodología, pase al (la) Coordinador (a) de Carrera correspondiente, para que emita visto bueno sobre la propuesta de Asesor.

Atentamente,

"ID Y ENSEÑAD A TODOS"

Msc. Mike Hangelo Rivera Contreras
Director Escuela de Ciencia Política

Escuela de Ciencia Política, Universidad de San Carlos
DIRECCIÓN

Se envía el expediente
c.c.: Archivo
4/ javt

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLÍTICA

Guatemala,
14 de noviembre de 2019

Msc. Mike Hangelo Rivera Contreras
Director
Escuela de Ciencia Política
Presente

Respetable Msc. Rivera:

Me permito informarle que tuve a la vista el diseño de tesis titulado **"ANÁLISIS DE LOS BENEFICIOS PARA EL ESTADO DE GUATEMALA AL ADHERIRSE AL CONVENIO DE CIBERDELINCUENCIA FIRMADO EN LA CIUDAD DE BUDAPEST"** presentado por el (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** Carnet No. **201409994,** quien realizó las correcciones solicitadas y por lo tanto, mi dictamen es favorable para que se apruebe dicho diseño y se proceda a realizar la investigación.

Atentamente,

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA COORDINACION METODOLOGIA JORNADA VESPERTINA ECP

Msc. Nora Lizeth Gálvez García
Coordinadora del Área de Metodología

Se envía el expediente
c.c.: Archivo
3/javt

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLÍTICA

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, catorce de noviembre de dos mil diecinueve. ----------

ASUNTO: El (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** Carnet No. **201409994** continúa trámite para la realización de su Tesis.

Habiéndose aceptado el tema de tesis propuesto, por parte del (de la) Coordinador (a) de Carrera pase al (a la) Coordinador (a) del Área de Metodología, para que se sirva emitir dictamen correspondiente sobre el diseño de tesis.

Atentamente,

"ID Y ENSEÑAD A TODOS"

Msc. Mike Hangelo Rivera Contreras
Director Escuela de Ciencia Política

Escuela de Ciencia Política, Universidad de San Carlos DIRECCIÓN

Se envía expediente
c.c.: Archivo
2/javt

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLÍTICA

Guatemala,
14 de noviembre de 2019

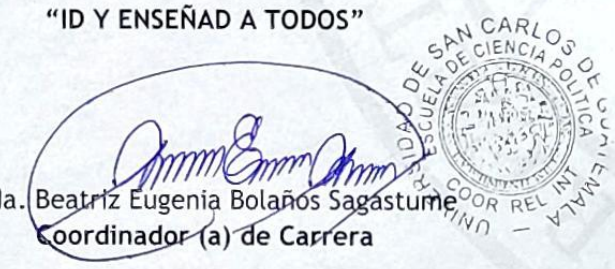
Msc. Mike Hangelo Rivera Contreras
Director
Escuela de Ciencia Política
Presente

Respetable Msc. Rivera:

Me permito informarle que el tema de tesis: **"ANÁLISIS DE LOS BENEFICIOS PARA EL ESTADO DE GUATEMALA AL ADHERIRSE AL CONVENIO DE CIBERDELINCUENCIA FIRMADO EN LA CIUDAD DE BUDAPEST"** Presentado por el (la) estudiante **EMELY PAOLA QUIXTAN VELÁSQUEZ** Carnet No. **201409994** puede autorizarse, dado que el mismo cumple con las exigencias mínimas de los contenidos de la carrera.

Cordialmente,

"ID Y ENSEÑAD A TODOS"



Licda. Beatriz Eugenia Bolaños Sagastume
Coordinador (a) de Carrera

c.c.: Archivo
1/javt

Dedicatoria:

A Dios: El acto de graduación se lo dedico a Dios por las múltiples bendiciones que he tenido a lo largo de mi vida, como agradecimiento a los talentos que me dio y darme la sabiduría necesaria para regir mi vida cada día.

A mi madre: Blanca Velásquez, por ser mi pilar más fuerte, por demostrarme que todo es posible con mucho esfuerzo y dedicación, por ser la mujer más fuerte y trabajadora que conozco y a pesar de todo siempre nos ha dado lo mejor. Gracias por acompañarme durante toda mi carrera, por creer en mí, por escucharme siempre y motivarme a seguir adelante y concluir está etapa. ¡Lo logramos!

A mi hermano: Edwar, por estar junto a mí siempre y apoyarme en cada decisión que he tomado.

A mi tía Amparo (†): Porque siempre confío en mi y en mi potencial. Por apoyarme hasta el último día de su vida, y porque sé que está orgullosa de este logro.

Agradecimientos:

A la Universidad San Carlos de Guatemala:	Por ser mi alma mater, mi casa de estudios, por brindarme la oportunidad de formarme profesional y socialmente.
A la Escuela de Ciencia Política:	Por formarme con valores éticos y profesionales y enseñarme a ser "crítica y analítica", por acogerme por 5 años y enseñarme el valor de la perseverancia.
A mi asesor:	Lic. Aldo Bonilla, por siempre estar al pendiente de mí, por toda su paciencia y apoyo durante la elaboración de mi tesis; sin su apoyo y sabiduría esto hubiera sido un poco más difícil, muchas gracias.
A mis amigas de la Universidad:	Karol, Ethel, Brigeth, Karina, Margarita y Tere con quienes compartí los años de universidad y sin ustedes nada hubiese sido igual, y a pesar del tiempo o la distancia siempre les agradeceré por su apoyo durante está etapa.
A familia:	Gracias porque de alguna manera u otra me apoyaban.
A mis amigos:	Azael por creer en mi potencial, por esos mensajes de ánimos y motivación que me ayudaron a completar esta etapa de mi vida; Elvis y Cristopher porque a pesar de tantos años y la distancia, siguen estando allí; Luis Bosque, Ale, Debbie por haberse cruzado en mi vida y siempre alegrarse de mis logros.

Por último, quisiera agradecerles a todos aquellos que estuvieron presentes durante mi carrera y han estado presente en mi vida, por creer en mis capacidades y potencial, gracias por motivarme siempre; por los mensajes de ánimos que sin pedirlo me enviaban, y sobre todo por la sabiduría que han compartido conmigo. ¡Muchas gracias!

Índice

Índice de Tablas i

Índice de Figuras ii

Introducción I

CAPÍTULO I 1

1. Abordaje metodológico y teórico 1

1.1 Abordaje metodológico 1

1.1.1 Justificación 1

1.1.2 Planteamiento del problema 3

1.1.3 Preguntas generadoras 5

1.1.4 Objetivos de la investigación 6

1.1.5 Delimitación de la investigación 6

1.1.6 Tipo de investigación 7

1.1.7 Métodos y técnicas 8

1.2 Abordaje teórico 9

1.2.1 Marco conceptual 9

1.2.2 Bases teóricas 13

1.2.1 Teoría de las Actividades Cotidianas 14

1.2.2 Teoría de la interdependencia compleja 15

CAPÍTULO II 17

2. Antecedentes históricos de los delitos informáticos y de los instrumentos internacionales para la mitigación de la ciberdelincuencia 17

2.1. Acerca de los delitos cibernéticos 17

2.2 Instrumentos internacionales para prevenir y mitigar la ciberdelincuencia 18

CAPÍTULO III 22

3. El uso de Internet y la importancia de la ciberseguridad 22

3.1 Penetración y acceso a Internet 22

3.1.1 Internet en Guatemala 25

3.2 Ciberseguridad 29

3.2.1 Ciberseguridad en América Latina y el Caribe 29

3.2.2 La seguridad cibernética en Guatemala 35

3.2.2.1 Marco institucional y legal en materia de seguridad cibernética en Guatemala 36

CAPÍTULO IV 48

5. Análisis prospectivo de la seguridad Cibernética en Guatemala 48

5.1 Análisis FODA de la Seguridad cibernética en Guatemala 48

5.2. Resultados de la Investigación 52

Conclusiones 56

Referencias 58

Anexos 63

Anexo 1. Tablas y Figuras. 63

Anexo 2. Guía de Entrevistas 69

Índice de Tablas

Tabla 1

Penetración de Internet en América Latina y el Caribe (2018-2020) 24

Tabla 2

Países de América que han presentado una Estrategia de Seguridad Cibernética y ratificado del Convenio sobre Ciberdelincuencia 33

Tabla 3

Cuadro comparativo del contenido del Convenio sobre ciberdelincuencia y la Iniciativa 5601 - Ley de prevención y protección contra la ciberdelincuencia 43

Tabla 4

Listado de países que han firmado y ratificado el Convenio sobre ciberdelincuencia 63

Tabla 5

Estados no miembros del Consejo de Europa que obtuvieron una invitación para firmar y ratificar o adherirse al Convenio sobre Ciberdelincuencia 66

Índice de Figuras

Figura 1

Estimación de personas a nivel mundial que utilizan Internet, 2015-2019 22

Figura 2

Número de personas que usan el servicio de internet por departamento en Guatemala.....26

Figura 3

Porcentaje de personas que utilizan las TIC a nivel nacional según el censo de población.....28

Figura 4

Modelo de madurez de la capacidad de ciberseguridad.....32

Figura 5

Línea del tiempo del desarrollo de la Estrategia Nacional de Ciberseguridad en Guatemala ...38

Figura 6

Delitos que se pretenden incorporar a la legislación penal guatemalteca.....42

Figura 7

Carta de Manifestación de Interés de Guatemala de Adherirse al Convenio de Budapest...67

Figura 8

Carta de respuesta del Comité Europeo de Ciberseguridad.....68

Introducción

El uso de las Tecnologías de la Información y Comunicación (TIC) e Internet ha aumentado progresivamente a lo largo de los años, el mundo virtual ha tenido un auge importante dentro de la comunidad internacional, aunado a ello, lo han hecho las actividades ilícitas por medio de Internet, que han podido irrumpir dentro de las infraestructuras críticas nacionales y han desafiado las formas tradicionales de seguridad nacional, ello a causa del alcance transnacional que tienen estos tipos de delitos, y en donde ha sido (y es necesario) reforzar la resiliencia cibernética para responder y mitigar los riesgos y amenazas inminentes que se pueden desarrollar en el ciberespacio.

La importancia trascendental que representa la seguridad cibernética a nivel internacional hace que este tema sea un objeto de estudio de las Relaciones Internacionales al tener un impacto crucial en la seguridad nacional de los Estados. Por lo que, la presente investigación aborda el tema de ciberdelincuencia y ciberseguridad dentro del marco de las Relaciones Internacionales tomando como referencia el Convenio sobre Ciberdelincuencia firmado en la ciudad Budapest en 2001. Es importante mencionar que la prevención, combate y mitigación de los delitos cibernéticos conlleva una serie de aspectos que el gobierno debe considerar, como adherirse a instrumentos internacionales que ayuden a crear alianzas para mitigar esta problemática, principalmente por medio de la cooperación internacional, en tal sentido, esta investigación también describe las acciones que ha tomado el gobierno de Guatemala para dar respuesta al proceso de prevención y mitigación de los delitos cibernéticos en el país, con el fin de tener las condiciones necesarias para adherirse al Convenio sobre Ciberdelincuencia.

En el primer capítulo, se presenta el abordaje teórico-metodológico y conceptual que respaldan esta investigación, describiendo los conceptos relacionados con el objeto de estudio, así como los objetivos, técnicas y métodos que sirvieron para la realización del presente trabajo de investigación.

En el segundo capítulo se amplía la información sobre los antecedentes de los delitos cibernéticos, describiendo conceptos aplicables al objeto de estudio. Más adelante, se abordan los antecedentes de los instrumentos internacionales que han surgido para prevenir y mitigar la ciberdelincuencia tanto a nivel mundial, como lo fue el Convenio sobre Ciberdelincuencia, así como a nivel regional en Latinoamérica y el caribe, como lo fue la Estrategia Interamericana Integral de Seguridad Cibernética.

En el tercer capítulo, se describe el auge en el uso del internet tanto a nivel mundial como en Guatemala, para posteriormente realizar un análisis de las implicaciones que el uso del internet ha generado en la seguridad cibernética en América Latina y el Caribe, principalmente en el territorio guatemalteco, dando énfasis en los mecanismos y herramientas que el gobierno guatemalteco ha creado para fortalecer la resiliencia cibernética en el país, principalmente en lo que respecta al marco institucional y legal en materia de seguridad cibernética Guatemala.

En el cuarto capítulo se realizó un análisis de las fortalezas, oportunidades, debilidades, amenazas que tiene el Estado de Guatemala respecto a la prevención y mitigación de los delitos cibernéticos en el país, con el fin de identificar las condiciones en las que se encuentra Guatemala. Además, se presenta un análisis de los resultados para dar respuesta a los beneficios que conlleva la adhesión de Guatemala al Convenio sobre Ciberdelincuencia. Y finalmente, se presentan las conclusiones a las que se llegó luego de haber realizado la investigación y tomando en cuenta la opinión de los diferentes especialistas entrevistados.

CAPÍTULO I

1. Abordaje metodológico y teórico

1.1 Abordaje metodológico

1.1.1 Justificación

La ciberdelincuencia en un mundo globalizado e interconectado por las Tecnologías de la Información y la Comunicación (TIC) al estar relacionado con la seguridad nacional y principalmente la seguridad cibernética, es un tema de interés en el marco de las Relaciones Internacionales. Muchas de las implicaciones que conllevan los sistemas, redes y datos informáticos, tienen que ver con la seguridad y la confidencialidad de la información de millones de personas en el mundo que utilizan internet para trabajar, estudiar o simplemente interactuar; la libertad que da internet para navegar es amplia y muchas veces insegura, lo cual da paso a que se cometan delitos en el espacio cibernético.

En virtud de lo anterior, diferentes países han unido esfuerzos para crear mecanismos y protocolos con el fin de salvaguardar los datos informáticos de la población mundial, así como la confidencialidad de estos, por medio de la seguridad cibernética. Por tal motivo, la Estrategia Interamericana Integral de Seguridad Cibernética presentada por la OEA, reconoció:

> La urgente necesidad de incrementar la seguridad de las redes y sistemas de información comúnmente denominados Internet, a fin de abordar las vulnerabilidades y proteger a los usuarios, la seguridad nacional y las infraestructuras esenciales frente a las graves y perjudiciales amenazas que representan aquellos que podrían llevar a cabo ataques en el espacio cibernético con fines maliciosos o delictivos(Organización de Estados Americanos (OEA), 2004, p. 3).

La automatización y digitalización llevada a cabo por la tercera revolución industrial, introdujo avances tecnológicos muy importantes que hasta hoy en día han facilitado las actividades de la población mundial que tiene acceso a las TIC, principalmente a Internet; no obstante, esos mismos avances han servido como plataforma de actividades ilegales cometidas por medio del espacio cibernético los cuales han ocasionado nuevos retos para la comunidad internacional, principalmente los Estados, ya que estos deben de salvaguardar los derechos humanos de sus habitantes. Por tal motivo, el tema de seguridad cibernética es de suma importancia, debido a que gran parte de la población mundial utiliza Internet en su vida cotidiana. En 2001, los Estados miembros del Consejo de Europa firmaron el Convenio sobre ciberdelincuencia en la ciudad de Budapest, "convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional" (Convenio sobre ciberdelincuencia, 2001).

Si bien el Convenio sobre ciberdelincuencia fue celebrado, firmado y publicado por el Consejo de Europa, así como ratificado por los Estados miembros de esta organización internacional; este es un convenio multilateral abierto, por lo que cualquier Estado puede unirse a él; y el cual es considerado el único convenio internacional vinculante en esta materia. Respecto a lo anterior, en el caso de América Latina, países como Argentina, Chile, Colombia, Paraguay, Perú ya han ratificado el Convenio sobre Ciberdelincuencia. Por otro lado, países como México, El Salvador y Guatemala, ya han mostrado su interés en adherirse a dicho Convenio.

En el caso de Guatemala, se presentó en 2016 por medio del Ministerio de Relaciones Exteriores una carta al Consejo de Europa para mostrar el interés que Guatemala tiene para unirse al Convenio sobre ciberdelincuencia, y a partir de esa fecha las entidades gubernamentales correspondientes han implementado una serie de mecanismos y estrategias relacionadas con la seguridad cibernética en el territorio guatemalteco, como lo es el establecimiento de la estrategia de seguridad cibernética en 2018, la creación del Equipo de

Respuesta ante Emergencias Informáticas CERT por sus siglas en inglés, así como la presentación ante el Congreso de la República de Guatemala de varias iniciativas de ley tales como: la Iniciativa No. 4055, Ley de Delitos informáticos; Iniciativa No. 5254, Ley sobre la Ciberdelincuencia; e Iniciativa No. 5601, Ley de Prevención y Protección contra la Ciberdelincuencia, esta última presentada el 17 de septiembre de 2019. El análisis de los mecanismos anteriormente descritos fue indispensable para determinar las condiciones en las que se encuentra el estado de Guatemala respecto a la seguridad cibernética en el país previo a su adhesión al Convenio sobre Ciberdelincuencia.

Es menester mencionar que el presente tema de investigación pretendió servir como fuente de conocimiento para futuras investigaciones relacionadas con los temas de seguridad cibernética, ciberdelincuencia, y el Convenio de Budapest. Así como el análisis de los beneficios que el estado de Guatemala tendrá al adherirse a dicho Convenio.

