UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
ESCUELA DE ESTUDIOS DE POSTGRADO
DOCTORADO EN SEGURIDAD ESTRATÉGICA

TESIS DOCTORAL

NECESIDAD DE UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRÍTICAS EN GUATEMALA

MSc. WALTER FRANCISCO GIRÓN FIGUEROA

GUATEMALA, ENERO DE 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
ESCUELA DE ESTUDIOS DE POSTGRADO
DOCTORADO EN SEGURIDAD ESTRATÉGICA

NECESIDAD DE UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRÍTICAS EN GUATEMALA

TESIS DOCTORAL

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

por el

M. Sc. WALTER FRANCISCO GIRÓN FIGUEROA

previo a conferírsele el Grado Académico de

DOCTOR EN SEGURIDAD ESTRATÉGICA

Guatemala, enero de 2021

HONORABLE JUNTA DIRECTIVA

DE LA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DE LA

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

VOCAL I EN SUSTITUCIÓN		
DEL DECANO:	Licda.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	M. Sc.	Henry Manuel Arriaga Contreras
VOCAL III:	M. Sc.	Juan José Bolaños Mejía
VOCAL IV:	Br.	Denis Ernesto Velásquez González
VOCAL V:	Br.	Abidán Carías Palencia
SECRETARIO:	M. Sc.	Luis Renato Pineda

CONSEJO ACADÉMICO DE ESTUDIOS DE POSTGRADO

VOCAL I EN SUSTITUCIÓN		
DEL DECANO:	Licda.	Astrid Jeannette Lemus Rodríguez
DIRECTOR:	M. Sc.	Luis Ernesto Cáceres Rodríguez
VOCAL:	Dr.	Carlos Estuardo Gálvez Barrios
VOCAL:	Dr.	Nery Roberto Muñoz
VOCAL:	Dr.	William Enrique López Morataya

TRIBUNAL EXAMINADOR

PRESIDENTE:	Dr.	Aníbal González Dubón
VOCAL:	Dr.	Saúl González Cabrera
SECRETARIO:	Dr.	Olmedo Aisar Vásquez Toledo

Ciudad Guatemala, 25 de noviembre de 2016

Señor

Director de la Escuela de Estudios de Postgrado

Facultad de Ciencias Jurídicas y Sociales

Universidad de San Carlos de Guatemala

Me dirijo a usted para emitir OPINIÓN FAVORABLE de la investigación de tesis titulada «Necesidad de una Política Nacional de Ciberseguridad para Infraestructuras Críticas en Guatemala», presentada por el MSc WALTER FRANCISCO GIRÓN FIGUEROA, como requisito para obtener el grado y título de DOCTOR EN SEGURIDAD ESTRATÉGICA.

La tesis del Maestro WALTER FRANCISCO GIRÓN FIGUEROA principia por advertir que las relaciones sociales, económicas y culturales dependen, cada vez más, de las tecnologías e infraestructuras de la información y comunicación (ciberespacio), circunstancia que hace necesaria la articulación de un sistema nacional de seguridad (ciberseguridad), que gestione los riesgos que amenazan su funcionamiento. Dicha articulación se daría por dos medios: (1) un ente coordinador que el sustentante denomina Ministerio de Tecnología y (2) por una Estrategia Nacional de Ciberseguridad.

La tesis del Maestro WALTER FRANCISCO GIRÓN FIGUEROA sostiene que las Tecnologías de la Información y la Comunicación (TIC) han coadyuvado al bienestar y progreso de las sociedades, de tal manera que gran parte de las relaciones públicas y privadas dependen de estas

tecnologías. Debido al desarrollo vertiginoso de las TIC, han surgido amenazas que hacen necesaria la gestión de su seguridad.

Inicialmente, la ciberseguridad se encargó de proteger la información de un modo reactivo, pero posteriormente ha evolucionado hacia una posición proactiva que identifica y gestiona las amenazas provenientes del ciberespacio. El sustentante realiza una aproximación a los conceptos de ciberespacio, ciberseguridad y ciberdefensa, los riesgos y amenazas conocidos, la inexistencia de la gestión en Guatemala y, por lo mismo, sobre la necesidad de desarrollar un sistema nacional por medio de una Estrategia Nacional de Ciberseguridad, que fomente la integración de todos los actores e instrumentos, públicos o privados, para aprovechar las oportunidades de las nuevas tecnologías y hacer frente a los retos que presentan.

El Estado de Guatemala, por medio de su representación el Gobierno de la República, como garante de la seguridad y tranquilidad de sus habitantes, debe adaptar sus estructuras y marcos normativos para prevenir y enfrentar estas amenazas emergentes, que surgen de nuevo escenario en donde las fronteras no son claras, y los actores no pueden identificarse claramente.

La tesis del Maestro WALTER FRANCISCO GIRÓN FIGUEROA se enfoca en la situación de Guatemala en lo referente a su grado de seguridad y capacidad de defensa en el ciberespacio. Para ello, inicialmente presenta las nuevas amenazas identificadas por la legislación nacional, para pasar luego al detalle de las estructuras más importantes encargadas de prevenir o repeler un eventual ataque. Al final presenta las dimensiones que hay que tomar en cuenta al formular una Estrategia Nacional de Ciberseguridad.

Otros países como Estados Unidos, Francia, el Reino Unido, Israel y Corea del Sur, así como la ONU y la OTAN, entre otras organizaciones

internacionales, han tomado conciencia de la importancia y necesidad de un ciberespacio seguro. De ahí que han desarrollado o están desarrollando marcos normativos, planes y estrategias específicas para la defensa del ciberespacio. O sea, decidieron gestionar la seguridad del ciberespacio, bajo su responsabilidad y de manera sistemática. Esta concientización no existe en nuestro país, a pesar de que se reconoce que la continua y acelerada evolución de las TIC ha propiciado que los ciberataques sean cada vez más sofisticados, dando lugar a un ciberespacio cada vez más hostil.

En la actualidad, el Gobierno de Guatemala no mantiene ninguna iniciativa oficial para fomentar una cultura de seguridad cibernética. Sin embargo, hay personas que de manera individual desarrollan diferentes tareas en el área de la seguridad cibernética. Sus esfuerzos se encaminan a crear conciencia y promover una cultura de mayor seguridad, por ejemplo, por medio de *blogs*.

