UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

ESCUELA DE CIENCIA POLITICA

ESTUDIO EN EL MARCO DE LAS RELACIONES INTERNACIONALES DEL ROL DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO DE LA OEA EN EL COMBATE DEL TERRORISMO CIBERNÉTICO: ANÁLISIS DE LOS AVANCES DEL ESTADO DE GUATEMALA AÑO 2011-2012

MARTHA YADIRA PAIZ LOPEZ

GUATEMALA, NOVIEMBRE DE 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
ESCUELA DE CIENCIA POLITICA

ESTUDIO EN EL MARCO DE LAS RELACIONES INTERNACIONALES DEL ROL DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO DE LA OEA EN EL COMBATE DEL TERRORISMO CIBERNÉTICO: ANÁLISIS DE LOS AVANCES DEL ESTADO DE GUATEMALA AÑO 2011-2012

TESIS

Presentada al Consejo Directivo

De la

Escuela de Ciencia Política

De la

Universidad de San Carlos de Guatemala

Por

MARTHA YADIRA PAIZ LOPEZ

Previo a conferírsele el grado académico de

LICENCIADA EN RELACIONES INTERNACIONALES

Y el título profesional de

INTERNACIONALISTA

Guatemala, Noviembre 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

RECTOR MAGNIFICO
Lic. Carlos Guillermo Alvarado Cerezo

SECRETARIO GENERAL
Dr. Carlos Enrique Camey Rodas

CONSEJO DIRECTIVO DE LA ESCUELA DE CIENCIA POLITICA

DIRECTOR:	Lic.	Marcio Palacios Aragón
VOCAL I:	Licda.	Mayra Villatoro Del Valle
VOCAL II:	Lic.	Juan Carlos Guzmán Morán
VOCAL III:	Licda.	Ana Margarita Castillo Chacón
VOCAL IV:	Profa.	Florentina Puac Puac
VOCAL V:	Br.	José Rolando Samayoa Lara
SECRETARIO:	Lic.	Marvin Norberto Morán Corzo

TRIBUNAL QUE PRACTICO EL EXAMEN GENERAL DE CONOCIMIENTOS

COORDINADOR:	Lic.	Francisco José Lemus Miranda
EXAMINADOR:	Licda.	Cindy Lisbeth Poroj Caraballo
EXAMINADOR:	Lic.	Juan Carlos Guzmán Morán
EXAMINADOR:	Lic.	Oscar Estuardo Bautista Soto
EXAMINADOR:	Lic.	Roberto Rubio Rodas

TRIBUNAL QUE PRACTICO EL EXAMEN PÚBLICO DE TESIS

DIRECTOR:	Lic.	Marcio Palacios Aragón
SECRETARIO:	Lic.	Marvin Norberto Morán Corzo
COORDINADOR:	Lic.	Francisco José Lemus Miranda
EXAMINADOR:	Lic.	Secil Oswaldo de León
EXAMINADOR:	Lic.	Luis David Winter Luther

Nota: Únicamente el autor es responsable de las doctrinas sustentadas en la tesis. (Artículo 74 del Reglamento de Evaluación y Promoción de Estudiantes de la Escuela de Ciencia Política)

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

Escuela de Ciencia Política

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, diez de octubre del dos mil catorce.----------

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: **"ESTUDIO EN EL MARCO DE LAS RELACIONES INTERNACIONALES DEL ROL DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO DE LA OEA EN EL COMBATE DEL TERRORISMO CIBERNÉTICO: ANÁLISIS DE LOS AVANCES DEL ESTADO DE GUATEMALA AÑO 2011-2012".** Presentada por el (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, carnet No. 200512305**

Atentamente,

"ID Y ENSEÑAD A TODOS"

Lic. Marcio Palacios Aragón
Director Escuela de Ciencia Política

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
Escuela de Ciencia Política
DIRECCION

Se envía el expediente
c.c.: Archivo
9/myda

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

Escuela de Ciencia Política

ACTA DE DEFENSA DE TESIS

En la ciudad de Guatemala, el día veintinueve de septiembre del dos mil catorce, se efectuó el proceso de verificar la incorporación de observaciones hechas por el Tribunal Examinador, conformado por: Lic. Luis David Winter Luther, Lic. Secil Oswaldo de León y Lic. Francisco José Lemus Miranda Coordinador (a) de la Carrera de Relaciones Internacionales, el trabajo de tesis: **"ESTUDIO EN EL MARCO DE LAS RELACIONES INTERNACIONALES DEL ROL DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO DE LA OEA EN EL COMBATE DEL TERRORISMO CIBERNÉTICO: ANÁLISIS DE LOS AVANCES DEL ESTADO DE GUATEMALA AÑO 2011-2012".** Presentado por el (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, carnet no. 200512305** razón por la que se da por **APROBADO** para que continúe con su trámite.

"ID Y ENSEÑAD A TODOS"

Lic. Francisco José Lemus Miranda
Coordinador de Carrera

c.c.: Archivo
8c/ myda.

Edificio M5, Ciudad Universitaria, zona 12
PBX USAC: 2418 8000
EXTS.: 1471, 1473 y 1476
Guatemala, Centroamérica

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

Escuela de Ciencia Política

ACTA DE DEFENSA DE TESIS

En la ciudad de Guatemala, el día once de septiembre del dos mil catorce, se realizó la defensa de tesis presentada por el (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, carnet no. 200512305**, para optar al grado de Licenciado (a) en **RELACIONES INTERNACIONALES** titulada: **"ESTUDIO EN EL MARCO DE LAS RELACIONES INTERNACIONALES DEL ROL DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO DE LA OEA EN EL COMBATE DEL TERRORISMO CIBERNÉTICO: ANÁLISIS DE LOS AVANCES DEL ESTADO DE GUATEMALA AÑO 2011-2012"** ante el Tribunal Examinador integrado por: Lic. Luis David Winter Luther, Lic. Secil Oswaldo de León y Lic. Francisco José Lemus Miranda, Coordinador (a) 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. Luis David Winter Luther
Examinador

Lic. Secil Oswaldo de León
Examinador

Lic. Francisco José Lémus Miranda
Coordinador(a) de Carrera

c.c.: Archivo
8b /myda.

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, veintiocho de agosto del dos mil catorce.----------

ASUNTO: El (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, carnet no. 200512305**, continúa trámite para la realización de su Tesis.

Habiéndose emitido el dictamen correspondiente por parte del (la) Lic. Luis Fernando De León Laparra, 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"

Lic. Marcio Palacios Aragón
Director Escuela de Ciencia Política

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
Escuela de Ciencia Política
DIRECCION

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

Luis Fernando de León Laparra
Licenciado en Relaciones Internacionales
Colegiado 1,160

Guatemala, 26 de agosto de 2014

Licenciado
Marcio Palacios Aragón
Director
Escuela de Ciencia Política
Universidad de San Carlos de Guatemala.

Estimado señor Director:

Con atento saludo me dirijo a usted para informarle que he procedido a asesorar y revisar el trabajo de tesis presentado por la estudiante **MARTHA YADIRA PAIZ LOPEZ**, con carne No. **200512305**, titulado **ESTUDIO EN EL MARCO DE LAS RELACIONES INTERNACIONALES DEL ROL DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO DE LA OEA EN EL COMBATE DEL TERRORISMO CIBERNÉTICO: ANÁLISIS DE LOS AVANCES DEL ESTADO DE GUATEMALA AÑO 2011-2012**, el cual presenta como requisito académico previo a obtener el título de Internacionalista, en el grado de licenciada.

Por lo anterior, me permito manifestarle que los planteamientos desarrollados son un aporte importante al estudio de la problemática mencionada desde la perspectiva de las Relaciones Internacionales.

Por tal virtud me es grato informarle que la investigación presentada por la estudiante **MARTHA YADIRA PAIZ LOPEZ**, tiene las cualidades y requisitos necesarios de un trabajo de tesis, por lo tanto la recomiendo apta para ser presentada al Honorable Tribunal Examinador.

Sin otro particular, me suscribo aprovechando la presente para manifestarle mis más altas muestras de consideración y respeto.

Licenciado Luis Fernando de León Laparra
Asesor

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
Escuela de Ciencia Política
SECRETARIA

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, quince de julio del dos mil trece.----------

ASUNTO: El (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, carnet no. 200512305** 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 (a la) Asesor (a) de Tesis, Lic. Luis Fernando De León Laparra para que brinde la asesoría correspondiente y emita dictamen.

Atentamente,

"ID Y ENSEÑAD A TODOS"

Licda. Geidy Magali De Mata Medrano
Director(a) Escuela de Ciencia Política

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
Escuela de Ciencia Política
DIRECCION

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

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

Escuela de Ciencia Política

Guatemala, 10 de julio del 2013

Licenciado(a)
Geidy Magali De Mata Medrano
Director(a)
Escuela de Ciencia Política
Universidad de San Carlos de Guatemala

Respetable Licenciada De Mata

Me permito informarle que para desarrollar la tesis titulada: "**ESTUDIO EN EL MARCO DE LAS RELACIONES INTERNACIONALES DEL ROL DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO DE LA OEA EN EL COMBATE DEL TERRORISMO CIBERNÉTICO: ANÁLISIS DE LOS AVANCES DEL ESTADO DE GUATEMALA AÑO 2011-2012**", presentado por el (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, carnet no. 200512305** puede autorizarse como Asesor (a) a Lic. Luis Fernando de León Laparra.

Cordialmente,

"ID Y ENSEÑAD A TODOS"

Lic. Francisco José Lemus Miranda
Coordinador(a) de Carrera

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
Escuela de Ciencia Política
SECRETARIA

c.c.: Archivo
myda
5/

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, trece de junio del dos mil trece----------

ASUNTO: El (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, Carnet 200512305**, 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 (a la) Coordinador (a) de Carrera correspondiente, para que emita visto bueno sobre la propuesta de Asesor.

Atentamente,

"ID Y ENSEÑAD A TODOS"

Licda. Geidy Magali De Mata Medrano
Director(a) Escuela de Ciencia Política

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
Escuela de Ciencia Política
DIRECCION

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

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

Escuela de Ciencia Política

Guatemala, 24 de mayo del 2013.

Licenciado(a)
Geidy Magali De Mata Medrano
Director(a)
Escuela de Ciencia Política
Universidad de San Carlos de Guatemala

Respetable Licenciada De Mata::

Me permito informarle que tuve a la vista el diseño de tesis titulado: "**ESTUDIO EN EL MARCO DE LAS RELACIONES INTERNACIONALES DEL ROL DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO DE LA OEA EN EL COMBATE DEL TERRORISMO CIBERNÉTICO: ANÁLISIS DE LOS AVANCES DEL ESTADO DE GUATEMALA AÑO 2011-2012".** Presentado por el (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, carnet no. 200512305**, 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"

Dr. Gustavo Palma Murga
Coordinador(a) del Área de Metodología

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

ESCUELA DE CIENCIA POLITICA DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Guatemala, quince de mayo del año dos mil trece.----------

ASUNTO: El (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, carnet no. 200512305**, 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"

Licda. Geidy Magali De Mata Medrano,
Director(a) Escuela de Ciencia Política

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
Escuela de Ciencia Política
DIRECCION

c.c.: Archivo
2/ myda.

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

Escuela de Ciencia Política

Guatemala, 8 de mayo del 2013

Licenciado(a)
Geidy Magali De Mata Medrano
Director(a)
Escuela de Ciencia Política
Universidad de San Carlos de Guatemala

Respetable Licenciada De Mata:

Me permito informarle que el tema de tesis: "**ESTUDIO EN EL MARCO DE LAS RELACIONES INTERNACIONALES DEL ROL DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO DE LA OEA EN EL COMBATE DEL TERRORISMO CIBERNÉTICO: ANÁLISIS DE LOS AVANCES DEL ESTADO DE GUATEMALA AÑO 2011-2012".** Propuesto por el (la) estudiante **MARTHA YADIRA PAIZ LÓPEZ, carnet no. 200512305** puede autorizarse, dado que el mismo cumple con las exigencias mínimas de los contenidos de la carrera.

Cordialmente,

"ID Y ENSEÑAD A TODOS"

Lic. Francisco José Lemus Miranda
Coordinador (a) de Carrera

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
Escuela de Ciencia Política
SECRETARIA

c.c.: Archivo
myda/
1

DEDICATORIA

A DIOS:	Por darme la vida y la oportunidad de cumplir esta meta.
A MI MADRE:	Oty López de León, por brindarme su apoyo incondicional y sabias enseñanzas.
A MI GRAN FAMILIA:	Por estar siempre presentes en cada momento de mi vida.
A MI ASESOR DE TESIS:	Licenciado Luis Fernando de León por su ayuda, sus consejos y motivación que me ayudaron a finalizar esta etapa.
A MIS AMIGOS:	Especialmente Carolina Rodríguez, Roberto Bauce y Julio Castillo. Por su ánimo y apoyo a lo largo de mi carrera.
A MIS COMPAÑERAS DE ESTUDIO:	Karen Calderón, Sandra Miculax, Nancy Coronado, Nineth García , y Angélica Guevara, por su compañerismo y amistad en todos los momentos que hemos compartido.
A:	La Tricentenaria Universidad de San Carlos de Guatemala, en especial a la Escuela de Ciencia Política, por la formación académica y profesional.

ÍNDICE

CAPÍTULO IV

INTRODUCCIÓN

Partiendo de la importancia del tema de la Seguridad Cibernética y el Terrorismo Cibernético en el marco de las Relaciones Internacionales, el uso de la computadora para fines terroristas se ha convertido en una de las mayores amenazas del siglo XXI para todo el mundo, y mientras mas dependientes sean nuestras sociedades al uso del Internet, existe mas peligro de sufrir este tipo de ataques, lo cual tiene un impacto trascendental en el ámbito nacional e internacional de gran magnitud, que afecta a las Relaciones Internacionales, con consecuencias políticas, sociales y económicas, y dado el hecho de que Guatemala presenta enormes retos en el tema, surge el presente estudio de investigación.

El territorio de Guatemala no está a salvo de sufrir actos que atenten contra la seguridad cibernética, tanto en el sector privado como en el público y sin las herramientas legales o técnicas para combatir este problema provoca una gran vulnerabilidad que puede conducir a grandes riesgos o incluso desastres. Prueba de ello fueron las acciones registradas durante el año 2011 y 2012 por el colectivo de ciber hacktivistas Anonymous en Guatemala contra el gobierno de Guatemala.

El estudio de las acciones del Comité Interamericano Contra el Terrorismo y el Gobierno de Guatemala en función de la seguridad cibernética en nuestro país generaron una serie de inquietudes durante el proceso de investigación en el marco de las Relaciones Internacionales, debido al involucramiento de diversos sectores en el esfuerzo de reducir y combatir las amenazas virtuales.

El tema de investigación se desarrolla a lo largo de cinco capítulos. El primer capítulo abarca brevemente el abordaje teórico-metodológico de la investigación. Explicando la teoría funcionalista de las Relaciones Internacionales y su relación con el objeto de estudio. Asimismo se desglosan los objetivos, técnicas y mecanismos que sirvieron para la realización de la investigación.

En el segundo capítulo se abordan los antecedentes del Sistema Interamericano, para conocer ampliamente la historia de la integración latinoamericana. Posteriormente se desarrolla el tema de la Organización de Estados Americanos con el fin de explicar su estructura y funciones. Asimismo se expone el Comité Interamericano Contra el Terrorismo, su origen, estructura, y funciones principales, haciendo énfasis en el programa de seguridad cibernética.

El tercer capítulo abarca el tema del terrorismo desde sus orígenes en la historia mundial, la diversidad de definiciones del mismo y una clasificación de los tipos de terrorismo existentes. También se explica ampliamente el tema de terrorismo cibernético, las diversas acciones delictivas en los sistemas informáticos, la problemática que existe dentro del Internet profundo. Luego se exponen los tipos de ciberdelincuentes, describiendo las características de cada uno y resaltando las acciones realizadas por el ciber hacktivismo en Guatemala. Posteriormente se realiza una compilación de las principales acciones en contra de las páginas Web del gobierno de Guatemala realizadas por cibercriminales en el período de estudio, así como también un análisis del efecto en la opinión pública, el manejo del tema por los medios de comunicación y el accionar gubernamental.

En el cuarto capítulo se expone el tema del Estado de Guatemala frente al terrorismo, enfatizando la problemática del terrorismo cibernético. Se aborda un análisis del marco legal nacional e internacional que abarcan el tema del terrorismo cibernético, así como también de los principales crímenes a la seguridad informática. Luego se explica el rol del Comité Interamericano Contra el Terrorismo y su Incidencia en el Estado de Guatemala, el papel y acciones del CSIRT en Guatemala, así como diversos ejemplos de Centros de Respuesta a Incidentes de Seguridad Informática en América Latina. Se expone el plan de trabajo del CICTE a nivel regional y cuales de las actividades planeadas se han aplicado en Guatemala; también la opinión de la OEA acerca de la problemática en el país en base a la entrevista con el Embajador Permanente de Guatemala ante la OEA, Presidente del

CICTE 2012-2013, y Viceministro de Relaciones Exteriores, Embajador Rodrigo Vielmann. Después un análisis de las principales amenazas y retos basado en las entrevistas realizadas planteándolo desde las diversas perspectivas y puntos de vista de los técnicos de informática, Ministerio de Gobernación y del Centro de Respuesta Inmediata a Incidentes CSIRT-gt.

Para finalizar, el capítulo cuatro aporta la propuesta de un proyecto de creación de una Estrategia Nacional de Ciberseguridad en Guatemala, con el fin de mejorar la coordinación interinstitucional y la legislación en el ámbito nacional, así como el fortalecimiento de las relaciones de cooperación en materia de seguridad cibernética, que podría ser de gran valor y aplicada en las políticas publicas nacionales.

ACRÓNIMOS

CE	Consejo de Europa
CICTE	Comité Interamericano Contra el Terrorismo
CITEL	Comisión Interamericana de Telecomunicaciones
CME	Ejercicio de Manejo de Crisis en Seguridad Cibernética
CSIRT	Equipo de Respuesta ante Incidencias de Seguridad en tecnologías de la información
DOITS	Departamento de Información y Tecnología de la Organización de Estados Americanos
ETA	Organización Terrorista Independiente Vasca
IRA	Ejercito Republicano Irlandés
OEA	Organización de Estados Americanos
ONU	Organización de las Naciones Unidas
REMJA	Reunión de Ministros de Justicia o de Ministros o de Procuradores Generales de las Américas
TIAR	Tratado Interamericano de Asistencia Recíproca
UIT	Unión Internacional de Telecomunicaciones

GLOSARIO

- **Cibernética:** La Real Academia Española la define como el estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas, y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología.
- **Convenio:** Acuerdo escrito entre dos o mas Estados que establecen normas de conducta, de cooperación, de política. (Larios, C. 2005. p.28)
- **Datos:** Unidad mínima de información, sin sentido en sí misma, pero que adquiere significado en conjunción con otras precedentes de la aplicación que las creó.
- **Delito:** Conducta humana consciente y voluntaria que produce un efecto en el mundo exterior, que se encuentra prohibida por la ley.
- **Delito de dispositivos de acceso:** Quien de manera deliberada cree, utilice, altere, grabe, copie o transfiera de un dispositivo de acceso a otro los códigos de acceso al servicio o sistema informático.
- **Dirección IP:** Es un número único e irrepetible con el cual se identifica el origen de una computadora conectada a Internet.
- **Dominio:** nombre que identifica a un sitio Web.
- **Hardware:** Conjunto de componentes que integran la parte física de una computadora.
- **Informática:** Según el diccionario de la Real Academia Española informática puede definirse como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores. (Barrios, O. 2007. p. 2-9)
- **Infraestructura crítica informática**: son los activos, sistemas, redes, físicas o virtuales, que son vitales para la sobrevivencia del Estado. Que su incapacidad o destrucción podría tener un efecto debilitante en la seguridad de la nación, seguridad económica, salud publica, seguridad financiera, servicios públicos, agua, luz, telefonía o en una combinación de ellos.

- **Pagina Web:** Documento capaz de contener sonido, video, imágenes o texto, que situado en una red informática, al que se accede mediante el uso de Internet. (Alvarado y Morales. 2012. p. 10)
- **Resolución:** Es una moción escrita por una Asamblea. Se refiere a medidas que no se han convertido en ley y es usada a menudo para expresar aprobación o desaprobación de un tema en específico.
- **Software:** Programa o conjunto de programas que se utilizan en computación para procesar los datos e información y que interactúan entre el usuario y el hardware.
- **Usuario:** Persona que utiliza funciones y aplicaciones del sistema informatizado.
- **Virus:** Programas de computadora que tienen por objeto introducirse en los sistemas informatizados para causar alguna clase de daño a la información, al sistema operativo, programas en general.
- **Virtual:** la Real Academia Española lo define con propiedad para producir un efecto aunque no lo produzca, es decir que tiene existencia aparente y no real.

CAPITULO I

1. ABORDAJE TEÓRICO- METODOLÓGICO

Con el desarrollo de la globalización surgen nuevas oportunidades de desarrollo político, social y principalmente económico a través del uso de la tecnología en los diferentes países; asimismo nuevas amenazas que quizás hace 30 años ni siquiera podían preverse. Una de tales amenazas emergentes se conoce como ciberterrorismo que consiste en el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos con el fin de intimidación; que puede resultar en violencia por parte de grupos subnacionales o agentes clandestinos, el cual no tiene fronteras y en el que cualquier país es vulnerable, sin importar su condición política o económica. (Masana, 2002. p.12).

Es así como los peligros tecnológicos y sus alcances a nivel mundial han generado en cada nación la necesidad de poder protegerse, no solo de las amenazas dentro de su territorio, sino también combatir el peligro de ataques del exterior. A eso hay que sumarle la problemática de la soberanía y la resolución de problemas legales en Internet.

Por tal motivo las naciones han buscado asociarse, naciendo de una necesidad funcional, en que cada Estado decide integrarse a otro grupo de países con la finalidad de poder compartir información, experiencias, expertos y legislaciones para combatir juntos un problema que afecta a todos como lo es el terrorismo cibernético. Es por este motivo que se ha optado por analizar el terrorismo cibernético desde la perspectiva que nos presenta la teoría funcionalista de las relaciones internacionales, que analiza la imposibilidad del Estado de satisfacer las necesidades de la humanidad en el marco de su territorio (Vieira, 2008. p. 169); cuando las necesidades sobrepasan sus fronteras, motivadas por el crecimiento de obligaciones cada vez mas técnicas, conduce a la creación de asociaciones internacionales, no en términos de reparto de poder, sino de satisfacer el bienestar de la población.

Los orígenes del Funcionalismo surgen en Inglaterra en los años 1930 en las ciencias sociales. Sus principales exponentes son:

- **Emile Durkheim:** Estudiaba como ciertas sociedades mantenían su estabilidad a lo interno y sobreviven en el tiempo. Propuso que estas sociedades tienden a segmentarse con partes que permaneces unidas por valores compartidos o sistemas de intercambios. Es decir, que muchas sociedades se mantenían unidas para sostenerse en su conjunto a través de "solidaridad social mecánica", la cual se encontraba fundada en la similitud de sentimientos sociales, los cuales son compartidos por todos los individuos que componen el sistema social, basados en la especialización y la interdependencia. Para Durkheim el orden social es el resultado de la solidaridad social. (Romero y Vera. 2010. P.149)

- **David Mitrany:** Analizaba la imposibilidad del Estado de satisfacer las necesidades de la humanidad en el marco de su territorio, cuando las necesidades sobrepasaban sus fronteras, motivadas por el crecimiento de obligaciones cada vez mas técnicas, ya no políticas, que enfrentaban los gobiernos (Vieira E. 2008. p.169). Tales tareas no solo creaban una demanda de especialistas altamente entrenados en el nivel nacional, sino que también contribuían a la emergencia de problemas esencialmente técnicos en el nivel internacional, cuya solución está en la colaboración entre los técnicos más que en las élites políticas. (Dougherty J. 1993. p.444) Esta transferencia de funciones técnicas implicaba a su vez el crecimiento de las interdependencias entre los Estados, sin embargo Miltrany insistió en la necesidad de limitar el poder de dichas organizaciones, preservando su carácter funcional-sectorial, con objeto de evitar que llegaran a convertirse en superestados. Se preocupaba por el proceso por el cual las comunidades políticas se integran.

Se dice que el crecimiento en importancia de los temas del siglo XX ha hecho necesaria la creación de marcos para la cooperación internacional. Tales organizaciones funcionales podría esperarse que se expandieran tanto en su número y alcance en la medida que crecen los problemas técnicos que enfrenta la

humanidad tanto en tamaño como en magnitud. Miltrany suponía que la actividad funcional podría reorientar la actividad internacional y contribuir a la paz mundial.

- **Talcott Parsons**, propone una teoría social que aspiraba a explicar a la sociedad como un sistema general; y desde un modelo teórico que se pudiera aplicar a todas las sociedades. (Hidalgo. 2001. p. 85) Afirma que los grupos humanos necesitaban mantener un patrón latente u ordenamiento básico, mantener una serie de metas, deben adaptarse y por último integrase, esta integración se obtiene en virtud de existir un sentido de pertenencia o comunidad, un ordenamiento jurídico y normas o valores culturales y sociales. Pone un énfasis particular en el mantenimiento de la cohesión del sistema social. Para Parsons la sociedad existe porque la gente comparte un sentimiento de adhesión o solidaridad colectiva.

Los funcionalistas juzgan al Estado-nación poco competente para hacer frente a la interdependencia creciente del mundo moderno, pues se muestra ineficaz en el manejo de los temas económicos y sociales y por ello la resultante de la guerra (Vieira. 2005. P. 246), ante la ineficacia de las instituciones nacionales, incapaces de promover el desarrollo económico y social.

Básicamente la teoría funcionalista (Orantes. 1968 p. 176) consiste en etapas primordiales a saber: la identificación de ciertos puntos de consenso entre los actores, la iniciación de un proceso de aprendizaje bajo la supervisión de expertos, quienes se encargan de situar siempre el interés común en un plano mas alto que el que cada uno de los participantes.

El funcionalismo incentiva la búsqueda de labores específicas en las cuales predominaría el consenso por encima del conflicto entre Estados. Se trata de realidades en las cuales solo un esfuerzo mancomunado entre países puede transformar las relaciones interestatales.(Hidalgo. 2001. P.84) Este esfuerzo debe ser delegado a organizaciones especializadas (especialidad funcional), en base a las

cuales se establecerían las pautas de un amplio sistema de cooperación internacional.

La aplicación de la teoría funcionalista a las relaciones internacionales (Orantes. p. 169) encuentra su mas grande expresión en la elaboración de una estrategia que permite alcanzar un gobierno mundial, o varios estados regionales, yendo “más allá de la nación”. En suma la teoría funcionalista en relaciones internacionales se basa en la esperanza de que delegando cada vez más tareas comunes en tales organizaciones internacionales, las naciones del mundo se irán integrando gradualmente con fines pacíficos de lo cual resultará imposible la guerra.

Es este el valor de la teoría funcionalista correlacionada al terrorismo cibernético, ya que las necesidades y problematización que genera el cibercrimen y sus secuelas económicas, políticas y sociales en la sociedad contemporánea exige la solidaridad y asociación de naciones agrupadas en organizaciones internacionales especializadas; como el Comité Interamericano Contra el Terrorismo y los Centros de Respuesta Inmediata a Incidentes Cibernéticos Nacionales e Internacionales, en la búsqueda de soluciones conjuntas, experiencias, expertos, capacitaciones, normativas, que contribuyan a reducir las secuelas, prevenir los ataques y crear nuevas herramientas legales y operativas, que permitan una seguridad tecnológica regional y mundial, con el objetivo común de la preservación de la paz y el bienestar común.

Tomando en cuenta el funcionalismo, así como también la teoría de la interdependencia compleja desarrollada por Robert Keohane y Joseph Nye en la que indican que no debe existir la centralidad al Estado-Nación, sino se busca redefinir la concepción del Estado en las relaciones internacionales. Se trata de explicar las vinculaciones y relaciones que no tengan como eje de estudio al Estado, sino que las uniones transnacionales entre Estados remiten a un proceso de dependencia mutua . Se pueden analizar ciertos factores determinantes de la misma vinculados al tema de la ciberseguridad y terrorismo cibernético.

Una de las características principales de este modelo es la existencia de múltiples canales de comunicación conectando las sociedades. Estos canales son las relaciones estatales, transgubernamentales, y de organismos internacionales especializados en la paz y la seguridad como es el caso de la ONU, OEA y CICTE con los propios Estados.

Otro elemento de la teoría de la interdependencia es que establece una ausencia de jerarquía, en la cual, no hay subordinación a los temas ni actores del Sistema Internacional y la distinción entre problemas internos y externos se diluye.

Sin embargo es importante mencionar en esta situación no siempre se cumple a cabalidad esta premisa y específicamente en el caso de la ciberseguridad existe una doble moral y una falta de simetría, en la cual países dominantes juegan un papel de control sobre el presupuesto y toma de decisiones de la seguridad internacional a través de las organizaciones internacionales de las cuales forma parte, generalmente a su beneficio o en algunos casos apoyando a otros con intereses de trasfondo siempre encaminados al mantenimiento del poder.