1.1.2 Planteamiento del problema

El Convenio sobre ciberdelincuencia fue creado con el objetivo de "prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos" (Convenio sobre Ciberdelincuencia, 2001, p. 2), y ha sido aplicado principalmente en países desarrollados, sobre los cuales los avances tecnológicos han tenido mayor auge, desde hace más de 20 años; sin embargo, en los últimos 10 años, el acceso a internet por parte de la población latinoamericana ha tenido un crecimiento considerable; a pesar de ello, debido al retraso tecnológico de dicha región, existe una considerable brecha respecto a la legislación, regulaciones, mecanismos y protocolos en temas de seguridad cibernética, en comparación con países desarrollados que han implementado los mecanismos de defensa y estrategias estipuladas en el convenio desde su entrada en vigor y su ratificación por cada país signatario respectivamente.

En lo que corresponde al uso de la tecnología en Guatemala, a pesar de que el incremento en el uso de las TIC e Internet ha sido notorio en los últimos años, aún existe una

brecha considerable en el uso de estas herramientas principalmente por parte de la población rural del país según los resultados del XII Censo Nacional de Población y VII Censo Nacional de Vivienda de 2018, no obstante, se ha visualizado un incremento en las actividades ilícitas por medio de internet; de acuerdo a las estadísticas nacionales del Observatorio Guatemalteco de Delitos Informáticos (OGDI), en el primer trimestre del año 2020 las ciberamenazas, el ciberacoso, la pornovenganza, el robo de identidad, el sexting, las difamaciones, la pornografía infantil y las ciberestafas fueron las actividades ilícitas por medio de internet que más afectaron a la población guatemalteca. Como resultado, la implementación de estrategias y mecanismos que busquen mitigar, prevenir y combatir este tipo de amenazas, principalmente aquellas que no están correctamente tipificadas dentro de las legislaciones nacionales ya establecidas, ha sido suma de importancia tanto a nivel nacional como internacional, al ser una problemática que va más allá de las fronteras territoriales ya establecidas.

En Latinoamérica, la necesidad de regular los sistemas, redes y datos informáticos ha hecho que se establezcan mesas de diálogo con el fin de crear lineamientos, estrategias, protocolos y mecanismos para regular la seguridad cibernética en la región. Dichas mesas de diálogo principalmente en Latinoamérica, han sido moderadas por organizaciones internacionales y regionales como lo son: la Unión Internacional de Telecomunicaciones de Naciones Unidas (UIT), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Organización de Estados Americanos (OEA); este último tiene como prioridad en el marco de la seguridad cibernética en la región, respaldar los esfuerzos e iniciativas de los Estados Miembros destinados a fortalecer las capacidades necesarias para que el dominio informático sea más seguro, estable y productivo (OEA, 2014, p. 4).

Guatemala junto a otros países del mundo, muestra deficiencias respecto a la seguridad cibernética en el país; la falta de la aprobación de una legislación que tipifique correctamente los delitos cibernéticos, así como la insuficiente concientización sobre la esta problemática, son factores que afectan el fortalecimiento de la resiliencia cibernética en el

país, como se ve reflejado en los indicadores del reporte de ciberseguridad de 2016 y 2020 del Banco Interamericano de Desarrollo (BID). Es importante mencionar que existen medidas que el gobierno de Guatemala ha tomado para hacer frente a esta problemática como lo fue la manifestación de su interés de adherirse al Convenio sobre ciberdelincuencia por medio de una carta dirigida al Comité Europeo de ciberseguridad en 2016; así como la solicitud, en ese mismo año, a la OEA, de apoyo técnico para la elaboración de una estrategia de seguridad cibernética. Ambas solicitudes fueron aceptadas y respondidas por el Comité Europeo de Ciberseguridad y la OEA respectivamente, por lo que en 2018 fue presentada formalmente, por parte del Ministerio de Gobernación de Guatemala (MINGOB), la Estrategia Nacional de Seguridad Cibernética, lo que constituye uno de los primeros pasos por parte del estado de Guatemala para cumplir con los requerimientos para formar parte del Convenio.

La Estrategia Nacional de Seguridad Cibernética establece metas de mejoramiento de los mecanismos de seguridad y resiliencia, especialmente de las infraestructuras críticas y servicios públicos nacionales, siempre con la ayuda del sector privado, debe considerarse que aún existe una brecha de comunicación entre el sector público y las entidades privadas en Guatemala lo cual puede convertirse en un lastre que ralentice el esfuerzo.

1.1.3 Preguntas generadoras

Si bien la Estrategia Nacional de Seguridad Cibernética y la presentación de iniciativas de ley sobre ciberdelincuencia muestran algunos de los avances del estado de Guatemala para poder adherirse al Convenio sobre ciberdelincuencia, existen otros mecanismos para fortalecer la seguridad cibernética en el país que deben ser tomados en cuenta. Por tal motivo, se formularon las siguientes preguntas generadoras, así como los objetivos que se pretendieron alcanzar en la presente investigación, todo lo cual contribuyó a evidenciar los esfuerzos y avances del gobierno de Guatemala en el tema de seguridad cibernética para el combate de la ciberdelincuencia: ¿Cuáles son los beneficios que el estado de Guatemala adquiere al adherirse al Convenio de Ciberseguridad?

En cuestiones relativas a la cooperación internacional, ¿Qué implicaciones, retos y experiencias tendría el Estado guatemalteco como miembro de la comunidad internacional al formar parte del Convenio sobre ciberdelincuencia?

¿Cuáles son las condiciones en las que se encuentra el estado de Guatemala respecto al combate de los delitos cibernéticos para optar a la adhesión al Convenio sobre Ciberdelincuencia?

1.1.4 Objetivos de la investigación

1.1.4.1 Objetivo general

Analizar la importancia del Convenio sobre ciberdelincuencia para la seguridad cibernética en Guatemala y los beneficios que tendría al adherirse a dicho Convenio.

1.1.4.2 Objetivos específicos

Estudiar las disposiciones establecidas en el Convenio sobre ciberdelincuencia respecto a los delitos cibernéticos, así como las condiciones actuales en las que se encuentra Guatemala en la lucha contra la ciberdelincuencia.

Identificar la estrategia técnica y legal que posee el estado de Guatemala para la lucha contra la ciberdelincuencia y los logros obtenidos mediante la aplicación de esta.

1.1.5 Delimitación de la investigación

Para el estudio del presente tema se tomó como base el Convenio de Budapest y la resolución AG/RES 2014 sobre la “adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética”, así como los informes oficiales de la OEA y el BID, acerca de la Seguridad Cibernética en América Latina y el Caribe, publicaciones digitales,

revistas digitales y otros textos nacionales e internacionales relacionados con el tema en cuestión.

1.1.5.1 Delimitación temporal

El estudio comprende el periodo 2016-2020, en donde se realizó el análisis de la ciberdelincuencia y la seguridad cibernética en Guatemala, ya que fue a partir de del año 2016 en donde Guatemala empezó a llevar a cabo una serie de mecanismos y estrategias, en calidad de prerrequisitos, para su adhesión al Convenio de Budapest; entre los cuales se encuentra, el desarrollo de la Estrategia Nacional de Seguridad Cibernética, así como la presentación del GT.CERT y la presentación de la Iniciativa No. 5254 Ley sobre la Ciberdelincuencia, en 2017; y la Iniciativa No. 5601 Ley de Prevención y Protección contra la Ciberdelincuencia, en 2019.

1.1.5.2 Ámbito Geográfico

Se estudió las estrategias y mecanismos para fortalecer la resiliencia cibernética en el territorio guatemalteco, por lo cual la investigación se llevó a cabo en la ciudad de Guatemala, no obstante, la información y estrategias de las instituciones especializadas en temas de seguridad nacional en Guatemala comprenden todo el territorio guatemalteco.

1.1.6 Tipo de investigación

Se realizó una revisión documental con el fin de llevar a cabo un análisis sobre la ciberseguridad en Guatemala, se consultaron informes y revistas relacionadas al análisis de la ciberdelincuencia y la seguridad cibernética como lo fueron los reportes de ciberseguridad del BID. Además, se estudiaron las iniciativas de ley, estrategias de ciberseguridad, organismos y tratados de cooperación internacionales para hacer frente a la ciberdelincuencia. Al ser una investigación cualitativa, se pudo evidenciar los avances y desafíos que ha tenido en Guatemala para reforzar la resiliencia cibernética en el país con

base al estudio de los mecanismos y estrategias que el Gobierno guatemalteco ha implementado, en calidad de prerrequisitos, para adherirse al Convenio.

1.1.7 Métodos y técnicas

Para esta investigación, las técnicas utilizadas fueron la lectura y análisis de fuentes investigación bibliográfica de fuentes secundarias, la observación no participativa y fundamentalmente la implementación de entrevistas semiestructuradas elaboradas de manera virtual, así como la asesoría de expertos relacionados con las TIC y la seguridad cibernética en el país.

Entrevistados:

Primero se realizó una entrevista virtual por medio de la plataforma Zoom, el 13 de octubre de 2020, al ingeniero Carlos Giovanni Guzmán de León, exsubdirector de Ciberseguridad y encargado del GT. CERT hasta marzo 2020, quién también fue parte del equipo técnico que trabajó en la iniciativa de ley número 5254 en 2017.

Posteriormente, el día 14 de octubre de 2020, también por el mismo medio se entrevistó a la ingeniera Devora Meza Orellana, exviceministra de Tecnología de las Comunicaciones del MINGOB, quien es especialista en temas de ciberseguridad y docente de la Universidad Mariano Gálvez en la Maestría de Seguridad Informática.

El día 15 de octubre de 2020, respecto al tema del Internet en Guatemala, se entrevistó virtualmente al ingeniero Luis Roberto Furlán, director del Centro de Estudios de Informática Aplicada de la Universidad del Valle de Guatemala, considerado como el pionero del Internet en Guatemala al introducir el servicio en 1990.

Durante las entrevistas se lograron identificar aspectos claves que ayudaron a complementar el trabajo de investigación y dar cumplimiento a los objetivos de estudio de esta investigación.

1.2 Abordaje teórico

1.2.1 Marco conceptual

El espacio virtual creado con el uso de las TIC y el acceso a Internet en el mundo ha generado una serie de conductas delictivas que además de afectar la seguridad de las estructuras críticas de los Estados, también afecta la seguridad de la información y datos de millones de personas, empresas, e instituciones a nivel mundial; en donde ha sido necesario crear y unir esfuerzos, por medio de la cooperación internacional, para combatir la ciberdelincuencia y fortalecer la seguridad cibernética tanto a nivel nacional, regional e internacional. Por lo cual, los conceptos claves para la presente investigación, fueron los conceptos de ciberdelincuencia, ciberseguridad y cooperación internacional.

Ante falta de una definición universal para el concepto de ciberdelincuencia, la Comisión Europea en la comunicación denominada: Hacia una política general de lucha contra la ciberdelincuencia presentada en Bruselas, Bélgica, definió el concepto de ciberdelincuencia como “las actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas” (Comisión de las Comunidades Europeas, 2007, p. 2). La cual también estableció tres tipos de actividades delictivas:

En primer lugar, menciona las formas tradicionales de delincuencia las cuales han incursionado en el mundo de la virtualidad al ser cometidas mediante medios electrónicos como los son el fraude y la falsificación. En segundo lugar, los contenidos ilegales que engloban una serie de actividades ilícitas que involucran el contenido que circula en la red y que de alguna manera afectan la integridad de las personas como lo es la pornografía infantil, el sexting, y el odio racial. Por último, aquellas actividades ilícitas específicas de las redes electrónicas como lo es la denegación de servicio, y los ataques contra sistemas informáticos.

Se entiende por ciberdelincuencia al conjunto de acciones cometidas a través de un sistema informático, cuya consecuencia final recae en un hecho considerado como ilícito. En

otras palabras, se trata de una vertiente del crimen tradicional que utiliza las nuevas tecnologías para extenderse y desarrollarse de manera exponencial. (Mateos Pascual, 2013)

Al hablar de ciberdelincuencia, es importante hablar de los mecanismos de defensa para hacer frente a ese tipo de actividades ilícitas, siendo la seguridad de las TIC o en términos más modernos como: ciberseguridad o seguridad cibernética, el área que diseña las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable (Aguilera López, 2010, p. 9).

La definición del concepto de ciberseguridad ha sido compleja debido a que no solo se refiere a la seguridad de las estructuras críticas de los Estados, sino que también a la protección de los sistemas, las redes, y los datos informáticos que se encuentran almacenados en Internet, "la Ciberseguridad es definida en líneas generales como la seguridad de la información digital almacenada en redes electrónicas, aunque aún hoy no hay un consenso en su definición"(Castro y Monteverde, 2018, p. 5).

En esta línea, la Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos refiere que:

> El concepto de ciberseguridad solía emplearse como un término bastante amplio al referirse a diversos temas como la seguridad de la infraestructura nacional y de las redes a través de las cuales se provee el servicio de Internet, hasta la seguridad o integridad de los usuarios. Sin embargo, fue necesario limitar este concepto al resguardo de los sistemas y datos informáticos que permitiría una mejor comprensión del tema y la identificación de soluciones para proteger la seguridad de la información. (Botero Marino, 2013, p. 58)

Por su parte la Unión Internacional de Comunicaciones, UIT (2008) mediante la Recomendación UIT-T X.1205 ha definido el término de ciberseguridad como:

> El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:
>
> • Disponibilidad;
>
> • Integridad, que puede incluir la autenticidad y el no repudio;
>
> • Confidencialidad.

Con la presente investigación se determinó que por medio de la Iniciativa de ley 5601, en el artículo 7 literal g., se pretendió adoptar la definición de la UIT para efecto de dicha iniciativa y otras leyes nacionales guatemaltecas que a ella se apeguen.

La ciberdelincuencia ha crecido a un ritmo acelerado en donde organizaciones internacionales han tenido que establecer un plan global a fin de fortalecer la seguridad cibernética en el mundo y en donde ha sido necesaria la cooperación internacional. En ese sentido, el Convenio sobre ciberdelincuencia de Budapest nace con la necesidad de crear un plan de cooperación entre estados con el objetivo de aplicar una política penal común destinada a la protección de la sociedad contra las actividades delictivas realizadas por medio de internet.

La cooperación internacional se entiende como “toda relación entre actores internacionales orientada a la mutua satisfacción de intereses o demandas, mediante la utilización complementaria de sus respectivos poderes en el desarrollo de actuaciones coordinadas y/o solidarias” (Calduch Cervera, 1991, p. 4). La cooperación internacional forma parte importante de las acciones llevadas a cabo por diferentes actores del sistema internacional en diferentes ámbitos, ya sea en lo económico, lo cultural, lo ambiental, en temas de seguridad alimentaria u otro ámbito en donde un país posee una dificultad y necesita ayuda para poder solucionarla.

La Carta de las Naciones Unidas en el artículo número 1, sobre a los principios de la organización referente a la cooperación internacional entre los países miembros, señala como principio el “realizar la cooperación internacional en la solución de problemas internacionales de carácter económico, social, cultural o humanitario, y en el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos” (Naciones Unidas, 1945, párr. 3).

Tras los nuevos retos de la ciberdelincuencia, la práctica actual de la cooperación internacional posee diferentes modalidades de cooperación, con actores, objetivos e instrumentos diferenciados. En lo que respecta a los delitos cibernéticos, la cooperación en seguridad tiene una modalidad de carácter multilateral, en donde los mecanismos de cooperación prioritarios han sido el intercambio de información, así como la Asesoría, entrenamiento y capacitación respecto a la temática. (PNUD, 2013, pp. 150–160)

> En materia de seguridad cibernética se refiere al esfuerzo conjunto de gobiernos, apoyado por el dinamismo de organismos internacionales, sociedad civil, academia y sector privado, para promover acciones que contribuyan a generar espacios de participación segura en el ciberespacio a través de la transferencia, recepción e intercambio de información, conocimientos, tecnologías, experiencias y recursos, respetando los principios del derecho internacional y respeto a los derechos humanos. (Ministerio de Gobernación, 2018, p. 31)

En este sentido, se ha determinado que la cooperación internacional es importante para solucionar problemas de carácter global como lo es la ciberdelincuencia, "facilitar el intercambio de información a todos los niveles es quizás la más importante de las ventajas que puede proporcionar la cooperación internacional, dada su transversalidad" (Díaz Gómez, 2010, p. 189).

1.2.2 Bases teóricas

El carácter supranacional de la ciberdelincuencia ha generado nuevos retos para la comunidad internacional, en donde la cooperación internacional ha sido indispensable en la creación de mecanismos conjuntos para mitigar los delitos cibernéticos. La cooperación internacional se ha convertido en un elemento clave en el ámbito de las relaciones internacionales; la cooperación entre Estados soberanos para dar solución a problemas de agenda global es un factor importante dentro de la interdependencia.

Dentro de la perspectiva de la política de la interdependencia se encuentran involucrados intereses internos, transnacionales y gubernamentales que incluyen tanto Estados soberanos como organizaciones internacionales y sociedad civil, como refieren Robert Keohane y Joseph Nye (1988), "la interdependencia reduce los conflictos de intereses y que la cooperación por sí sola es la respuesta a los problemas mundiales" (p. 20).

En política internacional, las amenazas a la seguridad son permanentes; ante las nuevas amenazas propiciadas por la globalización; los delitos tradicionales han evolucionado y para poder comprender la evolución de la delincuencia, se encuentra la Teoría de las Actividades Cotidianas. Además, se analizó el Convenio sobre ciberdelincuencia desde la perspectiva que proporciona la teoría de la interdependencia compleja, para comprender la importancia de la cooperación internacional en temas de agenda global.