No se ha establecido una Estrategia Nacional de Ciberseguridad, a pesar de que Guatemala ha sido blanco de ciberataques. Uno de los más notorios fue cuando el grupo de *hacktivistas* denominado "Anonymous" atacó portales del Congreso de la República, de la Presidencia de la República y de la Secretaría de Seguridad Alimentaria. Uno de los más relevantes fue el ataque cibernético, que duró 5 días continuos, al Ministerio de Finanzas en 2012. En ese entonces, los portales del Sistema de Contabilidad Integrada (SICOIN) y el sistema de compras del Estado de Guatemala (Guatecompras), y el propio portal www.minfin.gob.gt quedaron deshabilitados totalmente, porque un ataque denominado de denegación de servicio (DoSpor sus siglas en inglés) hizo imposible el acceso. Durante este tiempo, ninguna institución del Estado pudo realizar transacción alguna al sistema de Contabilidad Integrada. Estuvo en riesgo el pago de la nómina de los trabajadores del Estado.

La falta de una estrategia de Ciberseguridad y Ciberdefensa también se hizo evidente en 2011, ante las amenazas del grupo "Anonymous", junto a otro grupo hacktivista denominado "Metalsoft". El entonces Presidente de la República de Guatemala, Álvaro Colom, dio la orden de que todas las instituciones del Estado debían "apagar" sus servidores para no sufrir ningún ataque y la información de las instituciones no se viera comprometida. Esta decisión en pleno Siglo Veintiuno dejó al país en ridículo cuando la noticia trascendió a nivel internacional, pero refleja la total carencia de políticas, normas, marcos institucionales, respuesta ante ataques cibernéticos y que no se tiene una Estrategia Nacional en temas de Ciberseguridad y Ciberdefensa.

Actualmente, Guatemala no cuenta con legislación especial que regule normas relativas a los delitos informáticos cometidos por medio de sistemas que utilicen tecnologías de la información. Solo se encuentran algunas normas que fueron adicionadas a nuestro actual Código Penal, mismas que no responden a las necesidades actuales, debido a la irrefutable variación de las tecnologías de la información.

Estas situaciones sufridas en nuestro país, ponen en evidencia la necesidad de contar con gestores de la ciberseguridad que dispongan de medios técnicos y humanos vanguardistas, para poder enfrentar las ciberamenazas y sus posibles impactos.

Uno de los grandes méritos de la tesis del Maestro WALTER FRANCISCO GIRÓN FIGUEROA es proponer que el Gobierno de Guatemala asuma el liderazgo en materia de ciberseguridad, para sensibilizar a la ciudadanía sobre la necesidad de proteger el ciberespacio del que dependen nuestros servicios básicos, infraestructuras críticas, economía y progreso como sociedad.

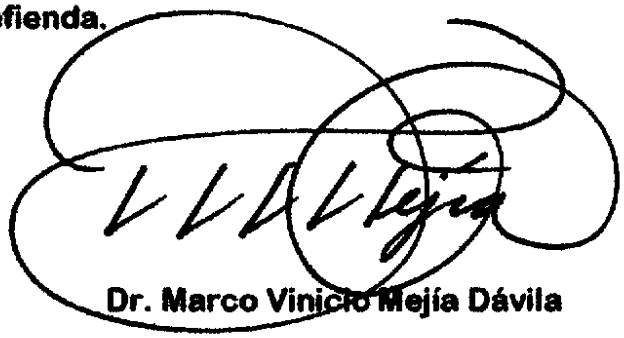
En sus conclusiones, advierte que las TIC no son el problema, son parte de la solución. Su protección y empleo seguro, no son solo

responsabilidad del Gobierno, sino de las demás administraciones municipales y locales, junto con el sector privado, empresarial y escolar. Todos son corresponsables, pero le corresponde al Gobierno el liderazgo y la dirección de la gestión nacional de la ciberseguridad. Estas responsabilidades no pueden delegarse y deben traducirse en proporcionar el impulso, las ideas y la dirección que Guatemala necesita.

Esta tesis es la primera que ha desarrollado los contenidos, la orientación y el sentido prospectivo del seminario sobre Derecho Informático y Seguridad de la Información, incluido en el diseño curricular del cual soy autor, pero que ha sido abordado desde un enfoque eminentemente legalista, como una concesión injustificada y de falta de comprensión sobre la multidimensionalidad de la Seguridad y la justificación de una simpleza ramplona es porque el Doctorado en Seguridad Estratégica funciona al alero de la Facultad de Ciencias Jurídicas y Sociales.

Emito mi opinión favorable y entusiasta para aprobar este estudio, el cual ubica el debate donde siempre debió estar, es decir, como un tema tanto de Seguridad Informática y Seguridad de la Información.

Por lo anteriormente expuesto, solicito la emisión de la resolución correspondiente y la designación del tribunal examinador de esta tesis, fijándose día y hora para que el Maestro WALTER FRANCISCO GIRÓN FIGUEROA la defienda.



Dr. Marco Vinicio Mejía Dávila

Doctor en Derecho y Doctor en Filosofía

Ciudad de Guatemala, 7 de abril de 2020

Doctor Luis Ernesto Cáceres Rodríguez
Director de la Escuela de Estudios de Posgrado
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala.

Señor Director:

Informo a usted que he revisado la tesis: *Necesidad de una política nacional de ciberseguridad para infraestructuras críticas en Guatemala,* cuyo autor es el Msc. Walter Francisco Girón Figueroa, estudiante del Doctorado en Seguridad estratégica.

Con base en la revisión, identifiqué los aspectos ortográficos (letras, tildes y signos de puntuación), sintácticos y de léxico que necesitaban ser corregidos o modificados. Posteriormente tuve a la vista la nueva versión trabajada por el autor, la cual puede, en consecuencia, pasar a la siguiente etapa del proceso establecido por la Escuela de Estudios de Posgrado.

Atentamente,

Dr. Enán Moreno
Colegiado 1,222.

cc. archivo.