Asimismo la agenda de la interdependencia compleja esta fundamentada en los principios de cooperación e integración con el fin de desarrollar instituciones supranacionales especializadas que permitan solventar necesidades, como el caso del resguardo de la seguridad cibernética, acciones basadas en el multilateralismo, ayuda mutua, y en el deber de cooperar como norma principal, lo cual comparte similitudes con el funcionalismo y sus principios de asociación entre Estados basadas en la solidaridad y el bienestar común.

También es relevante señalar que la interdependencia compleja se refiere a situaciones caracterizadas por efectos recíprocos entre países o entre actores de diferentes Estados, y si se parte de la idea que los Estados están inseparablemente unidos, tanto los aspectos positivos, como los negativos afectan a todos. Lo cual en el caso de la seguridad cibernética, el terrorismo y los ciberataques puede

desencadenar una vulnerabilidad entre los propios Estados, ya que si por el eslabón mas débil es por donde se rompe la cadena, si no se presentan las mismas oportunidades para todos los Estados de acceder a las mismas oportunidades técnicas y operativas relativas a la seguridad, es fácil que todos salgan afectados por el eslabón mas débil, por donde los ciberdelincuentes puedan vulnerar los sistemas de seguridad en la información internacional.

Esta investigación tuvo como finalidad comprobar los niveles de seguridad informática en Guatemala, especialmente enfocada al tema del terrorismo cibernético, y la relación que tiene con el Comité Interamericano Contra el Terrorismo de la Organización de Estados Americanos y sus estados miembros en el combate del mismo, así como conocer las debilidades institucionales con respecto al tema. Por lo cual surge como objetivo general analizar en el marco de las Relaciones Internacionales el rol del Comité Interamericano Contra el Terrorismo de la OEA en el combate del terrorismo cibernético en el Estado de Guatemala. Aunado a lo anterior, se definieron los objetivos específicos:

- Conocer científicamente las amenazas cibernéticas que afectan al Estado de Guatemala, con el fin de determinar los retos que el país enfrenta en esta problemática.

- Interpretar la aplicación por parte del Estado de Guatemala las medidas en materia técnica y legal para prevenir y sancionar los crímenes cibernéticos , con el fin de comprobar la eficacia de las mismas.

- Analizar las estrategias regionales en materia de seguridad cibernética emitidas por la Organización de Estados Americanos a través del Comité Interamericano Contra el Terrorismo para poder identificar el cumplimiento y eficiencia de las mismas.

Para delimitar el problema, la investigación se llevó a cabo en la Ciudad de Guatemala, enfocada en el Comité Interamericano Contra el Terrorismo de la OEA,

y Ministerio de Relaciones Exteriores por medio de la recopilación de información escrita, monitoreo de medios, videos y entrevistas a los expertos en el tema. Dicho estudio se tomó el período 2012-2013.

Desde la perspectiva metodológica adoptada, esta investigación es documental, la cual se basó en el análisis de documentos, siendo de gran utilidad para profundizar en el tema estudiado, donde también se abordó una estrategia metodológica cualitativa. Además fueron consultados para ampliar el tema trabajos e informes, asistencia a conferencias especializadas, puntos de vista de expertos del tema y experiencias personales.

A través de la revisión documental y la investigación bibliográfica y hemerográfica, se hizo un análisis y síntesis de la información recopilada para posteriormente estructurarla de forma clara y comprensible al lector en cada uno de los capítulos, apoyándose de la cronología para obtener un trabajo organizado.

Para realizar esta primera etapa de utilidad en la elaboración de la investigación, se hizo una reseña histórica tanto del origen del sistema de integración interamericano hasta la actualidad, como del terrorismo cibernético y su marco legal, así como también el manejo del tema desde la perspectiva de las relaciones internacionales y del ámbito nacional.

En la segunda etapa de la recolección de datos, la cual se refiere a la investigación de campo, con el objeto de acceder a la información, fue utilizada la técnica de la entrevista, con el fin de comprender la perspectiva desde la que entienden el problema las unidades de análisis, que son el Comité Interamericano Contra el Terrorismo –CICTE-, Ministerio de Relaciones Exteriores de Guatemala –MINEX- y Ministerio de Gobernación de Guatemala –MINGOB-. Por último, para elegir a los funcionarios con el fin de llevar a cabo la entrevista se recurrió al muestreo de tipo no probabilístico, ya que se consideró que era necesario entrevistar específicamente a personas claves debido al nivel de conocimiento específico y necesario al que había

que acceder y de esta forma ahondar aún mas en la problemática y poder atar cabos sueltos que habían quedado de la investigación bibliográfica.

Las entrevistas realizadas fueron estructuradas y se recogió la muestra conforme al conocimiento de los profesionales que complementaron la investigación. Las entrevistas fueron realizadas de forma individual, utilizando la guía de entrevista.

- Primero se entrevistó el día 10 de octubre del 2013 al Ing. Ronald Morales, creador del Centro de Respuesta Inmediata a Incidentes de Seguridad Cibernética en Guatemala (CSIRT-gt), y creador de la Iniciativa de Ley 4055, Ley de Delitos Informáticos. Dicha entrevista fue realizada posterior a la realización de su conferencia sobre “Cibercrimen” en el Congreso de Ciencia y Tecnología.

- Posteriormente al Ing. Joel Fock Way, Subjefe de Informática de la Contraloría General de Cuentas, 10 de abril 2014.

- Ing. Ronny Antonio Vásquez, Administrador de Servidores, Oficial de Seguridad de la Información, Contraloría General de Cuentas, 14 de abril 2014.

- Ing. Juan Carlos Argueta Medina, Viceministro de Tecnología del Ministerio de Gobernación, 30 de abril 2014.

- Ing. Luis Fernando Ruiz, Técnico de la Dirección Informática del Ministerio de Gobernación, 30 de abril 2014.

- Embajador Rodrigo Vielmann, Presidente del CICTE durante el período 2012-2013, y actual Viceministro de Relaciones Exteriores, 2 de junio 2014.

- Ing. Gabriel Juárez Lucas, Subdirector de Informática, de la Secretaría Técnica del Consejo Nacional de Seguridad el 12 de junio 2014.
- También durante el mes de junio se tuvo la posibilidad de hacer contacto en varias ocasiones con el grupo Anonymous Guatemala, quienes aceptaron la

realización de una entrevista. Sin embargo al conocer la naturaleza de las preguntas, decidieron no responderlas.

Antes de cada entrevista se realizó de manera introductoria una pequeña explicación del tema, además de anticiparle a cada funcionario vía correo electrónico que la entrevista estaría enfocada en los temas principales de seguridad de la información en Guatemala y su colaboración con el CICTE. Durante las entrevistas se identificaron áreas claves que ayudarían a cumplir los objetivos del estudio, ya que se logró completar con la información adquirida para poder concluir la investigación. Asimismo, para completar la visión del tema fue de suma importancia la asistencia a dos conferencias especializadas en seguridad informática:

- La primera organizada por la Secretaría Nacional de Ciencia y Tecnología (SENACYT), fue el Primer Congreso Internacional de Ciencia, Tecnología e Innovación, realizada en octubre del 2013,

- Posteriormente, Info Security Tour VIP, realizado en la Ciudad de Guatemala en mayo 2014, actividad que estuvo integrada por doce conferencias de doce empresas privadas cuyo trabajo se enfoca en la seguridad cibernética, de los cuales los temas fundamentales fueron hacking, antivirus, modelos de seguridad cibernética, por empresas internacionales de renombre como HP, DELL , CISCO, Kaspersky, y Sophos; lo cual permitió tener una visión de la seguridad de la información desde el punto de vista de los proveedores de empresas privadas, y que en algunos casos colaboran con algunos entes gubernamentales, electos según el criterio de cada Dirección de Informática de las instituciones del Estado.

Las entrevistas y las conferencias fueron fundamentales para completar el conocimiento respecto al tema de investigación, el cual es trascendental tanto en el ámbito nacional como internacional. Los resultados de la investigación se determinaron conforme a las entrevistas, conferencias, videos, informes y documentos consultados respecto al tema de estudio.

CAPITULO II

SISTEMA DE INTEGRACION INTERAMERICANO Y LA ORGANIZACIÓN DE ESTADOS AMERICANOS

2.1 Antecedentes Históricos del Sistema

Algunos historiadores remontan el origen del sistema interamericano al Congreso de Panamá convocado por Simón Bolívar en 1826. Sin embargo, En 1880, el presidente de los Estados Unidos envió una invitación a los diferentes gobiernos del continente para reunirse en la ciudad de Washington para discutir la aceptación de que Estados Unidos fuera árbitro de las relaciones internacionales en el Hemisferio así como la creación de la Unión Aduanera Americana, pero fue en 1889 cuando finalmente esta reunión se llevó a cabo.

Boersner (1996, p.186) menciona que Estados Unidos quería tomar el papel de árbitro en las relaciones internacionales de América; empezaron a promover el concepto de un sistema panamericano dirigido por el gobierno norteamericano en lo económico se buscaría una unión aduanera y en lo político, se trataría de establecer un sistema de arbitraje obligatorio, a través del cual Estados Unidos asumiría el puesto de gran juez.

Ninguna de las dos propuestas iniciales de Estados Unidos fue aprobada. Como comenta Boersner: “los delegados latinoamericanos estaban conscientes de que la primera iniciativa alteraba su soberanía, mientras que la segunda propuesta traería beneficios únicamente a la potencia del norte*.” (p.187)* recién en 1889 los Estados americanos decidieron reunirse de manera periódica y comenzar a forjar un sistema común de normas e instituciones.

Dieciocho Estados americanos participaron de esta Conferencia, en la que se acordó establecer una Unión Internacional de Repúblicas Americanas, con sede en Washington, D.C., “por medio de la cual se pueda obtener la pronta y exacta publicación, a costa y en provecho común, de datos comerciales importantes”.

La segunda Conferencia Interamericana se llevó a cabo en la Ciudad de México por iniciativa del Ministro de Relaciones Exteriores Mexicano. Dicha conferencia se celebró entre el 22 de octubre de 1901 y el 31 de enero de 1902, participaron representantes de 19 naciones. Se estableció una corte de arbitraje para la solución pacífica de controversias con la participación de todos los miembros de la Unión. (Fenwick, 1963, p.73)

La tercera Conferencia se llevó a cabo en 1906 en Río de Janeiro Brasil. Con la presencia de los gobiernos que habían asistido a México. Según Fenwick esta conferencia no tuvo grandes avances en materia de integración regional, pero por primera vez contó con la ratificación del gobierno de los Estados Unidos. (1963, p. 77)

En 1933 se llevó a cabo una nueva Conferencia Interamericana en Montevideo, Uruguay. El avance más importante de esta conferencia fue la firma de la Convención sobre derechos y obligaciones de los estados que tenía como objetivo la protección a la soberanía nacional y por lo tanto prohibía a cualquier otro el intervenir en asuntos internos (Franco J. 1968, p.4). En las siguientes conferencias, el tema principal fue la cooperación en defensa y acuerdos que reafirmaran la paz en el área. Durante la Conferencia de Paz de Buenos Aires se decretaron acuerdos sobre la neutralidad en caso de conflicto y reacción común en caso de agresión externa a alguna nación del continente.

En la Ciudad de México se llevó a cabo la “Conferencia sobre Problemas de la Guerra y de la Paz”, para discutir problemas de seguridad recíproca de cara al final de la Segunda Guerra Mundial. Según la Secretaría de Relaciones Exteriores de México, el Acta de Chapultepec era un documento de singular importancia en el derecho americano que consagró el principio de que todo atentado contra la integridad o la inviolabilidad del territorio o contra la soberanía o independencia política de un Estado americano, será considerado como un acto de agresión contra todos los demás Estados americanos.

El Tratado Interamericano de Asistencia Recíproca (TIAR) quedó finalmente establecido en 1947 en la ciudad de Río de Janeiro en el marco de la guerra fría. El tratado surgió como resultado de todas estas negociaciones previas y a la vez se consolidó como el primer instrumento tangible de vinculación en el área y representó el antecedente más próximo a lo que posteriormente sería la creación de la Organización de los Estados Americanos, el Organismo de Cooperación Regional más serio hasta el momento en el continente. (Fenwick, 1963 p.103) Surgió con el fin de asegurar la legítima defensa colectiva ante un eventual ataque de una potencia de otra región y decidir acciones conjuntas en caso de un conflicto entre dos Estados partes del Tratado.

La Novena Conferencia Internacional Americana, que reunió a 21 Estados en Bogotá, Colombia, en 1948, adoptó la Carta de la Organización de los Estados Americanos, el Tratado Americano de Soluciones Pacíficas (“Pacto de Bogotá) y la Declaración Americana de los Derechos y Deberes del Hombre. En la misma, se aprobó el Convenio Económico de Bogotá, que se propuso fomentar la cooperación económica entre los Estados americanos, pero que nunca entró en vigencia.

De la misma manera que la Carta de la OEA, el Pacto de Bogotá obliga a las Altas Partes Contratantes a resolver las controversias entre los Estados americanos por medios pacíficos y enumera una lista de procedimientos a seguir: buenos oficios y mediación, investigación y conciliación, y arbitraje. Si no se logra una solución mediante el procedimiento de conciliación establecido, las partes tienen derecho a recurrir a la Corte Internacional de Justicia. De hecho, algunas controversias han llegado hasta esta instancia.

La Carta de 1948 ha sido modificada mediante Protocolos de Reformas en cuatro oportunidades: Buenos Aires, en 1967; Cartagena de Indias, en 1985; Washington, en 1992, y Managua, en 1993.

Si bien no están previstas en la Carta, desde 1994 se han celebrado Cumbres de Jefes de Estado y de Gobierno de las Américas, que constituyen foros políticamente importantes en los que se emiten decisiones y recomendaciones, generalmente en forma de una Declaración y Plan de Acción, respecto de los objetivos que deben cumplir las organizaciones del sistema interamericano, especialmente la OEA.

La OEA también se desempeña como secretaría de varias reuniones ministeriales, en particular de las reuniones de Ministros de Justicia, Trabajo, Ciencia y Tecnología y Educación de las Américas.

Además de la Organización de Estados Americanos [1], gradualmente se estableció un conjunto de instituciones con miras a facilitar la cooperación y emprender una importante labor en esferas específicas. Después del establecimiento de la OEA, se crearon, entre otros, el Banco Interamericano de Desarrollo, la Comisión Interamericana de Derechos Humanos, la Corte Interamericana de Derechos Humanos, la Comisión Interamericana para el Control del Abuso de Drogas, la Comisión Interamericana de Telecomunicaciones, la Comisión Interamericana de Puertos y el Centro de Estudios de Justicia de las Américas. En 1923 se propuso establecer una Corte Interamericana de Justicia. Si bien ésta nunca se materializó, sirvió de precedente para la Corte Centroamericana de Justicia, que funcionó desde 1907 hasta 1918. De esta manera se creó una red de instituciones internacionales regionales para fortalecer la cooperación entre los Estados americanos en una amplia variedad de temas de la agenda regional.

2.2. Organización de Estados Americanos

La Organización de los Estados Americanos (OEA) es una organización internacional de ámbito regional y continental creado el 8 de mayo de 1948, con la finalidad ser un mecanismo para el diálogo multilateral, integración y la toma de decisiones de ámbito

[1] Nuestra Historia (2013) de http://www.oas.org/es/acerca/nuestra_historia.asp .

americano.[2] La organización es creada el objeto de alcanzar propósitos comunes como la paz, justicia, solidaridad y respeto a la soberanía.

2.2.1. Propósitos:

La Organización de los Estados Americanos, para realizar los principios en que se funda y cumplir sus obligaciones regionales de acuerdo con la Carta de las Naciones Unidas, establece los siguientes propósitos esenciales:

a. Afianzar la paz y la seguridad del Continente;

b. Promover y consolidar la democracia representativa dentro del respeto al principio de no intervención;

c. Prevenir las posibles causas de dificultades y asegurar la solución pacífica de controversias que surjan entre los Estados miembros;

d. Organizar la acción solidaria de éstos en caso de agresión;

e. Procurar la solución de los problemas políticos, jurídicos y económicos que se susciten entre ellos;

f. Promover, por medio de la acción cooperativa, su desarrollo económico, social y cultural;

2.2.2. Principios:

Según la Carta de la Organización de Estados Americanos (Cap II. Principios. P.8) Los Estados americanos reafirman los siguientes principios:

a. El derecho internacional es norma de conducta de los Estados en sus relaciones recíprocas.

b. El orden internacional está esencialmente constituido por el respeto a la personalidad, soberanía e independencia de los Estados y por el fiel cumplimiento de

[2] Quienes Somos (2013) de http://www.oas.org/es/acerca/quienes_somos.asp

las obligaciones emanadas de los tratados y de otras fuentes del derecho internacional.

c. La buena fe debe regir las relaciones de los Estados entre sí.

d. La solidaridad de los Estados americanos y los altos fines que con ella se persiguen, requieren la organización política de los mismos sobre la base del ejercicio efectivo de la democracia representativa.

e. La agresión a un Estado americano constituye una agresión a todos los demás Estados americanos.

f. Las controversias de carácter internacional que surjan entre dos o más Estados americanos deben ser resueltas por medio de procedimientos pacíficos.

g. La justicia y la seguridad sociales son bases de una paz duradera.

2.2.3. Miembros de la Organización:

Los 35 países independientes de las Américas han ratificado la Carta de la OEA y pertenecen a la Organización.

Miembros originales: Los siguientes veintiún países se reunieron en Bogotá en 1948 para la firma de la Carta de la OEA: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba (suspendida entre 1962-2009, reincorporada pero aún no participa), Ecuador, El Salvador, Estados Unidos de América, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Uruguay y Venezuela (República Bolivariana de).

Miembros posteriores: Barbados, Trinidad y Tobago, Jamaica, Grenada, Suriname , Dominica, Santa Lucía, Antigua y Barbuda, San Vicente y las Granadinas , Bahamas, St. Kitts y Nevis, Canadá, Belice, Guyana.

2.2.4. Pilares Fundamentales

La OEA apoya los esfuerzos de sus Estados Miembros por reducir la pobreza y lograr el desarrollo económico. Utiliza cuatro pilares para ejecutar efectivamente estos propósitos esenciales:

· Consolidación de las democracias
· Fortalecimiento de los Derechos Humanos
· Confrontación de amenazas a la seguridad hemisférica
· Desarrollo.[3]

2.2.5. Estructura

La OEA realiza sus fines por medio de los siguientes órganos:

- **Asamblea General:**

Es el órgano supremo de la Organización de los Estados Americanos y está compuesta por las delegaciones de todos los Estados Miembros, quienes tienen derecho a hacerse representar y a emitir su voto.

La definición de los mecanismos, políticas, acciones y mandatos de la Organización tienen su origen en la Asamblea General. Sus atribuciones se encuentran definidas en el Capítulo IX de la Carta.

- **Reunión de Consulta de Ministros de Relaciones Exteriores**

Dicha reunión se celebra con el fin de considerar problemas de carácter urgente y de interés común para los Estados americanos, y para servir de Órgano de Consulta en la aplicación del Tratado Interamericano de Asistencia Recíproca (TIAR), que es el principal instrumento para la acción solidaria en caso de agresión.

- **Consejos**

[3] Que Hacemos (2013) de http://www.oas.org/es/acerca/que_hacemos.asp

El Consejo Permanente de la Organización y el Consejo Interamericano para el Desarrollo Integral, dependen directamente de la Asamblea General y tienen la competencia que a cada uno de ellos asignan la Carta y otros instrumentos interamericanos, así como las funciones que les encomienden la Asamblea General y la Reunión de Consulta de Ministros de Relaciones Exteriores.

-Consejo Permanente

Vela por el mantenimiento de las relaciones de amistad entre los Estados Miembros y, con tal fin, ayuda de una manera efectiva en la solución pacífica de sus controversias. Prepara, a petición de los Estados Miembros, proyectos de acuerdo para promover y facilitar la colaboración entre la OEA y la ONU y otros organismos americanos. Formula recomendaciones a la Asamblea General sobre el funcionamiento de la Organización y la coordinación de sus órganos subsidiarios, organismos y comisiones.

-Consejo Interamericano para el Desarrollo Integral (CIDI)

Es un órgano de la Organización que depende directamente de la Asamblea General, con capacidad decisoria en materia de cooperación solidaria para el desarrollo integral, que se estableció con la entrada en vigencia del Protocolo de Managua el 29 de enero de 1996 (Capítulo XIII).

- **Comité Jurídico Interamericano**

Es uno de los órganos por medio de los cuales la OEA realiza sus fines (Art. 53 de la Carta). El Capítulo XIV de la Carta define su composición, atribuciones y funciones de la siguiente forma: sirve de cuerpo consultivo de la Organización en asuntos jurídicos; promueve el desarrollo progresivo y la codificación del derecho internacional; y estudia los problemas jurídicos referentes a la integración de los países para el desarrollo del Hemisferio.

- **Comisión Interamericana de Derechos Humanos (CIDH)**

La Comisión Interamericana de Derechos Humanos es uno de los dos órganos del Sistema Interamericano responsables de la promoción y protección de los derechos humanos. Está integrada por siete miembros, elegidos por la Asamblea General, quienes ejercen sus funciones con carácter individual por un período de cuatro años, reelegibles por una sola vez.

- **Secretaría General**

Según la Carta de Organización Estados Americanos. (Cap XVI. La Secretaría General. Art. 112). Es el órgano central y permanente de la Organización de los Estados Americanos. La Secretaría General desempeña además las siguientes funciones:

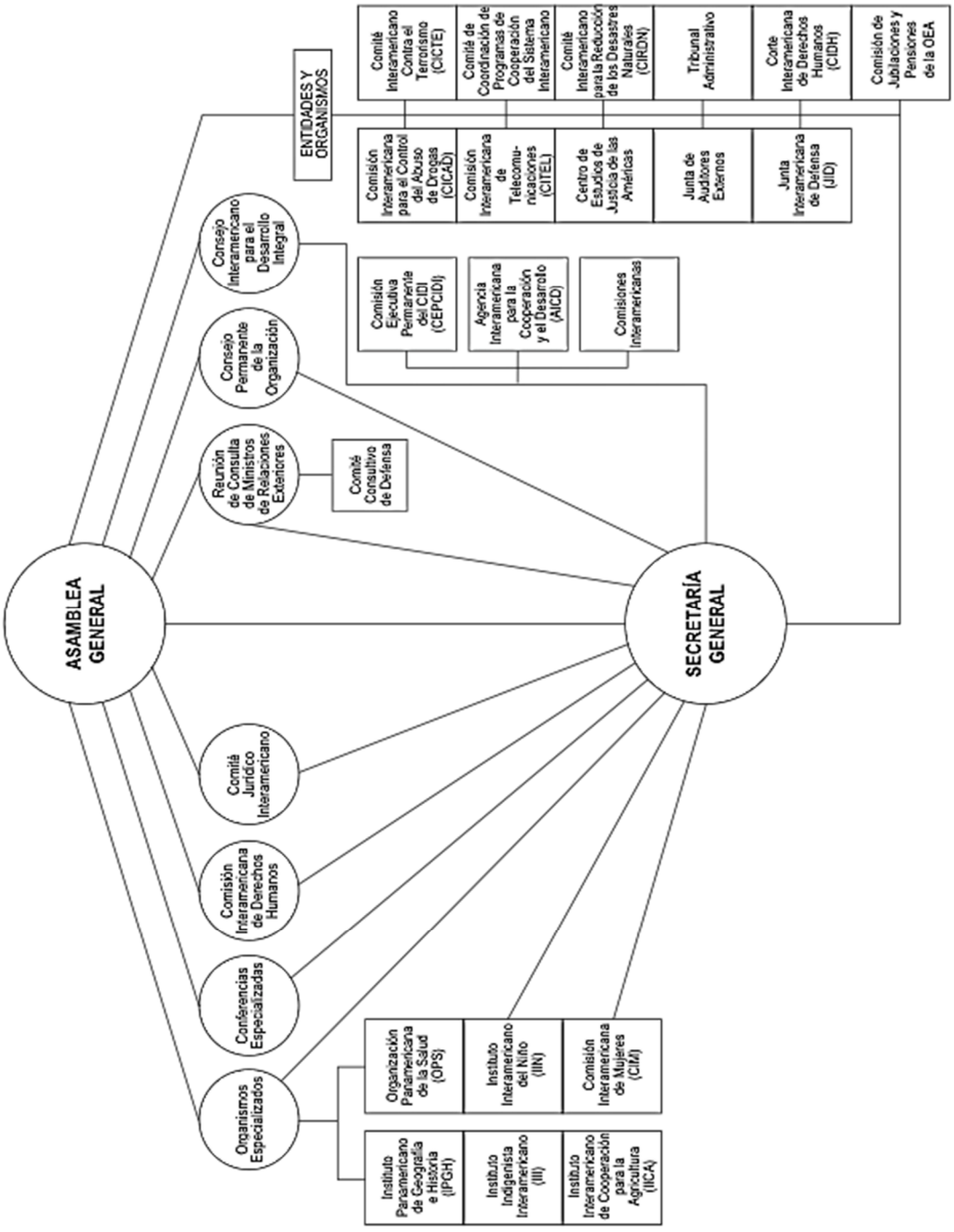
- Asesorar a los otros órganos, según corresponda, en la preparación de los temarios y reglamentos;
- Preparar el proyecto de programa-presupuesto de la Organización
- Proporcionar a la Asamblea General y a los demás órganos servicios permanentes y adecuados de secretaría y cumplir sus mandatos y encargos.
- Servir de depositaria de los tratados y acuerdos interamericanos, así como de los instrumentos de ratificación de los mismos;
- Establecer relaciones de cooperación, de acuerdo con lo que resuelva la Asamblea General o los consejos, con los Organismos Especializados y otros organismos nacionales e internacionales.

- **Conferencias Especializadas**

Son reuniones intergubernamentales para tratar asuntos técnicos especiales o para desarrollar determinados aspectos de la cooperación interamericana. Disfrutan de amplia autonomía técnica, dentro del marco de las recomendaciones de la Asamblea General y de los Consejos.

Imagen No. 1

Organigrama Estructura de la Organización de Estados Americanos OEA



Fuente: página Web institucional www.oas.org/es

2.3. Comité Interamericano Contra el Terrorismo

El Comité Interamericano contra el Terrorismo (CICTE) tiene como propósito principal promover y desarrollar la cooperación entre los Estados Miembros para prevenir, combatir y eliminar el terrorismo, de acuerdo con los principios de la Carta de la OEA, con la Convención Interamericana contra el Terrorismo, y con pleno respeto a la soberanía de los países, al estado de derecho y al derecho internacional, incluidos el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho internacional de los refugiados.

El CICTE está integrado por todos los Estados Miembros de la OEA y organiza una sesión regular anual, a través de un foro de discusión y toma de decisiones en temas contra el terrorismo, medidas y de cooperación. Los Estados Miembros designan a las autoridades nacionales competentes, al representante titular, a los suplentes y a los asesores que estime conveniente para representarlo ante el CICTE. Los Estados Miembros designan también uno o más puntos de contacto nacionales con competencia en materia de prevención y eliminación del terrorismo, para servir como el principal enlace entre los gobiernos de los Estados Miembros para desarrollar la cooperación entre los mismos y el CICTE.

2.3.1 Origen

Los actos de terrorismo no son nuevos en las Américas. Durante los años 1990, los cambios en el modus operandi y nacionalidad de esos actores produjeron una llamada de atención entre los gobiernos del hemisferio occidental. A consecuencia de ello, llevaron a cabo una serie de reuniones en las que se comprometieron a "prevenir, combatir y eliminar el terrorismo" –la Primera Cumbre de las Américas, celebrada en 1994, la Primera Conferencia Especializada en Terrorismo, celebrada en Lima en 1996 (Declaración de Lima), y una Segunda Conferencia Especializada en Terrorismo, celebrada en Mar del Plata en 1998. Esta última

concluyó con la adopción del llamado Compromiso de Mar del Plata, el cual urgía al establecimiento, dentro de la Organización de los Estados Americanos, de un “Comité Interamericano contra el Terrorismo” compuesto de las “competentes autoridades nacionales” de sus Estados Miembros. Este esfuerzo fue reafirmado por los jefes de Estado del hemisferio a través del Plan de Acción surgido en el contexto de la Segunda Cumbre de las Américas, celebrada en Chile en 1998.

En 1999, la Asamblea General respaldó las recomendaciones y decisiones contenidas en el Compromiso de Mar Del Plata y estableció el CICTE mediante la resolución AG/RES. 1650. El primer período ordinario de sesiones del CICTE se realizó en Miami, Florida en Octubre de 1999 y durante el mismo se desarrolló un plan de trabajo. Ninguna sesión fue programada en 2001.