1.2.1 Teoría de las Actividades Cotidianas

La Teoría de las Actividades Cotidianas (TAC), presentada por Lawrence E. Cohen y Marcus Felson en 1979, aporta un modelo de explicación para comprehender los factores por los cuales la delincuencia tradicional evolucionó a raíz del espacio virtual proporcionado por las TIC.

La teoría de las Actividades Cotidianas se basa en lo que se denomina: el modelo de la oportunidad, la cual establece que un delincuente encuentra un terreno ad-hoc para cometer actos delictivos dependiendo del espacio y tiempo disponible, factores que favorecen la internacionalización del crimen, cuando el contacto, la información y los datos trascienden fronteras físicas. En relación con lo anterior Miró (2013), menciona que:

> La evolución de las Tecnologías de la Información y la Comunicación, especialmente en la última década, han convertido Internet en un medio nuevo e indispensable para la comunicación entre las personas, lo cual ha hecho del ciberespacio un ámbito de oportunidad delictiva distinto al espacio físico, en el que la víctima adquiere especial relevancia para la explicación y prevención del delito. (p. 2)

Desde la perspectiva de la seguridad internacional, las TIC han propiciado el espacio pertinente para incentivar la evolución de la delincuencia tradicional, como lo es la estafa o el fraude, y ha originado nuevas formas de delincuencia, como lo son los delitos específicos de las redes informáticas, Villacampa Estiarte et al. (2019) señala que la victimización posee tres factores establecidos:

- Delincuentes motivados principalmente con inclinación delictiva.
- Presencia de objetos o víctimas propensas a estar en el punto de mira del victimario con preferencia a aquellas que se encuentran próximas, física o virtualmente al lugar en donde se comete el delito. Así mismo, víctimas expuestas (aquellas que por sus actividades cotidianas se relacionan con delincuentes, como los policías) y víctimas

atractivas (aquellas que presentan características personales, económicas o de accesibilidad que las ponen en el punto de mira del victimario, como, por ejemplo, las joyerías).

- Por último, la ausencia o escasez de protectores eficaces o recursos de seguridad como agentes policiales y de control, unido a la peligrosidad de determinados espacios y tiempos.

Por estas razones, la ciberdelincuencia sigue un patrón en donde las actividades delictivas se dan a consecuencia del espacio virtual abierto que proporciona Internet. En la actualidad, las actividades cotidianas de personas, instituciones, empresas y gobiernos alrededor del mundo se basan en interacciones por medio de internet. Estos actos tienden a compartir información personal y confidencial por medio de las tecnologías de la información y comunicación, lo cual los vuelve blancos de criminales cibernéticos que buscan causar daño principalmente a ordenadores y sistemas informáticos. La ausencia de una policía cibernética mundial convierte al delito cibernético en una actividad que se vuelve más fuerte conforme la evolución de las TIC.

1.2.2 Teoría de la interdependencia compleja

La Real Academia Española define interdependencia como: dependencia mutua, por lo que es importante diferenciar los términos de dependencia e interdependencia. En ese sentido, Robert Keohane y Joseph Nye (1998), considerados como los como los dos grandes referentes de la Teoría de la Interdependencia Compleja, refieren que:

> En el lenguaje común, dependencia significa un estado en el cual se está determinado o significativamente afectado por fuerzas externas. Interdependencia, en su definición más simple, significa dependencia mutua. En política mundial, interdependencia se refiere a situaciones caracterizadas por efectos recíprocos entre los países o entre actores de diferentes países. (p. 22)

La teoría de la Interdependencia Compleja se basa en principios de cooperación e integración, en donde el concepto de vulnerabilidad es clave ya que se refiere a la capacidad de un estado para afrontar la problemática. En temas de seguridad, la vulnerabilidad se manifiesta en la capacidad de los estados para ajustar sus políticas nacionales y reforzar su resiliencia. El análisis internacional ofrece conceptos claves para entender los fenómenos mundiales desde la dinámica de la globalización, Keohane & Nye (1988), afirman que:

> La interdependencia afecta la política mundial y el comportamiento de los Estados, pero las acciones gubernamentales también influyen sobre los modelos de interdependencia. Al crear o aceptar procedimientos, normas o instituciones para ciertas clases de actividades, los gobiernos regulan y controlan las relaciones transnacionales e interestatales. A estos acuerdos gubernamentales los denominaremos *regímenes internacionales.* (p.8)

Otra de las caracteristicas de esta teoría refiere que “la fuerza militar no es empleada por los gobiernos de la región cuando predomina la interdependencia compleja” (Keohane y Nye, 1988, p. 41). Aunque la fuerza militar sigue siendo un factor importante en las relaciones de poder, esta no resuelve otras problemáticas actuales como lo es la seguridad cibernética. Por lo que, la teoría de la interdependencia compleja se adapta a los retos de la seguridad cibernética al proporcionar un enfoque de cooperación entre estados en donde la fuerza militar se vuelva obsoleta en el combate contra los delitos cibernéticos; las alianzas interestatales, gubernamentales e intergubernamentales para combatir la delincuencia transnacional requieren aspectos más técnicos como compartir información, experiencias, legislaciones, y expertos.

Cualquier relación con otros países, en términos de dependencia teniendo en cuenta los niveles de desarrollo tecnológico manejado por los países desarrollados, evidencia la necesidad que tienen los Estados de asociarse y hacer frente a las problemáticas que ponen en riesgo tanto la seguridad nacional como la internacional.

CAPÍTULO II

2. Antecedentes históricos de los delitos informáticos y de los instrumentos internacionales para la mitigación de la ciberdelincuencia

A lo largo de los años, la demanda en el uso de las TIC y el acceso a Internet, tomando en consideración que este último en donde la ubicación e identidad del usuario es compleja, ha hecho que los delitos tradicionales como el fraude y la suplantación de identidad evolucionaran, generando la transnacionalización del delito y ocasionando un desafío a nivel internacional. El aumento de los delitos cibernéticos y los peligros ocasionados por el uso inadecuado de las TIC, Internet y las redes informáticas ocasionó la necesidad de crear mecanismos y estrategias a nivel internacional para combatir, prevenir y mitigar la ciberdelincuencia.

En virtud de lo anterior, el presente capitulo aborda los antecedentes históricos de la ciberdelincuencia, en donde posteriormente se describen los instrumentos internacionales que han surgido a nivel internacional para prevenir y mitigar los delitos cibernéticos.

2.1. Acerca de los delitos cibernéticos

El auge de Internet a partir del siglo XX trajo aunado el incremento de la ciberdelincuencia en el mundo. Los historiadores remontan el primer ataque cibernético al año de 1971 con el primer virus informático: el programa CREEPER escrito por el ingeniero Bob Thomas, el cual mostraba el mensaje *"Soy una enredadera... ¡atrápame si puedes!"*. CREEPER fue un experimento de seguridad creado para fines no maliciosos, que pretendía demostrar la habilidad que podía tener un programa para expandirse rápidamente en diferentes ordenadores a través de la red; siendo la base para el desarrollo de ataques posteriores con pérdidas multimillonarias (Loredo y Ramírez, 2013).

Posteriormente, existieron diferentes ataques a sistemas informáticos que afectaron diversas instituciones a nivel mundial, siendo las más afectadas las instituciones financieras.

2.2 Instrumentos internacionales para prevenir y mitigar la ciberdelincuencia

El origen de la protección contra los delitos cibernéticos se centró desde un plano internacional, al ser una problemática de carácter transnacional; por lo cual se presenta un repaso cronológico de los esfuerzos más notorios de regulación y persecución de los abusos informáticos a nivel internacional. Se tomó como punto de partida los esfuerzos realizados por la Organización para la Cooperación y Desarrollo Económico (OCDE) desde 1983 que tenían como fin la protección del uso indebido de los programas informáticos; por otro lado, se presenta lo que supuso el hito de regulación a nivel penal contra los delitos informáticos, la Ley de Abuso y Fraude Informático de 1986. Años después surge el Convenio sobre Ciberseguridad firmado en 2001, el cual se ha posicionado como el único instrumento internacional en materia de delitos cibernéticos y el cual también ha sido punto de referencia para diferentes instrumentos internacionales que buscan mitigar, prevenir y combatir los delitos cibernéticos, como lo fue la Estrategia Interamericana Integral de Seguridad Cibernética de 2004.

Como se mencionó en el apartado anterior, los primeros esfuerzos de crear mecanismos de respuesta y defensa frente a amenazas cibernéticas a nivel internacional fueron realizados por la OCDE en 1983, cuando un grupo de expertos se reunió y recomendó a esta Organización Internacional, la necesidad de armonización en los delitos informáticos, lo que finalmente se materializa en el informe denominado: Delitos de informática: análisis de la normativa jurídica, que incluía recomendaciones sobre las cuáles los distintos países podrían prohibir y sancionar a través de sus leyes penales los usos indebidos de los sistemas y redes de la información en el marco de una cultura de seguridad (UIT, 2009, p. 110).

En 1986, Estados unidos promovería la creación de la ley federal: Ley de Abuso y Fraude Informático, CFAA por sus siglas en inglés; la cual tuvo como objetivo proteger información clasificada del gobierno de Estados Unidos e instituciones financieras, convirtiéndose en la primera legislación penal para la protección y regulación de los ataques ante sistemas informáticos (Computer Fraud and Abuse Act, 1986).

En 1989 el Comité de ministros del Consejo de Europa adopta la Recomendación No. R (89) 9 sobre delitos informáticos del Comité Europeo de problemas de delincuencia, en la que se recomienda a los gobiernos de los estados miembros tomar en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre delitos informáticos elaborado por la Comisión Europea de problemas delictivos y, en particular, las directrices de las legislaturas nacionales (Council of Europe, 1990, p. 7).

Además, dentro de la Resolución No. R (89) 9, se promovió una guía para las legislaciones nacionales en donde también figuraba una lista mínima de delitos cibernéticos que debían legislarse; entre los cuales se encontraba el fraude informático, el daño a los datos y programas de la computadora, el sabotaje informático, el acceso e interceptación no autorizada, así como una lista opcional en la que figuraban otros delitos como: la alteración de datos informáticos o programas informáticos, el espionaje informático y el uso no autorizado de la computadora (Council of Europe, 1990).

En 1990 el Comité de políticas de información, informática y comunicación creó un grupo de expertos que tenían como tarea la creación de una lista de directrices de seguridad de la información, que posteriormente fueron adoptadas por el comité de la OCDE. Las directrices pretendían:

a) Sensibilizar sobre los riesgos para los sistemas de información y sobre las salvaguardias disponibles para hacer frente a esos riesgos;

b) Crear un marco general para ayudar a los responsables, en los sectores público y privado, para el desarrollo e implementación de medidas, prácticas y procedimientos coherentes para la seguridad de los sistemas de información;

c) Promover la cooperación entre los sectores público y privado en el desarrollo e implementación de tales medidas, prácticas y procedimientos;

d) Fomentar la confianza en los sistemas de información y la forma en que se proporcionan y utilizan;

e) Facilitar el desarrollo y uso de sistemas de información, a nivel nacional e internacional; y

f) Promover la cooperación internacional para lograr la seguridad de los sistemas de información. (OECD, 1992)

Debido a la naturaleza transfronteriza de la ciberdelincuencia, el sistema internacional se vio en la necesidad de concretar la creación un marco común de trabajo para combatir la ciberdelincuencia transnacional. Por lo cual, en 1995 el Consejo de Europa tomó la iniciativa de crear un comité de expertos en delitos informáticos para trabajar sobre el tema de la ciberdelincuencia y así crear una serie de recomendaciones que más adelante se convertiría en el Convenio sobre ciberdelincuencia firmado en Budapest.

En 2001 se presenta finalmente el Convenio sobre Ciberdelincuencia, firmado en la ciudad de Budapest, Hungría, y el cual fue adoptado durante la celebración de la sesión No. 109 del Comité de ministros del Consejo de Europa; entrando en vigor el 1 de julio de 2004. El Convenio sobre Ciberdelincuencia fue creado con la finalidad de establecer los lineamentos necesarios para que cada Estado miembro pudiese crear dentro de su ordenamiento jurídico, las bases y herramientas necesarias para hacer frente a los desafíos que constituyen las TIC y así proteger los intereses de la comunidad internacional, así como, el fortalecimiento y mejora de la cooperación internacional para hacer frente a la ciberdelincuencia mediante la pronta y rápida acción generada por la comunidad internacional.

Su principal objetivo fue aplicar una política penal común destinada a la protección de la sociedad contra las actividades delictivas realizadas por medio de internet, ciberdelincuencia como son conocidas este tipo de actividades, especialmente mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional (Convenio sobre Ciberdelincuencia, 2001).

En 2002 la lista de directrices presentada por la OCDE en 1992, es revisada y surge una nueva versión de directrices de seguridad de los sistemas y redes de información en el

marco de una cultura de seguridad de la OCDE, para poder establecer un marco de principios que se aplican a todos los participantes para mejorar la seguridad de los sistemas y redes de información a fin de fomentar la prosperidad económica y el desarrollo social, llamada: Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad (OECD, 2004).

En 2004 en la Asamblea General de la OEA, los Estados miembros aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética en la resolución AG/RES. 2004 (XXXIV-O/04), titulada: Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética. Esta estrategia fomenta la cooperación interamericana en la prevención y el combate a la ciberdelincuencia por medio de estrategias y políticas de ciberseguridad como la creación de Estrategias Nacionales de Seguridad Cibernética y Equipos de Respuesta a Emergencias Informáticas CERT, convirtiéndose en el primer instrumento regional en fomentar la cooperación hemisférica en América en el combate contra la ciberdelincuencia.

CAPÍTULO III

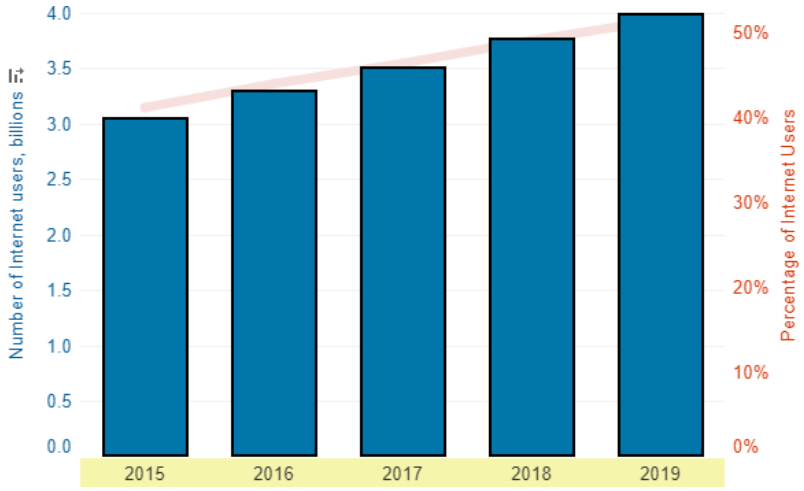
3. El uso de Internet y la importancia de la ciberseguridad

3.1 Penetración y acceso a Internet

La presencia de las Tecnologías de la Información y la Comunicación para mejorar la calidad de vida de la población alrededor del mundo ha incrementado exponencialmente con el paso de los años debido a la conectividad y dependencia que estas generan, aunado a ello, la necesidad de estar en conexión constante ha hecho que el uso de Internet incrementará considerablemente con más de 4.0 billones de usuarios alrededor del mundo en 2019, cifra que aumenta diariamente, según estimaciones de la Unión Internacional de Telecomunicaciones (UIT) como se muestra en la **¡Error! No se encuentra el origen de la r eferencia.**, la cual refleja un aumento del 2% en comparación con 2018. Además, la UIT, estima que la tasa de penetración de Internet a nivel mundial aumentó de 41% de usuarios en 2015 a más del 51% en 2019. (ITU, 2020)

Figura 1

Estimación de personas a nivel mundial que utilizan Internet, 2015-2019



Nota. Adaptado de las estimaciones de la UIT de 2005-2019 sobre el uso de internet en la población mundial. Fuente: Individuals using Internet de International Telecommunication Union (2020).

El uso de las TIC e Internet ha generado oportunidades de crecimiento a nivel internacional ante la necesidad de digitalizar la mayoría de las actividades humanas, oportunidades que ofrecen el desarrollo y bienestar de la población. La llegada de Internet ha generado un gran cambio en el ámbito internacional, cual que involucra diferentes sectores en donde se desenvuelve la sociedad, sectores como el económico, el político, el social, el cultural, entre otros.

La cifra de usuarios a nivel mundial incrementa cada día y en la actualidad, buena parte del crecimiento proviene de los países emergentes y subdesarrollados, no obstante, existe una brecha en el acceso a internet entre países más desarrollados y los países menos desarrollados o subdesarrollados, el informe de la ITU titulado Measuring digital development Facts and figures (2019), señala que: en los países desarrollados, la mayoría de las personas están en línea, y cerca del 87 por ciento de las personas utilizan Internet; por otro lado, en los países menos adelantados, se estimó que solo el 19% de las personas estuvieron en línea para el año 2019. La brecha más notable se da en las tasas de uso de internet entre Europa y África, siendo la población europea la que tiene una tasa más alta en el uso de internet y África la región con las tasas de uso de Internet más bajas.