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

D.E.E.P. ORDEN DE IMPRESIÓN

LA ESCUELA DE ESTUDIOS DE POSTGRADO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, Guatemala, 21 de octubre del dos mil veinte.----------

En vista de que el MSc. Walter Francisco Girón Figueroa aprobó examen privado de tesis en el **Doctorado en Seguridad Estratégicas**, lo cual consta en el acta número 137-2019 suscrita por el Tribunal Examinador y habiéndose cumplido con la revisión gramatical, se autoriza la impresión de la tesis titulada **"NECESIDAD DE UNA POLÍTICA NACIONAL DE CIBERSEGURIDAD PARA INFRAESTRUTURAS CRÍTICAS EN GUATEMALA"**. Previo a realizar el acto de investidura de conformidad con lo establecido en el Artículo 21 del Normativo de Tesis de Maestría y Doctorado.----------

"ID Y ENSEÑAD A TODOS"

ESCUELA DE ESTUDIOS DE POSTGRADO FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES USAC DIRECCIÓN

Dr. Luis Ernesto Cáceres Rodríguez
DIRECTOR DE LA ESCUELA DE ESTUDIOS DE POSTGRADO

ÍNDICE

INTRODUCCIÓN

Es imperativo que el gobierno de Guatemala actúe de una forma integral frente a las amenazas informáticas. Se hace necesario establecer una Política Nacional de Ciberseguridad que plantee un modelo de seguridad informática a las infraestructuras críticas del país, que fortalezca la institucionalidad, e incluso contemple la creación de instancias adecuadas que permitan ejercer una labor de Ciberseguridad; contar con un marco jurídico actualizado que responda ante las nuevas modalidades de delitos en los cuales la tecnología se utiliza como medio y como fin; la cooperación internacional y las alianzas público-privadas para hacer frente a cualquier amenaza o incidente informático que pueda comprometer información, afectar infraestructura crítica del país y poner en riesgo la seguridad y defensa del Estado, el tejido empresarial, las libertades y derechos individuales.

La ciberseguridad en las infraestructuras críticas del país es un tema al que debe darse la mayor de las prioridades, pues adolece de graves vulnerabilidades.

El Estado es el obligado a brindar seguridad a todos los guatemaltecos por medio de las instituciones especialmente creadas para ello, las cuales deben echar mano de las herramientas tecnológicas actuales en la prevención y reacción a los delitos incluidos, los que usan la tecnología como medio o como fin, denominados ciberdelitos.

La realización de esta tesis brinda un marco de referencia para establecer la realidad que caracteriza a nuestra población y a nuestro territorio en materia de seguridad informática; identifica los problemas de seguridad de la información, la carencia de un marco jurídico adecuado para el combate del ciberdelito; la casi nula institucionalidad para combatir la amenaza de ciberataques. Presenta una propuesta para una primera aproximación a lo que podría catalogarse como

infraestructura crítica en el país, y propone un modelo de ciberseguridad factible de implementar bajo el paraguas de una política nacional.

La falta de cooperación general con el sector privado se debe, en gran medida, a la ausencia de una política y estrategia nacional en materia de seguridad cibernética, además de la falta de un marco jurídico para procesar la mayoría de las actividades que pueden considerarse delitos cibernéticos. En la actualidad, se solicita directamente a la entidad en el sector privado en cuestión, que, por no existir regulación para compartir información, la mayoría de las veces no responden, por lo que son bajas las tasas de cumplimiento de dichas solicitudes.

La cooperación entre las autoridades de Guatemala y sus autoridades homólogas de otros países es limitada y, generalmente, se produce en situaciones informales para propósitos específicos, entre personas u oficinas que han establecido contacto a través de la participación en talleres regionales u otras actividades.

En la actualidad, el Gobierno de Guatemala no mantiene ninguna iniciativa oficial para fomentar una cultura de seguridad cibernética. No obstante, existen empresas privadas que desarrollan diferentes tareas en dicha área, realizan sus propios esfuerzos para crear conciencia y promover una cultura de mayor seguridad, por ejemplo, con blogs y entrevistas a diarios locales. Una de las iniciativas dignas de mención para crear cultura de seguridad en el ciberespacio, es "me conecto sin clavos"[1] llevada a cabo por UNICEF Guatemala.

Referente a la seguridad cibernética, Guatemala ha sido blanco de ataques. Uno de los más notorios fue cuando el grupo de hacktivistas denominado «Anonymous» atacó portales del Congreso de la República, de la Presidencia de la Republica y de la Secretaría de Seguridad Alimentaria.

[1] http://meconectosinclavos.net.gt/. Consultado el 18/01/2020

Otro de los más relevantes fue el ataque cibernético, de cinco días continuos, al Ministerio de Finanzas, en 2012, cuando los portales del Sistema de Contabilidad Integrada (SICOIN), el sistema de compras del Estado de Guatemala (Guatecompras) y el propio portal www.minfin.gob.gt quedaron deshabilitados totalmente, porque un ataque denominado de denegación de servicio (DoS, por sus siglas en inglés) hizo imposible el acceso. Durante este tiempo, ninguna institución del Estado pudo realizar transacción alguna al Sistema de Contabilidad Integrada. A raíz de ello, estuvo en riesgo el pago de la nómina de los trabajadores del Estado.[2]

Actualmente, Guatemala no cuenta con legislación especial que regule normas relativas a los delitos informáticos cometidos por medio de sistemas que utilicen tecnologías de la información. Únicamente se encuentran algunas normas que fueron adicionadas a nuestro actual Código Penal, pero no responden a las necesidades actuales, debido a la irrefutable variación de las citadas.

El 18 de agosto de 2009, el Pleno del Congreso de la República conoció la iniciativa número 4055, denominada «Ley de Delitos Informáticos», la cual recibió dictamen favorable de la Comisión de Legislación y Puntos Constitucionales.

En el año 2016 se presentó ante el Pleno del Congreso la iniciativa 5254[3] Ley contra la Ciberdelincuencia, una versión mejorada y actualizada de la iniciativa anterior que busca apuntalar la lucha contra los delitos informáticos por medio de una legislación apegada al convenio de Budapest. Contar con una legislación contra el ciberdelito es una variable vital que el país debe adoptar para prevenir y combatir el ciberdelito.[4] La variable sobre legislación será parte importante del modelo de ciberseguridad que se plantea en la presente tesis.

---

[2] http://revistasumma.com/30309/. Consultado el 15/04/2019
[3] https://leyes.infile.com/index.php?id=198&id_iniciativa=925 . consultado el 15/04/2019
[4] https://www.prensalibre.com/guatemala/justicia/gobernacion-elaborara-ley-para-combatir-el-cibercrimen/ . consultado el 15/04/2019

La elaboración de la Estrategia Nacional de Ciberseguridad inició en 2016 en el Ministerio de Gobernación,[5] siendo un esfuerzo de Guatemala con la Organización de los Estados Americanos para dotar al país de un norte en el combate del cibercrimen y la seguridad nacional,[6] consciente de que el país necesita un instrumento institucional más robusto, como lo es una Política Nacional de Ciberseguridad que proponga un modelo integral para el combate del ciberdelito hacia las infraestructuras críticas del país. Una estrategia es un buen inicio en medio de nuestra realidad en donde los instrumentos para afrontar amenazas cibernéticas son casi nulos.