Los acontecimientos del 11 de septiembre de 2001 provocaron la adopción de un nuevo enfoque sobre los esfuerzos interamericanos para hacer frente al terrorismo. Los ataques fueron inmediatamente condenados por la Asamblea General, la cual estaba reunida en Sesión Especial en Lima, Perú, para aprobar la Carta Democrática Interamericana. El 21 de septiembre de 2001, durante la 23 Reunión de Consulta de Ministros de Relaciones Exteriores, llevada a cabo en Washington D.C., los ministros adoptaron la Resolución para el Fortalecimiento de la Cooperación Hemisférica para Prevenir, Combatir y Eliminar el Terrorismo.

Inmediatamente después, los Ministros de Relaciones Exteriores volvieron a reunirse durante la 24 Reunión de Consulta y aprobaron la Resolución "Amenaza Terrorista en las Américas” declarando que “Estos ataques terroristas contra los Estados Unidos de América son ataques contra todos los Estados americanos” e invocando el Tratado Interamericano de Asistencia Recíproca (TIAR – Tratado de Río).

La resolución RC.23/RES.1/01 incluía entre otros asuntos las siguientes acciones pertinentes al CICTE:

- Exhortar a todos los Estados Miembros a reforzar la cooperación, en los planos regional e internacional, para perseguir, capturar, enjuiciar, sancionar y cuando corresponda, acelerar la extradición de los perpetradores, organizadores y patrocinadores de actos terroristas, así como fortalecer la cooperación judicial recíproca y el intercambio oportuno de información.
- Instruir al Consejo Permanente para que convoque lo antes posible una reunión del Comité Interamericano contra el Terrorismo, a fin de que identifique acciones urgentes dirigidas a fortalecer la cooperación interamericana para prevenir, combatir y eliminar el terrorismo en el hemisferio.
- Encomendar al Consejo Permanente la elaboración de un proyecto de Convención Interamericana contra el Terrorismo, con miras a presentarlo a la próxima Asamblea General de la OEA. Asimismo, instar a los Estados a estudiar la repercusión jurídica internacional de la conducta de las autoridades gubernamentales que apoyan con financiamiento, protección o amparo a personas y grupos terroristas.

En vista de estas y otras resoluciones posteriores de los órganos del Sistema Interamericano, el CICTE realizó dos sesiones extraordinarias el 15 de octubre de 2001 y el 29 de noviembre de 2001. Entre estas sesiones, tres subcomités (Controles Financieros, Controles Fronterizos y Plan de Trabajo) trabajaron diligentemente a fin de identificar acciones antiterroristas a ser implementadas por los Estados Miembros de la OEA, al nivel regional, sub-regional y nacional, y para redactar una agenda concreta pero ambiciosa para el CICTE, a ser cumplida en 2002-2003.

En la Segunda Sesión Ordinaria del CICTE realizada el 28 y 29 de enero de 2002 en Washington, DC, los ministros del Interior y Seguridad Pública y los demás jefes de delegaciones informaron sobre las medidas adoptadas por sus respectivos países para implementar la Resolución RC 23 del 21 de septiembre. El 30 de enero, los expertos en políticas de los Estados Miembros participaron en un

Ejercicio de simulación de Desarrollo de Políticas auspiciado por Estados Unidos para examinar los posibles cursos de acción en respuesta a un escenario terrorista.

En el año 2002, el CICTE estableció un Secretariado Ejecutivo en el marco del Secretariado General de la OEA. El Secretariado del CICTE fue integrado con tres Adscriptos al mismo, en representación de los gobiernos de El Salvador, Estados Unidos y Uruguay respectivamente. El Secretario General de la OEA designó un Secretario Ejecutivo en octubre del 2002, para dirigir las tareas del Secretariado. Durante el año 2002, el Secretariado del CICTE ha diseñado y desplegado una Base de Datos on-line del CICTE, en apoyo al plan de trabajo 2002-2003. Adicionalmente el CICTE ha participado en la confección de los borradores de reglamentos modelos con el Grupo de Expertos del CICAD-OEA. El CICTE ha participado también en diversos encuentros del Comité Contraterrorismo de Consejo de Seguridad de la ONU (CTC) y otras organizaciones internacionales y regionales.

Un éxito fundamental en 2002 fue la ***elaboración y firma de la Convención Interamericano contra el Terrorismo AG/RES. 1840 Convención Interamericana contra el Terrorismo.*** Este documento capital fue firmado por 30 Estados Miembros durante la Asamblea General de la OEA en Bridgetown, Barbados, el día 3 de junio, y entró en vigor en julio de 2003. A fecha de noviembre de 2006, 22 Estados Miembros son Estados Parte de la Convención.

Desde 2002, la Secretaría del CICTE ha desarrollado una amplia gama de actividades de asistencia técnica y de programas de fortalecimiento de capacidades para apoyar a los Estados Miembros de la OEA para prevenir, combatir y eliminar el terrorismo. Hoy, existen 10 programas, los cuales están divididos en seis amplias áreas: controles fronterizos, controles financieros, protección de infraestructura crítica, asistencia legislativa y consultas, ejercicios de gestión de crisis, y desarrollo de políticas y coordinación internacional. Este último

está centrado en promover la cooperación internacional y la coordinación con otras organizaciones internacionales, regionales y sub-regionales, así como con el sector privado.[4]

2.3.2. Misión

El Comité Interamericano contra el Terrorismo (CICTE) tiene como propósito principal promover y desarrollar la cooperación entre los Estados Miembros para prevenir, combatir y eliminar el terrorismo, de acuerdo con los principios de la Carta de la OEA, con la Convención Interamericana contra el Terrorismo, y con pleno respeto a la soberanía de los países, al estado de derecho y al derecho internacional, incluidos el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho internacional de los refugiados.

2.3.3. Estructura y Funciones

El CICTE está integrado por todos los Estados Miembros de la OEA y organiza una sesión regular anual, un foro de discusión y toma de decisiones en temas de contra terrorismo, medidas y cooperación. Los Estados Miembros designan a las autoridades nacionales competentes, al representante titular, a los suplentes y a los asesores que estime conveniente para representarlo ante el CICTE. Los Estados Miembros designan también uno o más puntos de contacto nacionales con competencia en materia de prevención y eliminación del terrorismo, para servir como el principal enlace entre los gobiernos de los Estados Miembros para desarrollar la cooperación entre los mismos y el CICTE.

El CICTE tiene un presidente y un vicepresidente que serán elegidos entre los Estados Miembros cuyos cargos tendrán una duración de un año.

El Secretario General de la Organización de los Estados Americanos (OEA) designa al Secretario del CICTE para dirigir la Secretaría, la cual está localizada en las oficinas principales de la OEA en Washington, D.C., con el fin de cumplir con los

[4] Acerca de Nosotros (2013) de http://www.oas.org/es/sms/cicte/acerca_nosotros_historia.asp

mandatos establecidos por los Estados Miembros en el Plan de Trabajo del CICTE, la Secretaría:

- Proporciona soporte técnico y administrativo para las sesiones del CICTE y mantiene la comunicación y coordinación entre las sesiones
- Proporciona asistencia técnica y capacitación a los Estados Miembros en respuesta de sus necesidades y solicitudes
- Coordina con otras organizaciones internacionales, regionales y subregionales.

2.3.4. Programas

El Comité Interamericano Contra el Terrorismo trabaja en conjunto en una serie de programas con la finalidad de alcanzar la mayor calidad en seguridad desde un aspecto técnico y práctico a nivel local y regional, tomando siempre en cuenta el respeto a la soberanía como uno de sus pilares fundamentales.

2.3.4.1 Controles Fronterizos

- **Seguridad Aeroportuaria**

El Programa de Seguridad Aeroportuaria tiene como objetivo fortalecer las capacidades de los Estados Miembros de la OEA para cumplir con los estándares relacionados a la protección de la aviación civil internacional y sus instalaciones, para prevenir y combatir posibles actos de terrorismo como también otros actos de interferencia legal.

- **Seguridad de Documentos y Prevención de Fraude**

El objetivo principal es fortalecer la seguridad en la emisión y control de documentos de viaje e identidad en los Estados Miembros de la OEA. Esto incluye fomentar el desarrollo de sistemas nacionales de gestión de identidad integrados y seguros, así como un control más efectivo sobre el uso de estos documentos, con el fin de detectar el uso fraudulento de los mismos.

- **Inmigración y Aduanas**

El programa de inmigración y aduanas tiene como objetivo el entrenamiento de los funcionarios de control fronterizo para mejorar su conocimiento y habilidades en el combate contra las drogas, trata de personas y otras formas de tráfico ilícito para mejorar sus controles sobre el movimiento de personas y mercancías en los aeropuertos de su país, los puertos marítimos y las fronteras terrestres, y para coordinar más eficazmente con otras entidades, incluyendo las fiscales.

- **Implementación de UNSCR 1540. Protección y Control de Materiales Nucleares, Biológicos, Químicos y Radiológicos**

El objetivo principal del Programa Implementación de la Resolución 1540 (2004) del Consejo de Seguridad de las Naciones Unidas es el de identificar necesidades y retos concretos que los países beneficiarios puedan identificar en materia de protección y control de materiales Nucleares, Biológicos, Químicos y Radiológicos

Desde el 2006, ha proporcionado, conjuntamente con sus socios internacionales, actividades de fortalecimiento de las capacidades y de asistencia técnica a los Estados Miembros con el fin de prevenir, combatir y eliminar el terrorismo y hacer frente a la amenaza planteada por el uso de armas de destrucción masiva por parte de terroristas y actores no- estatales en general.

- **Seguridad Marítima**

El Programa de Seguridad Marítima tiene como objetivo proporcionar asistencia técnica y capacitación a los Estados Miembros para ayudarles a cumplir con las normas de la Organización Marítima Internacional (OMI) y otros estándares internacionales para la protección portuaria. Los objetivos del CICTE son fortalecer la lucha contra el terrorismo y la capacidad de hacer cumplir la ley dentro de las instalaciones portuarias y a su vez mejorara la coordinación entre las autoridades gubernamentales competentes encargadas de la seguridad marítima.

2.3.4.2. Programas de Cooperación Internacional y Alianzas

La Secretaría del CICTE sirve en nombre de los Estados Miembros de la OEA como centro de intercambio de información y asistencia técnica en políticas y programas contra el terrorismo. Con este fin, la Secretaría promueve la coordinación con diferentes socios internacionales como las Naciones Unidas (UNCTED, ONUDD, UNICRI), otras organizaciones internacionales (OACI, OMI, INTERPOL), organizaciones regionales (APEC, OSCE, el Consejo de Europa, la Secretaría del Commonwealth), organizaciones subregionales (CARICOM, SICA), y las agencias técnicas de importantes donantes, como el Departamento de Seguridad de EEUU (Guardia Costera, la Administración de Seguridad del Transporte, el Servicio de Aduanas y Protección de Fronteras), Canadá (Transportes Canadá, la Agencia para Servicios Fronterizos de Canadá), España e Israel. Una red de Puntos de Contacto Nacionales de cada país sirve como medio de comunicación entre ellos y con la Secretaría de CICTE, en asuntos técnicos.

2.3.4.3. Asistencia Legislativa y Lucha Contra el Financiamiento del Terrorismo

La Secretaría del CICTE ofrece actividades de asistencia técnica y fortalecimiento de las capacidades a los Estados Miembros con el fin de apoyarles en el proceso de ratificación e implementación como legislación nacional, de los instrumentos legales internacionales contra el terrorismo—incluida la Resolución 1373 del Consejo de Seguridad de la ONU (2001), la Convención Interamericana contra el Terrorismo (CIACT), y los 18 instrumentos jurídicos universales—, así como de otros estándares internacionales como las nuevas 40 Recomendaciones contra el Lavado de Activos y la Financiación del Terrorismo del Grupo de Acción Financiera (GAFI).

Las actividades se implementan a través de dos sub-programas: ***Asistencia Legislativa y Lucha contra el Financiamiento del Terrorismo.*** El programa de Asistencia Legislativa engloba tres tipos de actividades: 1) misiones de asistencia técnica legislativa—es decir, consultas con altos funcionarios y cargos de los tres poderes del Estado, y talleres nacionales con legisladores; 2) capacitaciones nacionales especializadas con fiscales, jueces y agentes del orden; y 3) actividades

regionales o subregionales (por ejemplo, capacitaciones o conferencias ministeriales).

Las actividades del CICTE en este programa están implementadas principalmente a través de una asociación estratégica con la Subdivisión para la Prevención del Terrorismo de la Oficina de las Naciones Unidas contra la Droga y el Delito y con la Unidad Anti-Lavado de Activos de la Comisión Interamericana para el Control del Abuso de Drogas.

2.3.4.4. Fortaleciendo Estrategias Sobre Amenazas Terroristas Emergentes

El objetivo del Programa Fortaleciendo Estrategias sobre Amenazas Terroristas Emergentes es, fortalecer las capacidades de los Estados Miembros para prepararse mejor para enfrentar de manera coordinada, potenciales amenazas terroristas.

Este programa se desarrolla a través de una serie de "***ejercicios de simulación***" que reúnen a las autoridades de alto nivel responsables de tomar decisiones de los Estados Miembros con el objetivo de destacar temas específicos de planificación de contingencias y reducción de amenazas. Juntos a los especialistas en materia contra el terrorismo, participan en un simulacro basado en el escenario de un ataque terrorista diseñado sobre la base de las particularidades de un Estado o grupo de Estados. Cada escenario destaca una potencial amenaza terrorista específica y requiere que los participantes elaboren soluciones en tiempo real para los problemas que se les presenten. Después de cada ejercicio se lleva a cabo una discusión durante la cual las autoridades recibirán evaluaciones profesionales que les ayudarán a mejorar su planeamiento de contingencias nacionales y coordinación.

2.3.4.5. Protección de Infraestructura Crítica

La Secretaría del CICTE emplea un enfoque integral en la construcción de capacidades de seguridad cibernética entre los Estados Miembros, reconociendo que

la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio.

Dado a que la realidad de cada país es diferente, las necesidades en el área de la seguridad cibernética también lo son. Por este motivo, la Secretaría del CICTE junto con autoridades gubernamentales en cada país de las Américas realizan una evaluación de las necesidades específicas, y basados en estos resultados se procede a iniciar con un proceso que permita apoyar el fortalecimiento de cada Estado Miembro en esta área. En todo caso, cada solicitud de asistencia técnica es especialmente examinada, y en la mayoría de los casos, la Secretaría del CICTE es capaz de proporcionar el apoyo y asistencia requerida.

- **Programa de Seguridad Cibernética**

La Secretaría del CICTE ha trabajado en mejorar las capacidades de los Estados Miembros en materia de seguridad cibernética desde la Tercera Sesión Ordinaria del CICTE en 2003. En la Asamblea General de la OEA en 2004, 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), proporcionando así el mandato que permite a la Secretaría del CICTE trabajar en asuntos de Seguridad Cibernética.

Entre los principales objetivos de la Secretaría, se encuentran el establecimiento de grupos nacionales de "alerta, vigilancia y prevención", también conocidos como Equipos de Respuesta a Incidentes (CSIRT) en cada país; crear una red de alerta Hemisférica que proporciona a formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas; promover el desarrollo de

Estrategias Nacionales sobre Seguridad Cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio.[5]

Los principales esfuerzos de la Secretaría están orientados a desarrollar y mejorar las capacidades que se refieren sobre todo a la vigilancia, prevención y lucha contra las amenazas de seguridad cibernética, en respuesta a incidentes cibernéticos, y la coordinación efectiva tanto a nivel nacional y regional.

Con la finalidad de alcanzar este objetivo, la Estrategia de Seguridad Cibernética de la OEA y el Plan de Trabajo del CICTE han encomendado a la Secretaría el proveer asistencia técnica a los Estados Miembros, generar conciencia en temas de seguridad cibernética, facilitar la creación y el desarrollo de CSIRT nacionales, y promover la creación de una Red Hemisférica de CSIRT y expertos en seguridad cibernética.

Desde el 2007, la Secretaría del CICTE se ha esforzado en construir un programa comprehensivo de desarrollo de capacidades, el cual ha estado basado en conferencias, cursos técnicos, talleres, mesas de discusión entre desarrolladores de políticas de seguridad cibernética, entre otras actividades, las cuales han permitido desarrollar y fortalecer la agenda de la Seguridad Cibernética en las Américas. Entre los resultados que podemos ver de estos esfuerzos se puede evidenciar el creciente número de CSIRTs Nacionales (tanto privados como públicos), los cuales han aumentado de 4 a 16 en los últimos cinco años. De la misma forma, el Programa de Seguridad Cibernética de la Secretaría del CICTE ha venido implementando una serie de misiones de asistencia técnica nacionales especializadas, enfocándose en las necesidades y características específicas de los diferentes países de la región.

En marzo de 2012, el CICTE adoptó el “Fortalecimiento de la Seguridad Cibernética en las Américas” como tema central de su decimosegundo Período Ordinario de

[5] Seguridad Cibernética (2013) Sitio oficial http://www.oas.org/es/ssm/cyber/default.asp

Sesiones. Durante esta período de sesiones, el CICTE reiteró la importancia de reforzar la seguridad y la resistencia de tecnologías de infraestructura crítica de información y comunicaciones (TIC) ante las ciber amenazas, con especial énfasis en las instituciones gubernamentales críticas así como en los sectores críticos para la seguridad nacional, incluyendo los sistemas de energía, financieros, transporte y telecomunicaciones. Entre las acciones que fueron encomendadas en el 2012 al Programa de Seguridad Cibernética del CICTE se encuentran la de crear una plataforma que permita la participación, cooperación e intercambio de información de los interesados del sector público y privado, así como de otros actores que trabajen en aspectos de seguridad cibernética, así como apoyar a los Estados Miembros a desarrollar campañas nacionales que aborden buenas y seguras prácticas para el uso de tecnologías de la información y la comunicación.

-Objetivos

- Desarrollar la capacidad de los Estados miembros para cumplir efectivamente con los principios establecidos en la Estrategia Interamericana de la OEA para combatir la Amenazas de Seguridad cibernética.
- Ayudar a los Estados miembros en la adopción de estrategias nacionales de seguridad cibernética
- Facilitar la creación de una red hemisférica de CSIRT para promover el intercambio de información y buenas prácticas
- Promover la inclusión de la sociedad civil, el sector privado y a los usuarios finales en temas relacionados a la seguridad cibernética
- Fortalecer alianzas con otras organizaciones que trabajan en temas de seguridad cibernética en la región

-Modo de Trabajo

Dado a que la realidad de cada país es diferente, las necesidades en el área de la seguridad cibernética también lo son. Por este motivo, la Secretaría del CICTE junto

con autoridades gubernamentales en cada país de las Américas realizan una evaluación de las necesidades específicas, y basados en estos resultados se procede a iniciar con un proceso que permita apoyar el fortalecimiento de cada Estado Miembro en esta área. En todo caso, cada solicitud de asistencia técnica es especialmente examinada, y en la mayoría de los casos, la Secretaría del CICTE es capaz de proporcionar el apoyo y asistencia requerida.[6]

[6] Como Trabajamos (2013) http://www.oas.org/es/ssm/cyber/acerca _de_nosotros_como_trabajamos .asp

CAPITULO III

TERRORISMO, ACTORES Y EL ESTADO COMO BLANCO

3.1. Antecedentes del Terrorismo

Existen discrepancias entre diversos autores acerca del origen del terrorismo, por ejemplo José Juan Olloqui en Reflexiones en Torno al Terrorismo (2004, p. 51) afirma que el terrorismo es un fenómeno moderno, que las guerras y enfrentamientos en la antigüedad eran percibidos como sucesos cotidianos. Asimismo que al no existir la figura del Estado, no existía una responsabilidad definida para la protección de la sociedad civil de ataques como los de los terroristas.

William F. Shughart II (2006, p. 35) efectúa un resumen de la evolución del terrorismo moderno desde la Segunda Guerra Mundial hasta el año 2000, que se divide en 3 etapas: terrorismo al servicio de los separatismos de liberación nacional y étnica, terrorismo de izquierdas y terrorismo islamista.

Por otra parte, Rapoport (2004, p. 47) distingue cuatro grandes oleadas, cada una de las cuales ha cerrado un ciclo de violencia cuya duración aproximada ha sido de cuatro décadas, que se corresponden con el ciclo de vida de una generación. Estas son: la ola anarquista -que se extendió entre 1880 y la década de los veinte en el siglo XX-, la ola anticolonial -que sustituyó a la anterior y tuvo su cierre al finalizar el decenio de los cincuenta-, la ola del terrorismo de la nueva izquierda –que nace en los años sesenta, principalmente, tras la revolución de mayo de 1968 y se agota con el final de la guerra fría- dentro de la cual se inscribe el terrorismo nacionalista de izquierda que todavía persiste en España, Sri Lanka y Colombia, y finalmente la ola religiosa –que comenzó en 1979, con la revolución iraní, y llega hasta nuestros días. Se espera que esta pueda desaparecer alrededor del año 2025 para dar lugar al origen de una nueva ola.

Sin embargo para fines del presente estudio se describirán los sucesos históricos violentos e intimidatorios mas relevantes que han generado terror en la población y sus gobernantes. Analizando así que el terrorismo no es una práctica reciente ni

desorganizada, sino un medio para alcanzar diversos objetivos tanto a nivel nacional como internacional.

En el año 0 D.C. una secta judía llamada “Zelotes” llevaban a cabo campañas de terror y violencia para forzar al pueblo a una rebelión en contra de los romanos en oposición al régimen de Herodes El Grande. El registro histórico de su actividad se remonta hasta el segundo siglo de nuestra era.

En el Siglo XII un grupo de musulmanes chiíes llamados “Asesinos” emprendían acciones terroristas contra musulmanes sunníes, para luego suicidarse inmediatamente. En Irlanda, grupos protestantes y católicos se aterrorizaron mutuamente tras la Reforma.

El período entre el uso de la pólvora en la guerra y las revoluciones americana y francesa se puede caracterizar como un período de transición que finaliza con el desarrollo de un verdadero terrorismo revolucionario.

Durante la Revolución Francesa, más específicamente en el período que transcurrió entre abril de 1793 y julio de 1794 y que se ha dado por llamar el Reinado del Terror liderado por Robespierre - murieron cerca de 17.000 personas.

Durante la revolución americana (1775-1783), los colonos usaron la guerra de guerrilla contra los británicos, mientras que los Torries usaron la guerra de guerrilla contra el ejército continental y el terror contra los colonos. Ambos bandos utilizaron indios hostiles para aterrorizar a la población, (Minolli, 2003, p.2).

El nacionalismo imperialista que en Japón condujo a la restauración Meiji en 1868 estuvo acompañado de frecuentes ataques terroristas al shogunado Tokugawa.

El Ku Klux Klan nace en los Estados Unidos al terminar la Guerra Civil (1861- 1865) para aterrorizar a los antiguos esclavos y a los representantes de las administraciones de la reconstrucción impuestas por el Gobierno Federal.

Sin embargo, el origen del terrorismo contemporáneo se remonta al siglo XIX en Rusia. El asesinato del Zar Alejandro perpetrado por un grupo revolucionario causó una serie de incidentes que culminó en la revolución rusa mientras que el asesinato del archiduque Francisco Fernando de Habsburgo, en Sarajevo, a manos del revolucionario serbio Gavril Princip, fue un acto terrorista que dio comienzo a la primera Guerra Mundial, causó millones de muertes, destruyó tres dinastías reales y concluyó con la formación de una nueva Europa.

Esta filosofía revolucionaria terrorista se propagó hacia Europa central y occidental donde los partidarios del anarquismo realizaron ataques terroristas contra altos mandatarios y/o ciudadanos comunes.

Tanto el comunismo como el fascismo utilizaron el terrorismo como instrumento de su política, contando con promotores tan conocidos como Lev Trotski, por ejemplo. La inestabilidad política existente durante las décadas de 1920 y 1930 dio pie a frecuentes actividades terroristas facilitando la integración de esta táctica dentro del conflicto más amplio de la Segunda Guerra Mundial.

La manifestación más importante del terrorismo tras la Segunda Guerra Mundial fue la ola de violencia internacional de la década de 1960 que tuvo su origen en el conflicto que en el Oriente Medio enfrenta a las naciones árabes con los israelíes. A fines de la década de 1940 algunos radicales judíos como la banda Stern y el Irgun Zvai Leumi utilizaron el terrorismo contra las comunidades árabes y contra otros grupos en su lucha por la Independencia de Israel. Durante y después de la década de 1960, sus adversarios árabes decidieron utilizar el terrorismo de forma mucho más sistemática. La expulsión de guerrillas palestinas de Jordania en septiembre de 1970 fue conmemorada con la creación de un brazo terrorista extremista llamado Septiembre Negro. La Organización para la Liberación de Palestina ha llevado a cabo operaciones terroristas y de comando tanto en Israel como en diversos países del mundo.

El avance del terrorismo más allá de Oriente Medio en la década de los sesenta fue evidente en las tres naciones industrializadas en las que la transición del autoritarismo a la democracia:

- En Alemania la banda Baader-Meinhoff tristemente célebre por el secuestro y asesinato de un importante industrial, Hans-Martin Schleyer, en 1977 y el posterior secuestro de un avión de la compañía alemana de aviación Lufthansa.

- En el caso de Italia, las Brigadas Rojas que en 1978 secuestraron y asesinaron al primer ministro Aldo Moro y los atentados que las Galerías Uffizi de Florencia sufrieron en 1993.

- En Japón nació el Rengo Segikum (Ejército Rojo) con el objetivo de establecer una república popular uniéndose a los sectores más oprimidos por el imperialismo japonés y buscando crear un "frente unido" de todas las fuerzas izquierdistas de ese país. Sin embargo, impedido de actuar internamente debido a la seguridad imperial existente, dirigió su accionar al terreno internacional donde causó innumerables pérdidas en vidas humanas y tuvo éxito en la aplicación de la violencia indiscriminada .(Minolli, 2003, p.3).

En América Latina diferentes grupos asolaron la región siendo tristemente célebres las FARC colombianas, Sendero Luminoso en Perú, el MIR chileno, los Tupamaros uruguayos, los Montoneros y el ERP argentinos y otros muchos en diferentes países. La última década del siglo veinte presentaba una relativa disminución del terrorismo, lo que quedó desestimado después del 11 de septiembre de 2001.

En la actualidad el IRA en Irlanda, la ETA en España, Jihad, Hamas, Hezbollah, Al Qaeda en oriente medio son, entre otras, organizaciones que mantienen vivo el espíritu del terrorismo y continúan con su histórica tradición violenta.

3.2. Acercamiento Conceptual al Terrorismo

Según el diccionario de la Real Academia Española terrorismo se define como la sucesión de actos de violencia ejecutados para infundir terror.

Para el autor Cook C. (1997, p.482) el terrorismo es la tentativa de alcanzar fines políticos gracias a la creación de un clima de temor mediante bombas, asesinatos, secuestros y piratería aérea, con el objeto de socavar la capacidad en la confianza de un Estado para proteger a sus ciudadanos, o de lograr publicidad para una causa.

Desde el punto de vista jurídico de Osorio M. (1992, p.1030) , define el terrorismo como: *"los actos de violencia en contra de personas, la libertad, la propiedad, la seguridad común, la tranquilidad pública, los poderes públicos y el orden constitucional o contra la administración pública".*

Para Pearson & Rochester en su libro las Relaciones Internacionales situación global en el siglo XXI (2003, p.406), terrorismo es: "La amenaza, la puesta en practica o la promoción de la fuerza como objetivos políticos por parte de una organización o una o varias personas cuyas acciones están dirigidas a influir sobre las actitudes políticas o las disposiciones políticas de un tercero, siempre que la amenaza, practica o promoción de la fuerza este directamente orientada hacia: a. no *combatientes, b. personal militar no involucrado en ese momento en acciones de combate o en papeles de preservación de la paz"*

En esta definición es importante mencionar que el terrorismo tiene una connotación política y es por ello que ataca a la población civil y causa fuertes efectos en la opinión pública. Estas acciones también tienen como fin promover causas ideológicas y brindar esperanza en los que creen en ellas, por medio de demostraciones de fuerza como son los ataques violentos.

En el ámbito de las organizaciones internacionales el concepto de terrorismo puede variar, debido a que ninguna de las convenciones existentes en la materia,

emanadas del sistema de Naciones Unidas, contiene una definición de terrorismo, sino que cada uno de estos instrumentos abordan en forma separada diversas manifestaciones terroristas.

En el caso de los convenios emanados de organismos regionales, la mayoría de ellos al momento de estipular qué ha de entenderse por este delito, realizan un reenvío a los distintos tratados celebrados en el marco de la ONU.

Sin embargo, a pesar de no existir a nivel mundial un consenso en torno al concepto normativo para el terrorismo, lo más cercano a ello se encuentra en la resolución de la Asamblea de las Naciones Unidas Res/56/88 titulada “medidas para eliminar el terrorismo”, la cual ofrece una definición práctica a efecto de ser empleada en las distintas operaciones que lleve a cabo la organización para contrarrestar la actividad terrorista, señalando que se trata de “actos criminales con fines políticos realizados con la intención de provocar un estado de terror en la población en general, en un grupo de personas o en determinadas personas injustificables en toda las circunstancia, cualesquiera sean las consideraciones políticas, filosóficas, ideológicas, raciales, étnicas, religiosas o de cualquier otra índole que se hagan valer para justificarlos”.