En el caso de América Latina y el Caribe, las oportunidades de desarrollo y crecimiento económico aumentan cada día más, así como los desafíos de la era digital. Se estima que la región obtuvo un crecimiento en la penetración de internet en los hogares latinoamericanos y caribeños de 68,66 % en 2018 a 78,78%, lo cual incluye un incremento de casi un 10.12% en el uso de internet en la región; siendo Brasil, República Dominicana, Venezuela los países de la región que obtuvieron más del 15% de incremento en la penetración de Internet de 2018 a 2020; países como Barbados, México y Uruguay tuvieron un incremento de menos del 5% en la penetración de Internet. Con respecto a Chile, los datos obtenidos por la Unión Internacional de Telecomunicaciones señalan que fue el único país en la región que no reflejo un incremento, como se muestra la Tabla 1, en la cual se describe

las tasas de penetración de internet en los años 2018, 2019 y 2020 haciendo un análisis comparativo de 2018 y 2020 para determinar cuál fue el aumento en cada país de la región.

Tabla 1

Penetración de Internet en América Latina y el Caribe (2018-2020)

	2018	2019	2020	Aumento de 2018 a 2020
Argentina	77.78%	81.42%	85.20%	7.42%
Barbados	84.03%	86.37%	88.77%	4.74%
Bolivia	48.22%	53.04%	58.34%	10.12%
Brasil	74.33%	81.64%	89.80%	15.47%
Chile	82.33%	82.33%	82.33%	0.00%
Colombia	66.68%	71.40%	76.47%	9.79%
Costa Rica	74.09%	76.88%	79.79%	5.70%
Ecuador	60.67%	64.27%	68.09%	7.42%
El Salvador	37.30%	40.92%	45.02%	7.72%
Guatemala	72.50%	78.65%	86.52%	14.02%
Honduras	34.06%	36.60%	39.33%	5.27%
Jamaica	60.58%	66.64%	73.30%	12.72%
México	65.77%	67.75%	69.79%	4.02%
Panamá	62.01%	66.45%	71.20%	9.19%
Paraguay	64.99%	69.16%	73.60%	8.61%
Perú	52.54%	56.65%	61.08%	8.54%
República Dominicana	74.82%	82.31%	90.54%	15.72%
Trinidad & Tobago	81.58%	86.06%	90.79%	9.21%
Uruguay	70.21%	72.20%	74.24%	4.03%
Venezuela	79.20%	87.12%	95.83%	16.63%
América Latina (promedio ponderado)	68.66%	73.52%	78.78%	10.12%
OCDE (promedio ponderado)	83.93%	86.07%	88.33%	4.40%

Nota. Los últimos datos provistos por la UIT son para el 2017 y el 2018 según el país. Los datos del 2019 y el 2020 han sido extrapolados en base a la tasa de crecimiento del último año con información provista por la UIT. Fuente: Unión Internacional de Telecomunicaciones; análisis Telecom Advisory Services, CAF (2020)

3.1.1 Internet en Guatemala

La historia del Registro de Dominios.GT (2018) hace referencia al inicio del Internet en Guatemala a 1990, cuando el Ingeniero Luis Furlán, quien fungía como director del Centro de Estudios en Informática Aplicada (CEIA) del Instituto de Investigaciones de la Universidad del Valle de Guatemala estableció la primera conexión Internet desde Guatemala por medio del proyecto denominado Proyecto Huracán el cual permitía a miembros de instituciones educativas de Costa Rica, conectarse a Internet por medio del protocolo UUCP, utilizando módems para conectar computadoras por medio del sistema telefónico.

Además, refiere que "la Internet era de carácter netamente científico/académico y que el procedimiento estándar, era que alguna universidad administrara los nombres de dominio de nivel superior, en especial fuera de EEUU" (Registro de Dominios.gt, 2018), fue así como la Universidad del Valle de Guatemala fue la primera institución a quien se le asignó el dominio de Internet uvg.edu y quien desde 1992 hasta la fecha administra los nombres de dominio de Internet en Guatemala.

> Cabe resaltar que la implementación de una red de Internet en Guatemala tuvo complicaciones, no fue sino hasta diciembre de 1995 que GUATEL que en aquel entonces era el monopolio estatal de las telecomunicaciones, dio su aprobación y fue así como empezó formalmente a funcionar el internet en Guatemala a nivel académico y también comercial. (Registro de Dominios.gt, 2018)

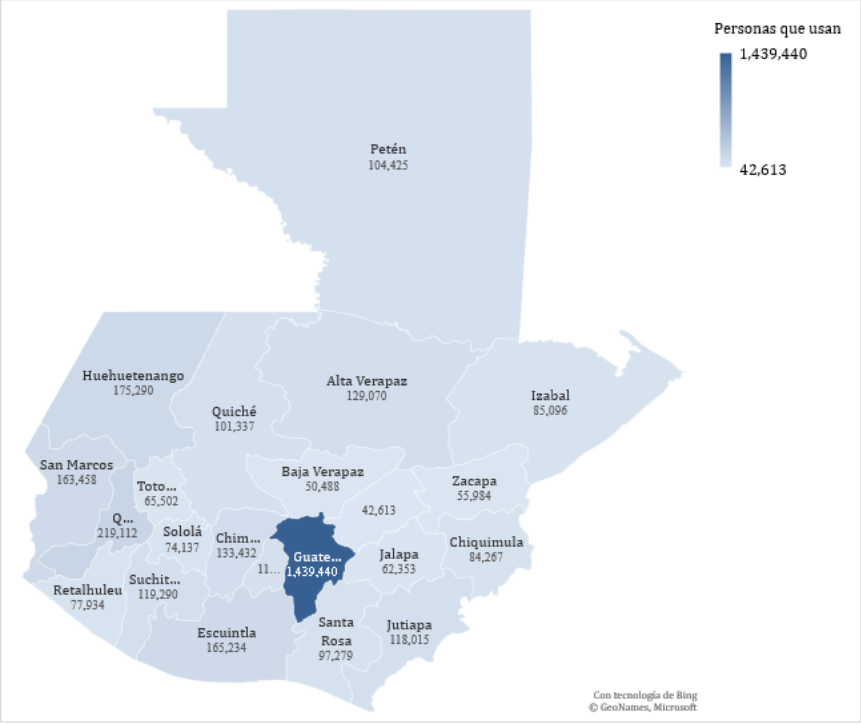
Fue de esa manera que Internet dejó de ser un instrumento especializado de la comunidad científica para transformarse en el instrumento de comunicación más rápido en crecimiento, modificando las pautas de interacción social y convirtiéndose en una herramienta de desarrollo para Guatemala. Desde la liberación del sector de telecomunicaciones en el año 1996 a través del Decreto 94-96 del Congreso de la República,

Ley General de Telecomunicaciones, Guatemala ha visto un incremento en el uso de las TIC. (Centro de Investigaciones Económicas Nacionales, 2015, p. 3)

A partir de la liberación comercial del acceso a Internet en Guatemala, el uso de este espacio cibernético fue creciendo paulatinamente en el país. Según los resultados sobre la población de más de 7 años que declaró el uso de celular, computadora y/o internet en el censo de población de Guatemala realizado en 2018, señala que solo un 29% de la población guatemalteca censada usa el servicio de internet. De ese 29% que equivale a 3,673,979 habitantes, la mayoría se concentra en el área metropolitana con 1,439,440 personas como se muestra en la **¡Error! No se encuentra el origen de la referencia.**, la cual también refleja q ue existe una brecha significativa entre la población de áreas urbanas y rurales que tienen acceso a internet (INE, 2019).

Figura 2

Número de personas que usan el servicio de internet por departamento en Guatemala



Nota: Adaptado de los datos de la Población de 7 años o más por uso de Internet datos a nivel nacional, INE, 2018. XII Censo Nacional de Población y VII de Vivienda.

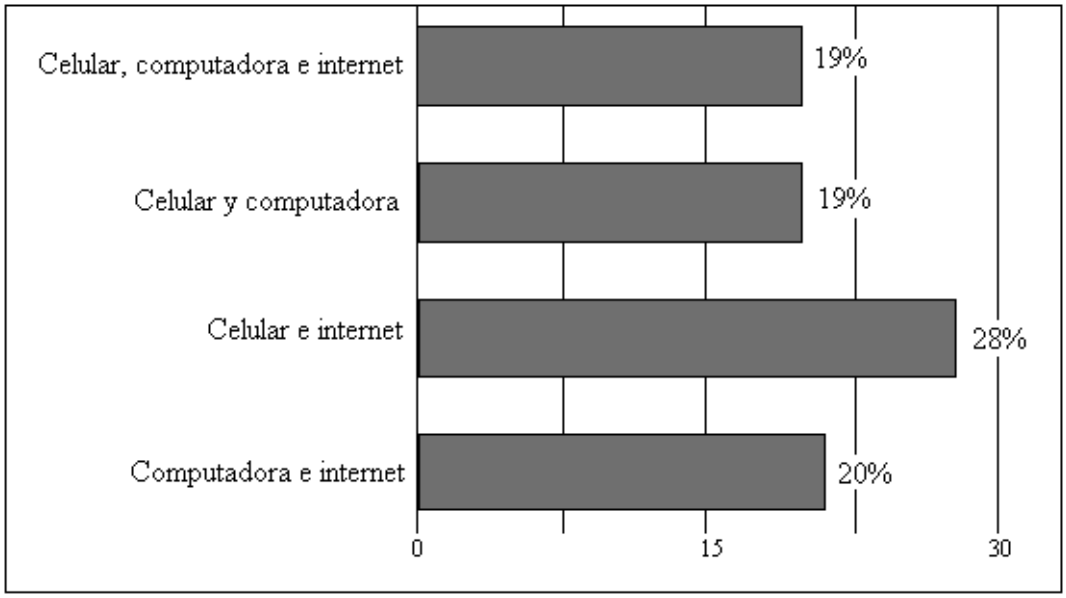
Para el ingeniero Luis Furlán, la cifra de personas que tienen acceso a internet es sumamente baja. Además, señala que el gobierno no tiene una agenda digital (en calidad de política pública) que favorezca corregir esas deficiencias. Por otro lado, se encuentran los proveedores de servicios de internet, los cuales proveen uno de los servicios más caros en todo el hemisferio occidental al respecto, lo cual ocasiona que mucha gente no puede tener acceso al servicio de internet. También, existen otros aspectos que deben considerarse, como el nivel de analfabetismo en Guatemala, y la topografía del país que, técnicamente, es un desafío más para alcanzar el máximo de usuarios. (L.R. Furlán, comunicación personal, 14 de octubre de 2020)

Como se puede evidenciar, Internet se ha convertido en una necesidad para el desarrollo de la población guatemalteca, fue por ello por lo que Guatemala se unió a la Alianza para una Internet Asequible en junio de 2018 con el objetivo de contribuir en el desarrollo y la implementación de políticas públicas y regulatorias diseñadas para reducir el costo del acceso a la internet y de esa manera hacer más asequible el acceso a la internet para toda la población guatemalteca, mediante la unión del sector público, privado y la sociedad civil en el país; creando un ambiente de equidad e inclusión digital de toda la población de Guatemala (Internet Governance Forum, 2017).

Respecto al uso de las TIC la Figura 3 muestra que, en el Censo Nacional el 28% de la población declaró tener acceso a un teléfono celular con internet, sobre un 20% que tiene acceso a una computadora con internet.

Figura 3

Porcentaje de personas que utilizan las TIC a nivel nacional según el censo de población de 2018



Nota: Adaptado de los datos sobre el uso de las TIC e internet a nivel nacional, INE, 2018.

Las facilidades tecnológicas proveídas por la introducción de teléfonos de la denominada gama media y alta de accesibilidad (es decir aquellos aparatos telefónicos que cuentan con la integración de elementos tecnológicos para facilitar el acceso a servicios web, inalámbricos y otros), generó que la penetración de internet aumentase en el país de manera acelerada en los últimos años; a pesar de lo cual, las estadísticas aún reflejan un bajo índice de penetración. Según el Índice de Competitividad Global 2019 elaborado por el Foro Económico Mundial (WEF), se ubica a Guatemala en el puesto 98 de 141 países, con una puntuación de 53.5, en donde las áreas peores calificadas para Guatemala son: Capacidad de innovación (31.5), adopción de las TIC (37.7), institucionalidad (42.4), mercado laboral (50.9) e infraestructura (55.9) (Forbes Staff, 2019).

3.2 Ciberseguridad

El creciente aumento en el uso de Internet como se detalló en el apartado anterior, así como la facilidad de comunicación entre pares, el acceso web y los otros servicios que provee Internet, ha ocasionado que se subestimen los peligros a los que se ven expuestos los usuarios de internet al navegar en el ciberespacio, en ese sentido la seguridad de la información toma cada día una mayor importancia dentro de la agenda mundial. En virtud de lo anterior y mediante la resolución 181 de la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones, se aprobó la definición de ciberseguridad adoptada en la Recomendación UIT-T X.1205 de la Unión Internacional de Telecomunicaciones, la cual establece que:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías; que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. (UIT, 2010)

Para el establecimiento de un espacio cibernético seguro, se requiere la implementación de estrategias de ciberseguridad con fin de dirigir, controlar y gestionar el sistema de seguridad cibernética; no obstante, el Banco Mundial en los indicadores del desarrollo mundial denominado: La sociedad de la información, estimó un promedio de 1,964.1 de servidores de Internet seguros por cada millón de personas en América Latina y el Caribe para 2020 (World Bank Group, 2021), lo cual denota un espacio cibernético que no cuenta con una infraestructura completamente segura en comparación al número de usuarios de Internet.

3.2.1 Ciberseguridad en América Latina y el Caribe

América Latina y el Caribe comparten rasgos económicos, políticos y culturales similares, por lo que cuando se trata de seguridad cibernética, los gobiernos de la región se han visto en la necesidad de tomar las medidas necesarias para proteger la infraestructura

crítica de su país, promoviendo leyes, políticas y estrategias sobre ciberseguridad, y fortaleciendo de esa manera la cooperación internacional en la región; a este respecto, la Organización de Estados Americanos constituye el punto de apoyo para el combate, mitigación y prevención de los delitos cibernéticos en la región latinoamericana y del caribe; la OEA ha estado comprometida principalmente con temas de seguridad y delincuencia cibernética, fomentando y apoyando la labor de sus Estados Miembros para fortalecer la infraestructura crítica de la región contra la delincuencia o incidentes cibernéticos (Banco Interamericano de Desarrollo, 2016).

Tras la adopción por unanimidad de la Estrategia Interamericana Integral de Seguridad Cibernética en 2004, los Estados Miembros de la OEA reconocieron que combatir los delitos cibernéticos y fortalecer la resiliencia cibernética eran cuestiones imperativas en la agenda de la Organización, dentro del contexto de la seguridad nacional e internacional, por lo cual se comprometieron a tomar las medidas pertinentes para promover el intercambio de estrategias, técnicas y políticas para mitigar los riesgos cibernéticos. Al priorizar el alcance de la resiliencia cibernética y promover una cooperación efectiva entre los interesados en la ciberseguridad, la OEA y otros actores regionales e internacionales desempeñan un rol fundamental en el contexto dentro del cual se han adaptado iniciativas de desarrollo de capacidad a las necesidades de cada país (OEA, 2014, p. 4).

Es menester mencionar que la demanda en el uso de Internet y las TIC por parte de la población latinoamericana y caribeña, también generó un incremento en las actividades delictivas en el entorno cibernético; de hecho, el reporte de la OEA de 2013, titulado Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos, señala que en 2012 la región latinoamericana experimentó un incremento de incidentes cibernéticos de entre el 8% y el 40%, principalmente de ataques hacktivistas, realizados por individuos que utilizan las TIC para irrumpir sistemas informáticos y los cuales van dirigidos, en su mayoría, contra entidades gubernamentales e instituciones financieras para dar a conocer su postura política y social. Así mismo, refiere que “en

América Latina, dos factores bloquean comúnmente los esfuerzos: la falta de recursos dedicados al fortalecimiento de la capacidad en seguridad cibernética y la escasez de conocimientos especializados y experiencia práctica para la implementación de políticas o capacidad técnicas" (OEA, 2013, p. 24).

Por su parte, el informe de la OEA (2014), sobre las Tendencias de Seguridad Cibernética en América Latina y el Caribe, revela que en 2013 muchos países de la región lograron importantes avances en la elaboración de sus políticas y marcos jurídicos, y en el desarrollo de una estrategia técnica que les facilite fortalecer la resiliencia cibernética y proteger las infraestructuras críticas. En este orden de ideas, los informes de Ciberseguridad del BID; el primero presentado en el año 2016 y titulado: Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?; y la actualización presentada en 2020 denominada: Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe, permitieron la evaluación de los niveles de madurez frente a los delitos cibernéticos, por parte de los gobiernos de América Latina y el Caribe.

Estos niveles de madurez se basaron en las 5 dimensiones presentadas en la figura 4, dicho estudio fue desarrollado por el Centro Global de Capacidad en Seguridad Cibernética de la Universidad de Oxford con la finalidad de ofrecer una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país, y de esa manera determinar el fortalecimiento de la resiliencia cibernética de cada estado latinoamericano y caribeño (Banco Interamericano de Desarrollo, 2020).

Figura 4

Modelo de madurez de la capacidad de ciberseguridad

Nota. La figura representa las cinco dimensiones en las cuales se desarrolló el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones. Fuente: Banco Interamericano de Desarrollo (2020, p. 44).

Las dimensiones del Modelo de Madurez de la Capacidad de Ciberseguridad permitieron realizar un perfil de cada país, en donde se evaluaron las acciones y esfuerzos de cada estado por crear mecanismos de respuesta, mitigación y prevención ante incidentes cibernéticos. Dicho modelo se presentó como un análisis comparativo de los años 2016 y 2020, en donde los datos de las cinco dimensiones estudiadas y analizadas dan como resultado una evaluación de la resiliencia cibernética en la región de Latinoamérica y el Caribe.