Esta investigación pone de relieve que el gobierno guatemalteco debe asumir el liderazgo en materia de ciberseguridad. Proteger el ciberespacio del que dependen los servicios básicos, infraestructuras críticas, economía y progreso como sociedad.

Las TICs no son el problema, son parte de la solución. Su protección y empleo seguro no son solo responsabilidad del gobierno, sino de las demás administraciones municipales y locales, junto con el sector privado y educativo. Todos son corresponsables, pero le corresponde al gobierno el liderazgo y la dirección de la gestión nacional de la ciberseguridad, responsabilidades que no pueden delegarse y que deben traducirse en proporcionar el impulso, las ideas y la dirección que Guatemala necesita.

La presente tesis se enfoca en la protección tecnológica que deberían recibir las infraestructuras críticas, denominación que recibe toda aquella infraestructura que permite que un país funcione, y de la cual dependen servicios que, de faltar, ponen en riesgo la seguridad nacional.

---

[5] http://mingob.gob.gt/realizan-primer-borrador-de-la-estrategia-nacional-de-ciberseguridad/ . consultado el 15/04/2019

[6] https://www.prensalibre.com/guatemala/justicia/gobierno-busca-protegerse-de-los-ciberdelitos/ . consultado el 15/04/2019

Utilizando el método hipotético-deductivo, un método empírico que permite exponer el problema y la posible solución al mismo, ¿cómo puede el Estado de Guatemala garantizar la ciberseguridad de la infraestructura crítica del país?

La Hipótesis principal del presente trabajo es: “El Estado de Guatemala necesita definir e implementar un modelo de ciberseguridad, para garantizar el funcionamiento continuo de sus infraestructuras críticas ante la amenaza de los ciberataques a la seguridad de la nación”.

En este trabajo el autor pretende analizar, exponer el nivel de vulnerabilidad actual, riesgos, proponer un modelo integral para el combate del ciberdelito, utilizando como medio de implementación una política pública y una propuesta de catálogo de infraestructuras críticas. El modelo de ciberseguridad debe atender, primordialmente, las variables principales que se presentan en la Hipótesis secundaria: “La falta de institucionalidad, marco jurídico y alianzas público-privadas generan que el país sea vulnerable al ciberdelito.

El objetivo general de la investigación es formular un modelo nacional de ciberseguridad que garantice la disponibilidad, integridad y confidencialidad de la información y los sistemas informáticos que controlan las infraestructuras críticas del país, ante la amenaza del ciberdelito a la seguridad de la nación.

Entre los objetivos específicos se intentará:

1. Analizar el Marco Jurídico en materia de la protección de la información en Guatemala.

2. Proponer un marco jurídico mínimo necesario para el combate al ciberdelito.

3. Proponer una definición y clasificación de infraestructura crítica nacional.

4. Definir los niveles y medios para una cooperación internacional efectiva, en materia de seguridad en el ciberespacio.

5. Proponer un modelo institucional para la respuesta ante emergencias cibernéticas.

6. Proponer un modelo de política nacional de ciberseguridad para la implementación del modelo nacional de ciberseguridad planteado.

Este estudio se justifica porque la Agenda Nacional de Riesgos y Amenazas 2018 del Sistema Nacional de Inteligencia considera una amenaza a la seguridad nacional los Ciberataques[7]. La Política Nacional de Seguridad 2017 coloca a los ciberataques como un problema de seguridad nacional, aunque no hay ninguna directriz sobre cómo el país debe afrontar este problema transnacional.

En el primer capítulo se analiza el marco jurídico nacional e internacional que rige actualmente en Guatemala, así como algunos tratados y convenciones internacionales que el país ha suscrito. En cuanto al capítulo dos, en este se analiza y propone un catálogo preliminar de lo que puede ser infraestructura crítica en Guatemala, la importancia de su protección y las amenazas a las cuales está expuesta. Mientas tanto en el capítulo tres se propone un modelo nacional de ciberseguridad que es factible de implementar como marco para que el país afronte el problema actual de ciberseguridad de manera integral, priorizando los ejes legislativo, institucional, cooperación internacional, políticas y estrategias, alianzas público-privadas y proyectos tecnológicos estratégicos. En el capítulo cuatro se plantea una política nacional de ciberseguridad para infraestructuras críticas en Guatemala, la cual puede servir como instrumento técnico político para implementar y monitorear el modelo nacional de ciberseguridad.

En el anexo 1 de gráficas se presenta información relevante de la Organización de los Estados Americanos, acerca de estudios realizados en la región sobre la situación en la que se encuentra Latinoamérica respecto de sus infraestructuras críticas y su ciberseguridad. También se expone información

[7] https://www.sie.gob.gt/portal/images/DocumentosVarios/anra/2018_ANRA.pdf . consultado el 15/01/2019

relevante del nivel de madurez tecnológica de Guatemala, según el Foro Económico Mundial en el anexo 2.

El anexo 3 de imágenes contempla contenido de trabajo realizado en hitos nacionales en el combate del ciberdelito, como: la creación de la estrategia nacional de ciberseguridad; la elaboración del borrador cero del proyecto de ley contra la ciberdelincuencia, que se convirtió en la iniciativa de ley 5254; algunos documentos oficiales que marcaron el inicio del camino institucional y diplomático de los proyectos nacionales antes mencionados, con el acompañamiento de la cooperación internacional. En el anexo 4 se muestra el esquema del contenido del convenio de Budapest, mientas que el anexo 5 presenta la tabla que contiene las variables utilizadas por la OEA en la evaluación de madurez cibernética de Guatemala, así como la respectiva calificación de país para cada índice y subíndice. El anexo 6 contiene los criterios de la legislación española para catalogar infraestructura crítica.

Finalmente se presentan las conclusiones del estudio, relacionadas con la Hipótesis del trabajo y los objetivos que fueron planteados.