En conclusión terrorismo puede definirse como todas aquellas acciones de carácter criminal y violento cuyo fin es generar terror, independientemente si la motivación para realizarlas sea política, ideológica, religiosa, o económica; y cuyos efectos pueden perturbar tanto a nivel nacional como internacional.

3.3. Tipos de Terrorismo

Terrorismo Político: Es el que tiene un propósito específico de naturaleza política. Aquí, lo político se considera como un fenómeno que se manifiesta en todos los ámbitos de la vida social, ya sean públicos o privados.

Terrorismo de Estado: conocido también como violencia parainstitucional, es el que representa una modalidad de extremo control social. Los Estados, sobre todo en ausencia de controles democráticos, pueden utilizar de manera ilegal vicios de seguridad para reprimir a los opositores políticos o para contener un enemigo externo, bien sea que éste utilice o no métodos terroristas (Castro P. 1999, p.35). Un ejemplo puede presentarse en los regímenes totalitarios y en dictaduras.

Terrorismo de Amenazas: Es el que se limita a anunciar un atentado sin que éste llegue a producirse, bien con el propósito de intimidar o desinformar a la autoridad. Una muestra de esto es el terrorismo telefónico.

Terrorismo de Acciones: Es el que se produce mediante atentados que destruyen objetos o personas. Puede tener móviles políticos, o comunes.

Terrorismo Sistemático: Se realiza repetidamente sobre un mismo objetivo o blanco de acción; en este aspecto también se diferencia del individual en que este es generalmente realizado por una sola vez.

Terrorismo Común: Es el que utiliza bandas delincuenciales no estructuradas y que por consiguiente carece de fundamentos ideológicos. Para el autor, delincuente, es considerado como sujeto activo del delito (1999, p.38) . Como ejemplo de esto podemos encontrar al sicariato.

Terrorismo Revolucionario: El terrorismo revolucionario pretende modificar conductas y actitudes políticas mediante el deterioro de los lazos entre autoridades establecidas y gobernados. Según Borrero Mansilla (2004, p.98) este tipo de terrorismo se caracteriza por cuatro atributos: es un fenómeno de grupo, las acciones siempre están justificadas por una ideología; el grupo tiene líderes capaces de movilizar gentes a favor de su proyecto; y se crean estructuras institucionales alternativas porque el movimiento debe crear sus propios organismos de ejecución política.

Terrorismo Provocado por Organizaciones Privadas: Una modalidad diferente es el terrorismo represivo por organizaciones de justicia privada. Este terrorismo puede contar con la complicidad del Estado o ser completamente independiente del mismo y hasta enemigo de las instituciones. Algunos ejemplos pueden ser las “manos negras”, el Ku Klux Klan, los movimientos de autodefensa, las “hermandades santas”, toda suerte de grupos que reprimen a los opositores quienes son vistos como enemigos del orden establecido.

Terrorismo Cibernético: Es la convergencia del ciberespacio con el terrorismo (Masana, 2002 p.12). Son todas aquellas acciones terroristas claramente premeditadas que hacen uso de los sistemas de computación para alcanzar diversos fines , ya sea por intereses económicos, políticos o sociales.

Terrorismo Religioso: Se trata de actos terroristas que son cometidos en nombre de religión. Marighella C. (1979, p.5) sostiene que algunos grupos existen fuera del control del gobierno y podrían ser considerados como cultos religiosos radicales, mientras que otros existen como parte de religiones organizadas nacionales o internacionales.

Narco Terrorismo: Por años el traficar en drogas ha sido ligado exclusivamente a elementos criminales profesionales. En años mas recientes una nueva influencia se ha movido hacia el mundo de las drogas, motivados por una determinación para desestabilizar la sociedad. Su método es intercambiar armas por drogas. Un claro ejemplo de esta situación son las FARC en Colombia, en donde se utiliza la venta de drogas como mecanismo para financiar sus actividades.

3.4 . TERRORISMO CIBERNÉTICO

Al referirse al término terrorismo inmediatamente se asocia con grupos rebeldes, armamento, bombas, actos que vulneran la seguridad física y humana. Sin embargo usualmente se ignora las brechas de seguridad y los alcances que se tiene cuando se violenta la infraestructura informática al punto de llegar al terrorismo cibernético.

Según Alvarado y Morales (2004. P. 49) un acto de terrorismo cibernético, va dirigido a la infraestructura crítica informática, y se puede considerar el acto más paradigmático de un daño informático, puesto que, lo que se busca es la inutilización, por cualquier medio de los activos informáticos. Otras definiciones de terrorismo cibernético que deben considerarse:

Mark Pollit, un agente del FBI que se dedicó a estudiar el tema, desarrolló la siguiente definición : "El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos".

Dorothy E. Denning directora del Instituto de Seguridad de la Información de Georgetown, de la Universidad Georgetown, explica que "Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo. Serios ataques contra la infraestructura crítica de un país podrían ser actos de ciberterrorismo, dependiendo de su impacto". (Masana, 2002. p.12)

El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas, programas y datos informatizados no combatientes, por parte de grupos terroristas o agentes encubiertos de potencias extranjeras; si bien en la actualidad el concepto aparece más y mejor definido... El ciberterrorismo es la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista, extranjero subnacional, con objetivo político, utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet y otros muchos ... El objeto de un ataque ciberterrorista no es solo impactar sobre la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población

en general ... El ciberterrorismo existe porque es en el reino cibernético donde son más débiles la mayoría de las naciones industrializadas. (Hernández, L. 2006. P. 82)

En el marco legal internacional, a pesar de que no existe una definición común o uniforme acerca del término "terrorismo cibernético" es importante mencionar que fue en el año 2002 a través de la Unión Europea, a través de la Decisión Marco del Consejo que se empleó por primera vez el término "ciberterrorismo", asociándolo a los ataques terroristas contra los sistemas de información vitales en la Unión Europea.

Actualmente, sea a nivel local, regional o mundial el terrorismo cibernético tiene en común el hecho de ser una amenaza a la seguridad, son ataques contra software, computadoras y tecnologías de información, por motivos políticos, sociales, ideológicos o económicos realizados por una persona o grupo determinado y cuya finalidad principal aparte de generar temor en la población es vulnerar los sistemas de seguridad de la información vitales para el Estado.

Partiendo de la premisa que el terrorismo cibernético conlleva toda una serie de actos que vulneren la seguridad en la tecnología y la información, se pueden describir una serie acciones deliberadas que cumplen con estos objetivos:

3.4.1 Daño Informático

Es la conducta encaminada a alterar, destruir, inutilizar, suprimir o modificar o de cualquier modo o por cualquier motivo dañar un sistema que utilice tecnologías de la información o un componente de éste. (Alvarado y Morales.2012. p.48)
Algunos de los mecanismos para realizar este tipo de daño son:

- **Virus:**

Son claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Habitualmente suprimen o alteran archivos ejecutables por otros infectados, los cuales pueden inutilizar o destruir, de

manera intencional los datos almacenados en el computador. Antes se manifestaban haciendo la computadora mas lenta, actualmente pueden atacar sin que la persona se dé cuenta hasta que el daño está hecho.

- **Armas Cibernéticas:**

Consiste en Cualquier dispositivo que pueda ser utilizado en tareas de ataque, defensa y destrucción de fuerzas o instalaciones enemigas ubicadas en el ciberespacio, y que sus efectos pueden trascender en el mundo físico. A diferencia de los virus que utilizan mecanismos de destrucción de datos en un computador sin aspectos bélicos, las armas cibernéticas se emplean generalmente cuando se encuentra en una situación de conflicto bélico o en asuntos de guerras cibernéticas que involucra dos o más Estados.

3.4.2. El Espionaje Informático y el Robo de Software:

La información confidencial se guarda frecuentemente en los sistemas informáticos, independientemente si es para fines personales, comerciales o políticos. Y cuando la computadora está conectada o tiene acceso a Internet existe la vulnerabilidad de robo de esta información desde cualquier parte del mundo.

Los delincuentes utilizan varias técnicas para obtener esta información:
• Uso de software para eludir las medidas de protección;
• ingeniería social

La "ingeniería social" es una de las técnicas mas famosas y habituales para accesar a la información que posee mucha protección en los sistemas de seguridad informáticos; debido a que los delincuentes tienen que hacer uso de la "interacción humana" y se enfoca en engañar a otras personas para romper los procedimientos normales de seguridad. Por ejemplo: llamar por teléfono, hacerse pasar por el jefe o un alto mando dentro de la empresa, pretender que urge un dato y que han olvidado la agenda o el celular y que no tienen otra manera de obtenerlos, mas que con la ayuda de la persona que está del otro lado del teléfono.

Sorprendentemente es uno de los métodos más efectivos y exitosos para poder accesar a los programas internos de una institución sin realizar mayor esfuerzo en el área tecnológica, debido a que el eslabón más débil de la seguridad informática es a menudo los usuarios que operan el sistema informático.

3.4.3 Fraude Informático

Es la manipulación del sistema informático, con el fin de obtener algún beneficio para sí mismo o para un tercero (Iniciativa de Ley 4055. 2009. Art. 11). Los más comunes son:

- **Manipulación de Programas o los Caballos de Troya:**

Consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

- **La Técnica del Salami:**

Es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes. (Acurio S. p. 23)

- **Pishing:**

Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto. El delito consiste en obtener información tal como números de tarjetas de crédito contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

- **Estafa Nigeriana:**

Consiste en que una persona recibe un ofrecimiento a cambio de aportar determinada suma de dinero, lo cual termina siendo un engaño.

- **Secuestro Cibernético:**

Es una modalidad de estafa que utiliza un programa malicioso llamado ransomware que al ejecutarse desactiva la funcionalidad de la computadora y muestra un mensaje que exige cierta cantidad de dinero como rescate para restaurar la funcionalidad.

Otra modalidad es el del mensaje que personifica al departamento de la policía local dependiendo de cada país o del FBI; el mensaje indica que se ha detectado actividad ilegal en tu computadora tal como pornografía infantil y otros actos delictivos y se solicita el pago de una multa para desbloquear el equipo. El método para darle credibilidad a este mensaje es que los atacantes acceden al sistema operativo de la víctima, utilizan la WebCam, toman fotografías y video sin que la persona se dé cuenta y lo incluyen dentro del mensaje de la policía.

Imagen No. 2
Ejemplo de Secuestro Cibernético

Fuente: www.sophosnews.files.wordpress.com , foto Ransom UK.

3.4.4. Falsificación Informática

Se realiza cuando se alteran o modifican los datos de los documentos de un sistema que haga uso de tecnologías de la información generando un resultado no auténtico. (Nava G. p.41)

3.4.5. Acceso Ilícito

El acceso ilícito se refiere al ingreso no autorizado a uno o varios sistemas que utilicen tecnologías de la información. A la persona que realiza la intromisión de le denomina “hacker” y sus actos se originan para determinar vulnerabilidades se sistemas, burlar medidas de seguridad o a través de la motivación política (conocido como hacktivismo). En la mayoría de los casos, el acceso ilegal al sistema informático es sólo un primer paso vital para cometer una serie de acciones delictivas en el sistema informático. (Unión Internacional de Telecomunicaciones. 2009. p. 26)

3.4.6. Violación a la Disponibilidad

La disponibilidad informática se refiere al aseguramiento de que la información se encuentre disponible para que, la persona autorizada para tenerla, la posea en el lugar y en el tiempo que desee; y cuando se obstaculiza una persona el acceso a la información puede afectar gravemente en el aspecto económico de una empresa, político o social de un país o comunidad.

Garantizar la disponibilidad implica, también, la prevención de ataque de *denegación de servicio.*

- **Ataque de Denegación de Servicio (DoS)*:***

Se basan en utilizar la mayor cantidad posible de recursos del sistema, de manera que nadie más pueda usarlos, dejando indisponible el sistema (página Web, aplicaciones, servidores) especialmente si debe dar servicio a mucho usuarios. (Mateu R. y Cendoya J. 2000. p.148) Ejemplos típicos de este ataque son: los realizados por Anonymous Guatemala, los cuales saturan una página con solicitudes hasta dejarla indisponible.

3.4.7. Interceptación Ilícita

Consiste en interceptar las comunicaciones entre los usuarios (tales como e-mails, o cualquier tipo de medio virtual que sirva como medio de comunicación) para registrar la información intercambiada.

La mayoría de los países se han movido para proteger el uso de los servicios de telecomunicaciones mediante la criminalización de la interceptación ilegal de conversaciones telefónicas.

Sin embargo, en el caso específico de Guatemala en el artículo 48 de la Ley Contra la Delincuencia Organizada, se regula la interceptación "lícita". "Cuando sea necesario evitar, interrumpir o investigar…podrá interceptarse, grabarse y reproducirse con autorización judicial, comunicaciones orales, escritas telefónicas, radiotelefónicas, informáticas y similares que utilicen el espectro electromagnético".

Lo cual ha abierto la puerta al debate, ya que muchos expertos insisten que ninguna acción puede ser objeto de espionaje, ya que en este caso se está violando la confidencialidad sin importar quien lo ejecute.

3.4.8. SPAM

Consiste en la emisión de mensajes masivos no solicitados. Los delincuentes envían millones de correos electrónicos a los usuarios, que a menudo contienen publicidad de productos y servicios, pero también incluyen secretamente programas con frecuencia maliciosos.

3.4.9. OTRAS ACTIVIDADES CLANDESTINAS:

- **Cyberlaundering**

Consiste en el lavado de dinero a través de Internet. Servicios financieros en línea ofrecen la opción de realizar varias transacciones financieras en todo el mundo, con gran rapidez. Las transferencias electrónicas reemplazan el transporte de dinero en

efectivo como el primer paso inicial en la eliminación de la dependencia física del mismo. Para colocarlo generalmente va a casinos en línea y a través de monedas virtuales.

- **Robos Bancarios en Línea**

El robo bancario en línea se ha expandido ampliamente en América Latina. Estas actividades tienen características distintivas, que dependen del país o banco al que están orientadas y de la naturaleza de las medidas de autentificación y seguridad que protegen sus datos financieros. Para efectuarlos se hace uso de paquetes de crimeware que son programas maliciosos que eliminan los componentes de seguridad en las computadoras que usan para obtener acceso a cuentas bancarias.

Al igual que en muchas regiones, los hackers utilizan sus propios canales de comunicación para comprar y vender información sobre tarjetas de crédito, paquetes de crimeware y demás información de identidad personal de los clientes bancarios.

En contraste con las normas mundiales, los delincuentes cibernéticos en América Latina usan servicios de transferencia de dinero comunes para pagar los bienes y servicios de los delincuentes cibernéticos. Puesto que esto puede conducir a su identificación por parte de las autoridades, los delincuentes cibernéticos contratan mulas para llevar a cabo las transacciones. Las mulas reciben un porcentaje del dinero a cambio de realizar las transacciones y sufrir mayor riesgo de ser rastreados. (Insulza, J. 2013. P 13-14)

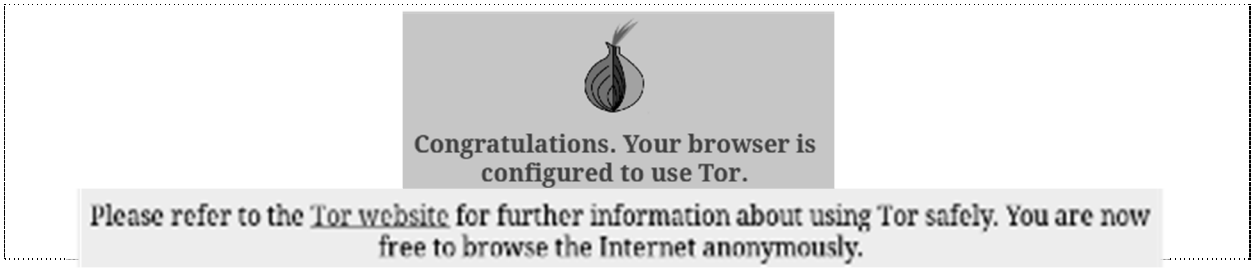
Esto es relevante dentro de la investigación, ya que el robo bancario en línea es un mecanismo que puede ser utilizado para el financiamiento del terrorismo. Y según las entrevistas realizadas a las autoridades guatemaltecas es un tema de preocupación, debido a que diversos bancos nacionales han sufrido estos ataques perdiendo sustanciales cantidades de dinero; datos que obviamente no son publicados por los medios de comunicación, ya que sería un desprestigio para la seguridad del banco atacado.

3.4.10. Deep Web o Internet Profunda

Es todo aquel contenido que no forma parte del Web Visible o Superficial (aquella parte de la red cuyo contenido puede ser recuperado por los motores de búsqueda tradicionales como Google, Bing o Yahoo), mientras que para acceder al deep Web es necesario utilizar una caja de búsqueda para cada base de datos especializada o como generalmente se utiliza a través de un navegador especial llamado TOR. (Bojo, et al. 2004. P. 7) A través de este navegador se puede accesar a sitios con dominios distintos a los tradicionales (.com o .gt, por ejemplo), en este caso se utiliza el dominio .onion, que no figura en ningún navegador.

Onion se ilustra gráficamente como una cebolla, debido a que la deep Web está constituida por capas, cada una mas profunda y encriptada, mas difícil de accesar que la anterior. Por ejemplo el grupo Wikileaks, conocido por filtrar documentos internos del gobierno norteamericano entre otros, se maneja dentro de esta red.

Imagen No. 3
Computador Configurado Con Sistema Tor Para Navegación de Internet Anónima



Fuente: The Deep Web; los suburbios de Internet. Disponible en www.paoladry.weebly.com

El contenido que existe allí es sumamente privado, protegido y en algunos casos ilegal. Y es importante recalcar que solamente el 5% de la información que navega en la red de Internet es interceptada por los motores de búsqueda tradicional, el otro 95% queda dentro de la Internet profunda.

La información que se encuentra allí es sumamente variada, desde documentos de seguridad interna de diversos gobiernos, NASA, información confidencial. Sin embargo no toda la información es legal, ya que existe todo un universo oscuro que involucra financiamiento voluntario a organizaciones terroristas, drogas, armas, sicariato, experimentos humanos, venta de órganos, tráfico de personas, canibalismo, pornografía, necrofilia y principalmente pedofilia. Muchos de ellos son fotografías o videos de los cuales algunos se pueden ver libremente, algunos existentes se pueden comprar, o en algunos casos y por el precio solicitado se puede ordenar nuevos videos de cualquiera de estos actos a gusto y preferencias del cliente. Tener acceso a estos servicios es publicado con la simplicidad de estar comprando un objeto en un sitio Web tradicional como Amazon o eBay.

Imagen No. 4
Ejemplo Mercado Negro en Línea y Uso del Bitcoin

Fuente: Comprar Armas, Explosivos y Software en el Back Market. Disponible en www.elladodelmal.com

Para poder pagar estos servicios no se utiliza una moneda común, sino hay que cambiarla por una moneda llamada “bitcoin” (BTC), la cual es muy volátil. Un bitcoin puede equivaler trece dólares americanos un mes y uno por mil dólares en los

siguientes días o semanas. Para poder comprarla debe realizarse con tarjeta de crédito y por una comisión una serie de compañías como Robocoin canjean la moneda.(Becerra. 2014. P.3) El bitcoin también se usa para blanquear dinero.

Accesar al Deep Web es ilegal en la mayoría de países, sin embargo es una práctica común en todos. El gobierno norteamericano reúne esfuerzos a través del FBI y coloca sitios falsos para atraer criminales que les interese adquirir este tipo de servicios.

Sin embargo para poder acceder a esta red se toman una serie de medidas de seguridad, desde un buen antivirus, hasta cambiar la ubicación desde donde se tiene acceso a Internet, la clave es siempre mantener el anonimato; por ejemplo si la persona se encuentra en Guatemala debe cambiar su IP por otro país en otro continente, así dejan de ser rastreables.

De esta manera existen entes gubernamentales que se encargan de la seguridad cibernética en varios países como Estados Unidos y España, que accesan todos los días de pesca intentando atrapar criminales, sin embargo es casi una labor imposible rastrearlos. Es relevante en el caso de Guatemala, ya que al entrevistar al Viceministro de Tecnologías de la Información del Ministerio de Gobernación, Ing. Carlos Argueta afirma que tienen conocimiento que en Guatemala existen personas que ingresan a esta red aunque no siempre con fines delictivos, sin embargo el Gobierno de Guatemala actualmente no cuenta con la posibilidad de poder investigar este tipo de casos.

3.4.11. Armas Cibernéticas, Malware y Ciberespionaje Desarrollado por Gobiernos

Las armas cibernéticas son creadas como política de algunos Estados para defender su soberanía en el campo de batalla del ciberespacio, pero sus efectos son sensibles en el espacio físico, alterando armas o dispositivos tangibles. También pueden ser utilizadas para el ciberespionaje.

Generalmente como la mayoría de crímenes cibernéticos, tiene un trasfondo de interés económico, ya que los secretos comerciales o de seguridad nacional pueden valer mucho dinero en las manos interesadas. Por ejemplo en la década de los años ochenta una serie de hackers alemanes lograron entrar a los sistemas informáticos militares del gobierno de Estados Unidos robar la información y venderla a la Unión Soviética.

Recientemente Estados Unidos de América creó un Cibercomando encargado de defender redes militares estadounidenses y realizar ofensivas cibernéticas entre otras funciones. El 1 de junio de 2012 el presidente Barack Obama ordenó en forma secreta y durante los siguientes meses incrementar sofisticados ataques contra los sistemas informáticos de Irán para sabotear sus instalaciones nucleares. Éste es conocido como el primer ataque de Estados Unidos usando armas cibernéticas (Alvarado y Morales.2012. p.56).

Se considera que el año 2011 fue el año de auge de las armas cibernéticas, ya que muchos Estados manifestaron su interés y disposición para desarrollar y desplegar dichos mecanismos de carácter bélico.

Como las mas recientes y potentes armas cibernéticas podemos citar:

- **Stuxnet:** El objetivo principal de este programa malicioso fueron los sistemas especiales que empleaban los programas de monitorización y control industrial de Siemens, empresa multinacional de origen alemán que opera en los sectores industrial, energético, salud e infraestructuras y que en el 2011 también formaba parte del negocio de la energía nuclear.

Este malware, por sus características pasó inadvertido dentro del sistema, incubándolo por un tiempo prolongado y cambiando paulatinamente el proceso al interceptar las órdenes del software de Siemens SCADA y reemplazarlas con

comandos maliciosos variando el funcionamiento del equipo, hizo pensar a muchos expertos que los diseñadores de Stuxnet tenían en mente como objeto de ataque las centrífugas de enriquecimiento de uranio en la planta iraní de Natanz.

Algo novedoso e importante de Stuxnet, es que no solo fue dirigido contra objetos virtuales, sino contra una infraestructura real.

- **Flame (Worm.Win32.Flame):** Arma cibernética utilizada en el año 2012. En el mes de junio 2012 el Diario New York Times, informó que Stuxnet y Flame fueron desarrollados por dos servicios secretos en conjunto: la Agencia Central de Inteligencia CIA de Estados Unidos y la Unidad 8200 del servicio de inteligencia militar israelí. (2012. p.57)

Esta arma cibernética fue descubierta por la compañía de seguridad en Internet KASPERSKY, quienes consideran que Flame es el software de espionaje más complejo descubierto a la fecha.

Este es un programa malicioso especializado en ciberespionaje, a través del cual se puede sustraer información valiosa, incluyendo contenidos de la pantalla de ordenador, información sobre sistemas específicos, archivos almacenados, datos de contacto y conversaciones. Es capaz de obtener información de audio.

- **Espionaje de la Agencia de Seguridad Nacional de Estados Unidos – NSA- a Nivel Internacional:**

Tanto por ubicación geográfica como por perfil socio-político, se establecen las áreas prioritaria para el NSA. La abogada de Derechos Humanos guatemalteca Renata Ávila en su artículo “Centroamericanos, en la Mira del Espionaje de la NSA” publicado en la revista en línea Nómada.gt, afirma que Honduras, El Salvador y Guatemala han sido descritos como un área que puede ser “una amenaza a la seguridad nacional de los Estados Unidos”, por el narcotráfico y las pandillas. Estos territorios son prioritarios para las operaciones de recolección de “inteligencia de

señales" o SIGINT, palabra código utilizada por el aparato de inteligencia estadounidense, incluyendo vigilancia dirigida a objetivos estratégicos y vigilancia masiva.

La magnitud de esta vigilancia fue dada a conocer por el periodista Jacob Appelbaum, de la revista alemana Der Spiegel. Se trata del TAO –el sistema de Operaciones de Acceso a la Medida– que incluye una gama posibilidades para penetrar y tomar control de cualquier equipo usado por una persona sujeta a vigilancia.

Y ser un objetivo no es ser enemigo de las naciones que espían. Tanto Angela Merkel, Dilma Rousseff como Enrique Peña Nieto fueron víctimas de espionaje intenso; países en paz, amigos, aliados. Es más, en algunos casos, como en Turquía, el gobierno es al mismo tiempo colaborador y víctima del espionaje.

Los nombres que utiliza la NSA para sus programas no pasan desapercibidos: Bulldozer, Monkeycalendar (ataque a tarjetas SIM) , Cottonmouth (ataques a USBs). Flatliquid y Whitetamale fueron los nombres claves con los que la NSA vigiló tanto al presidente de México como a su Secretaría Nacional de Seguridad, capturando absolutamente toda su información.

En Guatemala también se realizó espionaje a través de la intervención en las comunicaciones durante el período 2008-2012 al exgobernante Álvaro Colom, lo cual provocó una disculpa pública por parte del presidente Barack Obama y reiteró que actualmente "están siendo mucho mas cuidadosos en la vigilancia de las comunicaciones y que únicamente se están concretando en lo que pueda representar una amenaza en contra de Estados Unidos".

Estas revelaciones por el ex analista de la CIA y activista Edward Snowden han sacado a luz cómo la misión de las agencias de inteligencia de recabar todos los datos posibles se traduce en operaciones intensas de recolección, intercepción,

alteración de equipo desde la fábrica y control de software, hardware, equipo para redes inalámbricas, redes de seguridad, cámaras de vigilancia, así como escuchas, ataques activos dirigidos a infraestructura clave, intercepción de mensajes de texto y de servicios de mensajería.

Todas estas acciones, así como la aplicación de programas maliciosos que no sólo afectan objetivos virtuales sino en muchos casos también la infraestructura real, pone en cuestionamiento la manera como es concebido el ciberterrorismo en cada país y los límites que se sobrepasan con el "fin de defender la seguridad nacional"; ya que es evidente por ejemplo en el caso de Estados Unidos como puede realizar acciones que vulneran la seguridad de la información de otros países, sin asumir la responsabilidad internacional correspondiente, ya que hasta la fecha este país se niega a aceptar una definición oficial de terrorismo porque esto podría utilizarse en su contra por motivos de justicia. En el fondo el concepto de terrorismo es bastante sencillo: son todas aquellas acciones que, independientemente de la motivación generen terror en la población y que vulneren los sistemas de seguridad nacionales vitales con el fin de acceder, destruir o alterar los mismos sin importar el mecanismo que se utilice.

- **Intervención en las Comunicaciones, Monitoreo de Redes Sociales, Espionaje y Ciberataques por parte del Gobierno de Guatemala**

El resguardo de la seguridad nacional ha sido el motivo por el cual el Gobierno de Guatemala ha realizado intervención en las comunicaciones, lo cual fue confirmado en entrevista con el Ing. Juan Carlos Argueta, Viceministro de Tecnología del Ministerio de Gobernación, quien afirma que el Gobierno posee un equipo de trabajo encargado de la inspección y control de llamadas telefónicas a personas sospechosas que puedan estar relacionadas en acciones delictivas. Estos mecanismos han servido en muchas ocasiones como medios de prueba en juicios de corrupción y crimen organizado.

Sin embargo, han existido denuncias por parte de algunos diputados y políticos que sospechan pueden estar siendo vigilados por parte del gobierno y no solamente en escuchas telefónicas, sino también a través de sus correos electrónicos. El confirmar si han sido vigilados por el gobierno no ha sido posible y solamente es un delito si se hace público el contenido de la información, según el artículo 219 del Código Penal Guatemalteco.

Por otra parte se ha hecho evidente a través de los medios de comunicación y confirmado públicamente por el Subsecretario de Comunicación Social de la Presidencia, Oscar Ismatul que esa dependencia tiene una oficina ubicada en el nivel 13 del edificio del Instituto Guatemalteco de Turismo –INGUAT-, “desde la cual monitorean la opinión pública de redes sociales de las cuentas institucionales y se hace la defensa del gobierno y el ataque contra los detractores del gobierno”. A pesar de las aclaraciones, ha despertado dudas en la bancada de oposición los cuales han hecho públicos sus cuestionamientos, así como en la población en general si en realidad de trata de una oficina de información que se dedique a investigar a personas o funcionarios y no monitoreo en redes como se afirma.