Después de las consideraciones anteriores, se infiere que la mayoría de los gobiernos en América Latina y el Caribe carecían de estrategias de seguridad cibernéticas, legislaciones o un plan de protección nacional para 2011; no obstante, desde el informe de la OEA en 2013 hasta el último informe presentado en 2020 por el BID, se evidencia que los gobiernos han adoptado planes de acción para mitigar y responder a ataques potenciales mediante la

modernización y el fortalecimiento de sus marcos jurídicos y legales por medio de sus leyes nacionales.

Los países que ya han presentado una Estrategia Nacional de Seguridad Cibernética y aquellos que hasta 2020 declararon que están trabajando en las mismas, se presentan en la Tabla 2. Los resultados indican que catorce países en América ya cuentan con una Estrategia Nacional de Seguridad Cibernética, siete de ellos están trabajando actualmente en el desarrollo de su Estrategia y solo trece aún no cuentan o están desarrollando una Estrategia. Además, debe acotarse que diez países de América ya han ratificado el Convenio sobre ciberdelincuencia de 2001 y dos tienen una invitación vigente para firmar y ratificar dicho Convenio, uno de ellos es Guatemala. Esto refleja el interés de más del 50% de los gobiernos que han manifestado su interés por desarrollar e implementar los mecanismos necesarios para proteger a su población de la ciberdelincuencia, así como reforzar su resiliencia cibernética.

Tabla 2

Países de América que han presentado una Estrategia de Seguridad Cibernética y ratificado del Convenio sobre Ciberdelincuencia

País	*Estrategia de Seguridad Cibernética		Convención sobre Ciberdelincuencia	
	Estado	Fecha	Estado	Fecha
Antigua y Barbuda				
Argentina	Presentada	2019	Ratificó	5/06/2018
Bahamas				
Barbados	En desarrollo			
Belice	En desarrollo			
Bolivia				
Brasil	Presentada	2018	Invitado	
Canadá	Presentada	2018	Ratificó	8/07/2015
Chile	Presentada	2017	Ratificó	20/04/2017
Colombia	Presentada	2011 y 2016	Ratificó	16/03/2020

Costa Rica	Presentada	2017	Ratificó	22/09/2017
Cuba				
Dominica				
Ecuador	En desarrollo			
El Salvador				
Estados Unidos	Presentada	2018	Ratificó	29/09/2006
Granada	En desarrollo			
Guatemala	Presentada	2018	Invitado	
Guyana	En desarrollo			
Haití				
Honduras				
Jamaica	Presentada	2015		
México	Presentada	2017		
Nicaragua				
Panamá	Presentada	2013	Ratificó	5/03/2014
Paraguay	Presentada	2017	Ratificó	30/07/2018
Perú	En desarrollo		Ratificó	26/08/2019
República Dominicana	Presentada	2018	Ratificó	7/02/2013
San Cristóbal y Nieves				
San Vicente y las Granadinas				
Santa Lucía				
Surinam	En desarrollo			
Trinidad y Tobago	Presentada	2013		
Uruguay				

Nota. Elaboración propia basada en los datos del cuadro de firmas y ratificaciones del Tratado 185 Convenio sobre el delito cibernético del Consejo de Europa, disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

* Los datos utilizados en este apartado fueron tomados del Informe del BID (2020)

3.2.2 La seguridad cibernética en Guatemala

Como se pudo evidenciar en los apartados anteriores, la facilidad de comunicación entre pares, el acceso web y los otros servicios que provee internet, ha generado un incremento en el uso de Internet y las TIC en Guatemala; no obstante, esa conectividad exige la previsión de situaciones delictivas debido a que varios usuarios de este tipo de servicio subestiman los peligros a los que se ven expuestos al navegar en el ciberespacio.

Ante dicha situación, el Estado de Guatemala debe garantizar el bienestar de la población de acuerdo con lo establecido en la Constitución Política de la República de Guatemala, por lo que el fortalecimiento de la resiliencia cibernética en el país ha constituido el punto clave para la mitigación y prevención de los incidentes cibernéticos en el país. En esta línea y considerando que Guatemala cuenta con factores positivos frente a los mecanismos de respuesta ante incidentes cibernéticos, el informe sobre Ciberseguridad del BID señala que:

> Guatemala mostró una fuerte capacidad diplomática cibernética en 2012, al presidir el Comité Interamericano contra el Terrorismo de la OEA. El país lideró una declaración sobre el fortalecimiento de la seguridad cibernética en las américas, que dio lugar a su adopción unánime y elevó el reconocimiento de la seguridad y la resiliencia de la infraestructura de información crítica, especialmente para las instituciones esenciales, para los sectores de seguridad nacional, como comunicaciones, energía, finanzas y transporte. (Banco Interamericano de Desarrollo, 2016, p. 33)

Los primeros esfuerzos en formar parte del único tratado internacional sobre ciberdelincuencia fueron evidenciados por el gobierno de Guatemala en 2016, cuando se mostró el interés del estado de Guatemala ante el Consejo de Europa de adherirse al Convenio sobre ciberdelincuencia. A raíz de ello, en la 1374ª sesión realizada el 22 de abril de 2020 los diputados del Comité de ministros del Consejo de Europa invitaron a Guatemala a adherirse

al Convenio sobre ciberdelincuencia lo cual constituye un avance para el país en dicha materia, esta invitación tiene vigencia de cinco años a partir de su adopción y se encuentra válida para Guatemala hasta el 23 de abril del año 2025 (Treaty Office, 2020).

Con la solicitud de la adhesión al Convenio sobre Ciberdelincuencia, Guatemala ha trabajado en una serie de acciones tales como la creación de una Estrategia de Seguridad Cibernética, el establecimiento de un CERT nacional, así como el desarrollo de iniciativas de ley para dar vida a una ley sobre delitos cibernéticos como se detalla en la Estrategia Nacional de Seguridad Cibernética, presentada en 2018 por el gobierno de Guatemala.

3.2.2.1 Marco institucional y legal en materia de seguridad cibernética en Guatemala

Con el aumento en el uso de las TIC, el mundo cibernético juega un papel importante en la seguridad y desarrollo del país haciendo necesario el fortalecimiento de los vínculos de cooperación y coordinación entre las instituciones nacionales e internacionales; en Guatemala es el IV Viceministerio de Tecnología de la Información y las Comunicaciones del Ministerio de Gobernación quien se encarga de los planes de mitigación, prevención y combate, en conjunto con las instituciones que integran el Consejo Nacional de Seguridad, de acuerdo con lo establecido en el artículo 10 del decreto 18-2008, Ley Marco del Sistema Nacional de Seguridad, dentro de las funciones del Consejo Nacional de Seguridad está: el definir las políticas y estrategias específicas en materia de seguridad exterior, seguridad interior e inteligencia, así como definir la Política Nacional de Seguridad.

En lo que corresponde al el IV Viceministerio de Tecnología de la Información y las Comunicaciones del Ministerio de Gobernación, el artículo 9 del Acuerdo Gubernativo 635-2007, Reglamento Orgánico del Ministerio de Gobernación, el cual fue reformado por el artículo 3 del Acuerdo Gubernativo Número 313- 2012 de fecha 3 de diciembre del año 2012, dentro de las funciones del Cuarto Viceministerio de Gobernación, correspondientes a las TIC en el país, se encuentran: el promover el uso de las tecnologías de la información y la comunicación entre los ciudadanos, las empresas, el gobierno y demás instancias nacionales,

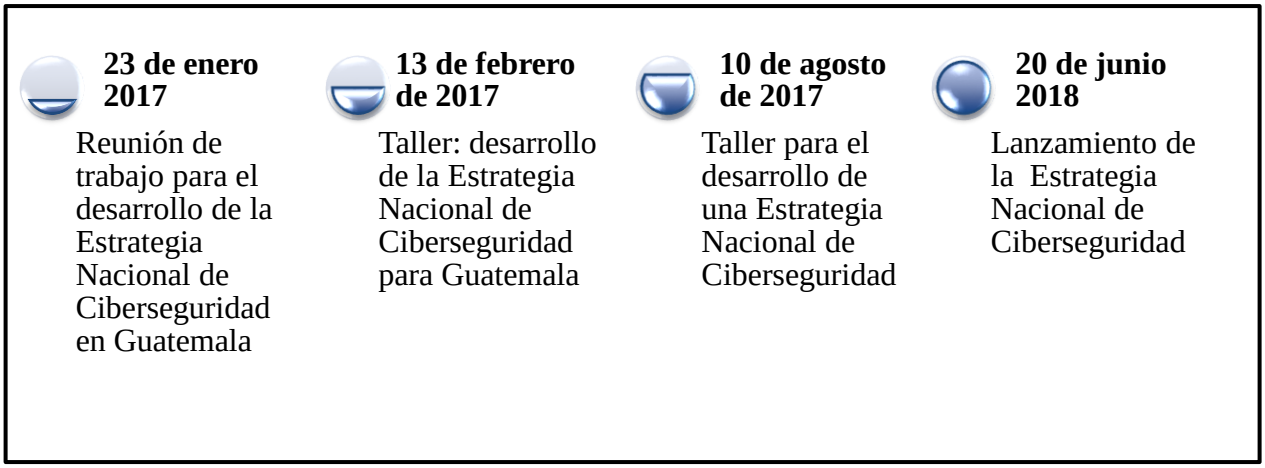
como soporte del desarrollo de la seguridad y transparencia, apoyando también las gestiones en materia de Gobierno Electrónico; además de gestionar, en coordinación con las Unidades del Ministerio de Gobernación, la cooperación internacional en apoyo al desarrollo de las TIC.

Fue por ello por lo que el IV Viceministerio de Tecnología de la Información y las Comunicaciones del Ministerio de Gobernación en conjunto con la Organización de Estados Americanos, establecieron los planes de trabajo para dar vida a lo que es la Estrategia Nacional de Seguridad de Guatemala.

En lo que refiere a la estrategia de seguridad cibernética, el gobierno de Guatemala a través del IV Viceministerio de Tecnologías de Información del Ministerio de Gobernación de Guatemala y con el apoyo del Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos inicio el desarrollo de la Estrategia Nacional de Ciberseguridad de Guatemala, en enero de 2017, mediante la segunda reunión de trabajo realizada en Antigua Guatemala; más adelante en febrero y agosto del mismo año se realizaron dos talleres, como se muestra en la figura 5, en donde se pretendió recopilar información sobre el estado de la seguridad cibernética en el territorio guatemalteco, y de esa manera formular propuestas y acciones para dar vida a la primera Estrategia Nacional de Seguridad Cibernética en Guatemala. (Oficina de la OEA en Guatemala, 2018)

Figura 5

Línea del tiempo del desarrollo de la Estrategia Nacional de Ciberseguridad en Guatemala



Nota. Elaboración propia basada en los eventos realizados por la Oficina de la OEA en Guatemala, disponible en http://oea.org/es/acerca/offices_events.asp?sCode=GUA

En los talleres citados anteriormente, para el desarrollo de la Estrategia Nacional de Ciberseguridad, el Ministerio de Gobernación de Guatemala con el apoyo de la Organización de los Estados Americanos a través del CICTE y el Concejo de Europa realizaron una misión consultiva sobre legislación en delitos cibernéticos y pruebas electrónicas en el marco de la Estrategia Nacional de Ciberseguridad, con el objetivo de poder realizar un proceso de revisión de la legislación guatemalteca y preparar un borrador de legislación en materia de delito cibernético, de conformidad con las normas internacionales mencionadas en el Convenio sobre Ciberdelincuencia, quedando como objetivos de mediano y largo plazo que Guatemala pueda aprobar una legislación en materia de delitos cibernéticos adecuada, y que permita su adhesión a dicho Convenio. (Oficina de la OEA en Guatemala, 2018)

Finalmente, en junio del año 2018 se presenta oficialmente por el Gobierno de Guatemala la Estrategia Nacional de Ciberseguridad. El objetivo principal de la Estrategia Nacional de Seguridad Cibernética fue “fortalecer las capacidades de la Nación, creando el

ambiente y las condiciones necesarias para asegurar la participación, el desarrollo y el ejercicio de los derechos de las personas en el ciberespacio" (Ministerio de Gobernación, 2018, p. 32). Esta estrategia se basa en cuatro pilares:

- Marcos Legales,
- Educación,
- Cultura y Sociedad, y
- Tecnologías de la información.

El marco legal que se menciona en la Estrategia Nacional De Seguridad Cibernética de Guatemala, se centra en "adecuar el marco legal guatemalteco con un enfoque de prevención y manejo de riesgos cibernéticos para fortalecer la seguridad cibernética" (Ministerio de Gobernación, 2018, p. 36), debido a que los delitos cibernéticos no se encuentran tipificados como tal en la legislación nacional vigente, de hecho desde 2009, en Guatemala se han promovido iniciativas de ley que buscan combatir los delitos cibernéticos, para dar cumplimiento al establecimiento de un marco legal y jurídico, lo cual es uno de los objetivos del Convenio sobre ciberdelincuencia, siendo este último el marco internacional de referencia para la creación de legislaciones y protocolos que ayuden a mitigar y prevenir los delitos cibernéticos.

Las primeras propuestas de ley presentadas ante el pleno del Congreso de la República de Guatemala fueron: 1. La iniciativa No. 4054 titulada: Iniciativa que dispone aprobar Ley Contra el Cibercrimen, y 2. La iniciativa No. 4055 denominada: Iniciativa que dispone aprobar Ley de Delitos Informáticos, ambas presentadas el 18 de agosto de 2009 ante el pleno del congreso, y las cuales pretendían establecer los lineamientos para establecer un marco legal acorde a los estándares internacionales en materia de seguridad cibernética. La iniciativa No. 4054 llegó a ser presentada ante el pleno del congreso en agosto del 2009, pero no recibió ningún dictamen; sin embargo, la iniciativa No. 4055 recibió dictamen favorable en octubre de 2011, tras ser presentada al pleno del congreso en 2009, llagando a segundo debate en el año 2016; no obstante, ninguna de las dos iniciativas fue aprobada por

el pleno del Congreso y quedaron archivadas (Congreso de la República de Guatemala, 2016).

Posterior a las iniciativas de ley anteriormente citadas, en marzo de 2017, se presentó una nueva iniciativa de ley identificada como Iniciativa No. 5254 Ley sobre la Ciberdelincuencia, que no obtuvo seguimiento por parte de la Comisión de Gobernación (Congreso de la República de Guatemala, 2017).

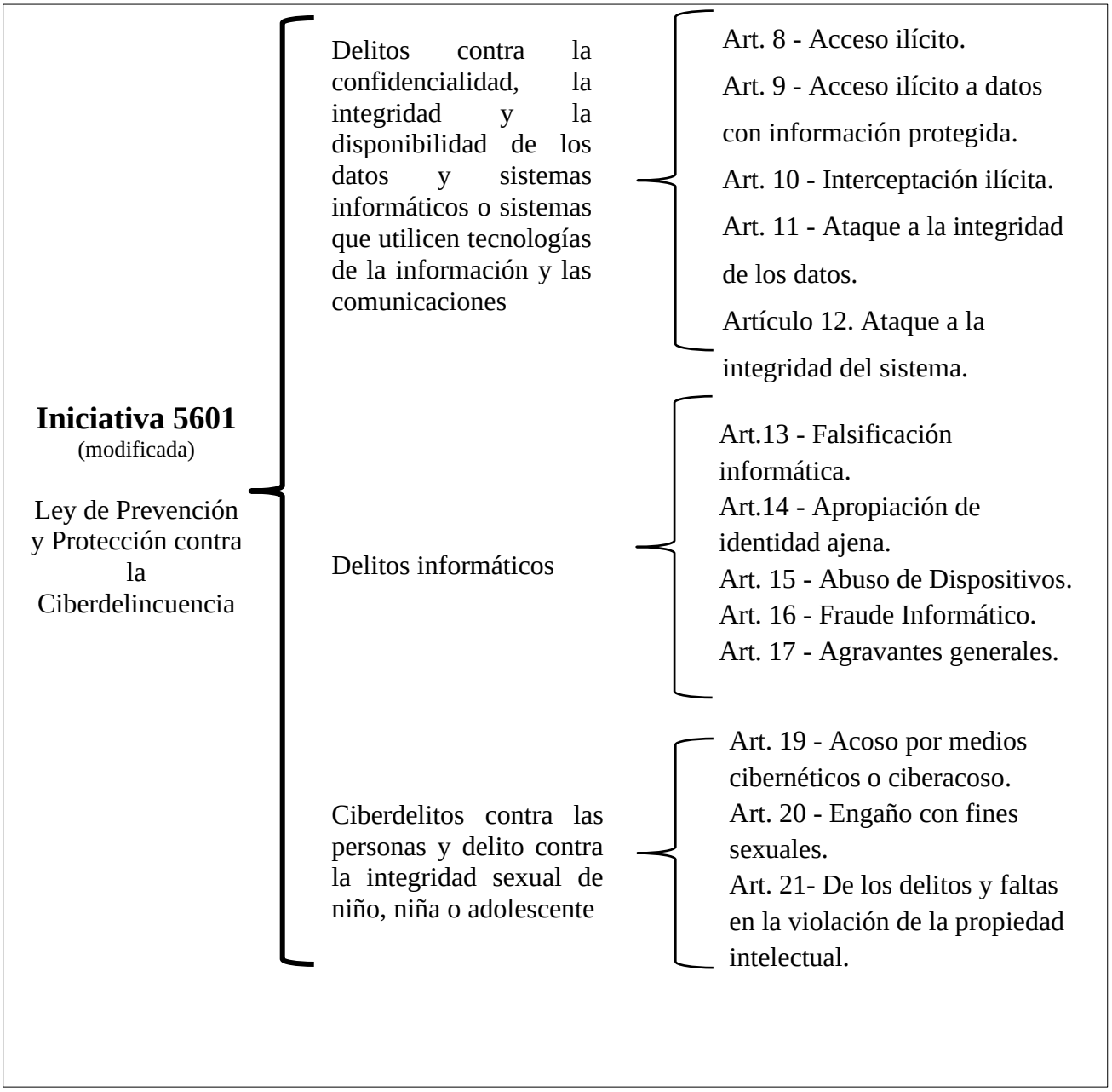
La última iniciativa de ley en materia de delitos cibernéticos hasta el año 2020 fue la número 5601, denominada: Ley de Prevención y Protección contra la Ciberdelincuencia, presentada por el diputado José Rodrigo Valladares Guillén el 6 de agosto de 2019; la citada iniciativa fue conocida por el pleno del Congreso el 17 de septiembre de 2019, y ante la necesidad de contar con una legislación específica para contemplar los procesos específicos en la recopilación de las evidencias y pruebas, así como el apoyo institucional que se debe de prestar en las actividades delictivas que se desarrollan y en donde se utilizan las tecnologías de la información y comunicación, y sus dispositivos, el 18 de noviembre del año 2019, la Comisión de Asuntos de Seguridad Nacional, emitió el dictamen favorable con modificaciones al contenido de la iniciativa 5601, que disponía aprobar la Ley de prevención y protección contra la ciberdelincuencia. (Comisión de Asuntos de Seguridad Nacional, 2019)