CAPÍTULO UNO

1. Ciberseguridad y el Marco Jurídico de la protección de la información en Guatemala

Los ataques cibernéticos ocurren todos los días. Vásquez (2016) los denomina “guerra de cuarta generación”[8]. Otros lo llaman terrorismo cibernético. A los métodos utilizados se les denomina ataques a los sistemas. Sus resultados son: robo de información, secuestro de información, sistemas compuestos por hardware y softwares inoperables, sitios web alterados, sistemas que no responden debido a la saturación de peticiones falsas, alteración de información. Por su naturaleza pueden originarse de personas individuales, crimen organizado o de Estados. Los objetivos pueden ser personas, empresas o Estados. Son los Ataques cibernéticos o Ciberataques que constituyen un problema mundial de seguridad para los países, y Guatemala no es la excepción.

En el presente capítulo se analizarán conceptos principales relacionados con el tema de ciberseguridad en el marco de seguridad nacional y se expondrán algunas de las tecnologías emergentes que están causando gran impacto en la seguridad de las naciones. Además, se analizarán algunas leyes del marco jurídico de Guatemala relativas al tema de protección de información. Así también las propuestas de ley contra el ciberdelito, pues se consideran fundamentales para la construcción de un modelo de ciberseguridad nacional.

1.1 Seguridad

El diccionario Webster define el vocablo seguridad como “libre de ansiedad, preocupación o temor”. [9]

[8] Olmedo Vásquez. *Guerras de cuarta generación y sus efectos en la Seguridad Estratégica de Guatemala*. Biblioteca Digital, USAC. 2016. http://biblioteca.usac.edu.gt/tesis/04/04_13444.pdf. Consultado el 20 de enero 2020

[9] https://www.merriam-webster.com/dictionary/security. Consultado el 15 de enero 2020

La Real Academia Española define seguridad como “cualidad de seguro”.

En el estudio tradicional de la seguridad, el concepto se modificará según el adjetivo que le sucede.

1.1.1 Seguridad Ciudadana

Según la RAE:
“Situación de tranquilidad pública y de libre ejercicio de los derechos individuales, cuya protección efectiva se encomienda a las fuerzas de orden público”. [10]

1.1.2 Seguridad Jurídica

“Cualidad del ordenamiento jurídico que implica la certeza de sus normas y, consiguientemente, la previsibilidad de su aplicación”.[11]

1.1.3 Seguridad Social

“Sistema público de prestaciones de carácter económico o asistencial, que atiende necesidades determinadas de la población, como las derivadas de la enfermedad, el desempleo, la ancianidad, etc.” [12]

1.2 Seguridad Nacional

Los conceptos de seguridad nacional están históricamente asociados al Estado, al poder y a las relaciones internacionales.

En su célebre obra *Leviatán*, Hobbes presenta al Estado como un gran monstruo, cuyos miembros describe como acciones o atribuciones que el Estado ejecuta y es responsable.

---

[10] https://dle.rae.es/seguridad%20?m=form2. Consultado el 15 de enero 2020
[11] Ídem.
[12] Ídem.

"En una condición de estado de naturaleza (sin estado), no hay lugar para el trabajo, ya que el fruto del mismo se presenta como incierto; y, consecuentemente, no hay cultivo de la tierra; no hay navegación, y no hay uso de productos que podrían importarse por mar; no hay construcción de viviendas, ni de instrumentos para mover y transportar objetos que requieran la ayuda de una fuerza grande; no hay conocimiento en toda la faz de la tierra, no hay cómputo del tiempo; no hay artes; no hay letras; no hay sociedad. Y lo peor de todo, hay un constante miedo y peligro de perecer con muerte violenta. Y la vida del hombre es solitaria, pobre, desagradable, brutal y corta".[13] Hobbes expresa que el ser humano no puede vivir sin la protección social, económica, humana y jurídica del Estado. Por ello, aboga por un Estado fuerte que impida la anarquía en la sociedad.

La seguridad es una de las principales razones para la existencia del Estado. Según Hobbes: "De esta igualdad en las facultades surge una igualdad en la esperanza de conseguir nuestros fines. Y, por lo tanto, si dos hombres desean una misma cosa que no puede ser disfrutada por ambos, se convierten en enemigos; y, para lograr su fin, que es, principalmente, su propia conservación y, algunas veces, solo su deleite, se empeñan en destruirse y someterse mutuamente. De esto proviene el que allí donde un usurpador no tiene otra cosa que temer más que el poder de un solo hombre, es muy probable que una sus fuerzas con las de otros y vaya contra el que ha conseguido sembrar, cultivar y hacerse una posición ventajosa. Y tratará, así, de desposeerlo, no solo del fruto de su trabajo, sino también de su vida o de su libertad. Y, a su vez, el usurpador se verá después expuesto a la amenaza de otros"[14].

Para Hobbes nadie es tan fuerte como para librarse de todas las amenazas y agresores, por lo que necesitamos un Estado que se encargue de la seguridad de sus ciudadanos.

---

[13] Thomas Hobbes. *Leviatán*. Alianza Editorial. Madrid. 1993. Pág. 108
[14] Ibídem. Pág. 184

Hobbes llama estado de naturaleza a la condición de personas viviendo sin la organización de Estado con leyes y cuerpos administrativos que cumplan y hagan cumplir las leyes. Concibe tres razones importantes para atacar a otros en el estado de naturaleza: "por ganancias, por seguridad y por gloria o reputación".[15] Cualquiera de estos sería el móvil por lo que las personas atacarían unas a otras. No quiere decir que eso no suceda, incluso, en sociedades modernas que se rigen por leyes.

Hobbes resalta que esto sería aún más común y que no permitiría el desarrollo pleno del ser humano en su entorno. Pues no habría certeza de poseer los bienes por los cuales ha trabajado y se ha esforzado tanto. Destaca, también, que aún en un Estado con leyes habrá una minoría que robe y haga el mal a la comunidad. Pero el Estado con sus leyes evitará que esa situación nos lleve a una guerra de todos contra todos.

El estado de guerra este autor no lo define como una lucha constante, sino como una disposición constante a luchar. Lo causaría el vivir sin un Estado y sin leyes[16]. La seguridad es, para Hobbes, uno de los tres pilares que justifican la creación del Estado.

Acerca de ese constante miedo y temor del que Hobbes habla se refirió Zygmund Bauman en su libro en Busca de la Política, en el cual expresa que la misma naturaleza de la inseguridad evita que las medidas colectivas tomadas por la clase política para evitarla sean eficientes y eficaces. Según Bauman, las personas tienen tanto temor interno derivado de miedos, frustraciones y estereotipos que son incapaces de accionar contra la inseguridad.