Con respecto al tema de espionaje y ciberataques a sitios Web de medios de comunicación, el presidente del diario elPeriódico, Lic. José Rubén Zamora acusa al gobierno del presidente Otto Pérez de ser responsable de seis ataques cibernéticos que han deshabilitado temporalmente su sitio de Internet. Esto a causa de que los ataques han coincidido con los trabajos investigativos que se han hecho sobre corrupción en el gobierno de Pérez, el enriquecimiento de funcionarios y abusos de poder. Por lo que se supone que son realizados con la intención de evitar que los usuarios del sitio Web tengan acceso a la información, ya que la cantidad de usuarios de la pagina son bastante mayores que los de la edición impresa.

También se estableció que los ataques cibernéticos tienen su origen en la zona 1 de la capital de Guatemala, aunque los responsables utilizaron diversos mecanismos

como manejar IP falsas para encubrirse y hacer pensar que los ataques venían de Europa.

Asimismo, aunque fuera del período establecido por esta tesis en el mes de septiembre 2014 el gobierno de Guatemala publicó en la página Web de vicepresidencia un reportaje investigativo de el Periódico un día antes de que se presentara al público relativo a una propiedad de la Vicepresidenta Roxana Baldetti valorada en Q25 millones. Estas acciones son investigadas por la Fiscalía de Derechos Humanos del Ministerio Público, por medio de la Unidad de Delitos contra Periodistas, ya que se señala que se violó el Art. 274 F del Código Penal relativo a la utilización de registros informáticos de otro. Y el Art. 35 de la Constitución Política de la República relativo a la Libertad de Emisión del Pensamiento, referente a que es prohibida la “censura previa” o de cualquier tipo.

3.4.12. GRUPOS DE CIBERDELINCUENTES

3.4.12.1. Hackers:

Es el sujeto que utiliza su conocimiento en materia informática ingresando sin autorización a los sistemas informáticos. (Barrios Osorio. 2007. P. 380). Los hackers pueden clasificarse al menos en tres tipos :

- **White Hat hackers** (hackers de sombrero blanco). Son personas que no persiguen intereses delictivos, sino que por el contrario, creen que su misión (a veces remunerada y a veces no) es encontrar brechas en la seguridad de las computadoras y luego avisar a las partes involucradas para que puedan protegerse.

- **Black Hat hackers** (hackers de sombrero negro). Se trata de individuos que realizan tareas que van desde ingresar ilegalmente a distintos sitios y colocar información falsa o textos e imágenes obscenos, hasta robar números de tarjetas de crédito con la intención de cometer fraudes.

- **Grey Hat hackers** (hackers de sombrero gris). Son aquellos que en el pasado

realizaron actividades de hacking, pero que actualmente trabajan para empresas en el área de seguridad. (Masana. 2002. P. 18)

3.4.12.2. Hacktivistas

El hacktivismo puede definirse como la afinidad entre el hacking y el activismo social y político. Éste incluye la desobediencia civil electrónica, que traslada al ciberespacio el concepto tradicional de desobediencia civil, asimismo conlleva una serie de acciones de intromisión a los sistemas de manera ilegal, ataques DoS y en algunos casos espionaje con la justificación de cumplir sus objetivos de activismo y beneficio para la sociedad.

Existe mucha polémica en cuanto a la definición de estos grupos, ya que algunos de ello, lejos de formular una crítica constructiva ante políticas o actos que atentan en contra de su ideología, se han dedicado a destruir sistemas informáticos incurriendo en actos de "terrorismo cibernético". Uno de los grupos mas relevantes dentro del mundo cibernético y que se autodenominan hacktivistas son el grupo Anonymous.

- **Grupo Anonymous**

El término en inglés "anonymous" significa "anónimos", constituye un seudónimo utilizado a nivel mundial por un grupo de personas que no revelan su identidad y que publican, por medio de ataques cibernéticos: la libertad de expresión, independencia de la Internet y su oposición a las actividades de diversas organizaciones.

Principalmente este grupo realiza sus acciones o protestas por medio de ataques a sistemas de propiedad de los entes o personas que consideran como sus adversarios. Aparentemente no realizan funciones terroristas, sin embargo al realizar sus ataques cibernéticos facilitan la infiltración de información que podría ser utilizada en prejuicio de los Estados. Han hecho ataque a la CIA y han salido ilesos.

Generalmente Anonymous realiza ataques de denegación de servicio (DoS), que consiste en enviar un elevado numero de peticiones a un servidor que aloja una página Web de tal manera queda suspendido el servicio.

En Guatemala se creó pánico cuando apareció en Internet una supuesta amenaza de Anonymous en contra del gobierno guatemalteco por la pobre actuación al resolver los casos de asesinato en nuestro país. La amenaza decía que Anonymous tomaría el día 30 de agosto del 2011, las páginas Web del gobierno y del Ministerio Público en protesta al no resolver los cientos de casos que han enlutado a cientos de ciudadanos guatemaltecos. Esto generó preocupación y gastos en el gobierno y la búsqueda del fortalecimiento de la seguridad informática. Los mensajes de Anonymous y sus amenazas generalmente se difunden a través de la página de Youtube.

Imagen No. 5
Ejemplo de Anuncio de Ataque en Página de Facebook de Anonymous Guatemala

Fuente: Facebook/ Anonymous Guatemala

En entrevista a diversos expertos del área de informática difieren en el concepto de calificar al grupo Anonymous como terroristas, debido a que algunos consideran que es necesario cortar la luz, o crear una crisis masiva en el mundo físico. Sin embargo el Ing. Ronald Morales, creador del CSIRT-gt si los considera terroristas al considerar que inhabilitan las páginas Web de gobierno y el “Estado no puede quedar fuera de funcionamiento”.

Si se parte del concepto de terrorismo cibernético, que conlleva el ataque premeditado utilizando tecnología informática para paralizar o desactivar estructuras electrónicas con un objetivo político, puede calificarse que la inhabilitación de páginas Web del gobierno, de las cuales tienen derecho a accesar todos los guatemaltecos, así como también el hecho que el mismo grupo hacktivista publica y presume haber obtenido datos confidenciales de sitios como el del Congreso de la República de Guatemala, así que al lesionar la seguridad del Estado puede considerarse que el grupo Anonymous en Guatemala ha cometido actos de ciberterrorismo en el país.

Imagen No. 6
Ejemplo de Página Web Gubernamental Guatemalteca (Ministerio de Energía y Minas) Deshabilitada por Ataque DdoS

Fuente: Facebook/ Anonymous Guatemala

También es importante mencionar, el hecho de que expertos en informática como el Ing. Ronald Morales o el Ing. Ronny Vásquez, afirman que se ha podido comprobar que, aunque el concepto del grupo Anonymous se presente como algo atractivo para la Juventud pregonando justicia social, realmente se valen del "factor psicológico" para aprovecharse de los jóvenes y crear situaciones de pánico al realizar sus amenazas. También hacen uso de la "ingeniería social" para obtener los datos para accesar a los datos confidenciales.

Publican en su sitio oficial de Facebook Anonymous Guatemala que imparten cursos para los miembros acerca de diversos temas de problemáticas sociales nacionales, pero también realizan capacitaciones acerca de la ingeniería social para ampliar sus conocimientos al respecto:

"Buenas Noches Guate! se les recuerda que el prox lunes 31 de marzo se comenzara una actividad de reclutamiento anonymous comenzando la fecha ya mencionada y se estarán impartiendo a lo largo de todo el mes de abril, los temas que se abarcaran serán: Ideal anonymous, Problemática nacional, y también informática y hacking... todos están totalmente invitados si quieres entrar a recibir esta serie de clases y foros contáctanos vía Inbox y serás totalmente bienvenido.... Los esperamos Guatemala..".

Asimismo, la efectividad de sus acciones radica en que ellos si están bien organizados y crean sus propios manuales básicos y protocolos. También es relevante exponer que según los expertos, para poder unirse a este grupo hay que instalar un programa en la computadora, que parece muy normal, pero en realidad conforme se van descargando estos software se está haciendo que la máquina se instales algunos artefactos que permiten lanzar ataques: que pueden ser de denegación de servicio, pero también pueden ser dirigidos a capturas de direcciones electrónicas, a capturas de números de tarjetas de crédito, de cuentas financieras, de datos de usuarios. Básicamente en la computadora se puede instalar cualquier artefacto y a partir de allí, lanzar ataques a cualquier sitio en cualquier parte del mundo. Y el nuevo miembro, inocentemente no tiene conocimiento que está siendo co-participe de estos delitos.

3.4.13. El Estado Como Blanco Del Ciberterrorismo

A continuación se presenta un cuadro que reúne las principales acciones en contra de los sitios Web del Gobierno de Guatemala, así como a algunos medios de comunicación realizadas por cibercriminales en el período de estudio, donde se explica brevemente la motivación de los ataques y los responsables, asimismo un análisis del efecto en la opinión pública, el manejo del tema por los medios de comunicación y el accionar gubernamental.

Cuadro No. 1
Ataques a Sitios Web Estatales

Fecha	Ataque	Responsable	Sitios Afectados	Motivo
29/8/2011	OP GUATEMALA	Hackers argentinos xDarkSton3 y MetalSoft	• congreso.gob.gt • contraloria.gob.gt • guatemala.gob.gt • mp.gob.gt • mingob.gob.gt • biblioteca.usac. edu.gt • canal3.fideck.com • noti7.com.gt • sonora.com.gt • telecentro.com.gt	Se valieron de una amenaza lanzada por Anonymous Guatemala y perpetraron el ataque un día antes. Los ataques no fueron realizados por denegación de servicio (Ddos), estos fueron mucho más dañinos, alterando y extrayendo información dentro de la base de datos y páginas Web de los servidores vulnerables. La finalidad del ataque era indagar sobre la arquitectura e identificar vulnerabilidades dentro de los equipos (com.gt , gob.gt , edu.gt)
19/12/2011	OP MINERA	Anonymous Guatemala y Lulz Security Guatemala	• congreso.gob.gt • seprem.gob.gt • mem.gob.gt	Justifican una llamada de atención al gobierno y comunidad internacional sobre las actividades del Golcorp en Guatemala. Este ataque no fue solamente de denegación de servicio; Lulz Security se adjudica haber ingresado a la base de datos de la pagina del Congreso y

				publican alguna información como títulos de archivos privados, email de diputados, direcciones, números de teléfono, fechas y cifras de dinero, así como correos electrónicos internos.
18 y 19/2/2012	OP MINERA 2.0	Anonymous Guatemala y Lulz Security Guatemala	• marn.gob.gt • guatemala.gob.gt • minex.gob.gt • pdh.org.gt	Denegación de servicio a paginas del Ministerio de Relaciones Exteriores, Medio Ambiente, Procuraduría de Derechos Humanos, y Gobierno de Guatemala.
21/2/2012	OP MINERA 2.1 (operación relámpago)	Anonymous Guatemala	• congreso.gob.gt	Denegación de servicio a la pagina Congreso de Guatemala por la aprobación de la ley de minería que da acceso libre a las actividades mineras.
25/5/2012	OP NIÑOS LIBRES	Anonymous Guatemala en colaboración con hackers patogandalf y security tram Hack Gt	• congreso.gob.gt • pnc.gob.gt • ceg.org.gt	Denegación de servicio al Congreso, Policía Nacional y Centro de Estudios de Guatemala con el fin de manifestar descontento contra la violencia infantil en Guatemala, principalmente el caso de pederastas y explotadores de menores.
08/5/2012	OP HIDRO- ELECTRICA	Anonymous Guatemala	• guatemala.gob.gt	Denegación de servicio al sitio del Gobierno de Guatemala rechazando la militarización de Santa Cruz Barillas. Oposición a la construcción de hidroeléctricas. A favor de la consulta popular.
2/7/2012	OP EDUCACION GT	Anonymous Guatemala en colaboración con hacker patogandalf	• mineduc.gob.gt	Intento de denegación de servicio al sitio del Ministerio de Educación con el fin de promover la calidad educativa en Guatemala. No lograron concretar el ataque por falta de apoyo.

14/07/2012	OP SALUD	Anonymous Guatemala	• mspas.gob.gt • guatemala.gob.gt	Denegación de servicio a los sitios del Ministerio de Salud y al Gobierno de Guatemala para llamar la atención en la mejora del sector salud en el país.
02 al 8/08/2012	OP GREEN RIGHTS CA	Diversos grupos de Anonymous: Guatemala, El Salvador, Honduras, Costa Rica, Nicaragua y Panamá	• conap.gob.gt • congreso.gob.gt • serna.gob.hn • minapanama.com • petaquilla.com • marn.gov.sv	Ataque centroamericano de denegación de servicio a sitios del Congreso de Guatemala, Consejo Nacional de Áreas Protegidas de Guatemala, Medio Ambiente de Honduras, Medio Ambiente de El Salvador y dos mineras de Panamá. Con el fin de promover respeto al medio ambiente.
20/09/2012	ATAQUE MINFIN	Hackers provenientes de Alemania	• minfin.gob.gt	Intención de burlar la seguridad y accesar a los datos sensibles. Ante la imposibilidad de lograrlo realizaron un ataque denegación de servicio al Ministerio de Finanzas de Guatemala.
06/10/2012	OP INDIGNADOS TOTONICA-PAN	Anonymous Guatemala	• mindelf.mil.gt	Denegación de servicio al Ministerio de Defensa a causa de una publicación de la PDH que afirma que proyectiles de un fusil Galil, del tipo que usa el ejército, pudieron ser la causa de muerte de seis campesinos y de heridas a unas 30 personas en un enfrentamiento en Totonicapán.
30/12/2012	OP DEMOCRACIA GT	Anonymous Guatemala	• guatemala.gob.gt • congreso.gob.gt	Denegación de servicio a pagina del Congreso y del Gobierno como protesta a los gastos innecesarios del patrimonio nacional en viajes, viáticos y remodelaciones.

*Elaboración Propia en Base a Información de Facebook/Anonymous Guatemala, Prensa Libre e Informe de Empresa Devel Security.

El cuadro refleja una serie de características comunes: por ejemplo, el hecho de ser ataques de denegación de servicio. Sin embargo, esto es una representación parcial de los ataques, debido a que la información ha sido sustraída del sitio oficial de Anonymous Guatemala y medios de comunicación escrita.

Existen otros tipos de ataques informáticos, mucho mas severos a los que se enfrentan las instituciones de gobierno a diario. Que no son fácilmente prevenibles o notorios como los que comúnmente realiza Anonymous. Los empleados de informática de diversas instituciones tienen en común el indicar, que los grandes ataques a los que se enfrentan a veces ni siquiera son descubiertos en el momento, sino mucho tiempo después o a veces por terceras personas, que generalmente vienen de países de Europa del Este. O en otros casos ataques que pretenden accesar a la información sensible, generalmente de interés económico y que deshabilite por completo el equipo de computación.

Lo que sucede es que este tipo de datos son de carácter confidencial y hacerlos de carácter publico ante los medios de comunicación y personas particulares, serviría para mostrar las vulnerabilidades de cada sistema. Por este motivo , la dificultad de poder ejemplificar ataques de otra índole en el sector Gobierno es sumamente complicado; a esto hay que sumar el hecho de que no comparten las experiencias de los ataques, ni siquiera entre instituciones, sino se maneja un hermetismo, que no permite aprender de los errores de otros y compartir medidas efectivas que otros han experimentado.

Esto refleja un vacío de información y una carencia total de indicadores, cifras o estadísticas de ataques a nivel nacional. No ha existido una sola institución que haya podido hasta el momento publicar y categorizar los ataques cibernéticos en el Estado de Guatemala a nivel general, mucho menos a instituciones de Gobierno.

Esta situación se ve también claramente en los medios de comunicación. La información publicada en los periódicos o en la televisión es sumamente limitada, al

punto que los reportajes terminan siendo escuetos y delimitándose a un par de líneas. No reflejan la realidad de la problemática; ya sea manejando una imagen de instituciones de Gobierno sumamente preparadas para manejar cualquier tipo de amenazas.

No existe un interés investigativo del tema, mas bien informativo de los sucesos ocurridos y eventos sociales gubernamentales plasmados desde el punto de vista de la persona entrevistada. Esto tiene mucho que ver con lo que fue indicado en la entrevista al Viceministro de Tecnologías de la Información y Comunicación del Ministerio de Gobernación Ingeniero Juan Carlos Argueta, que es un “arma de dos filos” el manejo de la información, debido a que no se puede dar una imagen relajada ante los problemas de seguridad informática, pero tampoco se debe crear una imagen exagerada de peligro que pueda crear psicosis en la población. Al final, el manejo de medios de comunicación sobre el tema es limitado en forma y fondo, ya sea en reportajes audiovisuales y artículos escritos.

Por otro lado, Anonymous manifiesta públicamente que tiene la capacidad para poder realizar ataques mas fuertes y acceder a información confidencial. Sin embargo expresan que no es esa su intención y que no pretender realizar o promover este tipo actividades. Sino que básicamente su objetivo es sobrecargar las paginas gubernamentales como mecanismo para llamar la atención pública.

También han sido entrevistados a través de un programa de computadora por Internet y sus opiniones han sido presentadas en un noticiero nacional en el que declara que sus fines son pacíficos y que solamente buscan la justicia social.

Ante estas declaraciones, así como también lo que publican en su sitio de Facebook, los medios de comunicación básicamente plasman lo que les dicen sin ninguna opinión o aporte crítico que pueda contrastar las palabras con las acciones o con la opinión de las autoridades.

CAPITULO IV

ESTADO DE GUATEMALA FRENTE AL TERRORISMO: CASO TERRORISMO CIBERNÉTICO

4.1. Marco Legal del Terrorismo Cibernético

Comprende todos los acuerdos y leyes relativas al ciberterrorismo desde dos niveles: Legislación internacional, que abarca los acuerdos entre Estados a nivel mundial, haciendo un énfasis en el continente americano y por otra parte la legislación nacional guatemalteca.

4.1.1. Legislación Internacional

En esta se presentan los principales convenios internacionales relativos a la seguridad cibernética, ciberdelincuencia y tecnología delictiva con la participación de la Organización de las Naciones Unidas, Organización de Estados Americanos y Consejo de Europa.

4.1.1. 1. Organización de las Naciones Unidas

- **Lucha Contra la Utilización de la Tecnología de la Información con Fines Delictivos** (Asamblea General. Resolución A/RES/55/63. 22 de Enero de 2001)

Esta resolución reconoce el esfuerzo de los organismos internacionales como el Comité del Consejo de Europa sobre el crimen en el espacio cibernético relativa a un proyecto de convención sobre el delito cibernético, los principios de los Ministros de Justicia e Interior del Grupo de los Ocho en Washington D.C., Conferencia del Grupo de los Ocho acerca del diálogo entre la industria y el gobierno sobre seguridad y confianza en el espacio cibernético, Tercera Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas, en el marco de la Organización de los Estados Americanos por impedir la utilización de la tecnología de la información con fines delictivos y propone una serie de medidas para luchar contra esta problemática. Entre las medidas fundamentales se mencionan:

- La importancia que los Estados velen por fortalecer la legislación para evitar refugios para los criminales tecnológicos,

- Intercambio de Información entre Estados
- Vigilancia del cumplimiento de la ley, investigación y enjuiciamiento
- Capacitación del personal y equipo adecuado
- Protección de la confidencialidad, integridad y disponibilidad de los datos
- Conservación de datos electrónicos relativos a investigaciones criminales
- Sensibilización al público en general acerca de la prevención y combate de la tecnología con fines delictivos.

- **Creación de una Cultura Mundial de Seguridad Cibernética**

(Asamblea General. Resolución A/RES/57/239. 31 de Enero de 2003)

Es un documento que invita tanto a las organizaciones internacionales pertinentes y Estados miembros a que en toda labor en materia de seguridad cibernética tengan en cuenta los elementos planteados para el fortalecimiento en la creación de una cultura mundial de seguridad cibernética. Son nueve los elementos presentes:

1. Conciencia: de la necesidad de la seguridad de los sistemas y redes
2. Responsabilidad: responsabilidades individuales de los Estados en sus propias políticas, prácticas, medidas, procedimientos y evaluaciones en su contexto
3. Respuesta: la capacidad de actuar de manera oportuna y eficaz, así también compartir la información de amenazas y vulnerabilidades entre países.
4. Ética: el respeto a los legítimos intereses de los demás
5. Democracia: Libertad de intercambio de ideas, libre flujo de información, confidencialidad, protección de la información y transparencia.
6. Evaluación de Riesgos: A fin de determinar las amenazas.
7. Diseño y Puesta en Práctica de la Seguridad: implementación de planes.
8. Gestión de la Seguridad: Evaluación de los riesgos
9. Reevaluación: Examen de la seguridad y modificaciones en políticas, prácticas, medidas y procedimientos de seguridad.

4.1.1.2. Consejo de Europa

Convenio de Budapest sobre Ciberdelincuencia
(23 de noviembre de 2001)

Acuerdo cuyo objetivo fundamental es proteger a la sociedad frente a las amenazas de la ciberdelincuencia, mediante la adopción de legislación adecuada, un espacio político y jurídico común, así como también el fortalecimiento de la cooperación internacional. Actualmente es el único marco global que existe para aplicar una política penal común. Las conductas ilícitas, reguladas en el Convenio de Budapest son:

1. Delitos Contra la Confidencialidad, Integridad y la Disponibilidad de los datos y Sistemas Informáticos

- el acceso ilícito,
- interceptación ilegal,
- integridad de los datos,
- interferencia de sistema,
- abuso de los dispositivos,

2. Delitos Informáticos:

- falsificación informática,
- fraude informático,

3. Delitos Relacionados con la Pornografía Infantil

4. Delitos Relacionados con Infracciones de Propiedad Intelectual y de los Derechos Afines

También se establecen disposiciones de índole procesal para la preservación de datos almacenados, y todo lo relacionado a los actos procesales para producir prueba y aislar todo acto de cibercrimen. (Alvarado y Morales. 2012. P. 11)

Asimismo en el Artículo 35 del Convenio establece la creación de una Red 24/7, la cual establece que cada miembro debe designar un punto de contacto localizable las 24 horas del día, siete días a la semana con el fin de garantizar una asistencia inmediata para investigaciones relativas al cibercrimen.

Aunque está formado claramente por los miembros del continente europeo, existen algunos miembros de otras regiones debido a que no hay un impedimento legal para que otros países se integren. En este caso son Estados Unidos, Canadá, Japón, República Dominicana y actualmente ha sido Colombia invitada a formar parte del mismo. El requisito para poder adherirse es que el Estado cuente con una legislación apropiada y enfocada al crimen cibernético, que investigue y sancione penalmente este tipo de acciones criminales, que los resultados de estas acciones sean palpables. Asimismo debe demostrar un compromiso constante de formulación de políticas públicas nacionales de protección de cibercrimen con iniciativa publica y privada, y fundamentalmente una colaboración con otros países en el tema.

A pesar de la importancia de este Convenio Internacional, Guatemala aún no ha podido adherirse, actualmente lucha por demostrar esfuerzos en el desarrollo de normativas y buenas prácticas que le permitan perfilarse como un país que tiene como una de sus prioridades la seguridad cibernética. Sin embargo lo establecido en este Convenio ha servido como guía de seguridad de la red para todos los países del mundo, aunque no estén integrados.

4.1.1.3. Organización de Estados Americanos

Adopción de una Estrategia Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética

(Asamblea General .Resolución AG/RES. 2004 (XXXIV-O/04). 8 de junio de 2004)

La estrategia de seguridad integral es la acción mas relevante de ciberseguridad entre Estados americanos, cuyo fin es mantener la paz de este campo de acción.

Este documento reconoce la responsabilidad nacional y regional del sector público y privado en aspectos políticos y técnicos para la seguridad del ciberespacio.
La Estrategia Interamericana Integral de Seguridad Cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA).

Establece un marco para la protección de las redes y sistemas de información y para responder incidentes y recuperarse de los mismos a través de las siguientes acciones:

- Se proporcione información a los usuarios y operadores para ayudarles a asegurar sus computadoras y redes contra amenazas y vulnerabilidades
- Se fomenten asociaciones públicas y privadas para incrementar la educación y la concientización
- Se identifiquen y evalúen normas técnicas y prácticas óptimas para asegurar la seguridad de la información
- Se promueva la adopción de políticas y legislación sobre delito cibernético que protejan a los usuarios de Internet y prevengan y disuadan el uso indebido e ilícito de computadoras y redes informáticas, respetando a su vez la privacidad de los derechos individuales de los usuarios de Internet.

Este compromiso deben llevarse a cabo a través de las acciones de los Estados miembros y las actividades que emprenda el CICTE, CITEL, y REMJA que son:

a) Comisión Interamericana de Telecomunicaciones (CITEL):

Identificación y adopción de normas técnicas internacionales para una arquitectura segura de Internet a través de una alianza entre el gobierno de los Estados miembros, las industrias de telecomunicaciones y las industrias de tecnología de la información. Asimismo busca fomentar el intercambio de información para promover redes seguras, y evaluar los asuntos técnicos relativos a las normas requeridas para

la seguridad de las redes futuras y existentes de la región con apoyo del trabajo del Sector de Normalización de la Unión Internacional de Telecomunicaciones (UIT-T).

b) Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA)

Su papel fundamental es asegurar que las autoridades policiales y judiciales de Estados miembros cuenten con instrumentos jurídicos necesarios para proteger las redes de información a través de la investigación o enjuiciamiento; y para ello proponen la redacción y promulgación de legislación en materia de delito cibernético y mejoramiento de la cooperación internacional en asuntos relativos al tema.

También incluye que un Grupo de Expertos debe proporcionar a los Estados miembros asistencia técnica a través de talleres regionales para la redacción y promulgación de leyes que tipifiquen el delito cibernético, así como fomentar la cooperación entre los investigadores, las autoridades policiales y judiciales que investigan y procesan casos de delitos cibernéticos. Los talleres se concentran en la promulgación de dos categorías de leyes: Las Leyes Sustantivas sobre Delitos Cibernéticos y Leyes Procesales Para la Recopilación de Pruebas Electrónicas.

c) Comité Interamericano Contra el Terrorismo (CICTE):

- **Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSIRT):** Con la capacidad y el mandato de divulgar correcta y rápidamente información relacionada con la seguridad cibernética y proporcionar orientación y apoyo técnico en el caso de un incidente cibernético.

- **Creación de la red hemisférica de CSIRT:**
  Que trabaje a través de la Identificación de organizaciones CSIRT existentes para prevenir la duplicación de esfuerzos.

- **Establecimiento de un modelo de servicio**
  Los CSIRT nacionales deben ser designados por sus gobiernos respectivos y serán certificados y autorizados de acuerdo con las normas internacionales de

la comunidad de servicios informáticos. También deberán establecerse un conjunto mínimo de normas para la cooperación y el intercambio de información entre los CSIRT

- **Formación de una Red Interamericana de Vigilancia y Alerta 24/7:**
  Para la rápida divulgación de información sobre seguridad cibernética y la respuesta a crisis, incidentes y amenazas a la seguridad informática.

  En la actualidad Guatemala forma parte de la Red 24/7 que actualmente está a cargo de la Sección de Delitos Informáticos y Propiedad Intelectual de la OEA y a nivel nacional está funcionando por medio del MINISTERIO PUBLICO.

  La finalidad de ésta se concentra en la "preservación de los datos", es decir de la "evidencia digital" que sirve para fundamentar las acusaciones sobre ciberdelincuentes. Sin embargo no constituye un sustituto de los procedimientos formales establecidos en los tratados de asistencia jurídica mutua. (Alvarado y Morales. 2012. P. 176)

4.1.2. Legislación Nacional

El desarrollo de nuevas tecnologías a través del tiempo y los fenómenos sociales asociados a ellas generan una necesidad de reformas a las leyes, de lo contrario muchos elementos quedarían vulnerables. A causa de las modalidades innovadoras de hechos delictivos en materia tecnológica en Guatemala se hizo indispensable las reformas al Código Penal para prohibir y sancionar las conductas relacionadas.

De esa forma el Congreso de la República introdujo modificaciones a la ley sustantiva penal a través del Decreto 33- 96 publicado en fecha 21 de Junio de 1996. En la normativa se expone: "Que los avances de la tecnología obligan al Estado a

legislar en bien de la población de derechos de autor en materia informática tipos delictivos que nuestra legislación no ha desarrollado".

En ese sentido en materia de delitos informáticos se regulan los tipos siguientes:

4.1.2. 1. Delitos Informáticos del Código Penal que Afectan el Patrimonio y la Propiedad Intelectual

- **Violación de Derechos de Autor**

El artículo 274 del Código Penal determina que comete esta acción delictiva (en materia informática para fines del presente estudio) quien:

-Identifique falsamente la calidad de titular de un derecho de autor.

-La reproducción de una obra sin la autorización del autor o titular.

-La adaptación, arreglo o transformación de todo o parte de una obra protegida sin la autorización del autor o del titular del derecho;

-La comunicación al público por cualquier medio de una obra sin la autorización del titular del derecho correspondiente.