Esta iniciativa de ley pretendía proveer de garantías al usuario de internet al imponer penas a los delitos cibernéticos; esta fue elaborada con base al Convenio sobre ciberdelincuencia, tomando en consideración que aunque Guatemala aún no es parte de ese convenio internacional deberá adherirse a este en un futuro, a fin trabajar junto con la comunidad internacional en la mitigación, prevención y combate de los delitos cibernéticos, debido a la transaccionalidad de la ciberdelincuencia; esto proveerá las garantías a necesarias para los usuarios de internet en el país. (Iniciativa de ley 5601, de 17 de diciembre de 2019)

La iniciativa 5601 en consonancia con lo propuesto en el capítulo I del Convenio sobre Ciberdelincuencia; el cual ofrece las definiciones conceptuales sobre sistema informático, datos informáticos, proveedor de servicios y datos relativos al tráfico que son elementos esenciales para la adecuada tipificación de los delitos cibernéticos, propone una serie de veinticinco definiciones de elementos conceptuales, que fueron ampliados a veintisiete en el dictamen favorable emitido por la Comisión de Asuntos de Seguridad Nacional, los cuales tuvieron como fin la comprensión de la Iniciativa de Ley de prevención y protección contra la ciberdelincuencia en Guatemala. Adicional a la terminología, estipuló una serie de delitos que se pretendía establecer en la legislación guatemalteca como se contempla en la figura 6.

Figura 6

Delitos que se pretenden incorporar a la legislación penal guatemalteca



Nota. Elaboración propia basada en la Iniciativa 5601, 2019.

La estructura capitular de la iniciativa de ley 5601, fue adaptada a la estructura normativa del Convenio. Por consiguiente, la **¡Error! No se encuentra el origen de la r eferencia.** muestra una comparación del contenido de ambos instrumentos con el objeto de identificar sus similitudes.

Tabla 3

Cuadro comparativo del contenido del Convenio sobre ciberdelincuencia y la Iniciativa 5601 - Ley de prevención y protección contra la ciberdelincuencia

Convenio sobre ciberdelincuencia	**Iniciativa de ley 5601 (Modificado)**
Criterio de comparación: Terminología	
Para efectos del convenio, se establecieron cuatro términos relativos a los sistemas y datos informáticos: a. Sistema informático; b. Datos informáticos; c. Proveedor de servicios; y d. Datos relativos al tráfico	Para efectos de la Ley de prevención y protección sobre la Ciberdelincuencia, iniciativa 5601, en el artículo 7 se propuso una serie de veintisiete elementos conceptuales, con base en la terminología citada en el Convenio sobre Ciberdelincuencia y mediante el cual se pretendió dar cumplimiento a los lineamientos estipulados allí.
Criterio de comparación: delitos	
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos Dentro de esta categoría se establecen cuatro delitos: 1. Acceso ilícito 2. Intercepción ilícita 3. Ataques a la integridad de los datos 4. Abuso a los dispositivos	**Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos o sistemas que utilicen Tecnologías de la Información y la Comunicación** La iniciativa de ley además de incluir los tres primeros delitos estipulados en el Convenio agrega dos más correspondientes a la coyuntura del país: 1. Acceso Ilícito a Datos con Información Protegida, y 2. Ataque a la Integridad del Sistema.
Delitos informáticos Hace referencia a los dos delitos de Falsificación Informática y Fraude Informático	**Delitos informáticos** Hace referencia a los dos delitos de Falsificación Informática y Fraude Informático

Delitos relacionados con el contenido Se refiere a los delitos relacionados con la Pornografía Infantil **Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines** Hace referencia a las marcas, patentes, obras literarias y artísticas, entre otros.	**Ciberdelitos contra personas y delito contra la integridad sexual del niño, niña y adolescente** La iniciativa 5601unifica las dos categorizaciones del convenio, y los desglosa los delitos relacionados con el contenido de la siguiente manera: Acoso por Medios, Cibernéticos o Ciberacoso, Engaño con Fines Sexuales, de los delitos y faltas en la violación de la propiedad intelectual.
Convenio sobre ciberdelincuencia	**Iniciativa de ley 5601 (Modificado)**
Criterio de comparación: Formas de responsabilidad y sanción	
Otras formas de responsabilidad y sanción Hace referencia a las siguientes formas de responsabilidad y sanción: 1. Tentativa y Complicidad, 2. Responsabilidad de las Personas Jurídicas, 3. Sanciones y Medidas.	**Responsabilidad y penas accesorias de las personas individuales y jurídicas** Los artículos relacionados con esta categoría dentro de la Incitativa de ley son: el art.4 que trata sobre la responsabilidad de las personas jurídicas y sus representantes; art. 22 sobre la Responsabilidad Civil de las Personas Individuales y Penas Accesorias; y art. 23 sobre la Responsabilidad Civil de las Personas Jurídicas y Penas Accesorias.
Criterio de comparación: Medidas Cautelares, Procesales y Procedimentales	
Respecto a esta temática, en el Convenio se categoriza de la siguiente manera: 1. Ámbito de aplicación de las disposiciones de procedimiento 1.1 Condiciones y salvaguardias 2. Conservación rápida de datos informáticos almacenados 2.1 Conservación y revelación parcial rápidas relativos al tráfico 3. Orden de presentación, que incluye:	En lo que respecta a la iniciativa, los que corresponde al ámbito de aplicación se encuentra en el artículo 3 - Ámbito territorial y personal de aplicación; y artículo 26- Ámbito de aplicación de las disposiciones de procedimiento. Lo que respecta a esta categorización se encuentra estipulado en el art. 27 Aseguramiento de datos; y art. 37 Reglamento para el Aseguramiento de Datos de la Información, Cadena de Custodia y otras disposiciones. Estipulado en el art. 28 Orden de Envío de Credenciales y Datos; art. 29 Registro y secuestro

1. Registro y confiscación de datos informáticos almacenados 2. Obtención en tiempo real de datos informáticos 3. Intercepción de datos relativos al contenido 4. Jurisdicción	de medios digitales o electrónicos; y art. 30 Interceptaciones.

Convenio sobre ciberdelincuencia	**Iniciativa de ley 5601 (Modificado)**
Criterio de comparación: Cooperación Internacional	
En términos generales la asistencia mutua y cooperación internacional es importante para hacer frente a esta problemática, por lo que se presentan una seria de disposiciones que deberían ser adaptadas a las legislaciones nacionales: 1. Sobre la cooperación internacionala, lo referente a la extradición 2. Sobre la asistencia mutua: procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables	El artículo 31 de esta iniciativa de ley hace referencia a la cooperación en materia penal y procesal penal y el artículo 35 a la Cooperación en Materia de extradición.
Criterio de comparación: Asistencia Mutua	
3. Asistencia mutua en materia de medidas provisionales. Conservación rápida de datos informáticos almacenados b. Revelación rápida de datos conservados 4. Asistencia mutua en relación con los poderes de investigación. Asistencia mutua en relación con el acceso a datos almacenados. Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público 5. Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico 6. Asistencia mutua en relación con la intercepción de datos relativos al contenido	Respecto a la asistencia mutua con relación a la obtención de datos a tiempo real, el artículo 34 refiere el establecimiento de una Red internacional de asistencia mutua contra delitos informáticos (RED 24/7 Guatemala), la cual debe ser creada por el MINGOB, e integrada a través de redes a las que Guatemala se adhiera o forme parte; la que se denominará Red internacional de asistencia mutua contra delitos informáticos o RED 24/7 Guatemala

Criterio de comparación: Red 24/7	
Estipula que cada parte designara un punto de contacto localizable las 24 horas del día, los siete días de la semana con el fin de garantizar una asistencia inmediata para las investigaciones relativas a los delitos cibernético.	Artículo 34. RED 24/7 Guatemala, punto de contacto localizable las veinticuatro (24) horas del día, siete (7) días a la semana para de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con los indicios de los delitos cibernéticos.

Nota. Elaboración propia con base en lo estipulado en el Convenio sobre ciberdelincuencia y la iniciativa de ley 5601, denominada: Ley de Prevención y Protección contra la Ciberdelincuencia

En lo que corresponde a la RED 24/7 Guatemala que se propone en la iniciativa 5601, se pretende que sea el punto de contacto principal que garantice la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con los indicios de los delitos vinculados a sistemas y datos informáticos. Cabe mencionar que, en Guatemala, ya existen algunos grupos similares tanto públicos como privados, lo cuales son los denominados Equipos de Respuestas ante Incidentes CERT (o CSIRT), los cuales están conformados por expertos en temas de seguridad informática y funcionarios gubernamentales de diversas instituciones, quienes tienen la tarea de implementar protocolos que permitan dar respuesta a incidentes que se realicen en el ciberespacio.

Estos equipos de respuesta ante incidentes cibernéticos iniciaron a principio de los años 90 en el continente americano con la finalidad de responder y mitigar los actos terroristas ocurridos en la región. Posteriormente, la ciberdelincuencia empezó a formar parte de este proceso, ya no era prever situaciones de riesgo institucionales, sino preservar la seguridad pública en el entorno virtual. A nivel regional la Asamblea General de la OEA consideró que los Estados Miembros de la OEA deberían de crear un CSIRT o CERT nacional para dar respuesta a los incidentes Cibernéticos. Es por ello por lo que, en Guatemala, desde el año 2006, se han realizado esfuerzos por conformar un CSIRT o CERT nacional.

El primer Equipo de Respuestas ante Incidentes Cibernéticos en Guatemala fue el Centro de Respuestas para Incidentes de Seguridad Informática (CSIRT, en inglés) creado por el Ingeniero Ronald Morales en 2006 y el cual tenía como finalidad proteger los sistemas de información del Gobierno; dicho centro pretendía operar mediante el amparo de la iniciativa 4055 de ley denominada: Ley de Delitos Informáticos, de la cual el ingeniero Ronald Morales fue parte del equipo profesional en temas de seguridad de la información, que trabajó en ella.

La iniciativa 4055 recibió dictamen favorable por el pleno del Congreso de la República de Guatemala en 2011, pero al no continuar con el desarrollo de la ley, eventualmente el CSIRT que estaba operando ad hoc bajo la gestión del Ministerio de la Defensa dejó de funcionar. Posterior a ello, el Ministerio de Gobernación tomo el cargo del Centro de Respuestas a Incidentes Cibernéticos (GT-CERT) el cual fue creado en 2018, como parte de la Estrategia Nacional de Ciberseguridad. Es importante mencionar que la iniciativa de ley 5601 que dispone aprobar Ley de prevención y protección contra la ciberdelincuencia, establece dos tipos de CIRT, uno de ciberseguridad y el otro de ciberdefensa: el primero estaría a cargo del Ministerio de Gobernación y el segundo a cargo del Ministerio de la Defensa, ambos deberán trabajar en conjunto con sus dependencias y rendir cuentas al Consejo Nacional de Seguridad; sin embargo, se pretende que sea el CSIRT-GT, de ciberseguridad, a cargo del Ministerio de Gobernación el que tendrá funciones como CSIRT-GT de gobierno.

CAPÍTULO IV

5. Análisis prospectivo de la seguridad Cibernética en Guatemala

5.1 Análisis FODA de la Seguridad cibernética en Guatemala

En este apartado se realizó el análisis e interpretación de los datos obtenidos en el trabajo de investigación, en el cual fue utilizada como instrumento para la recolección de datos, una guía de entrevista, mediante la cual se pretendió conocer la opinión sobre la situación del país frente a los delitos cibernéticos de diferentes especialistas en el área de las Tecnologías de la Información y Comunicación, así como la seguridad cibernética en Guatemala. Con base a las entrevistas realizadas, se analizaron los resultados obtenidos, los cuales se presentan a continuación:

Fortalezas

Las fortalezas que fueron identificadas dentro del análisis de las entrevistas efectuadas presentan los aspectos positivos que deben mantenerse y deben permanecer para el fortalecimiento de la resiliencia cibernética en el país. El primer aspecto responde al acceso a Internet por parte de la población guatemalteca en los próximos años, la unión del Estado de Guatemala a la Alianza para una Internet Asequible tiene mucho potencial, principalmente en lo que corresponde a la concientización de la importancia del uso del internet en el país.

Respecto a la Seguridad Cibernética en el país, el sector financiero es uno de los sectores que tiene más reforzada la parte de ciberseguridad principalmente por el tipo de actividades financieras que realiza. En lo que respecta al sector público, Guatemala ya cuenta con algunas instituciones públicas como la Policía Nacional Civil (PNC), el Ministerio Público (MP), el Ministerio de Gobernación y el Ministerio de la Defensa Nacional, los cuales tienen conocimiento de la problemática y ya la están abordando. Cada uno cuenta con unidades y personal especializado, los cuales han recibido capacitación internacional y

trabajan en el área de ciberdelitos para mitigar el impacto que tiene la ciberdelincuencia en el país.

Dentro de las fortalezas identificadas, también se encuentran las herramientas en las que el Estado de Guatemala ha estado trabajando para prevenir, combatir y mitigar los delitos cibernéticos tales como el establecimiento de un Centro de Respuesta ante Incidentes Cibernéticos (GT-CERT), y la presentación de la Estrategia Nacional de Seguridad Cibernética, la cual constituye un elemento técnico bastante útil. Respecto a la legislación, como se evidenció en el capítulo III, Guatemala ya cuenta con una iniciativa de ley (5601) que busca prevenir y proteger al país de la ciberdelincuencia y la cual fue creada con base en el Convenio sobre Ciberdelincuencia, por lo que es bastante apropiada. Esta iniciativa de ley ya fue presentada ante el pleno del Congreso de la República de Guatemala, y cuenta con dictamen favorable por parte del legislativo lo que muestra un pequeño interés por parte del legislativo en aprobar, en cierto punto, una ley para combatir la ciberdelincuencia.

Para Guatemala, también existen otros elementos identificados como fortaleza en lo que respecta al fortalecimiento de su resiliencia cibernética, este constituye la futura adhesión al Convenio de Ciberdelincuencia, Guatemala recibió en abril de 2020 una invitación para participar como país número 65 en el Convenio sobre Ciberdelincuencia, lo cual constituye un paso importante en la prevención y mitigación de la ciberdelincuencia.

Todos los elementos mencionados con anterioridad representan las fortalezas del Estado de Guatemala en el proceso de fortalecer su resiliencia cibernética, es decir, se confirma que ya se está trabajando en la problemática.

Oportunidades

Las oportunidades identificadas en las entrevistas son factores que benefician al país en el combate, prevención y mitigación de los delitos cibernéticos. La primera oportunidad identificada se refiere al incremento del acceso a internet por parte de la población guatemalteca, la Alianza para una Internet Asequible ofrece un programa de divulgación y

concientización sobre la importancia del acceso a internet y el uso de esta herramienta por parte de toda la población, lo cual genera que cada vez más existan proyectos que tengan como objetivo proveer del servicio a la mayoría de la población latinoamericana, también genera un beneficio el hecho de que se declarara al Internet como derecho humano; esto también permite el desarrollo de proyectos que faciliten el acceso a Internet.

Otro de los factores identificados como oportunidad se refiere a la creación de medidas por parte del estado como, por ejemplo, la implementación de equipos preparados con tecnología de punta y equipos de respuesta que fortalezcan la defensa nacional en materia de ciberseguridad. Además del enriquecimiento del conocimiento, por medio de capacitaciones a los actores correspondientes por parte de organizaciones internacionales como lo es la OEA, quien ha apoyado en gran medida y es uno de los socios estratégicos para combatir los temas de ciberdelincuencia.

Por otro lado, la adhesión al Convenio sobre ciberdelincuencia es de suma importancia para el país debido a que la naturaleza transnacional de los delitos cibernéticos necesita que estos sean abordados a nivel internacional, por lo que la cooperación internacional se fortalece entre los países firmantes del Convenio.