La palabra alemana para inseguridad *Unsicherheit* fusiona tres del español: "incertidumbre", "inseguridad", "desprotección". Para Bauman, la inseguridad es el problema contemporáneo más siniestro y penoso. Analiza que lo único que pueden hacer los gobernantes y que hacen casi siempre es concentrarse en la seguridad,

[15] Wolff, Jonathan. *Filosofía Política*. Editorial Ariel. Buenos Aires. 2012. Pág. 29
16 Ibídem. Pág. 30

porque es lo único que pueden hacer que es visible, aunque siempre crean males mucho más grandes; en el nombre de la seguridad tienden a dividir, siembran la suspicacia mutua, separan a la gente, la inducen a suponer conspiradores y enemigos ante cualquier disenso o argumento y acaban por volver más solitarios a los solos[17].

Sicherheit es la palabra alemana que Bauman utiliza para seguridad y significa en español “seguridad”, “certeza” y “protección”. a) Seguridad de que todo aquello que hemos ganado o conseguido seguirá en nuestro poder, y que conservará su valor; creemos que el mundo es estable y confiable. b) Certeza. Implica profundo conocimiento para discernir entre lo razonable y lo insensato, lo confiable y lo engañoso, lo útil y lo inútil. c) Protección. Siempre que uno se comporte de manera correcta ningún peligro extremo amenazará nuestro cuerpo y sus extensiones, es decir, nuestras propiedades, nuestro hogar y lo que nos rodea.

Tanto para Bauman como para Hobbes, la inseguridad inicia dentro del ser humano mismo, dentro de sus miedos, temores conscientes o inconscientes de retener los bienes que él mismo ha ganado con su trabajo, su seguridad física y de su familia. Sin esa certeza de seguridad se crea un caldo de cultivo social de miedos que explotan ante cualquier amenaza real o aparente. Es esta la razón por la que la naturaleza humana, acerca del sentimiento de inseguridad, hace que los esfuerzos de los Estados sean inútiles en crear un sentimiento de seguridad ante la población.

Como se mencionó anteriormente, las soluciones de “seguridad” que se implementan causan daños mayores a la ya frágil situación emocional de las personas. Podríamos concluir que, para Bauman, la seguridad es y será un tema sin resolver, debido a que responde más a un tema más humano que social. Un tema más privado que público.

[17] Bauman, Zygmunt. *En Busca de la Política*. Fondo de Cultura Económica. Argentina. 2001. Pág. 60

Los Estados han reaccionado ante esas necesidades de la población de aliviar sus sensaciones de inseguridad, sea cual fuere el o los motivos interiores, invirtiendo y potenciando de una maquinaria que poco ha logrado que la población se sienta segura. En el caso de Guatemala, incluye: inteligencia civil, inteligencia militar, seguridad exterior, seguridad interior, gestión de riesgos y defensa civil.[18]

El concepto tradicional de seguridad nacional ha evolucionado durante décadas y, aun hoy, sigue el debate político y filosófico sobre su verdadera definición. Analizaremos sobre su evolución, partiendo del concepto de seguridad nacional de Walter Lippmann, a quien se le conoce, precisamente, como el padre del concepto de seguridad nacional. Llegó a ser asesor en materia de seguridad del presidente Woodrow Wilson durante la época de la Primera Guerra Mundial, así como del presidente Lyndon Johnson durante la guerra de Vietnam. Lippmann concebía la seguridad nacional al decir: "Una nación está segura cuando no tiene que sacrificar sus legítimos intereses para evitar la guerra y cuando es capaz, si fuera necesario, de mantenerlos a través de la guerra"[19]

Tomando como base la conceptualización de seguridad nacional de Lippmann, Sergio Aguayo y Bruce Michael Bagley definen seguridad nacional como "Una nación está segura cuando su gobierno tiene el suficiente poder y capacidad militar para impedir el ataque de otros estados a sus legítimos intereses y, en caso de ser atacada, para defenderlos por medio de la guerra" [20]

Otra definición de seguridad nacional la ofrece Javier Elguea: "En términos generales la noción de seguridad se ha asociado con la de protección y la de evitación de peligro o riesgo. La mayor parte de los especialistas dedicados a este campo se refieren a la "seguridad nacional" como la capacidad de un Estado-nación para defenderse de ataques extraños, y como la habilidad de este Estado-nación

---

[18] *Ley Marco del Consejo Nacional de Seguridad*. Congreso de la República de Guatemala. 2008. Art. 18
[19] Aguayo, Sergio et al. *En busca de la Seguridad Perdida*. Siglo Veintiuno Editores. México. 2002. Pág. 44
[20] Ídem

para defender sus intereses nacionales entendidos fundamentalmente como la integridad territorial y la soberanía política"[21]

Este es el concepto tradicional de Seguridad Nacional en donde los factores territorio- Estado son los principales y únicos. Dentro de ese modelo no tiene lugar modelo de ciberseguridad a las infraestructuras que soportan el funcionamiento del Estado.

La teoría tradicional de seguridad nacional en la cual las amenazas son externas no explica lo que ocurrió en Guatemala y demás países de Centroamérica después de la Segunda Guerra Mundial con las guerras internas de Guatemala, El Salvador y Nicaragua, en donde se vieron las consecuencias de la militarización de la región, y la política de los Estados Unidos del combate contra el comunismo, la aplicación de la Escuela realista del uso del poder militar y la "construcción" del Estado sumirían al país en una guerra interna de 36 años.

Existe un debate encarnizado entre intelectuales de la seguridad en cuanto a ampliar el concepto de seguridad nacional e incluir temas como cambio climático, agotamiento de recursos naturales no renovables, la migración internacional ilegal, entre otros. [22] Una de las corrientes modernas de pensamiento referente a seguridad es la denominada "poder inteligente"; este modelo de seguridad se basa en tres variables llamadas las 3D: diplomacia, defensa y desarrollo; en esta convergen el llamado "soft power" (poder blando) y el "hard power" (poder duro/militar), encontrando un balance para construir un modelo de seguridad basado en relaciones internacionales efectivas, negociaciones y el poderío militar tradicional. [23]

La ciberseguridad es imposible etiquetarla dentro de un contexto de seguridad interna o externa o entre civiles y militares. El ciberespacio y la

---

[21] Ibídem. Pág. 77
[22] Elguea, Javier. *Seguridad Internacional y el Desarrollo Nacional*. Alianza Editorial. 1993. Página 77
[23] http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM05-2011EvolucionConceptoSeguridad.pdf. Consultado el 17 de enero 2020

globalización del internet han borrado los límites fronterizos y han facilitado el poder de uso tanto a militares como a civiles, dando lugar a lo que encuadra en el concepto de guerras asimétricas. Pequeños grupos de especialistas en programación y redes de computadoras haciendo daños incalculables a naciones.