-La distribución no autorizada de reproducciones de todo o parte de una obra por medio de su venta, arrendamiento, préstamo o cualquier otra modalidad.

-La fijación, reproducción o retransmisión de una difusión transmitida por satélite, radio, hilo o cable, fibra óptica o cualquier otro medio sin la autorización del titular del derecho;

- **Destrucción de Registros Informáticos**

Dentro del Art. 274 "A" C.P. Realiza esta figura delictiva quien destruya, borre o de cualquier modo inutilice registros informáticos tanto públicos como privados; surge de la necesidad de proteger los archivos, bases de datos y en general todo registro informático que se encuentre en un ordenador tanto en la esfera gubernamental pública como la empresarial o personal.

- **Reproducción de Instrucciones o Programas de Computación**

El Art. 274 “C” C.P. afirma que comete este delito el que sin autorización del autor copia o de cualquier modo reproduzca las instrucciones o programas de computación. De estrecha relación con respecto al delito de violación a los derechos de autor y dirigida específicamente a su protección en el ámbito informático, esta figura delictiva busca proteger los bienes jurídicos tutelados de carácter patrimonial, así como el reconocimiento de la calidad de autor o inventor de instrucciones o programas informáticos.

Un ejemplo de los programas informáticos pueden ser los programas para la liquidación de la nómina, inventarios, manejo de cartera, etc. (Noriega. 2011. P.40)

- **Manipulación de Información**

En el Art. 274 “E” C.P. establece que presenta este delito cuando se utilizan registros informáticos o programas de computación para alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.

- **Registros Prohibidos**

Determina el Art. 274 “D” C.P que esta conducta se presenta por la persona que crea un banco de datos o un registro informático con datos que pudieran afectar la intimidad de las personas. Un ejemplo puede ser el caso de quien crea una página, un blog un foro de opinión en la red y en ella registra información íntima, privada o confidencial, que afecte la intimidad personal.

- **Programas Destructivos**

El Art. 274 “G” C.P. Se concentra en quien distribuya o ponga en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.

- **Delito de Pánico Financiero**

Contenido en el Art. 342 “B” C.P .Se tipifica cuando se elabora, divulga o reproduce por cualquier medio información falsa o inexacta (correo electrónico o uso de redes sociales por ejemplo) que perjudique la confianza de los usuarios de una institución bancaria o financiera de modo que se produzca un resultado negativo tanto para la institución, la economía nacional y el patrimonio de sus clientes. Dicha información debe atentar contra la reputación, el prestigio de la institución o provocar un retiro masivo de depósitos e inversiones. (Ídem. P.44)

4.1.2.2. Delitos Contra la Libertad, la Indemnidad Sexual y la Intimidad

El término indemnidad sexual definido por el autor Hans Noriega (2011. P. 45) está relacionado directamente al libre desarrollo de la sexualidad, es la seguridad y protección que deben tener todos en el ámbito sexual para contar con la capacidad de reflexión y decisión; se refiere a aquellas personas que carecen o que no han logrado un desarrollo de su madurez lo suficientemente adecuado para determinar la conveniencia o no de las relaciones sexuales, de esa cuenta que requiera especial atención por parte del Estado en aspectos específicos como es el caso de los menores de edad.

Dentro de los ilícitos de carácter informático que el Código Penal (reformado por la ley contra la violencia sexual) contempla en relación a este bien jurídico tutelado tenemos:

- **Ingreso a Espectáculos y Distribución de Material Pornográfico a Personas Menores de Edad**

Contenido en el Art. 189 del C.P. Se tipifica este ilícito penal en el ámbito informático cuando el sujeto activo se sirve de las facilidades que brindan las computadoras y sus programas para que personas menores de edad puedan acceder a material pornográfico.

- **Violación a la Intimidad Sexual**

En el Art. 190 del C.P. se afirma que el delito se materializa por la persona que por cualquier medio sin el consentimiento del sujeto pasivo atentare contra su intimidad sexual y se apodere o capte mensajes, conversaciones, comunicaciones, sonidos, imágenes en general o imágenes de su cuerpo para afectar su dignidad. Esta conducta se agrava cuando se difunde, cede o revela a terceros la información o las imágenes.

- **Producción de Pornografía de Personas Menores de Edad. Comercialización o Difusión de Pornografía de Personas Menores de Edad, Posesión de Material Pornográfico de Personas Menores de Edad.**

Los artículos 194 y 195 del C.P. buscan frenar la elaboración venta y posesión de pornografía en la que intervengan menores de edad o bien personas incapaces de voluntad o conocimiento. En este caso el acceso ilimitado a la información de carácter informático ha facilitado el aparecimiento de acciones como estas. Estos delitos se tipifican por quienes producen, fabriquen, elaboren, publiquen, reproduzcan, importen, exporten, distribuyan, transporten, exhiban, elaboren propaganda, difundan, comercien o bien adquieran material pornográfico infantil.

Ley de Acceso a la Información Pública en el artículo 64 del Decreto 57-2008 del Congreso de la República tipifica el delito de:

- **Comercialización de Datos Personales**

Se establece que quien comercializa o distribuya por cualquier medio archivos de información o datos personales, datos sensibles o personales sensibles protegidos por dicha ley comete esta acción delictiva. En ese sentido el espíritu de la norma va dirigido a la prohibición de venta o distribución de registros o archivos que contengan referencias o detalles personales o considerados sensibles.

Los datos sensibles según la misma ley se refieren a aquellos que se refieran a las características físicas o morales, hechos de la vida privada o actividad, origen racial, étnico, ideologías políticas, creencias religiosas, salud físicos o psíquicos, preferencia sexual, situación moral, familiar u otras cuestiones de similar naturaleza.

A continuación se presenta un cuadro comparativo de reformas a la legislación en materia de delitos informáticos en algunos países de América Latina, incluyendo Guatemala.

Cuadro No. 2
Reformas a la Legislación en Materia de Delitos Informáticos

REFORMAS EN MATERIA DE DELITOS INFORMÁTICOS

Países	Acto normativo	Contenido	Técnica
Chile	Ley 19.223/1993 sobre delitos informáticos	Figuras previstas: 1.- acceso indebido a información contenida en un sistema de tratamiento de la misma; 2.- destrucción de un sistema informático o alteración del funcionamiento del mismo; 3.- daño, alteración y divulgación indebida de datos informáticos. Nuevo proyecto de ley (mensaje del Ejecutivo boletín N° 3083-07) que introduce nuevos delitos informáticos, no especialmente incriminados en la legislación anterior; a saber: 1.- falsificación de documentos electrónicos y tarjetas de crédito 2.- fraude informático; y 3.- obtención indebida de servicios de telecomunicaciones.	Ley especial
Colombia	Ley 679 de 2001 sobre pornografía infantil en redes globales	Medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio	Ley especial (El Código Penal Colombiano expedido con la Ley 599 de 2000, no hace referencia expresa a los delitos informáticos como tales)
Costa Rica	Ley No. 8148	Adición de los artículos 196 bis, 217 bis y 229 bis al Código penal; ley n. 4573 para reprimir y sancionar los delitos informáticos. Figuras: Violación de comunicaciones electrónicas, Fraude informático, Alteración de datos y sabotaje informático,	Código penal
Cuba	Reglamento de Seguridad Informática en vigor desde Noviembre de 1996	Estipula que en todos los Órganos y Organismos de la Administración Central del Estado se deberán analizar, confeccionar y aplicar el "Plan de Seguridad Informática y de Contingencia"; y el Reglamento sobre la protección y seguridad técnica de los sistemas informáticos, emitido por el Ministerio de la Industria Sideromecánica y la Electrónica, también en vigor desde Noviembre de 1996.	Reglamento
Ecuador	Ley No. 2002-67, de comercio electrónico, firmas y mensajes de datos. Ningún instrumento legal específico. Referencia a la tipificación del código		Algunas normas penales en la ley de comercio electrónico.
El Salvador	Código penal. No consta disciplina específica		Código penal
Guatemala	Código penal - CAP VII (De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos) Código del 1973, reformado en este capítulo en 1996 y 2000.	Figuras: tutela derecho de autores (robo uso y gestión de obras sin la autorización del autor); destrucción de registros informáticos; manipulación de información; violación a los derechos de propiedad industrial	Código penal

Fuente. Jacopo Gamba. (2010) Panorama del Derecho Informático en América Latina y el Caribe. Comisión Económica para America Latina y el Caribe CEPAL. Chile

Según el cuadro el intento de regular estos fenómenos criminales ha encontrado diferentes soluciones a nivel legislativo. Aparentemente algunos países han preferido reformar sus Códigos Penales (**Costa Rica, Guatemala**), mientras que algunos han introducido leyes específicas en la materia (**Chile, Colombia**). **Ecuador** ha utilizado una ley de contenido civil-comercial como la de comercio electrónico para introducir normas penales. En Cuba existe un reglamento y El Salvador en su Código Penal no consta de la disciplina específica. Cabe señalar que en los países donde no ha habido todavía habido una reforma en este campo, se trata de reinterpretar la normativa vigente en materia penal para incluir tipos de delitos informáticos que no son regulados por leyes específicas. En este caso, esta situación de adaptación de la ley general a casos específicos que no están claramente previstos, aumenta el riesgo de impunidad, porque algunos delitos informáticos pueden no tener los requisitos mínimos de parecidos hechos penales clásicos. (Gamba J. 2010. p.24)

4.1.3. Iniciativa de Ley de Delitos Informáticos y Cibercrimen (Numero 4055 del Congreso de la República)

En la actualidad Guatemala no cuenta con una legislación especial que regule normas relativas a delitos informáticos cometidos a través de medios tecnológicos; únicamente como se presentó anteriormente en el estudio, se han hecho modificaciones al Código Penal, que no responden a todas las amenazas informáticas presentes y en constante desarrollo.

Por este motivo en el año 2009 se presentó en el Congreso de la República la iniciativa 4055, identificada como Ley de Delitos Informáticos. Esto surge como un mecanismo para la prevención y sanción de los delitos informáticos, haciendo énfasis en la protección a los tres elementos fundamentales y denominador común en las normativas de otros Estados relativas al tema: confidencialidad, integridad y disponibilidad de datos y tecnología de la información. También pretende ser una normativa que sea uniforme con los convenios internacionales sobre ciber delincuencia.

También es importante mencionar que esta ley incluye definiciones legales para el tema de ciber crimen y pretende sancionar actos como cracking (daño o sabotaje), hacking (acceso sin autorización), phishing, smashing, vishing (invitación de acceso a sitios o sistemas informáticos falsos o fraudulentos) , pornografía infantil entre otros delitos. (López, G. 2011. p. 47)

Asimismo de buscan la imposición de sanciones drásticas a los responsables de delitos tipificados en la ley y que refieren daño informático, fraude informático, reproducción de dispositivos de acceso[7], espionaje informático, pornografía infantil, acceso ilícito mediante interceptación, interferencia o utilización de sistemas o datos informáticos, posesión de equipos o prestación de servicios para daño informático, falsificación informática e invitación de acceso a sitios o sistemas informáticos falsos o fraudulentos. También incluye una sección donde plantea las facultades del Ministerio Publico en la investigación y mejores prácticas de recopilación de evidencia dentro de los estándares internacionales relativos al tema. Dentro del contenido es importante resaltar:

Artículo 10. Violación a la disponibilidad. Que establece como delito que quien por cualquier medio, provoque la denegación de acceso a redes, información y sistemas que utilicen tecnologías de información, a las personas que están legitimadas para hacerlo. La sanción se aplicará también cuando la denegación de acceso, sea provocada por el envío masivo de mensajes electrónicos, publicitarios o de cualquier otra índole.

Este es un elemento importante dentro del estudio, debido a que el grupo Anonymous en Guatemala se ha caracterizado a lo largo de cuatro años por ataques programados DoS (denegación de servicio) a las páginas de Internet gubernamentales, mediante la sobrecarga de solicitudes a una paina Web proveniente de una o varias computadoras. Y en este momento no existe una acción de investigación o sanción por parte de las autoridades debido a que este tipo de ataques no están tipificados en la legislación.

[7]

También es relevante el Capítulo III, relativo a los Delitos Contra la Nación y Actos de Terrorismo:

Art. 19. Delitos contra la Nación. Los define como los actos que se realicen a través de un sistema que utilice tecnologías de la información, que atenten contra los intereses fundamentales y seguridad de la Nación, tales como el sabotaje, el espionaje o proveer información no autorizada.

Art. 20. Actos de terrorismo informático. Establece que todo aquel que con el uso de sistemas que utilicen tecnologías de la información, ejerza actos de terrorismo contra la infoestructura del Estado, será castigado con pena de diez a veinte años de prisión.

Este artículo es importante debido a que incluye como delito el terrorismo informático; la dificultad radica en la definición o delimitación del término "terrorismo informático" para la aplicación de la ley tomando en cuenta que hasta el momento no existe una definición exacta del mismo. Alvarado y Morales. (2012) p.49, creadores del Proyecto de Ley 4055 en su "libro Cibercrimen" lo definen como "daño a la infraestructura crítica, es decir cualquiera que vulnere los activos, sistemas, redes físicas o virtuales que son vitales para la sobrevivencia del Estado".

El Art. 21 indica las funciones que debe cumplir el Comité de Respuesta a Incidentes de Seguridad Informática para Guatemala (CSIRT-gt) adscrito al Ministerio de Defensa. En este caso se delimitan a tres fundamentalmente: proactivas (educación, asesoría técnica), reactivas (asistencia a incidentes), e investigación y desarrollo.

El Art. 25 se refiere a la creación de una Fiscalía Especial del Ministerio Público encargada específicamente de la investigación y persecución de delitos contenidos en la ley.

El Título IV se refiere a la Cooperación Internacional y Asistencia Jurídica Mutua. Este apartado incluye del artículo 44 al 50 las disposiciones referentes a la

Cooperación Internacional en materia técnica y económica que Guatemala deberá propiciar, así también la promoción regular de la capacitación técnica para los funcionarios responsables de los controles de seguridad interna y externa relacionados con delitos informáticos.

Guatemala también deberá fomentar reuniones interinstitucionales de seguridad informática nacional e internacionalmente. Procurará concertar acuerdos bilaterales o multilaterales referentes a los delitos informáticos y uno de los elementos fundamentales: la asistencia jurídica mutua, la cual indica que el Estado de Guatemala podrá formalizar con otros Estados la prestación de asistencia judicial recíproca en las investigaciones, procesos y actuaciones judiciales frente a delitos informáticos, lo cual de ser aprobado representaría un cambio trascendental debido a que actualmente no existe una colaboración de Guatemala en el ámbito internacional ni en matería técnica, reactiva o legal relevante.

4.2. Rol del Comité Interamericano Contra el Terrorismo en su Incidencia en el Estado de Guatemala

Resolución de la Asamblea General de la Organización de Estados Americanos AG/RES. 1939 (XXXIII-O/03) “Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética” aprobada el 10 de junio del año 2,003.

A través de este instrumento se consideró que los Estados miembros de la OEA debían desarrollar una estrategia para hacer frente a las amenazas de seguridad cibernética. También se fundamenta esta resolución en la continuidad de la aprobación de la resolución de la Asamblea General de las Naciones Unidas, aprobada en 2002; resolución número 27/239 sobre los elementos para la creación de una ***Cultura Mundial de Seguridad Cibernética para Sistemas y Redes de Información***. En la parte resolutiva de la resolución AG/RES. 1939, se dispone:
1.2.1 Encomendar al Comité Interamericano Contra el Terrorismo (CICTE). La Comisión Interamericana de Telecomunicaciones (CITEL), y el Grupo de Expertos

Gubernamentales Sobre el Delito Cibernético de la Reunión de Ministros de Justicia o de Ministros o de Procuradores Generales de las Américas (REMJA), que se aseguren de que la Conferencia de la Organización de los Estados Americanos (OEA) sobre seguridad cibernética, propuesta por la Argentina, empiece a trabajar en el desarrollo de un proyecto de estrategia integral de la OEA sobre seguridad cibernética, que aborde los aspectos multidimensional y multidisciplinario de la seguridad cibernética, y que informen sobre los resultados de la reunión y sobre el trabajo de seguimiento que se considere apropiado, a la Comisión de seguridad Hemisférica para su consideración.

Fue así como los Estados del hemisferio, reunidos en el cuarto período de sesiones del Comité Interamericano Contra el Terrorismo CICTE, una vez mas declararon su compromiso para combatir el terrorismo incluidas las amenazas a la seguridad cibernética. En esta ocasión, el CICTE también consideró el documento **"Marco para Establecer una Red Interamericana CSIRT de Vigilancia y Alerta"**

Es así como Guatemala asume la responsabilidad de la formación de una Red Interamericana de Vigilancia y Alerta, para la rápida divulgación de información sobre seguridad cibernética y la respuesta a crisis, incidentes y amenazas de seguridad informática. Y crea a partir del 2009 un Comité Nacional de Prevención de Delitos Cibernéticos (CSIRT-gt). Su significado deriva del idioma inglés Computer Security Incident Response Team.

4.2.1. CSIRT en Guatemala

El Comité está integrado por funcionarios de los Ministerios de Defensa, Relaciones Exteriores, Ministerio Público e iniciativa Privada.

Según Ronald Morales, creador del CSIRT en Guatemala, en su libro Cibercrimen p.118 el CSIRT-gt en un repositorio de información de incidentes, un centro de respuesta y análisis de incidentes, así como un coordinador de respuestas a incidentes a través de la organización. A través de funciones:

a. Proactivas: Consistentes en educación, asesoramiento técnico, alertas y promoción de estándares de seguridad.

b. Reactivas: Consistentes en la asistencia a incidentes de seguridad informática, tanto a instituciones públicas como privadas y la realización de todos aquellos actos de mitigación de daño en materia informática.

c. Investigación y Desarrollo: Consistente en actividades que generen proyectos de investigación y desarrollo de tecnologías relativas a la seguridad informática.

El objetivo principal de un CSIRT es proteger infraestructuras críticas de información, en base al servicio al que esté destinado. En el caso del CSIRT nacional, deberá proteger la infraestructura crítica del país.

Cada país tiene recursos que son de carácter estratégico, cada uno de estos cuentan con sistemas de información que permiten conocer su ubicación, estado, producción y a medida que este recurso es más escaso o más cotizado en el mercado internacional, puede convertirse en más importante y esto convertirlo en fundamental para la supervivencia del Estado.

Sin embargo, en términos generales, se consideran infraestructuras críticas por sectores: Telecomunicaciones, Servicios de Agua potable, Energía, Industria, Salud Pública, Gobierno y Servicios financieros.

Actualmente el equipo coordinador lo conforman: Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional y 2 Asesores de seguridad de la información. Sin embargo, en más de alguna vez han participado las siguientes instituciones[8]:

[8] CSIRT Guatemala, (2013) de http://www.csirt.gt

- Ministerio de Relaciones Exteriores
- Superintendencia de Telecomunicaciones
- Ministerio de la Defensa Nacional
- Clúster de Tecnologías de la Información y Comunicación de Guatemala
- Ministerio de Gobernación
- Secretaría General de Planificación y Programación de la República, SEGEPLAN
- Superintendencia de Administración Tributaria
- Superintendencia de Bancos
- Procuraduría General de la Nación
- Comisión Portuaria Nacional
- Consejo Nacional de Ciencia y Tecnología
- Comisión Presidencial para la Reforma, Modernización y Fortalecimiento del Estado y de sus Entidades Descentralizadas, COPRE
- Organismo Judicial
- Universidad del Valle de Guatemala
- Universidad Rafael Landívar

Sin embargo, es importante mencionar que en la actualidad según entrevista al Señor Embajador ante la OEA y ex Presidente del CICTE Rodrigo Vielmann el CSIRT-gt ha perdido interés por parte de las entidades de Gobierno, principalmente por el Ministerio de Defensa, el cual estaba adscrito a éste. Actualmente se ha desligado y trabaja en colaboración tanto con iniciativa privada como pública. Asimismo, de palabras del Ing. Morales en el blog Retico, Tecnología desde Otra Óptica afirma que en "Guatemala actualmente se encuentra funcionando de manera reducida, dando únicamente asesoría y soporte en casos específicos en los cuales le han solicitado asistencia"[9].

Igualmente es relevante el tema de las limitaciones que posee el CSIRT-gt para poder trabajar, debido a que la falta de una ley enfocada al crimen cibernético, no le permite actuar o desarrollar las actividades proactivas, reactivas y de investigación a cabalidad. Asimismo en entrevista personal con el Ing. Morales afirma que

[9] Que es un CSIRT (2014) de http://retico.gt/2014/01/08/que-es-un-csirt-o-cert/

actualmente el CSIRT de Guatemala ha colaborado con CSIRT de otros países del continente, sin embargo ha sido muy poco, y lo que aportan no puede ser utilizado como medio de prueba y validado en un juicio, debido a que “no tienen la calidad en este momento para poder apuntar estas pruebas” a causa del problema de las normativas nacionales que no tipifican estos delitos.

4.2.2. Ejemplos de Centros de Respuesta a Incidentes de Seguridad Informática en América Latina

a. Brasil

En la República federativa de Brasil existe un Gabinete de Seguridad Institucional (GSIPR), el cual según el capítulo 6 de la Ley No. 10,683 tiene como competencia “coordinar las actividades de inteligencia y de seguridad de la información”. Alvarado y Morales (2012 p. 119).

Estas áreas están representadas por dos instituciones: Departamento de Seguridad de la Información y Comunicaciones (DSIC) y, La Agencia Brasileña de Inteligencia (ABIN). Según la ley los campos que abarca la seguridad de la información y comunicaciones son:

a) Seguridad de recursos humanos
b) Seguridad de los sistemas de información y comunicaciones
c) Seguridad de Áreas e Instalaciones
d) Seguridad de Materiales
e) Detección y preservación de amenazas
f) Valoración de las amenazas por quiebra de la seguridad

Las competencias establecidas en la Ley de Brasil para el DSIC, son:

- Estudiar legislaciones correlacionadas e implementar las propuestas sobre materiales relacionadas a la seguridad de la información y comunicaciones.

- Avalar tratados, acuerdos suscritos en actos internacionales, relacionados a la seguridad de la información y comunicaciones
- Adoptar las medidas necesarias y coordinar el funcionamiento del Sistema Nacional de Acreditamiento –SISC de personas y empresas, trato de asuntos, documentos y tecnología sigilosa.
- Planificar y coordinar la ejecución de actividades de seguridad de la información en la administración del manejo de documentos, información y tecnología reservada.
- Definir requisitos metodológicos para la implementación de seguridad de la información y comunicaciones, por los órganos de administración pública federal.
- Operacionalizar y mantener el Centro de Tratamiento y Respuesta a incidentes ocurridos en las redes de computadoras de la Administración pública federal.

El DSIC realiza las siguientes actividades:

- Revisión de la legislación aplicable
- Propuesta de Decreto Presidencial que norma la acreditación de la seguridad
- Acuerdos Internacionales sobre materias clasificadas
- Concepción del modelo Brasileño de gestión de materiales sensibles
- Proyecto de desarrollo de sistemas de información
- Cursos de formación de Gestores y multiplicadores de la seguridad de la información
- Entrenamiento en fundamentos de seguridad de la información.

Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad en Brasil CERT.br

Es el equivalente al Centro de Respuesta a Incidentes de Seguridad Informática CSIRT. Es el responsable de recibir, analizar y responder a incidentes de seguridad,

que relacionan a redes conectadas a Internet en Brasil. También actúa a través del trabajo de concientización sobre los problemas de seguridad, correlaciona los eventos en la Internet brasileña y da auxilio al establecimiento de nuevos CSIRTS en Brasil.

Los servicios que presta son:

- Ser un punto “único” para notificaciones a incidentes de seguridad a modo de proveer coordinación y apoyo necesario en el proceso de respuesta a incidentes, colaborando con las partes envueltas cuando sea necesario.
- Establecer un trabajo colaborativo con otras entidades, como la policía y proveedores de acceso a servicios de Internet.
- Dar soporte en el proceso de recuperación y análisis de sistemas comprometidos.
- Ofrecer entrenamiento en el área de respuesta a incidentes de seguridad

b. Uruguay

El CSIRT de la Administración Nacional de Telecomunicaciones ANTEL, es un Centro de Respuesta a Incidentes y tiene como servicio central realizar una gestión de incidentes de seguridad eficaz y eficiente. Para ello sus integrantes buscan, en el contexto de su Código de Conducta, relacionarse con equipos pares y con su comunidad, capacitarse permanentemente, estar al día tecnológicamente y mejor de manera continua los servicios brindados. (Alvarado y Morales. 2012 p. 124).

Los servicios que presta son:

a) Reactivos
    1. Alertas
    2. Manejo de incidentes

b) Proactivos
    1. Anuncios
    2. Detección de incidentes

También se dedica a:

- Desarrollo de técnicas y herramientas
- Elaboración de políticas y mejores prácticas
- Capacitación y entrenamiento
- Análisis de riesgos
- Consultoría en seguridad
- Concientización de la comunidad en temas de seguridad

c. Colombia

Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT

Creado en el año 2011 por el Ministerio de Defensa Nacional. Tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual está enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional[10].

Sus responsabilidades:

- Coordinar y asesorar a CSIRT's y entidades tanto del nivel público, como privado y de la sociedad civil para responder ante incidentes informáticos.

[10] Acerca de COLCERT. (2013) de http://www.colcert.gov.co/?q=acerca-de .

- Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos, así como a aquellos de información, sensibilización y formación en materia de seguridad informática.
- Actuar como punto de contacto internacional con sus homólogos en otros países, así como con organismos internacionales involucrados en esta técnica.
- Promover el desarrollo de capacidades locales/sectoriales, así como la creación de CSIRT's sectoriales para la gestión operativa de los incidentes de ciberseguridad en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.
- Desarrollar y promover procedimientos, protocolos y guías de buenas prácticas y recomendaciones de ciberdefensa y ciberseguridad para las infraestructuras críticas de la Nación en conjunto con los agentes correspondientes y velar por su implementación y cumplimiento.
- Coordinar la ejecución de políticas e iniciativas público-privadas de sensibilización y formación de talento humano especializado, relativas a la ciberdefensa y ciberseguridad.
- Apoyar a los organismos de seguridad e investigación del Estado para la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.
- Fomentar un sistema de gestión de conocimiento relativo a la ciberdefensa y ciberseguridad, orientado a la mejora de los servicios prestados por el colCERT.

Comando Cibernético Policial (CCP)

Su trabajo está enfocado en tres aspectos fundamentales:

a) Prevención:

   -Sensibilización -Difusión

b) Observatorio Nacional de Cibercrimen

-Análisis de Información -Atención de Incidentes

c) Investigaciones Tecnológicas

-Judicializaciones -Investigación Tecno-científica y desarrollo.

El trabajo entre el CCP y el colCERT ha sido muy coordinado y colaborativo. El colCERT ha suministrado al CCP, información de soporte para la identificación de perfiles de integrantes de Anonymous. (Ministerio de Defensa República de Colombia, 2012).

El CCP ha brindado apoyo constante al colCERT en la investigación judicial de diferentes casos en los que se ha comprometido la ciberseguridad de varias entidades del Gobierno y del sector privado.

En conjunto el colCERT y CCP han respondido a incidentes de ciberseguridad, en donde se ha asesorado a diferentes organismos en temas de ciberseguridad y se ha atendido judicialmente incidentes.

Colombia ha sido pionera en América Latina al crear la primera Política Nacional de Ciberseguridad y Ciberdefensa Nacional.

4.2.3. Plan de Trabajo 2012 del Comité Interamericano Contra el Terrorismo

A continuación se expone un fragmento del plan de trabajo correspondiente al año 2012 del CICTE, dentro del cual se desarrolla programa relativo a la seguridad cibernética, el cual está enfocado al área de trabajo de la protección a la infraestructura. Dentro del cuadro se incluyen las nueve actividades propuestas con una breve explicación de cada proyecto.