Debilidades

Se identificaron varias debilidades que no permiten que el fortalecimiento de la resiliencia cibernética se ejecute de manera adecuada y acorde a la gravedad del problema que engloba la ciberdelincuencia en el país. Estas debilidades corresponden a todos los actores involucrados, las cuales deben de conocerse con el fin de trabajar en su disminución.

A continuación, se describirán más a fondo cada una de las debilidades identificadas, cabe mencionar que no se ve un esfuerzo integral por parte de las partes involucradas, un esfuerzo de país, lo cual genera un esfuerzo aislado en el reforzamiento de la resiliencia cibernética. Primero se debe tomar en cuenta el acceso a internet por parte de la población guatemalteca, lo cual constituye una debilidad inminente debido a que la penetración de

Internet en el país es relativamente baja, en comparación a otros países de la región, aunado a ello, el uso del servicio de internet en el país se ve afectado por otros factores como lo es topografía del país, el alto nivel de analfabetismo y el monopolio creado por los proveedores de internet junto con el alto precio del servicio. Así mismo, se pudo identificar la ausencia de una política pública y una agenda digital que favorezca la conectividad.

En lo que respecta a la seguridad cibernética, se ve un deficiente esfuerzo integral por parte de todos los actores involucrados para dar continuidad a las acciones en las que se han trabajado para prevenir y mitigar la ciberdelincuencia en el país, aunado a la incapacidad burocrática de mantener la actualidad y ejecutar las herramientas que ya se tienen. En efecto, Guatemala no posee una ley sobre ciberdelincuencia legalmente aprobada para prevenir y mitigar los delitos cibernéticos por lo que el proceso investigativo queda mermado y los delitos también quedan impunes, lo cual constituye una de las debilidades más graves sobre las que se encuentra el combate a la problemática en el país.

Otra de las debilidades que fueron identificadas en la entrevista realizada a los especialistas, frente a la magnitud del problema que constituye la ciberdelincuencia, denota la limitada educación y concientización sobre el uso de internet y los peligros que existen en el ciberespacio. También se considera como debilidad el hecho de que Guatemala no se ha adherido aún a los grandes esfuerzos internacionales sobre el tema como lo es el Convenio sobre ciberdelincuencia el cual constituye el único instrumento internacional vinculante en esta materia.

Amenazas

Es menester mencionar que las amenazas identificadas son factores que de alguna manera pueden presentarse a lo largo del fortalecimiento de la seguridad cibernética en el país, son factores externos e internos que deben considerarse para evitar consecuencias a mediano y largo plazo.

La primera amenaza que debe ser considerada, es que gran parte de la población guatemalteca no está consciente de los peligros tan grandes que acechan Internet, como lo es el robo de identidad e información de cuentas bancarias, esto repercute en los esfuerzos del gobierno por mitigar los delitos cibernéticos en el país. Otro de los factores que amenaza el fortalecimiento de la resiliencia cibernética constituye en el incremento de la delincuencia cibernética. Con la coyuntura de la pandemia del COVID19 en 2019, los delitos tradicionales están migrando a la utilización de TIC, y el tema de ciberdelitos va a ser tan grande que el país no está preparado cuando está problemática tenga dimensiones mayores.

También se identificaron amenazas internas como el panorama político en el Congreso de la República, sus prioridades ahorita no están enfocadas precisamente en la aprobación una ley sobre la ciberdelincuencia, lo cual genera un inminente retraso en los esfuerzos del gobierno por crear un marco de respuesta ante estos incidentes. Por su parte, se encuentran los cambios de Gobierno, ya que no se les da continuidad a los planes que ya se han establecido previamente, y esto también genera un retroceso en el fortalecimiento de la resiliencia cibernética.

Cada uno de los factores anteriormente mencionados, puede influir drásticamente en el fortalecimiento de la resiliencia cibernética en el país, por lo que es importante que los actores correspondientes analicen y evalúen la situación para que se pueda dar cumplimiento a estos procesos.

5.2. Resultados de la Investigación

Con base al análisis de los resultados de las entrevistas realizadas y el estudio de investigación, se pudo evidenciar que el Convenio sobre ciberdelincuencia constituye el único instrumento internacional vinculante en materia de ciberdelincuencia y seguridad cibernética, convirtiéndose, en el marco de referencia para varios países en la comunidad internacional para crear políticas, mecanismos y estrategias que ayuden a combatir, prevenir y mitigar los delitos cibernéticos en sus jurisprudencias, con base en lo estipulado en dicho

Convenio. Por tal motivo, se vuelve indispensable que Guatemala se adhiera al Convenio sobre Ciberdelincuencia, tomando en cuenta que la ciberdelincuencia es una problemática de carácter transnacional, por lo que es necesario que el Estado de Guatemala forme parte en los espacios de cooperación técnica y profesional dentro de la cooperación internacional que engloba está problemática transnacional.

Es menester recalcar, como lo refiere Treaty Office (2020), que Guatemala ya posee una invitación oficial por parte del Consejo de Europa para formar parte de este Convenio. Esto posicionó al país en cuanto a que se tiene un interés genuino en combatir una amenaza tan grande como lo es la ciberdelincuencia, además de mejorar las relaciones internacionales de Guatemala posicionándolo como un país que busca proteger, combatir y prevenir este flagelo.

Dentro de este orden de ideas, el esfuerzo integral al respecto debe ser reforzado por medio de la creación de un conjunto de actividades, protocolos, y estructuras de comunicación técnicas y profesionales, que puedan unirse a la comunidad internacional para mantener un continuo monitoreo de protección a cualquier tipo de amenaza cibernética, además de promover la interacción con otros estados más avanzados, lo cual es fundamental para que la protección sea del más alto nivel.

En lo que corresponde a la estrategia técnica y legal que posee el Estado de Guatemala para la lucha contra la ciberdelincuencia, los instituciones correspondientes como lo es el Congreso de la República de Guatemala y otras dependencias del Estado que velan por la seguridad nacional en el país, continúan trabajando en varias iniciativas de ley que buscan acoplarse con lo estipulado en el Convenio sobre Ciberdelincuencia, y de esa manera crear un marco regulatorio de carácter legal para que se apliquen las acciones permitentes a los delitos que involucran los sistemas y datos informáticos en Guatemala; sin embargo, se pudo evidenciar que a pesar de que se ha trabajado en la creación de leyes nacionales que tipifiquen correctamente los delitos cibernéticos en el país y creen ese marco regulatorio, como lo fue

la última iniciativa de ley número 5601 presentada en 2019, solamente han llegado a ser en iniciativa que aún no logran ser aprobadas.

En virtud de lo anteriormente descrito, los procesos penales son de vital importancia para responder adecuadamente a los incidentes cibernéticos, hoy día sin una ley que tipifique correctamente los delitos cibernéticos, no se puede proceder adecuadamente. Para responder a esta necesidad, es indispensable la pronta aprobación de una ley contra la ciberdelincuencia en Guatemala, que permita tipificar correctamente los delitos cibernéticos y facilitar el procesamiento de los casos por parte de los órganos penales correspondientes, de esa manera conseguiría establecer una certeza jurídica.

Respecto a uno de los objetivos específicos de la investigación sobre las condiciones actuales en las que se encuentra Guatemala en la lucha contra la ciberdelincuencia, cabe considerar, que la creación de la Estrategia Nacional de Seguridad Cibernética de Guatemala, la cual responde al plan estratégico para crear los mecanismos y políticas en Guatemala para la mitigación, prevención y combate de los delitos cibernéticos en el país, ha sido uno de los logros más prominentes del gobierno de Guatemala, a pesar de ello, es importante tomar en cuenta que cada día los delitos cibernéticos en el mundo van en aumento y Guatemala no es ajena a los ataques que puedan poner el riesgo de los datos y sistemas informáticos de millones de guatemaltecos, por lo cual la adhesión de Guatemala al Convenio sobre Ciberdelincuencia antes del año 2023, cuando la invitación del Consejo de Europa venza, ayudaría a que Guatemala se posicione como un país que está interesado en modificar sus leyes nacionales.

Si bien es cierto que un país puede crear planes estratégicos para combatir una problemática sin necesidad de firmar un convenio internacional, la naturaleza transnacional de la ciberdelincuencia hace que la problemática no solo afecte a un país sino a todo el mundo, por lo cual, al ser un problema de carácter internacional, se necesita la cooperación entre los países. Con base a lo anterior, es necesario que un país se adhiera a instrumentos internacionales como lo es el Convenio sobre Ciberdelincuencia, debido a que, siendo

signatario de este tipo de convenio, le da al país el acceso a otros recursos como la donación de equipos, el intercambio de experiencias, conocimientos, expertos, etc. En este orden de ideas, se ha podido evidenciar que al ser signatario en un futuro el Estado de Guatemala al Convenio sobre Ciberdelincuencia, habría varios beneficios conexos para poder prevenir o mitigar este tipo de incidentes en el país.

Conclusiones

Después de haber desarrollado el análisis de los beneficios que conlleva para Guatemala el adherirse al Convenio de Ciberdelincuencia, se llegó a las siguientes conclusiones:

El auge en el uso del Internet por parte de la población guatemalteca en los últimos años ha generado un incremento en los delitos que se realizan por medio del ciberespacio, en donde cada vez más la ciberdelincuencia incursiona en las actividades ilícitas que ponen en riego los sistemas y datos informáticos de los guatemaltecos, lo cual ocasiona grandes desafíos a nivel mundial al ser una problemática transnacional, en la cual Guatemala no es ajena.

La coyuntura actual presenta un periodo decisivo en materia de seguridad cibernética la cual apunta a que el tema de ciberdelitos va a ser tan grande que no muchos países no van a estar preparados cuando esta problemática cobré dimensiones mayores, por lo cual el Gobierno de Guatemala debe de tomar las medidas pertinentes para fortalecer la resiliencia cibernética del país con el fin de proteger a sus habitantes e instituciones de actividades ilícitas desarrolladas por medio de Internet.

El estado de Guatemala no tiene en este momento la capacidad legal adecuada para combatir, mitigar y prevenir las actividades ilícitas que se susciten por medo de internet al no haber adoptado aún una ley que tipifique correctamente este tipo de actividades ilícitas, a pesar, que se han presentado varias iniciativas de ley en los últimos 10 años, el Congreso de la República de Guatemala no ha aprobado ninguna de ellas; por lo cual es evidente la falta de una legislación adecuada.

La Estrategia Nacional de Seguridad Cibernética constituye un elemento bastante útil; sin embargo, falta ejecutar una guía en la cual las organizaciones o las empresas puedan apegarse en la parte de ciberseguridad. Además, se debe considerar el fortalecimiento de los Centros de Respuesta ante Incidentes Cibernéticos por parte

del Ministerio de Gobernación y el Ministerio de la Defensa Nacional, respectivamente.

Se puede colegir que efectivamente la cooperación internacional es un aspecto fundamental en la seguridad cibernética debido a que la ciberdelincuencia constituye un problema transnacional que involucra a diferentes actores del sistema internacional.

En Latinoamérica y el Caribe, la Organización de Estados Americanos se ha posicionado como aquella organización internacional que ha realizado una serie de acciones con cada uno de los países miembros con fin de brindarles la asesoría técnica necesaria para crear estrategias de seguridad cibernética acopladas a las necesidades de cada país, en donde Guatemala no ha sido la excepción, ya que fue con la ayuda de la OEA que fue posible crear la estrategia que hoy en día está vigente. Esto evidencia que el apoyo internacional es y será necesario para combatir la ciberdelincuencia en la región.

Se logró alcanzar el objetivo principal, al establecer que debido a las carencias técnicas y profesionales que las instituciones públicas tienen, la adhesión al Convenio sobre ciberdelincuencia por parte de Guatemala permitiría que el país fortaleciera su resiliencia cibernética, y estar mejor preparado ante incidentes cibernéticos que se puedan suscitar o involucrar al país. Además, beneficiaría al país con una participación directa en espacios de decisión internacional al abrirle espacios en materia de seguridad cibernética.

Referencias

Aguilera López, P. (2010). Seguridad informática. En *Seguridad Informática* (pp. 7–27). Editex. http://gacetaii.iingen.unam.mx/GacetaII/index.php/gii/article/view/1744/1695

Banco Interamericano de Desarrollo. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?: Informe Ciberseguridad 2016. *Observatorio De La Ciberseguridad En América Latina Y El Caribe*, 193. www.observatoriociberseguridad.com

Banco Interamericano de Desarrollo. (2020). *CIBERSEGURIDAD: Riesgos, avances y el camino a seguir en América Latina y el Caribe*.

Botero Marino, C. (2013). Libertad de expresión en internet: Relatoría Especial para la Libertad de Expresión (CIDH). En *Comisión Interamericana de Derechos Humanos*.

CAF. (2020). El estado de la digitalización de América Latina frente a la pandemia del COVID-19. *CAF*, 1–40. https://scioteca.caf.com/handle/123456789/1540

Calduch Cervera, R. (1991). Las relaciones internacionales. En *Las Relaciones Internacionales*. https://www.ucm.es/data/cont/media/www/pag-55159/lib1cap4.pdf

Castro, H. J., y Monteverde, A. (2018). Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito. *Revista Espacios*, *39*, 31. http://revistaespacios.com/a18v39n39/a18v39n39p31.pdf

Centro de Investigaciones Económicas Nacionales. (2015). *Diagnóstico y Propuestas en Infraestructura de Telecomunicaciones*. https://cien.org.gt/wp-content/uploads/2018/09/Telecomunicaciones.pdf

Comisión de Asuntos de Seguridad Nacional. (2019). *Dictamen favorable de la iniciativa*

5601. https://www.congreso.gob.gt/assets/uploads/comisiones/dictamenes/e259d-dictamen-5601.pdf

Comisión de las Comunidades Europeas. (2007). *Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones, " Hacia una política general de lucha contra la ciberdelincuencia.* (Vol. 22, Número 5). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52007DC0267&from=ES

Congreso de la República de Guatemala. (2016). *Detalles iniciativa 4055*. https://www.congreso.gob.gt/detalle_pdf/iniciativas/4240#gsc.tab=0

Congreso de la República de Guatemala. (2017). *Detalles iniciativa 5254*. https://www.congreso.gob.gt/detalle_pdf/iniciativas/4266#gsc.tab=0

Congreso de la República de Guatemala. (2019). *Detalle iniciativa 5601*. https://www.congreso.gob.gt/detalle_pdf/iniciativas/5614

Computer Fraud and Abuse Act, 1030 1213 (1986).

Convenio sobre Ciberdelincuencia, Pub. L. No. Serie de Tratados Europeos No. 185, 26 (2001). https://rm.coe.int/16802fa41c

Council of Europe. (1990). *Computer-related crime: recommendation no. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems* (p. 114). http://www.oas.org/juridico/english/89-9&final Report.pdf

Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, *8*, 169. https://doi.org/10.18172/redur.4071

Forbes Staff. (2019). *A estos retos se enfrenta Guatemala en telecomunicaciones y*

penetración de internet. https://forbescentroamerica.com/2019/10/31/a-estos-retos-se-enfrenta-guatemala-en-telecomunicaciones-y-penetracion-de-internet/

INE. (2019). *Resultados del Censo 2018*. https://www.censopoblacion.gt/explorador

Internet Governance Forum. (2017). *Hacia la Internet Asequible en Guatemala*. Alianza para una Internet Asequible. https://igf.gt/a4ai-guatemala/

ITU. (2019). Measuring digital development: Facts and figures 2019. *ITU Publications*, 1–15. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

ITU. (2020). *Individuals Using Internet*. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Keohane, R. O., y Nye, J. S. (1988). *Poder e Interdependencia La política mundial en transición* (Vol. 53, Número 9). Grupo Editor Latinoamericano. https://doi.org/10.1017/CBO9781107415324.004

Loredo, J. A., y Ramírez, A. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. *Celerinet*, 45–51. http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Mateos Pascual, I. (2013). *Ciberdelincuencia. Desarrollo y persecución tecnológica*. Universidad Politécnica de Madrid.

Ministerio de Gobernación. (2018). *Estrategia Nacional de Seguridad Cibérnetica*.

Miró, F. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista Española de Investigación Criminológica: REIC*, *11*(5), 5–35. https://dialnet.unirioja.es/servlet/articulo?codigo=4783296

Naciones Unidas. (1945). Carta de las Naciones Unidas. En *Carta de San Francisco* (pp. 17–

18). https://www.oas.org/36ag/espanol/doc_referencia/Carta_NU.pdf

OECD. (1992). *Guidelines for the Security of Information Systems, 1992*. http://www.oecd.org/digital/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

OECD. (2004). Directrices de la OCDE para la seguridad de sistemas y redes de información. En *Directrices de la OCDE para la seguridad de sistemas y redes de información*. https://doi.org/10.1787/9789264065819-es

Oficina de la OEA en Guatemala. (2018). *Guatemala*. Eventos Actuales. http://oea.org/es/acerca/offices_events.asp?sCode=GUA

Organización de Estados Americanos (OEA). (2004). *Ag/res. 2004 Estrategia de Seguridad Cibernetica (Resolución)*. https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf

Organización de Estados Americanos (OEA). (2013). *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos*. http://www.oas.org/es/ssm/cyber/documents/oastrendmicrolac_spa.pdf

Organización de Estados Americanos (OEA). (2014). *Tendencias de Seguridad Cibérnetica en America Latina y el Caribe*. https://www.sites.oas.org/cyber/Documents/2014 - Tendencias de Seguridad Cibernética en América Latina y el Caribe.pdf

PNUD. (2013). Informe Regional de Desarrollo Humano 2013-104. En *Journal of Chemical Information and Modeling* (Vol. 53, Número 9). https://www.undp.org/content/dam/rblac/img/IDH/IDH-AL Informe completo.pdf

Registro de Dominios.gt. (2018). *Historia de Registro de Dominios .GT*. https://www.gt/sitio/ourhistory.php

Treaty Office. (2020). *Non-members States of the Council of Europe*. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cac22

UIT-T. (2008). *X.1205 : Aspectos generales de la ciberseguridad* (Vol. 1205). https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-S&type=items

UIT. (2009). El Ciberdelito: Guía para los países en Desarrollo. *División de Aplicaciones TIC y Ciberseguridad Departamento de Políticas y Estrategias Sector de Desarrollo de las Telecomunicaciones de la UIT*, 238. http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

UIT. (2010). *Resolución 181. Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación*. *181*, 744–749. https://www.itu.int/en/council/Documents/basic-texts/RES-181-S.pdf

Villacampa Estiarte, C. (coord. ., Cerezo Domínguez, A., y Gómez Gutiérrez, M. (2019). *Introducción a la victimología*. Editorial Síntesis.