Cuando se analiza la naturaleza de los ataques cibernéticos se deduce que los mismos pueden ser originados por civiles en busca de ganancias económicas, o grupos financiados por países; queda claro que la ciberseguridad no encuadra en el concepto tradicional de seguridad nacional, en el cual el territorio y el poderío militar son las variables principales.

Con el establecimiento de las Naciones Unidas en el año 1945 se incluyen aspectos no militares al concepto de seguridad. El artículo 55 de la carta de ONU señala que “con el propósito de crear las condiciones de estabilidad y bienestar necesarias para las relaciones pacíficas y amistosas entre las naciones, basadas en el respecto al principio de la igualdad de derechos y al de la libre determinación de los pueblos, la Organización promoverá: a) niveles de vida más elevados, trabajo permanente para todos, y condiciones de progreso y desarrollo económico y social; b) La solución de problemas internacionales de carácter económico, social y sanitario, y de otros problemas conexos; y la cooperación internacional en el orden cultural y educativo; y c) el respeto universal a los derechos humanos y a las libertades fundamentales de todos”[24]. Por primera vez se incluyen en el concepto de seguridad derechos humanos, desarrollo económico y social. El territorio y el Estado habían dejado de considerarse la principal razón de ser del concepto de seguridad nacional.

Con ello nace la escuela liberalista a la que se agregaron conceptos de seguridad como: seguridad común, seguridad colectiva, seguridad compartida, seguridad democrática, seguridad humana o seguridad cooperativa.

[24] https://www.un.org/es/sections/un-charter/chapter-ix/index.html. Consultado el 10 de enero 2020

Se incluyen nuevas amenazas que debe atender el Estado: “problemas globales, transfronterizos en su mayoría, tales como el crimen organizado, el terrorismo, la degradación del medio ambiente, la disputa por los recursos naturales, los flujos incontrolados de refugiados, la inmigración no regulada, la pobreza y el hambre se han convertido en riesgo para la humanidad de una importancia similar a la de la tradicional defensa militar”.[25]

La Política Nacional de seguridad en Guatemala presenta el enfoque no tradicional de seguridad: “establece un modelo de acción integral e interinstitucional para la seguridad de la nación”[26]. Con un modelo de seguridad denominado gobernanza integral propone “una visión amplia y compartida de responsabilidades institucionales para la seguridad de la persona, sus bienes e instituciones vinculada a la agenda de desarrollo, así como a la integración de todos los sectores sociales, para lograr resultados efectivos y sostenibles para la Seguridad de la Nación”[27]. Los niveles de los que trata son los mismos que los de la ley marco del sistema nacional de seguridad: Seguridad Interior, Seguridad Exterior, Inteligencia de Estado y Gestión de Riesgos y Defensa Civil.

Este concepto de seguridad nacional no tradicional, en el cual el Estado es el responsable de brindar protección ante cualquier amenaza a sus ciudadanos, abre el abanico de aristas conceptuales de seguridad no convencionales, provee un marco para modelos de prevención y reacción ante ataques cibernéticos a las infraestructuras críticas del país que requieren un alto grado de coordinación, no solo interinstitucional, sino que también colaboración público-privada nacional e internacional.

[25] http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM05-2011EvolucionConceptoSeguridad.pdf. Consultado el 17 de enero 2020
[26] *Política Nacional de Seguridad. Gobierno de Guatemala*. 2017. Pág. 9
[27] Ibídem. Pág. 23

1.3 Ciberseguridad

La Unión Internacional de Telecomunicaciones, organismo de las Naciones Unidas encargado de regular las telecomunicaciones a nivel internacional, presenta un concepto de ciberseguridad al cual se apegará el presente trabajo: "La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: a) disponibilidad; b) integridad, que puede incluir la autenticidad y el no repudio; c) confidencialidad." [28] Este será el concepto que se utilizará en el presente trabajo cuando se haga referencia al término ciberseguridad.

1.4 Infraestructuras Críticas

Seguidamente, se presenta la definición del gobierno español acerca de Infraestructura Crítica, que servirá de base para la propuesta de elaboración del modelo nacional de ciberseguridad y la política nacional de ciberseguridad para infraestructuras críticas en Guatemala. También en ello se fundamentará la propuesta del catálogo preliminar de infraestructuras críticas que se presenta en el capítulo dos.

[28] https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx. Consultado el 05 de enero 2020

El Instituto Español de Estudios Estratégicos (IEEE) define infraestructura crítica como: “Las infraestructuras que son necesarias para el funcionamiento normal de los servicios básicos y de los sistemas de producción de cualquier sociedad. De tal manera que cualquier interrupción no deseada, ya sea debida a causas naturales, técnicas, ya sea por ataques deliberados, tendrían graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, aparte de ser una fuente de perturbaciones graves en materia de seguridad.”

Los grandes sectores que fueron identificados como infraestructura crítica son: “agua, alimentación, energía, espacio, industria nuclear, industria química, instalaciones de investigación, salud, sistema financiero y tributario, transporte y tecnologías de la información y las comunicaciones”[29]. Guatemala no cuenta con un catálogo de infraestructuras críticas, uno de los objetivos específicos del presente trabajo es proponer un catálogo preliminar con base en la realidad tecnológica nacional.

1.5 Ciberamenazas

“Una amenaza digital o ciberamenaza es un acto malicioso que busca hacer daño a datos, robar datos, o afecta la vida digital en general. Los ciber ataques (sic) incluyen amenazas como virus, brechas de datos, ataques DDoS, entre otros.”[30] Los ataques pueden provenir de individuos llamados hackers, que son personas con alto nivel de conocimientos en programación en busca de lucro, el crimen organizado, terrorismo o incluso ataques de Estado a Estado. Guatemala no está exento de estos ataques.