Cuadro No. 3

Plan del Comité Interamericano Contra el Terrorismo Relativo a la Seguridad Cibernética

No.	PROYECTO	ACTIVIDAD
1.	Ejercicios nacionales de gestión de crisis de seguridad cibernética	2 ejercicios nacionales
2.	Crear un foro virtual en el que todos los CSIRTs en los Estados miembros tengan la oportunidad para relacionarse unos con otros, para incrementar la cooperación y el intercambio de información mediante buenas prácticas en seguridad cibernética, talleres y simposios.	2 actividades regionales
3.	Reuniones de discusión de funcionarios de desarrollo de políticas.	2 reuniones de discusión sub-regionales
4.	Desarrollar equipos nacionales de CSIRT mediante capacitaciones técnicas y actividades de desarrollo de capacidades.	1 taller sub-regional 2 talleres nacionales 4 cursos binacionales
5.	Becas para participar en cursos de capacitación en seguridad cibernética	10 becas
6.	Crear una plataforma paralela que permita la participación, cooperación e intercambio de información de los interesados del sector público y privado, así como de otros actores que trabajen en aspectos de seguridad cibernética.	A ser determinada según financiamiento
7.	Desarrollar una base de datos de estrategias nacionales e internacionales vigentes de seguridad cibernética y proveer conocimiento para apoyar a los Estados Miembros en sus esfuerzos para establecer sus respectivas estrategias nacionales.	A ser determinada según financiamiento
8.	Apoyar a los Estados Miembros, a su solicitud, a desarrollar campañas nacionales que aborden buenas y seguras prácticas para el uso de tecnologías de la información y la comunicación.	A ser determinada según financiamiento
9.	Identificar un equipo multinacional de expertos que estaría disponible para apoyar a los Estados miembros, a solicitud de éstos, en procesos y eventos de particular relevancia para proveer consejo y apoyo en análisis de vulnerabilidades, seguridad de las redes de información y bases de datos, prevención y mitigación de incidentes, y otras áreas relacionadas con la seguridad cibernética.	A ser determinada según financiamiento

Fuente: Elaboración propia en base a información de sitio Web oficial CICTE http://www.cicte.oas.org/

Según el cuadro anterior, de la serie de proyectos establecidos en este Plan Anual Continental, Guatemala tuvo la posibilidad de asistir a un taller regional sobre Delito y Seguridad Cibernética en Costa Rica en el mes de Marzo del 2012. La información de esta actividad fue recopilada de un informe privado de la Organización de Estados Americanos, brindado por Embajador de Guatemala ante la OEA y Ex Presidente del Comité Interamericano Contra el Terrorismo Rodrigo Vielmann.

Posteriormente fue anfitrión en Antigua Guatemala de una de las actividades planteadas en el inciso 4 relativa al desarrollo de equipos nacionales de CSIRT mediante las capacitaciones técnicas y actividades de desarrollo de capacidades, a través de un taller regional de Seguridad de la Información para el Personal Técnico, donde participaron los miembros de Costa Rica, Chile, Colombia, Ecuador, El Salvador, Jamaica, Panamá, Perú, Surinam, Trinidad y Tobago, Uruguay y Estados Unidos:

a. Curso de Seguridad de la Información Para el Personal Técnico

Antigua Guatemala , 4 al 8 junio 2012

Resultados previstos:

a . Proporcionar a los técnicos de respuesta a incidentes de los Estados Miembros de la OEA con la instrucción sobre las últimas técnicas de la información de seguridad.

b . Proporcionar un foro para la discusión sobre el manejo de incidentes y mejores prácticas del CSIRT.

c . Facilitar un examen de Certificación de Manejador de Incidentes de Seguridad Informática –CSIH- para 25 funcionarios de los Estados miembros.

Logros

La Secretaría del CICTE fue capaz de convocar a los representantes de 12 Estados Miembros de la OEA para asistir al curso donde se les enseñó muchos aspectos

técnicos de la seguridad de la información y se discuten a fondo. Veinticinco técnicos se sentaron para el examen CERT -CC .

El curso trató de avanzar en los esfuerzos ya realizados por la Secretaría del CICTE en el aumento de la capacidad técnica de los funcionarios que trabajan en la respuesta a incidentes en los Estados miembros de la OEA. Los países participantes fueron El Salvador, Costa Rica, Panamá, Colombia, Perú, Uruguay, Jamaica, Suriname, Trinidad y Tobago, Chile , Ecuador y Guatemala .

Además de ayudar a mejorar las capacidades técnicas de los que responden a incidentes cibernéticos en el gobierno de Guatemala y de otros Estados Miembros de la OEA , la Secretaría del CICTE dio a los asistentes la oportunidad de recibir la Certificación de Manejador de Incidentes de Seguridad Informática –CSIH-, ofrecido por CERT -CC . Para calificar para el examen , los participantes tenían que ser aprobados por el CERT -CC como tener suficiente trabajo 25 experiencia en responder o investigar incidentes de seguridad cibernética. Todos los dieciocho participantes extranjeros fueron aprobados para el examen, y el CICTE financiaron siete funcionarios guatemaltecos para tomar el examen .

Este evento acopló módulos teóricos con ejercicios prácticos. Los módulos previstos comenzaron con los elementos de fondo de la seguridad de red, tales como la conciencia de amenazas, la supervivencia, la gestión de riesgos, cumplimiento y gestión de la configuración. A medida que avanzaba la semana, la atención se desplazó más hacia la seguridad de la red se aplica con módulos sobre la seguridad TCP / IP , la criptografía , sistemas de detección de intrusos, proteger los servidores de red y seguridad de las infraestructuras de red. Los ejercicios de laboratorio dieron contexto a los estudiantes para los módulos teóricos y los desafiaron a emplear las herramientas y técnicas de seguridad cibernética actuales para diseñar una red segura.

b. Ejercicio de Manejo de Crisis en Cyber Seguridad

Es importante mencionar que este ejercicio fue realizado un año después de la delimitación del período de tema de investigación de la presente tesis, sin embargo su relevancia y resultados son de gran importancia, debido a que fue el primer ejercicio a nivel Americano utilizando un laboratorio móvil único en el mundo, que ha servido como modelo para el continente europeo, según entrevista e informe brindado por el ex Presidente del CICTE , Embajador Rodrigo Vielmann.

Participantes: 23 funcionarios

Objetivos: prueba actual de respuesta a incidentes cibernéticos, procedimientos y capacidades en Guatemala, para poner a prueba los mecanismos de coordinación y comunicación entre las entidades de respuesta a incidentes cibernéticos guatemaltecos cuando se enfrentan con ciber- incidentes, para simular un incidente cibernético gran escala contra la infraestructura de información crítica de Guatemala operado por el sector público y privado, y para crear conciencia sobre el impacto de los ciber- ataques a la infraestructura crítica.

Informe General: Este Ejercicio de Manejo de Crisis en Seguridad Cibernética -CME- fue un esfuerzo conjunto entre el la Secretaría del CICTE de la OEA y el Gobierno de Guatemala. Se convocó a las partes interesadas de seguridad cibernética pertinentes de los sectores público y privado de Guatemala para evaluar y fortalecer su mitigación incidente cibernético y la capacidad de respuesta. El ejercicio fue la primera vez que el guatemalteco National Computer Security Incident Response Team- CSIRTgt interactuó con muchos de los actores presentes, e incorporó operadores de infraestructuras críticas del país.

El CME expone a los participantes a las amenazas de seguridad cibernética en tiempo real, lo que obligó a tratar los ataques como lo harían en la vida real. Utiliza un laboratorio móvil desarrollado por el CICTE y el Departamento de Información y

Tecnología de la OEA -DOITS- . El laboratorio cuenta con hardware avanzado y una arquitectura virtual especialmente diseñada que exige a los participantes a contribuir con sus habilidades técnicas, así como las normas de respuesta a incidentes.

Aunque el objetivo final es fomentar la mejora de la coordinación a nivel nacional, el ejercicio pretendía también lograr varios resultados intermedios importantes. Para completar con éxito la simulación, los técnicos tenían que determinar el origen y destino de los ataques simulados, así como su gravedad; analizar los datos técnicos; coordinar con el CSIRT nacional; y resolver los incidentes cibernéticos lanzados por los facilitadores del ejercicio. Al exigir a los participantes para organizar una respuesta coordinada a varios ataques cibernéticos, el ejercicio mejoró los lazos a nivel nacional entre los respondedores de incidentes y brindaron oportunidades para que puedan practicar el uso de las herramientas técnicas y los procedimientos de prueba y los procesos establecidos para gestionar las emergencias cibernéticas. El ejercicio reveló a los participantes tanto donde los individuos y departamentos necesitan entrenamiento adicional, y también donde hay deficiencias en la política o procedimiento nacional de respuesta a incidentes.

Una variedad de técnicas de hacking probados respuesta de incidentes, incluidos los ataques de denegación de servicio, desfiguraciones, entre otros. Parte del ejercicio que se que mientras investigaba los ataques, los participantes tenían que decidir qué hacer, con quién hablar , y cuándo y cómo responder. Para simular una emergencia en el mundo real, se crearon un feed de Twitter y dos periódicos en línea que mostraron a la opinión pública la incertidumbre asociada a la interrupción de los servicios esenciales que se dan fuera de línea por los ataques cibernéticos.

Resultados: Los debates celebrados durante los dos días y las encuestas posteriores al ejercicio de relieve una serie de resultados y conclusiones de los participantes. Conclusiones generales indican que la CME era útil en la preparación de los técnicos e instituciones para futuros incidentes cibernéticos mediante la simulación de escenarios de la vida real con precisión. Aunque la mayoría de los

participantes afirmaron que el ejercicio les ayudó a comprender la función y la necesidad del CSIRT nacional, sostuvieron que la CME expuesto importante las deficiencias del equipo de respuesta incipiente, así como cuestiones más amplias en cuanto a la función y la coordinación en la resolución de los incidentes cibernéticos.
En general, el CSIRT no pudo responder en forma eficaz y dar seguimiento a las consultas de asistencia técnica y orientación sobre la gestión de incidentes. Esto significaba que los sectores afectados o de los operadores de infraestructuras críticas a menudo tenían que esperar demasiado tiempo para recibir orientación sobre cómo manejar un determinado tipo de ciber-ataque o incidente. El ejercicio similar mostró que la mayoría de las partes interesadas pertinentes de seguridad cibernética incluyendo el CSIRT carecía de cualquier tipo de plan de emergencia o sistema codificado para contener, informar y resolver incidentes cibernéticos. Todo se hizo sobre una base ad hoc, lo que afectó significativamente las capacidades de todas las partes para recuperarse de los ataques de moderador-lanzado, muchos de los cuales empleaban básica a las técnicas intermedias.

Las dificultades experimentadas por el CSIRT y sus mandantes dieron lugar a una serie de conclusiones importantes. En primer lugar, el país necesita un plan de respuesta a incidentes dedicado que se difunda a todos los departamentos gubernamentales y operadores de infraestructuras críticas. Este plan debe girar en torno al CSIRT nacional, que a su vez tiene que establecer normas y directrices para la comunicación durante y gestión de incidentes cibernéticos. Del mismo modo, todos los técnicos - tanto en el CSIRT y de otros departamentos – necesitan formación técnica adicional en el análisis de intrusiones en la red y la mitigación de los mismos. Relaciones con el público también debe ser abordado. Sin una campaña o un especialista en relaciones públicas, información sobre los ataques puede ser distorsionada por la prensa y los medios de comunicación social, lo que agrava los efectos de los incidentes cibernéticos ya peligrosos, como sucedió durante el ejercicio.

Los participantes señalaron en sus evaluaciones que el ejercicio fue muy revelador en cuanto a la falta de preparación Guatemala a la hora de responder a los ataques cibernéticos. Al mismo tiempo, consideraron que hay una forma clara de mejorar en muchos aspectos de las deficiencias resaltadas durante el evento. En primer lugar, un plan de respuesta clara necesita ser elaborado y difundido dentro del gobierno y por el CSIRT. En segundo lugar, los técnicos necesitan capacitación en seguridad cibernética adicional para diagnosticar con eficacia los problemas de seguridad de red y fortalecer su capacidad de resistencia.

4.2.4. Presidencia del CICTE por parte del Estado de Guatemala

Guatemala asumió la presidencia del CICTE durante el período 2012-2013. Fue el Embajador Permanente de Guatemala ante la OEA, y actual Viceministro del Ministerio de Relaciones Exteriores Rodrigo Vielmann quien fungió como representante y Presidente.

Durante la entrevista personal el Embajador manifestó que al asumir la presidencia se debe mantener una posición objetiva sobre cada país, y que tener una posición de poder no debe representar una mayor ventaja de un país sobre otro.

Asimismo explicó cómo se priorizan la elección y ejecución de actividades nacionales y regionales de CICTE. A través de tres elementos:

1. Depende del presupuesto
2. Prioridad del Donante
3. Manifestación de Interés del país

Por ejemplo, afirma que EEUU y Canadá son de los países que aportan mas donaciones. Se considera el presupuesto anual, y sobre esto se estipula la cantidad de dinero destinado a talleres: por ejemplo $50,000 que alcanzan para 8 talleres. Se estipulan los 8 países que recibirán los talleres en función que la fuente cooperante

lo determine como prioritario o que el país previamente lo haya solicitado. Los donantes toman en cuenta la situación fiscal y política de cada país.

Sostiene que el CICTE es la segunda fuente de captación de fondos de la OEA, y de mayor eficiencia en la ejecución de fondos. Sin embargo reitera que la vida del CICTE depende año con año del financiamiento.

También aclara que en el CICTE *"no hay acción operativa para combatir el crimen cibernético"*. Simplemente promueve la capacitación en cada país miembro para las autoridades y las instancias gubernamentales encargadas de cada país. No pretenden trabajar con una institución nacional en particular, sino trabajan con quien o quienes cada gobierno designe. "Ellos son abiertos a trabajar con cualquiera".

Con respecto a las acciones del CICTE en Guatemala y el panorama de la seguridad cibernética explica que generalmente ha sido la iniciativa privada la mejor protegida porque tienen que proteger sus elementos de interés, como por ejemplo el sector económico y financiero.

El Embajador Vielmann asegura que Guatemala al realizar el primer simulacro de ataque cibernético *"evidenció que el país en la actualidad no está preparado para este tipo de ataques. Que actualmente en el Gobierno:*

1. *no hay convicción del tema,*
2. *no ha permeado en otras instituciones publicas,*
3. *no hay interés*
4. *no hay presupuesto suficiente"*

También se le consultó si consideraba que existía terrorismo cibernético en Guatemala, a pesar de no existe una definición clara del mismo a nivel internacional. A esto respondió que "es muy delicado" poder definir lo que es terrorismo debido a que si encasilla en una serie de acciones, probablemente siempre existirían actos

que se queden fuera. Además de la sensibilidad de cada país ante los ataques violentos o amenazas.

Ante esta situación considera que Guatemala si ha sufrido ataques cibernéticos, quizás no al extremo como es el caso de países como EEUU, pero definitivamente si ha sufrido algún ataque. Afirma que actualmente existen algunas iniciativas de Gobierno y nuevos intentos por parte del Viceministerio de Tecnologías de la Información del Ministerio de Gobernación en desarrollar y promover la seguridad cibernética, lo cual es un elemento positivo, sin embargo falta mucho por trabajar y mejorar.

Asimismo, en entrevista al Ing. Luis Fernando Ruiz, Técnico de la Dirección Informática del Ministerio de Gobernación afirma que en la actualidad el Ministerio de Gobernación está trabajando con la OEA en el desarrollo del tema técnico de respuesta al ataque, la investigación y el fortalecimiento del sector justicia. A lo cual concuerda que, a pesar de las iniciativas, hay muchos elementos que deben trabajarse y mejorarse en el sector Gubernamental.

4.3. Análisis de Amenazas y Retos

A continuación se presenta un análisis de las amenazas y retos más relevantes basado en los resultados de las entrevistas a los diferentes elementos de Gobierno: técnicos de informática de diversos entes, Contraloría General de Cuentas, Ministerio de Gobernación, Secretaría Técnica del Consejo Nacional de Seguridad de Guatemala, que por seguridad y privacidad de los entrevistados se declara y transfiere la información proporcionada sin especificar su identidad. Por otra parte también se incluye la opinión del Ing. Juan Carlos Argueta, Viceministro de Tecnología del Ministerio de Gobernación y del Ing. Ronald Morales, Coordinador del Centro de Respuesta inmediata a Incidentes de Seguridad Cibernética en Guatemala –CSIRTgt-.

Cuadro No. 4 ANÁLISIS DE AMENAZAS		
OPINION DE TECNICOS DE INFORMATICA DE DIVERSOS ENTES GUBERNAMENTALES	a. Falta de Apoyo Gubernamental:	• Los empleados declaran que *"No existe un perfil de personal de seguridad en la información, lo que conduce a un patrón de personal mal capacitado"*. Por ejemplo en el caso de algunas instituciones cuentan con la información básica de seguridad en la información, sin embargo no cuentan con un asesor experto y no saben ni que solicitar para mejorar sus sistemas. • Al inicio del período de este gobierno no se consentía la posibilidad de seguridad en la población, por lo que el área informática de la mayoría de entes gubernamentales estaba enfocado en el mantenimiento de aire acondicionado y mantenimiento de las computadoras. • Sostienen que cada ente gubernamental trabaja su seguridad informática de manera independiente y con su propio presupuesto. Lo cual fue confirmado por la Vicepresidenta Roxana Baldetti en conferencia de prensa. • No trabajan en coordinación con otras instituciones gubernamentales, mucho menos con otros países. • Afirman que el gobierno no promueve la capacitación entre sus empleados justificado por la falta de presupuesto: -El gobierno no crea, ni apoya en la creación de las mismas ante propuestas de los empleados. Por lo cual deben buscar sus propias fuentes de capacitación, que por lo general surge a través de cursos virtuales de universidades internacionales. -En el caso de que el empleado no tenga la iniciativa de educarse por sus medios, la seguridad de la institución puede quedar vulnerable. Sin embargo este comentario difiere entre los diversos técnicos, ya que el 75% afirma la falta de apoyo en capacitación, mientras

		el 25% sostiene que a pesar del corto presupuesto el gobierno les ha provisto de capacitaciones en el extranjero, así como becas de estudio para profesionalización del tema en la Universidad. • Los técnicos de informática testifican que el gobierno no apoya las propuestas e iniciativas por parte de empleados: -Aseguran que en muchos casos se subestima la capacidad e iniciativa de algunos entes gubernamentales que no sean Ministerios, por lo cual no se aceptan propuestas, les dicen que no tienen la importancia, ni injerencia para dichas iniciativas. -Cuando está aprobado un proyecto, lo retrasan al punto que por "falta de tiempo no es posible" -Sostienen que en *"algunos casos les roban las ideas y no les aprueban el proyecto*". -Los trabajadores afirman que en ciertas ocasiones "*se ejecutan proyectos y se lo adjudican a otros que ni siquiera participaron y lo publican los medios de comunicación*". • La seguridad en la información únicamente se aplica al banco de Guatemala, debido a que se exigen regulaciones y condiciones mínimas, por parte de la comunidad internacional.
	b. Legislación Deficiente	Reiteran que no contamos con la legislación adecuada. "*Las leyes nacionales están enfocadas en proteger el comercio electrónico, y esto únicamente por imposición del Tratado de Libre comercio con EEUU"*.
	c. Equipo e Instrumentos de trabajo:	• Afirman que en las instituciones gubernamentales en algunos casos existe equipo de buena calidad, pero que no funciona de manera correcta debido a la mala configuración de personas mal capacitadas. • Por otra parte existen modas informáticas: Existe un "cuadrante mágico"

		de marcas que son de gran influencia en Guatemala que pretenden presentar soluciones mágicas en problemas en seguridad. La comunidad informática de Guatemala no es amplia. Existen malos asesores guiados por lo mágico que pretenden mostrar que los equipos que se encuentran dentro del cuadrante son lo mejor; cuando en realidad existen buenos y mejores equipos y elementos fuera de esto, solo hay que estar informado y preparado para conocer estas opciones.
	d. Amenazas Cibernéticas:	• Afirman que el 80% de instancias de gobierno no se han dado cuenta de los ataques que han sufrido, hasta mucho tiempo después de haberlo sufrido. • Manifiestan que el Gobierno solamente se enfoca en la protección de entidades bancarias y que manejen dinero. *"El resto no es amenaza o prioridad*". • Aseveran que los empleados en seguridad nacional subestiman la capacidad de los hacker nacionales, sin embargo son personas inteligentísimas; tanto es el caso que Guatemala a nivel latinoamericano se encuentra como 5to. País en creación de MALWARE o códigos maliciosos. • Consideran que hay otras amenazas aparte de anonymous mucho mas fuertes y desafiantes, que vulneran los sistemas de seguridad, al punto de robar información valiosa. A lo que se enfrentan todos los días • En el caso de Anonymous Guatemala consideran que es un grupo formado por personas sumamente inteligentes y con grandes conocimientos de seguridad cibernética que utilizan a jóvenes desinformados se integran por necesidad de aceptación social. -Aseguran que manejan o se valen del "Factor Psicológico" - Ellos elaboran herramientas y manuales básicos, que hasta niños de 14 años pueden atacar.

		- Realizan Cursos de Ingeniería Social, que consta en tratar de manipular a las personas para obtener beneficio propio. (en el caso de obtención de la información). Los cuales son los tipos de factores que ayudan a un ataque cibernético. -Todos los técnicos concuerdan que: a pesar de presentarse como hacktivistas con fines de justicia social no pueden inspirar confianza si son personas que motivan a otras a atacar al gobierno.
	e. Acciones Contra Ataques Gubernamentales:	• Los entrevistados aseguran que en el Gobierno pasado se consideraba que para evitar los ataques había que apagar el equipo lo cual es erróneo. "*Causa del mal asesoramiento de ingenieros. Mientras que el procedimiento correcto es repeler el ataque".* • Al momento que un hacker quiere obtener esta información, intenta con un programa que permite ubicar el password, intenta con cosas elementales y si esto no es necesario utiliza la ingeniería social con los empleados gubernamentales para obtener datos que sirven como herramienta para hallar el password, y en el caso de que los empleados públicos piden "acceso total" los hackers logran tener este mismo acceso. • Manifiestan que SONNY, Microsoft, y Google, son empresas que exponen cuando sus sistemas han sido vulnerados y han obtenido la información. *"En el caso de Guatemala esto no se cumple. No comparten estas situaciones que sirven como indicadores para otros elementos de seguridad informática nacional a prevenirse o tomar en cuenta ciertas situaciones*". • Las actividades informativas gubernamentales están basadas en la seguridad física, y no de la información.
	f. Trabajo del CICTE en Guatemala:	• Sugieren la posibilidad de que *"Guatemala asumió responsabilidad de la presidencia del Comité Interamericano*

		Contra el Terrorismo como justificación para la existencia del SYCTE, para obtener mayor presupuesto y que no desapareciera". • Tienen el conocimiento de una actividad de simulacro, sin embargo afirman que no se presentaron resultados , ni informes
	g. Deep Web en Guatemala:	• Aseguran que es bastante fácil de accesar para las personas particulares. • Y testifican que el desarrollo de la seguridad informática del Gobierno de Guatemala es escaso como para poder combatir el crimen en la deep Web.
SEGÚN MINISTERIO DE GOBERNACIÓN	a. Necesidad de una Legislación Adecuada:	• Afirman que la necesidad de la aprobación de una legislación que castigue este tipo de crímenes, pero sin retipificar los delitos que en este momento ya los considera la legislación como por ejemplo estafa. • Sostienen que si no existe una legislación que lo considere como delito, lamentablemente no hay consecuencias a este tipo de ataques cibernéticos. • A causa de este motivo *"No trabajan en la investigación forense cibernética"*. Por este motivo no se cuenta con estadísticas de los crímenes o ataques cibernéticos en Guatemala, aunque buscan el fortalecimiento del tema. • *Aseguran que actualmente "El Ministerio Publico tampoco se encuentra en este momento en condición de investigar estos temas".* Así que cuando ha habido casos de personas que por ejemplo presentan un ataque y deshabilitan su pagina Web y asisten a poner su denuncia, lamentablemente en el Ministerio no saben a que oficina enviarlos o como atender estos casos. *Básicamente si no hay ley, no hay crimen que investigar*. -Es así que los crímenes relacionados con redes sociales se investigan desde otras

		perspectivas como homicidio, secuestro, violencia contra la mujer, etc. "*Sostienen No se realiza una investigación cibernética".* -En el caso de los bancos han sido vulnerables a los ataques y han perdido dinero. Obviamente no es información que se haga publica debido a lo que representa la pérdida de confianza del banco para los cuentahabientes ."*Sin embargo aseguran que los bancos al sufrir estos ataques No tienen a quien acudir; así que básicamente reaccionan ante un ataque, aún no están en la posibilidad de prevenirlo"*.
	b. Personal Especializado:	Afirman que en lo que respecta al Ministerio de Gobernación cuentan con un fuerte, aunque joven equipo técnico en informática , lo cual les ha permitido sobrellevar los retos del día a día en los temas competentes al mismo. Sin embargo en el caso del Ministerio Público no existe personal especializado que investigue estos temas, por consiguiente no hay una unidad que se dedique a esclarecer estos; esto también en parte como consecuencia de la legislación.
	c. Resistencia a Nivel de Jueces:	Gobernación sostiene que existe un resistencia a nivel de los jueces *"en parte por falta de actualización en el conocimiento de la tecnología, así como del hecho que no han necesitado recursos tecnológicos en la aplicación de su trabajo".* Por ejemplo, se cuenta con elementos como brazaletes electrónicos, que afirman su uso ya es permitido por la legislación nacional, y que serían de gran ayuda para casos específicos, sin embargo no son utilizados.
	d. Falta de un Ente Rector Nacional	Afirman que es una gran debilidad que no exista un ente rector a nivel nacional para homologar procesos en materia de seguridad cibernética.
	e. Prioridad al Sector Privado:	Declaran que la seguridad cibernética se desarrolla más en el sector privado que en el público, esto debido a que en éste no lo consideran como una prioridad. Aunque las telecomunicaciones son una de las mayores debilidades en materia de

		telecomunicaciones.
	f. Amenazas Cibernéticas:	• Manifiestan que la principal motivación de los ataque cibernéticos son por dinero, por lo que los esfuerzos van enfocados en fortalecer la seguridad de las instituciones que manejan activos económicos. • Grupos como Anonymous, cuyos ataques consisten en deshabilitar páginas institucionales sin daño de equipo o accesar a información confidencial, son importantes pero no una prioridad.
	g. Problema de Concientización:	• Afirman que es importante mencionar que la percepción en materia de seguridad, es un arma de dos filos. Expresar vulnerabilidad en los ataques puede crear preocupaciones exageradas y sin motivos en la población. • Mientras tanto consideran que el ciudadano común no se preocupa por ser víctima del delito cibernético. Se piensa que son situaciones que se viven en países grandes, sin embargo considera que la evolución y conocimiento en materia cibernética en Guatemala es quizás mayor que la que existe en EEUU.
	h. Falta de Manual o Protocolo de Respuesta a Incidentes	Se les preguntó si existía un manual o protocolo escrito a seguir en caso de un ataque, *a lo cual respondieron que en la actualidad no existe algo escrito, pero que si "existe en la cabeza de todos" los que participan en la seguridad del ministerio.* Aunque existe el proyecto de institucionalizar un manual o protocolo.
	i. Deep Web en Guatemala:	El Ministerio de Gobernación no trabaja a través de la deep web, pero si tienen conocimiento que personas en Guatemala lo utilizan.
SEGÚN RONALD MORALES, COORDINADOR CSIRT-GT	a. Falta de Atención del Estado en Seguridad Cibernética Nacional :	Manifiesta que el eslabón mas débil es por donde se rompe la cadena. Si un Estado tiene cyberciudadanos y que todos nosotros navegamos en el ciberespacio y piensa que el ciberespacio no le compete a él, o no debe protegerlo está en un error.