Walter, G. (2016). *Situación Actual de la Ciberseguridad en Guatemala*. http://www.ebg.edu.gt/oldSite/wp-content/files_mf/1470853882WalterGiron.pdf

World Bank Group. (2021). *The information society*. 5.12 World Development Indicators: The information society. http://wdi.worldbank.org/table/5.12#

Anexos

Anexo 1. Tablas y Figuras.

Tabla 4

Listado de países que han firmado y ratificado el Convenio sobre ciberdelincuencia

Estados miembros del Consejo de Europa	Firma	Ratificación	Entrada en Vigor
Albania	23/11/2001	20/06/2002	1/07/2004
Andorra	23/04/2013	16/11/2016	1/03/2017
Armenia	23/11/2001	12/10/2006	1/02/2007
Austria	23/11/2001	13/06/2012	1/10/2012
Azerbaiyán	30/06/2008	15/03/2010	1/07/2010
Bélgica	23/11/2001	20/08/2012	1/12/2012
Bosnia y Herzegovina	9/02/2005	19/05/2006	1/09/2006
Bulgaria	23/11/2001	07/04/2005	1/08/2005
Croacia	23/11/2001	17/10/2002	1/07/2004
Chipre	23/11/2001	19/01/2005	1/05/2005
Republica checa	9/02/2005	22/08/2013	1/12/2013
Dinamarca	22/04/2003	21/06/2005	1/10/2005
Estonia	23/11/2001	12/05/2003	1/07/2004
Finlandia	23/11/2001	24/05/2007	1/09/2007
Francia	23/11/2001	10/01/2006	1/05/2006
Georgia	1/04/2008	06/06/2012	1/10/2012

Alemania	23/11/2001	09/03/2009	1/07/2009
Grecia	23/11/2001	25/01/2017	1/05/2017
Hungría	23/11/2001	04/12/2003	1/07/2004
Islandia	30/11/2001	29/01/2007	1/05/2007
Italia	23/11/2001	05/06/2008	1/10/2008
Letonia	5/05/2004	14/02/2007	1/06/2007
Liechtenstein	17/11/2008	27/01/2016	1/05/2016
Lituania	23/06/2003	18/03/2004	1/07/2004
Luxemburgo	28/01/2003	16/10/2014	1/02/2015
Malta	17/01/2002	12/04/2012	1/08/2012
Mónaco	2/05/2013	17/03/2017	1/07/2017
Montenegro	7/04/2005	03/03/2010	1/07/2010
Países Bajos	23/11/2001	16/11/2006	1/03/2007
Macedonia del Norte	23/11/2001	15/09/2004	1/01/2005
Noruega	23/11/2001	30/06/2006	1/10/2006
Polonia	23/11/2001	20/02/2015	1/06/2015
Portugal	23/11/2001	24/03/2010	1/07/2010
República de Moldova	23/11/2001	12/05/2009	1/09/2009
Rumania	23/11/2001	12/05/2004	1/09/2004
San Marino	17/03/2017	08/03/2019	1/07/2019
Serbia	7/04/2005	14/04/2009	1/08/2009
República Eslovaca	4/02/2005	08/01/2008	1/05/2008

Eslovenia	24/07/2002	08/09/2004	1/01/2005
España	23/11/2001	03/06/2010	1/10/2010
Suiza	23/11/2001	21/09/2011	1/01/2012
Turquía	10/11/2010	29/09/2014	1/01/2015
Ucrania	23/11/2001	10/03/2006	1/07/2006
Reino Unido	23/11/2001	25/05/2011	1/09/2011

Estados miembros del Consejo de Europa	Firma	Ratificación	Entrada en Vigor
Argentina		5/06/2018	1/10/2018
Australia		30/11/2012	1/03/2013
Cabo Verde		19/06/2018	1/10/2018
Canadá	23/11/2001	08/07/2015	1/11/2015
Chile		20/04/2017	1/08/2017
Colombia		16/03/2020	1/07/2020
Costa Rica		22/09/2017	1/01/2018
República Dominicana		7/02/2013	1/06/2013
Ghana		3/12/2018	1/04/2019
Israel		9/05/2016	1/09/2016
Japón	23/11/2001	03/07/2012	1/11/2012
Mauricio		15/11/2013	1/03/2014
Marruecos		29/06/2018	1/10/2018
Panamá		5/03/2014	1/07/2014
Paraguay		30/07/2018	1/11/2018

Perú		26/08/2019	1/12/2019
Filipinas		28/03/2018	1/07/2018
Senegal		16/12/2016	1/04/2017
Sri Lanka		29/05/2015	1/09/2015
Tonga		9/05/2017	1/09/2017
Estados Unidos de América	23/11/2001	29/09/2006	1/01/2007

Nota. Elaboración propia basada en el cuadro de firmas y ratificaciones del Tratado 185; Convenio sobre Ciberdelincuencia, hasta la fecha 08/09/2020.

Número total de ratificaciones y adhesiones hasta septiembre de 2020: 65.

Tabla 5

Estados no miembros del Consejo de Europa que obtuvieron una invitación para firmar y ratificar o adherirse al Convenio sobre Ciberdelincuencia

País	Válida hasta	Referencia de la invitación
Benín	20/06/2024	1350ª sesión, 19 de junio de 2019
Brasil	12/12/2024	1363ª sesión, 11 de diciembre de 2019
Burkina Faso	12/12/2024	1363ª sesión, 11 de diciembre de 2019
Guatemala	23/04/2025	1374ª sesión, 22 de abril de 2020
Níger	23/04/2025	1374ª sesión, 22 de abril de 2020
Nigeria	6/07/2022	1291ª sesión, 5 de julio de 2017
Túnez	8/02/2023	1306ª sesión, 7 de febrero de 2018

Nota. Elaboración propia basada en el cuadro de Estados no miembros del Consejo de Europa que han recibido invitación hasta julio 2020.

Figura 7

Carta de Manifestación de Interés de Guatemala de Adherirse al Convenio de Budapest

Gobierno de Guatemala
Ministerio de Gobernación

Guatemala, 12 de abril de 2016
Ref. DM-458-16/FMRL-WGF-fdl

Señor
Alexander Seger
Secretario de la Convención de Delitos Cibernéticos
Jefe de Protección de Datos y de la División de Delitos Cibernéticos
Consejo de Europa
Estrasburgo, Francia
Presente

Honorable Señor Seger:

En nombre del Gobierno de la República de Guatemala, me dirijo a usted, con el propósito de expresar el deseo de nuestro país de ser parte de la Convención de Delitos Cibernéticos del Consejo de Europa (ETS 185), así como de solicitar el apoyo de su Institución para poder cumplir con los requerimientos necesarios para poder acceder a este Convenio.

Aprovecho la oportunidad invitarle a formar parte de una Misión de Asistencia Técnica para desarrollar una Estrategia Nacional de Ciberseguridad, la cual está liderada por el Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA). Consideramos que la presencia de su institución sería clave para liderar el componente legislativo que cada Estrategia Nacional de Ciberseguridad debe tener incluido.

Sin otro particular, permítame expresar las seguridades de mi más alta y distinguida consideración.

MINISTERIO DE GOBERNACIÓN
DESPACHO MINISTERIAL

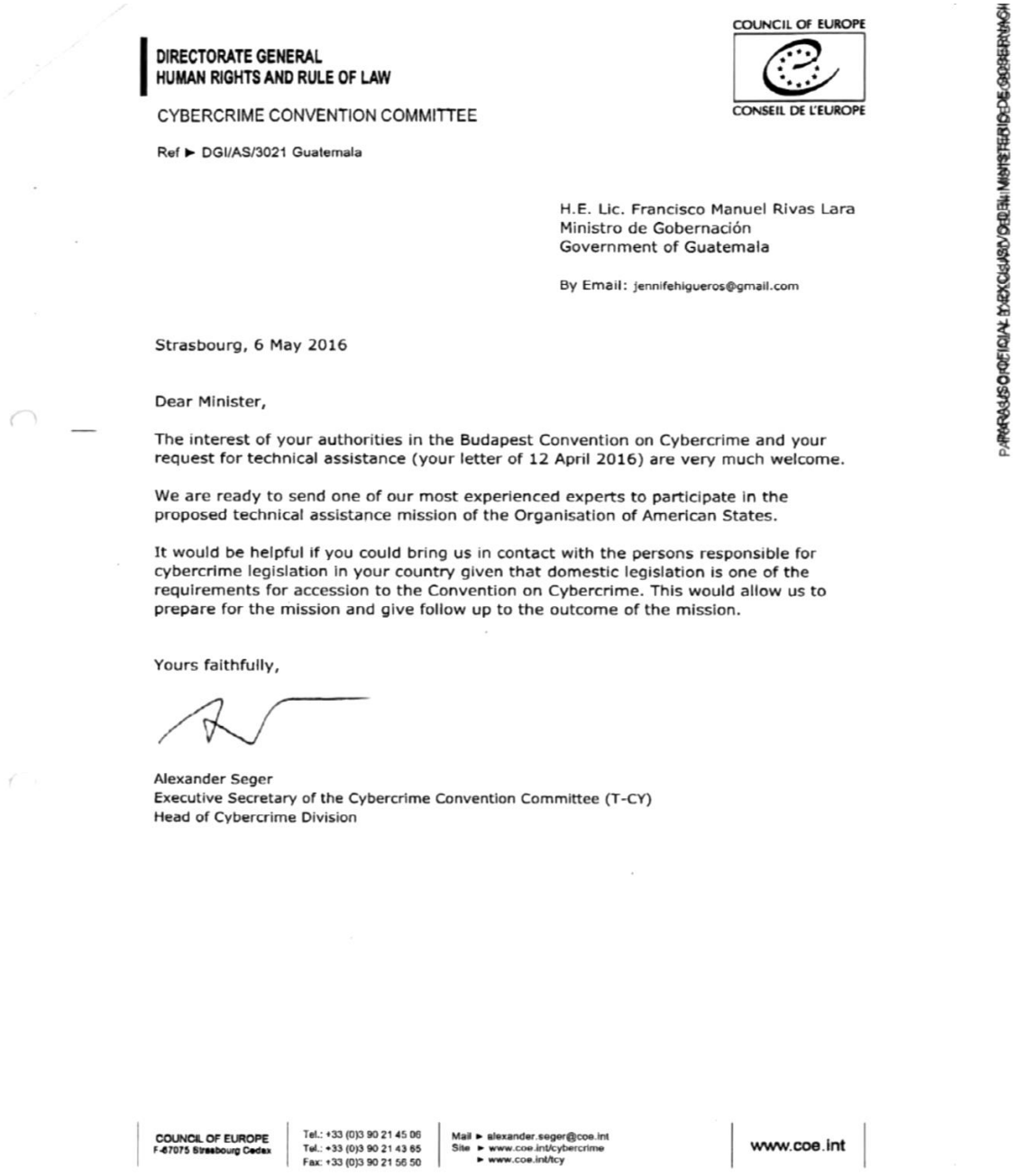
Lic. Francisco Manuel Rivas Lara
Ministro de Gobernación

6.° avenida 13-71, zona 1, PBX 2413 - 8888
www.mingob.gob.gt
www.guatemala.gob.gt

Nota. Tomado de *Situación Actual de la Ciberseguridad en Guatemala*, (diapositiva No. 19), por Walter Girón, 2016.

Figura 8

Carta de respuesta del Comité Europeo de Ciberseguridad



DIRECTORATE GENERAL
HUMAN RIGHTS AND RULE OF LAW

CYBERCRIME CONVENTION COMMITTEE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Ref ► DGI/AS/3021 Guatemala

H.E. Lic. Francisco Manuel Rivas Lara
Ministro de Gobernación
Government of Guatemala

By Email: jennifehigueros@gmail.com

Strasbourg, 6 May 2016

Dear Minister,

The interest of your authorities in the Budapest Convention on Cybercrime and your request for technical assistance (your letter of 12 April 2016) are very much welcome.

We are ready to send one of our most experienced experts to participate in the proposed technical assistance mission of the Organisation of American States.

It would be helpful if you could bring us in contact with the persons responsible for cybercrime legislation in your country given that domestic legislation is one of the requirements for accession to the Convention on Cybercrime. This would allow us to prepare for the mission and give follow up to the outcome of the mission.

Yours faithfully,

Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY)
Head of Cybercrime Division

COUNCIL OF EUROPE
F-67075 Strasbourg Cedex

Tel.: +33 (0)3 90 21 45 06
Tel.: +33 (0)3 90 21 43 65
Fax: +33 (0)3 90 21 56 50

Mail ► alexander.seger@coe.int
Site ► www.coe.int/cybercrime
► www.coe.int/tcy

www.coe.int

Nota. Tomado de *Situación Actual de la Ciberseguridad en Guatemala*, (diapositiva No. 26), por Walter Girón, 2016.

Anexo 2. Guía de Entrevistas

Universidad de San Carlos de Guatemala
Escuela de Ciencia Política
Octubre 2020

Entrevista

Para el desarrollo de Tesis: "**Análisis de los beneficios para el estado de Guatemala al adherirse al Convenio de Ciberdelincuencia firmado en la ciudad de Budapest".**

Nombre: _____

Cargo: _____

1. Basado en su experiencia, ¿Cuál considera que ha sido el mayor obstáculo para proveer del servicio de internet al todo el país desde su implementación hasta la fecha?

2. El acceso a la internet es hoy una herramienta fundamental para el desarrollo, sin embargo, como todo tiene sus riesgos. ¿Cuál cree Ud. que es el problema más grave que los ciudadanos enfrentan con el acceso a internet?

3. ¿Cuáles son las principales amenazas en Internet? Y desde esa tónica, ¿Cuáles deberían ser las medidas principales que el gobierno debe tomar para proteger a los ciudadanos ante incidentes cibernéticos?

4. Para hacer más accesible el acceso a la internet a la población guatemalteca, Guatemala se unió en 2017 a la Alianza para una Internet Asequible. En este contexto, ¿Cuáles considera Ud. que son los beneficios más importantes de esta alianza?

5. En términos generales, ¿Cuál sería la perspectiva respecto a los riesgos inherentes a la penetración de internet en los próximos años en el país?

6. En términos generales, ¿Cuáles son los delitos cibernéticos más frecuentes a los cuales se ven expuestos los guatemaltecos?

7. ¿Hasta qué punto considera usted que está preparado el gobierno para dar respuesta a estos incidentes?, y ¿Qué factores considera oportunos privilegiar para evitar esa exposición?

8. Basado en su experiencia, ¿Cuáles son los mayores desafíos que enfrenta el Estado de Guatemala para fortalecer su resiliencia cibernética?

9. En el marco de la seguridad cibernética, siendo esta, no solo el cibercrimen, sino la prevención contra los ataques cibernéticos, ¿Cuáles han sido los pasos que ha realizado la iniciativa privada para coordinar con los organismos del Estado la prevención y la protección contra estos actos delictivos?

10. Basada en su conocimiento, ¿Considera Ud. que el estado de Guatemala cuenta con la capacidad técnica y profesional para investigar delitos que se cometan en el ciberespacio?

11. En su opinión, ¿Es el CERT.gt la herramienta que necesita el estado para coordinar los esfuerzos nacionales frente al cibercrimen? ¿Si Ud. Pudiera implementar algunas estrategias que lo fortalezcan, ¿Cuáles serían?

12. ¿Considera que con una legislación adecuada para la prevención y protección contra la ciberdelincuencia facilitaría la persecución penal de los delitos cibernéticos en el país? Si su respuesta es sí, ¿De qué manera lo haría?

13. ¿Considera que tras los cambios de gobierno se ha proporcionado un adecuado seguimiento de las estrategias relacionadas con seguridad cibernética en el país?, y ¿Cuáles deberían de ser las prioridades del actual gobierno en este contexto?

14. El Convenio sobre ciberdelincuencia firmado en Budapest en 2001 es considerado el principal marco de referencia internacional, cuyo objetivo es servir de guía para que los estados puedan hacer frente a los delitos cibernéticos. En este contexto, ¿Considera importante que el Estado de Guatemala se adhiera y suscriba a este Convenio?, y en su opinión ¿Qué beneficios considera Ud. que obtendría el país al apegarse a este marco de referencia internacional?

¡Muchas gracias por su tiempo y colaboración!