		"Si como Estado no se pone atención a este ciberespacio vamos a ser el eslabón mas débil y nuestras redes van a poder ser utilizadas para realizar estos ataques a cualquier otra red del mundo". En Guatemala hay casos donde han utilizado nuestras redes para hacer ataques a otros sitios.
	b. Legislación Nacional e Internacional	• **Nacional:** -El Ing. Morales asegura que la legislación actual es insuficiente, la persecución del delito informático no se puede llevar a cabo completamente, hay muchos agujeros en la ley que pueden ser utilizados para poder evadir el delito para el que lo comete. No están totalmente tipificados. -Manifiesta que actualmente como CSIRT reconocido tienen contactos, y cuando han existido incidentes, han colaborado mutuamente. Afirma que de hecho hay una promulgación constante de Derecho. Que como CSIRT no pueden enviarle directamente a un país pruebas que tengan y que eso pueda ser validado como una prueba en un juicio, porque no tenemos la calidad en este momento para poder apuntar estas pruebas. • **Internacional:** En el caso de que Guatemala pueda integrarse al Convenio de Budapest tiene muchas ventajas debido a que es un acuerdo bastante poderoso, sin embargo tiene cuestiones en que se excede la soberanía. Porque puede permitir que las leyes de otros Estados puedan tener efecto sobre nuestro Estado.
	c. Amenazas Cibernéticas:	• El Ing. Afirma que el 92% de los incidentes fueron descubiertos por terceras partes (se dio cuenta que había algo extraño, que su información no estaba bien publicada, o que la información que están requiriendo está alterada, no es íntegra, etc.). Asimismo el 97% de las violaciones a la

		seguridad pudieron prevenirse con controles simples o intermedios (cambio constante de firewalls). • El entrevistado ratifica que el Hacktivismo puede llegar a ser amenaza de Estado. Que en el caso de Anonymous por ejemplo ha lanzado amenazas hacia el Estado de Guatemala diciendo que va a atacar determinados sitios. *"Ha atacado sitios del Congreso varias veces por varios hackers, pero en algún momento este activismo se vuelve una amenaza contra el Estado. Porque el Estado no puede quedar fuera de funcionamiento. Ninguna infraestructura crítica informática. Es un marco que lesiona la seguridad del Estado*". • Sostiene que Anonymous a pesar de parecer un grupo pacífico de personas con ideales de justicia, puede llegar a ser peligroso debido a que al suscribirse al grupo, se abren posibilidades a muchas cosas, porque al inscribirse a Anomymous da una serie de instrucciones y una serie de software que hay que ir descargando en la computadora. Conforme se van bajando estos software, se está haciendo que en la máquina se instalen algunos artefactos que permiten lanzar ataques: - de denegación de servicio -pueden ser dirigidos a capturas de direcciones electrónicas -puede ser dirigido a capturas de números de tarjetas de crédito, de cuentas financieras, usuarios. -En la máquina pueden instalar cualquier artefacto y a partir de allí lanzar ataques a cualquier sitio en cualquier parte del mundo. *"Así la persona que se inscribe, a veces sin saberlo se convierte en co-participe de ese delito*".
	d. Espionaje de los Gobiernos a Través de las Redes Sociales	Afirma que ninguna acción puede ser objeto de espionaje. Debe respetarse los 3 principios de seguridad informática (integridad, disponibilidad y

		confidencialidad). *"Si se esta violando la confidencialidad es un delito sin importar quien lo ejecute".*

Cuadro No. 5
ANÁLISIS DE RETOS

SEGÚN TECNICOS DE INFORMATICA GUBERNAMENTALES	a. La Creación de un Protocolo de Seguridad Nacional:	Representantes de Contraloría General de Cuentas reiteran que "*así como es aplicado en otros países como Estados Unidos, es importante la creación de un marco de referencia"* para que las instituciones de gobierno a nivel nacional sepan como manejar la seguridad informática al momento de un ataque.
	b. La Creación de una Mesa Técnica Nacional a Nivel de Gobierno:	Contraloría General de Cuentas considera de suma importancia "una mesa técnica conformada por representantes de todos los entes gubernamentales"; no solamente formado por el sector justicia como actualmente existe, sino por todos los ministerios y unidades de gobierno. Que obviamente no necesariamente deba reflejar las debilidades de cada sistema, sino que: - Comprenda el intercambio de experiencias - Intercambio de información - Buenas practicas
	c. Impulsar la Capacitación de los Empleados por medio de la Cooperación Internacional:	Si parte del problema surge por la falta de presupuesto en la formación técnica de los empleados, es importante acudir a nuevas alternativas como por ejemplo Agencias Sur y Norte americanas se ofrecen a dar capacitaciones gratis; únicamente que el gobierno debe asumir el costo de los viáticos. Anteriormente en algunos casos el gobierno no ha aceptado, porque muchas veces no saben que existen estas oportunidades y a veces por intereses personales. Sin embargo si se toma con seriedad y compromiso el tema, se pueden aprovechar fuentes de ayuda de terceros; siempre y cuando se analice responsablemente y de manera individual cada caso las implicaciones de aceptar este apoyo.
	d. La Publicación de la Información	En este momento no se da a conocer este tipo de información a otros entes

	Obtenida en Ejercicios de Seguridad y Simulacros:	gubernamentales que no hayan participado en estas actividades. Por lo que es de extrema importancia la publicación de la misma: no que muestre específicamente las vulnerabilidades, sino que básicamente compartan experiencias para que sirvan como referencia para todos a la hora de enfrentar algún tipo de ataque que vulnere la seguridad cibernética.
SEGÚN MINISTERIO DE GOBERNACION	a. Desarrollo de Un Plan Estratégico:	El Ministerio de Gobernación en este período de gobierno tiene como principal objetivo una Reingeniería Institucional, dentro de un plan estratégico. • REVOLUCION TECNOLOGICA Es el eje central: el cual pretende actualizar el ministerio, ya que con elementos del Siglo XX, hay que convertirlo en un Ministerio del Siglo XXI. Esto a través de una: -Plataforma Tecnológica Integrada: Pretende estandarizar soluciones tecnológicas publicas y privadas enfocadas a: -Lo primero a mejorar serian la red de telecomunicaciones seguras -Integración de base de datos (INTL BASC) -Creación de software (afirma que en MINGOB el 90% de software estas hechos en casa) Formado por un equipo de expertos en informática que oscilan en los 23 años. -Tecnologías especializadas: Huellas digitales, pruebas balísticas, rayos x en los puertos, -Infraestructura -sistema de video vigilancia (han avanzado de 1,900 a 9,000 cámaras)
	b. Creación de un Equipo de Respuesta ante Emergencias Informáticas -CERT- en Guatemala:	Ministerio de Gobernación reitera la importancia de un ente rector, que homologue la información, tecnología, etc., sin embargo hay que tomar en cuenta el análisis de ciertas normativas para no retifipicar delitos.
	c. Organización de Estados Americanos:	El ministerio de Gobernación está trabajando con la OEA básicamente en 3 elementos: 1. Tema Técnico: Es la respuesta inmediata al ataque 2. Forensica: Investigación Qué pasó? 3. Justicia: Cuales son los delitos a

		Juzgar, lo cual está ligado a la necesidad de una legislación adecuada. Todas estas acciones para ellos representan un reto en función de poder trabajar en colaboración, a pesar de las dificultades previamente descritas.
	d. Romper el Paradigma del Acceso a la Información:	-Afirman que el Ministerio de Gobernación pretende romper el paradigma del acceso o egoísmo de la información, mediante un proyecto de seguridad de 360º
SEGÚN RONALD MORALES, COORDINADOR CSIRT-GT	a. Aprobación de la Iniciativa de Ley 4055	Según el Ing. Morales es de carácter urgente y necesario su aprobación, debido a que en ésta se tipifican los delitos de cibercrimen. Se promueve la creación de fiscalía contra el delito cibernético y englobar en un solo núcleo todas las entidades de persecución del delito informático en un solo ente.
	b. Prioridad del Estado en Proteger el Ciberespacio	Debe poner mayor atención a la protección cibernética. Guatemala debe tener como mínimo la capacidad de ciberdefensa .
	c. Mejores Herramientas	Se necesitan combatir nuevas amenazas con nuevas herramientas y equipos preparados para enfrentarlas.
	d. Capacitación Necesaria de Profesionales	Considera que en Guatemala "*deberíamos tener profesionales, ingenieros en sistemas que ya estén diseñando herramientas propias de protección tanto hardware como software. Que no solo nos digan como nos debemos de proteger por medio de eso , sino que nosotros desarrollemos esta tecnología, ya que en la actualidad no existe; debemos ir a buscarlo".* Desarrollar nuestras propias herramientas nos ayudaría a evolucionar en el aspecto informático.

Fuente: elaboración propia basada en entrevistas.

4.4. PROPUESTA:

Creación de una Estrategia Nacional de Ciberseguridad en el Estado de Guatemala

Es de suma importancia que Guatemala cree una estrategia de ciberseguridad que pueda ser aplicada a nivel nacional por todas las instituciones de gobierno, sin discriminación o exclusión alguna. Para lograrlo debe comenzar por:

1. **La aprobación de una legislación** relativa a la ciberseguridad que tipifique, investigue y sancione delitos relativos a la informática y tecnología.

2. **Reforzar la cooperación internacional** para luchar contra la ciberdelincuencia, lo cual deberá incluir la adhesión a convenios internacionales de ciberseguridad, fortalecimiento del tema en la región centroamericana, ayudar y solicitar apoyo en el momento de ataques a gran escala en el que intervengan hackers internacionales.

3. **Capacitación técnica** para los empleados gubernamentales, que incluya cursos impartidos por expertos nacionales e internacionales, simulacros de ataques, y foros que sirvan de plataforma para exponer los ataques mas relevantes que han existido en los sitios gubernamentales, con el fin de compartir experiencias y fortalecerse en la medida de la búsqueda de mecanismos de respuesta a los mismos.

4. **Mejoras en el equipo de seguridad de las computadoras**. Que comprenda la calidad y modernidad física del equipo, así como también los programas de seguridad que sirvan de apoyo a los técnicos y encargados de resguardar la seguridad de la información.

5. **La creación de una Mesa Técnica Nacional** que involucre a todos los Ministerios y los principales entes gubernamentales con el fin de trabajar coordinadamente en los temas de seguridad informática, asimismo que sirva

de plataforma para exponer sus principales amenazas y retos para buscar soluciones conjuntas.

6. Lo mas trascendental y uno de los elementos de mayor utilidad, es la creación de un Protocolo de Respuesta a Incidentes Cibernéticos:

- **Protocolo de Respuesta a Incidentes Cibernéticos**

Es un mecanismo de respuesta necesario en cada Estado que cuente con servicio de telecomunicaciones y redes bancarias. Incluye un conjunto de normas, metodologías, procedimientos y procesos que alinean la política, los negocios y los enfoques tecnológicos para hacer frente a los riesgos cibernéticos y de la cual se puede realizar en colaboración entre el gobierno y iniciativa privada. Es una necesidad global, de la cual la búsqueda de soluciones ha impulsado a la creación y aplicación en varios países del mundo. Algunos ejemplos de esto puede ser España, Estados Unidos y Colombia, quien es el primer país latinoamericano en emplearlo.

A pesar, de que son iniciativas que han surgido en los últimos cinco años, siguen en constante crecimiento, y de la cual Guatemala no debe quedar fuera. Dicha estrategia debe comprender al menos cuatro funciones:

a) Proteger	-Controles de acceso: a activos y recursos a usuarios -Sensibilización y Capacitación**:** para los técnicos y encargados de la ciberseguridad -Seguridad de los datos: para proteger la confidencialidad, integridad y disponibilidad de la información. -Procesos y Procedimientos de Protección de Información -Tecnología emergente: soluciones de seguridad técnicas para garantizar la protección a los sistemas.

b) Detectar	-Anomalías en el sistema: a tiempo para prevenir el impacto. -Monitoreo Continuo de Seguridad en los sistemas de información -Procesos de Detección: Poniéndose a prueba para evitar nuevas amenazas, desde virus, intrusiones, hackeo, terrorismo, espionaje, etc.
c) Capacidad de Respuesta	- Fortalecimiento de las Comunicaciones entre CSIRT nacionales e internacionales - Análisis de causas y respuestas de ataques -Mitigación de efectos y erradicar el incidente -Mejoras al incorporar lecciones aprendidas
d) Recuperación	-Plan de recuperación: para restaurar sistemas o activos afectados. -Mejoras: en los procesos de recuperación basadas en lecciones aprendidas y actividades futuras. -Comunicación: coordinada interna y externa (CSIRT, víctimas, proveedores de Internet) como parte de las actividades de restauración.

*Elaboración propia basada en lecturas a informes Cybersecurity Framework (2014), Gobierno de Estados Unidos y en el Estudio para la implementación de una Estrategia Nacional de Ciberseguridad (2007), Gobierno de Colombia.

Aunque esta información es conocida por los encargados de salvaguardar la seguridad cibernética de nuestro país, es imperante la institucionalización de un manual nacional que dicte los protocolos de respuesta de manera ordenada, que brinde información útil y un marco de referencia y buenas prácticas para todos, que compartan información, valores y capacidades, siempre respetando la privacidad y libertades civiles, que se desarrolle la capacidad forensica digital de la investigación, y exista un ente encargado a donde dirigir estos casos para su debida persecución física y sanción en caso sea necesario, debido a que en la actualidad no existe nada de este genero en Guatemala.

CONCLUSIONES

Después de haber desarrollado la temática del Rol del Comité Interamericano Contra el Terrorismo de la OEA en el Combate del Terrorismo Cibernético, Analizando los Avances del Estado de Guatemala en el período 2011-2012 dentro del Marco de las Relaciones Internacionales se llegó a las conclusiones siguientes:

- Con respecto al dilema si existe o no terrorismo cibernético en Guatemala, existe una división de opiniones entre los elementos de seguridad informática del gobierno, sin embargo todos concuerdan en el hecho que el Estado si ha sufrido ataques cibernéticos, aunque no al nivel o intensidad de países desarrollados. Pero para fines del presente estudio se pudo concluir que las acciones que generen daño o vulneren la seguridad de la información del Estado, independientemente del mecanismo que se utilice para lograrlo, genera actos de terrorismo cibernético en Guatemala.

- El Estado de Guatemala no tiene en este momento la capacidad preventiva de crímenes cibernéticos en los sistemas de información; generalmente el Estado responde a los ataques en el momento en el que ya fueron ejecutados, y en muchos casos mucho tiempo después de haber sucedido y hallados por casualidad o por terceros. Esto se debe fundamentalmente a la falta de personal capacitado, carencia de interés Gubernamental en el tema y falta de herramientas o equipo necesario para poder realizar el trabajo con eficacia.

- No existe actualmente un trabajo de cooperación internacional efectivo en materia de seguridad informática. Todos los entrevistados, así como las herramientas bibliográficas y sondeo de medios demuestran que el gobierno de Guatemala no trabaja coordinadamente con los entes encargados de la seguridad en otros países, ya sea con la policía cibernética o los CSIRT locales en materia de investigación, a diferencia de otros temas de interés como el narcotráfico y crimen organizado.

- Es evidente que la falta de una legislación nacional adecuada al tema de seguridad informática impide el trabajo de investigación y sanción por parte del Ministerio Público, ya que en la actualidad estos casos simplemente son ignorados o desconocen en dónde poder ubicarlos, debido a que si no existe en la ley aparentemente no hay delito.

- La labor del CSIRT en Guatemala es sumamente limitada, no por falta de voluntad del equipo, sino por la falta de apoyo de las autoridades del Ministerio de Defensa, la carencia de presupuesto y de la legislación de cibercrimen. Lo cual reduce su capacidad de respuesta y de acciones coordinadas, ya que los resultados de su colaboración no pueden considerarse medios de prueba nacional o internacional.

- El Comité Interamericano Contra el Terrorismo realiza acciones en función de mejorar la calidad de seguridad cibernética en cada país, sin embargo su labor no es equitativa, ya que no todas las actividades son realizadas en cada país miembro, sino dependen del presupuesto y del interés de las fuentes cooperantes (generalmente Estados Unidos y Canadá) en brindar apoyo a los países que ellos consideren necesario.

- Asimismo el Comité realiza una labor formativa de carácter técnico que cuenta con herramientas innovadoras y expertos en el tema, pero no realizan acciones operativas en el combate del cibercrimen. Las capacitaciones y ejercicios técnicos en algunos países tienen un fin positivo, sin embargo no reflejan grandes resultados en los países donde se han realizado. Básicamente sirven de indicador para los gobiernos para conocer las carencias y limitaciones de la seguridad informática local.

BIBLIOGRAFÍA

1. Agustín López, Guillermo (2011) Tesis Licenciatura "**Los Conflictos de Jurisdicción que se Suscitan en los Delitos Informáticos y la Importancia de que Entre en Vigencia la Ley de Delitos Informáticos"** USAC. Guatemala

2. Barrios Osorio, Omar Ricardo. (2007). **Derecho e Informática, Aspectos Fundamentales**. Centro de Estudios de Derecho CEDE. Guatemala. Ediciones Mayte .

3. Bojo, C., Fraga, C., Hernández, S., Jaén, MB., Jiménez, V., Mohedano, L., Novillo,A. et al. (2004) **Internet Visible e Invisible: Búsqueda y Selección de Recursos de Información en Ciencias de la Salud**. Madrid: Instituto de Salud Carlos III

4. Borrero Mansilla, Armando (2004) **Terrorismo Político: Definición y Alcances de un Fenómeno Elusivo**. Revista Criminalidad. Volumen 47. Colombia. Dirección Central de Policía Judicial

5. Castro Peña, Gustavo (1999) **Terrorismo y Política Internacional.** Colombia. Sol Editorial

6. Cisneros Salvatierra, Máximo Cesar. (2004) **Perspectiva General de los Factores mas Influyentes del Terrorismo Internacional**. Universidad de San Martín de Porres, Lima, Perú

7. Cohen Orantes, Isaac. (1968) **Funcionalismo e Integración Centroamericana**. Revista Foro Internacional, Vol. 9. No. 2. México. Centro de Estudios Históricos El Colegio de México.

8. Cook, Chris.(1997) **Diccionario de Términos Históricos**. Altaya. Barcelona.

9. Del Pino, Santiago Acurio (2007) **Delitos Informáticos**. Quito. Pontificia Universidad Católica de Ecuador.

10. Dougherty, James E. y Pfaltzgraff, Robert. (1993) **Teorías en Pugna de las Relaciones Internacionales. Integración, Regionalismo y Cohesión de las Alianzas**. 1 Ed. Argentina. Grupo Editor Latinoamericano

11. Durán Sepúlveda, Roberto (1980) **La Corriente Funcionalista en la Teoría de Relaciones Internacionales. La Teoría de Relaciones Exteriores**. Revista de Ciencia Política. Vol. 2. Chile. Pontificia Universidad Católica de Chile.

12. Hernández García, Luis Fernando (2006) **Ciberterrorismo**. Revista a+ . Volumen 1. Jefatura del Servicio de Información. Dirección General de la Guardia Civil. España

13. Hidalgo González, Jorge. (2001). **El Envejecimiento Aspectos Sociales**. 1 Ed. Editorial de la Universidad de Costa Rica. Costa Rica

14. Insulza, José Miguel (2013) **Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuestas de los Gobiernos**. Secretaría de Seguridad Multidimensional de la OEA. Estados Unidos de Norte América.

15. Jacopo Gamba. (2010) **Panorama del Derecho Informático en América Latina y el Caribe. Comisión Económica para America Latina y el Caribe**. CEPAL. Chile

16. Laquer, Walter.(1980). **Terrorismo**. Madrid, España. Editorial Espasa-Calpe.

17. Larios Ochaita, Carlos (2005) **Derecho Internacional Público**. Editorial Lerena. Guatemala.

18. Marighella, Carlos (1969) **Introducción al Terrorismo, sus Organizaciones, Operaciones y Desarrollo.** Centro de Estudios Miguel Enríquez. Chile

19. Masana, Sebastián. (2002) Tesis magistral. **El ciberterrorismo: ¿una amenaza real para la paz mundial?** FLACSO – Facultad Latinoamericana de Ciencias Sociales. Argentina.

20. Mateu de Ros Rafael y Cendoya Juan Manuel. (2000) **Derecho de Internet**. España. Ed. Aranzadi.

21. Minolli, Cristina. (2003) **Terrorismo y Supervivencia**. Universidad del Cema UCEMA. Argentina

22. Muñoz Roldán, Luis Rodrigo. (2005) **El Tráfico Jurídico Electrónico y la Firma Digital**. Centro Superior de Estudios Jurídicos. España.

23. Nava Garcés, Alberto Enrique (2005) **Análisis de los Delitos Informáticos**. 1 Ed. México. Editorial Porrúa.

24. Organización de Estados Americanos.(2014) **Activities of the Inter-American Committee Against Terrorism in Guatemala 2012-2013**. Manuscrito no publicado. Estados Unidos.

25. Osorio, Manuel. (1992) **Diccionario de Ciencias Jurídicas, Políticas y Sociales.** Heliasta. Buenos Aires

26. Pearson, Frederic. S y Rochester, J. Martin.(2003). **Relaciones Internacionales, Situación Global en el Siglo XXI.** Cuarta Edición. Colombia. Mc Gral. Hill Internacional.

27. Prandini, Patricia y Maggiore, Marcia. (2013) **Ciberdelito en América Latina y el Caribe, Una Visión desde la Sociedad Civil**. Proyecto Amparo. LACNIC. Registro de Direcciones de Internet para América Latina y Caribe. Uruguay.

28. Rapoport, David. (2004) **The Four Waves of Modern Terrorism.** Departamento de Ciencias Políticas. Universidad de California UCLA. Estados Unidos.

29. Romero, Tonatiuh y Liendo Verae, Isidoro (2010**) La Influencia de Durkheim en la Teoría Funcionalista de Malinowski.** Revista Ciencia Ergo Sum. Red de Revistas Científicas de América Latina, el Caribe, España y Portugal, Vol. 10. México.

30. Ronaldo Alvarado y Ronald Morales. (2012) **Cibercrimen**. IUS Ediciones. Guatemala.

31. Noriega Salazar, Hans Aarón (2011) **Delitos Informáticos.** Instituto de la Defensa Publica Penal. Programa de Formación del Defensor Publico. Modulo de Autoformación. 1 ed. Guatemala

32. Unión Internacional de Telecomunicaciones (2009) . **Undertanding Cybercrime: A Guide for Developing Countries.** División de Aplicaciones y Ciberseguridad. Recursos de Legislación de Cibercrimen. Suiza.

33. Vieira, Edgar. (2005) **Evolución de las Teorías Sobre Integración en el Contexto de las Teorías de las Relaciones Internacionales**. Revista Papel Político. No. 18. Colombia. Universidad Javeriana

34. Vieira Posada, Edgar. (2008) **Formación de Espacios Regionales en la Integración de América Latina**. Colombia. Pontificia Universidad Javeriana.

a) Fuentes Virtuales

35. Anonymous.(2011) **El Manual Super Secreto**. Recuperado www.irc.anonworld.net

36. **Anonymous Guatemala.** Sitio Oficial https://www.facebook.com/AnonymousGT?fref=ts

37. Becerra, Juan Armando (2014) **Mitos y Realidades de la Internet Profunda.** Revista .Seguridad . Volumen 20. México. Recuperado el 1 de abril del 2014 en: http://revista.seguridad.unam.mx/numero-20/mitos-y-realidades-de-la-7internet-profunda

38. **CSIRT Guatemala**, Sitio Web Oficial. Consultado en http://www.csirt.gt

39. Devel Security. (2012) **Informe Qué Sucedió el 29 de Agosto? , La verdadera Historia Detrás de los Ataques del 29**. Recuperado: http://www.elperiodico.com.gt/attachment/000001741.pdf

40. **Estudio para la implementación de una Estrategia Nacional de Ciberseguridad** (2007) Comisión de Regulación de Telecomunicaciones. República de Colombia. Recopilado en: http://www.crcom.gov.co/index.php?idcategoria=62262

41. **Framework for Improving Critical Infrastructure Cybersecurity** (2014) National Institute of Standards and Technology. Estados . Consultado en: http://www.nist.gov/cyberframework/index.cfm

42. **Grupo de Respuesta a Emergencias Cibernéticas COLCERT**. Sitio web institucional. Colombia http://www.colcert.gov.co/

43. Olloqui, Jose Juan. (2004) **Reflexiones Sobre el Terrorismo.** Revista Derechos Humanos Año 11. Numero 68. Comisión de Derechos Humanos del Estado de México, CODHEM. Recuperado de: www.codhem.org.mx/ LocalUser/ codhem.org/ info/gaceta68.pdf

44. **Organización de Estados Americanos**. Sitio Web oficial : www.oas.org/es

45. RAE -Real Academia Espanola. (2014) **Dictionaries de la Real Academia Espanola.** www.rae.es

46. **The Deep Web, Los Suburbios de Internet**. Artículo Recuperado el 18 de abril de 2014: http://paoladry.weebly.com/uploads/2/5/7/2/25721613/162798.pdf

47. Universia España. (2014) **Los Misterios Ocultos de Internet; La Web Profunda. Área Tecnología**. Recuperado el 18 de marzo de 2014: http://noticias.universia.es/ciencia-nn-tt/noticia/2014/03/18/1088529/misterios-ocultos-internet-web-profunda.pdf

b) Fuentes Legales

48. **Código Penal de Guatemala**, Decreto 17-73 del Congreso de la República de Guatemala

49. Consejo de Europa (2001) **Convenio sobre Cibercriminalidad**, Budapest.

50. Proyecto de Ley:
51. **Iniciativa 4055 "Ley de Delitos Informáticos**" , Congreso de la República de Guatemala

52. OEA (1948) Carta de la Organización de Estados Americanos.

53. OEA (2004) Resolución 2004 (XXXIV-O/04) Asamblea General. **Adopción de una Estrategia Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética.**

54. ONU (2001) Resolución 55/63. Asamblea General. **Lucha Contra la Utilización de la Tecnología de la Información con Fines Delictivos.**

55. ONU (2002) Resolución 56/88 .Asamblea General. **Medidas para Eliminar el Terrorismo Internacional.**

56. ONU (2003) Resolución 57/239. Asamblea General. **Creación de una Cultura Mundial de Seguridad Cibernética**

c) Fuentes Hemerográficas

57. Barreto, Bill. (2012, 25 de Septiembre) **Portal del Ministerio de Finanzas Sufre Ataque Cibernético Sección Economía.** Prensa Libre. Guatemala

58. Barreto, Bill. (2013, 3 de Enero) **Agrupación Anonymous Guatemala se Atribuye Ataques a Páginas Web.** Sección Justicia. Prensa Libre. Guatemala

59. Fonseca, Martin. (2012, 24 de Septiembre) **Una Limpieza en el Mundo Virtual. Sección Tecnología**. Prensa Libre. Guatemala

60. Hernández, Manuel. (2012, 25 de Septiembre). **Ataque cibernético de Minfin Proviene de Alemania** . Sección Política. Prensa Libre. Guatemala

61. Hernández, Manuel. (2012, 14 de Noviembre) **Página Web del Ministerio de Finanzas, Sin Funcionamiento Sección Política**. Prensa Libre. Guatemala

62. Ortiz, Estuardo. (2013, 14 de Diciembre) **Anonymous Guatemala Lanza Concurso para Hackear Páginas Web del Gobierno.** Sección Tecnología. Prensa Libre. Guatemala.

d)Medios Audiovisuales

63. Cabrera, Dadiana. (2013) **Entrevista a Anonymous Guatemala**. Programa Sin Reservas, Guatevisión. Consultado en: http://www.youtube.com/watch?v=QSrB7loxZIM

64. Montenegro, Jaime. (2013) Reporte en Voz. **Gobierno Instalará Nuevos Sistemas en Páginas de Gobierno Ante Hackeos de Anonymous. Entrevista a Vicepresidente Roxana Baldetti.** Noticias Emisoras Unidas. Consultado en: http://noticias.emisorasunidas.com/noticias/nacionales/gobierno-instalara-nuevos-sistema-paginas-ante-hackeos-anonymous

65. Montenegro, Jaime. (2013) Reporte en Voz. **Presidente dice que Perseguirán a Quienes Ataquen Páginas de Gobierno. Entrevista a Presidente Otto Pérez**. Noticias Emisoras Unidas. Consultado en: http://noticias.emisorasunidas.com/noticias/nacionales/presidente-dice-que-perseguiran-quienes-ataquen-paginas-gobierno

66. Ramírez, Lester.(2013) Reporte en Voz. **Anonymous Hackea la Página del Congreso**. Noticias Emisoras Unidas. Consultado en: http://noticias.emisorasunidas.com/noticias/nacionales/anonymous-hackea-pagina-congreso

67. Video **Anonymous Guatemala le Responde al Presidente** (2013) Cuenta Anonymous Guatemala. Consultado en : http://www.youtube.com/watch?v=VsLu7ElhBXs&feature=youtu.be

68. Video **documental Internet Profunda** (2013) Programa Tercera Posición. España. Consultado en: http://www.youtube.com/watch?v=LlUlCyntWvw

69. Video **documental La Deep Web, la Web Oscura**. Programa Cuarto Milenio. España. Consultado en: http://www.youtube.com/watch?v=4hPAc1yI-bc

70. Video **Hackers en Guatemala (**2011) Cuenta Crackergt. Guatemala. Consultado en: http://www.youtube.com/watch?v=Rc2350mbIg0

71. Video **#Op Democracia GT 2.0** (2013) Cuenta Anonymous Guatemala. Consultado en: http://www.youtube.com/watch?feature=player_embedded&

e)Entrevistas

72. **Embajador Rodrigo Vielmann**, Presidente del CICTE durante el período 2012-2013, y actual Viceministro de Relaciones Exteriores de Guatemala.

73. **Ing. Gabriel Juárez Lucas**, Subdirector de Informática, de la Secretaría Técnica del Consejo Nacional de Seguridad de Guatemala.

74. **Ing. Joel Fock Way**, Subjefe de Informática de la Contraloría General de Cuentas de Guatemala.

75. **Ing. Juan Carlos Argueta Medina**, Viceministro de Tecnología del Ministerio de Gobernación de Guatemala.

76. **Ing. Luis Fernando Ruiz**, Técnico de la Dirección Informática del Ministerio de Gobernación de Guatemala.

77. **Ing. Ronald Morales**, creador del Centro de Respuesta Inmediata a Incidentes de Seguridad Cibernética en Guatemala (CSIRT-gt), y creador de la Iniciativa de Ley 4055, Ley de Delitos Informáticos.

78. **Ing. Ronny Antonio Vásquez**, Administrador de Servidores, Oficial de Seguridad de la Información, Contraloría General de Cuentas de Guatemala.

f)Conferencias

79. **Info Security Tour VIP, It's a Kind of Magic** (2014) Ciudad de Guatemala.

80. **Primer Congreso Internacional de Ciencia, Tecnología e Innovación**. (2013) Secretaría Nacional de Ciencia y Tecnología de Guatemala (SENACYT).