---

[29] *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*. Ministerio de la Defensa Española. Cuadernos de Estrategia 149. 2010. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

[30] https://preyproject.com/blog/es/ciberamenazas-que-son-como-te-afectan-y-que-puedes-hacer-al-respecto/. Consultado el 29/01/2020

Aunque el nivel de uso de tecnología del Estado y el nivel de gobierno electrónico no es tan alto como países desarrollados, el adoptar una política de ciberseguridad garantizará, tanto a los actuales servicios digitales, como a los que en el futuro se implementarán, que no se conviertan en blancos vulnerables de ataques de cualquier índole.

1.6 Avance de las Tecnologías de la Información y Comunicación y las amenazas a la seguridad nacional

Se presentan los avances tecnológicos que han ocurrido en la última década y como ha impactado esto en la seguridad nacional de muchos países. Son aspectos que deben tomarse en cuenta para el fortalecimiento del Ciberespacio en Guatemala.

En 1965 Gordon Moore escribió un artículo que originó lo que se denominó la Ley de Moore[31]. Predecía que la complejidad de los circuitos integrados se duplicaría cada año, con una alta reducción de costos. Aunque después cambió la versión original y la predicción fue para dos años, nadie duda de que la tendencia ha sido esa. Cada día se hace posible la integración de más circuitos electrónicos en espacios más pequeños, lo que ha ocasionado una revolución tecnológica y el abaratamiento de esta. Por eso, tenemos semiconductores a base de silicio, desde juguetes hasta naves espaciales. Esto ha dado lugar a computadores personales, internet, telefonía móvil, sistema de posicionamiento global (GPS, por sus siglas en inglés), aeronaves, sistemas de radar y satélites.

Evans identifica cinco indicios importantes en cuanto al avance de la tecnología.

[31] Moore, Gordon E. *"Cramming more components into integrated circuits"*. artículo en inglés en la revista *Electronics*, volumen 38, n.º 8; 19 de abril de 1965. Publicado en el sitio web Web Eng FIU.edu.

- El número de transistores de un circuito integrado se sigue duplicando cada dos años. La densidad de almacenamiento se duplica cada trece meses. La cantidad de datos transmisibles en fibra óptica se duplica cada nueve meses.

- El acceso a internet de banda ancha, dentro del G-20, ha crecido de 800 millones en 2010 a 27,000 millones en 2015. Hay entre 1,000 y 2,000 millones más de personas en el mundo que tienen un teléfono móvil que las que tienen una cuenta bancaria o un retrete.

- *Facebook* tiene 1,300 millones de usuarios activos, el 64% de los cuales visita el portal a diario (durante unos veinte minutos de media). Cada día hay 45,000 millones de "me gusta" nuevos. Cada año se sube a internet medio billón de fotografías y a *YouTube* cien horas de video por minuto.

- El número de sensores IP superará los 50,000 millones en 2020. Las tarjetas de identificación por radiofrecuencia (RFID, por sus siglas en inglés) cuestan hoy solo cinco centavos.

- El 90% de los datos almacenados en el mundo se generó en los últimos dos años. De ellos, el 99% está ya digitalizado y más de la mitad habilitado para internet.[32]

La información almacenada en forma digital y masiva ha creado nuevos conceptos de análisis de datos. El concepto de bigdata define al conjunto de tecnologías que integran y analizan grandes cantidades de información en tiempo real, a las cuales se les aplican algoritmos estadísticos y matemáticos en busca de modas, tendencias y patrones, información que luego es utilizada para la toma de decisiones en marketing, publicidad, economía y política.

En cuanto a información personal, las redes sociales han jugado un rol especialmente revolucionario. Nunca en la historia, la sociedad había compartido

[32] Evans, Phill. *Reconstruir la empresa en la Era Digital.* BBVA Press. Madrid. 2015. Págs. 19-21

tanto material gráfico o biográfico. Sus metas, sus ambiciones, sus gustos, sus intereses. Facebook, Twitter, Instagram, WhatsApp y otras decenas de redes sociales llegan a miles de millones de usuarios que comparten todo tipo de información, llegando al punto de ser herramientas no solo para compartir datos personales, sino que se convierten en indispensables herramientas políticas, sociales y de investigación. Parece que la prensa tradicional denominada El Cuarto Poder, por primera en la historia, tiene un serio competidor que amenaza con quitarle el trono.

En cuanto a la influencia en la política de las redes sociales, Moisés Naím, en su libro "El fin del Poder", hace el siguiente análisis: "son los jóvenes – irreverentes, deseosos de cambio, desafiantes, mejor informados, móviles, y conectados – quienes constituyen la mayoría de la población. Y como hemos visto en el norte de África y Oriente Próximo, los jóvenes tumban gobiernos."[33]

Naím también define que vivimos una época en la que aún existe un debate encarnizado sobre el impacto de las redes sociales en la creación de nuevos movimientos sociales de oposición política; lo cierto es que se han utilizado en ambos lados, pues también los gobiernos las han aprovechado para vigilar y reprimir.[34] En cuanto a esto último, se puede decir que los softwares o paquetes orientados a la investigación utilizando las redes sociales se vuelven cada vez más lucrativos y eficientes; paquetes diseñados para que su comercialización sea exclusivamente para gobiernos permiten monitorear, georreferenciar, analizar y almacenar sistemáticamente a miles de personas en tiempo real. Las redes sociales, tal como lo expone Naím, presentan dos caras: la primera de libre emisión del pensamiento y expresión ciudadana y la otra como herramienta de monitoreo de masas de los gobiernos.

Otro concepto que nos estamos acostumbrando a utilizar, pero se encuentra presente en nuestro trabajo y vivir diario, es la utilización de la "Nube", la cual no es

[33] Naím, Moisés. *El Fin del Poder*. Debate. Argentina. 2013. Pág. 107
[34] Ibidem. Pág. 88

más que el almacenamiento, análisis y recuperación de información en servidores remotos a los cuales, vía internet, nuestros dispositivos como celulares móviles o computadoras se conectan. Una de las ventajas más grandes es que no consumimos espacio de almacenamiento y algunas veces procesamiento en nuestros dispositivos locales, lo que permite descargar de esas tareas a nuestros dispositivos y dejarlo en manos de servidores remotos que ningún usuario final sabe dónde se encuentran y son los que realizan las tareas. A nivel estatal, empresarial y personal ha venido a cambiar la forma en la que estamos almacenando y recuperando nuestra información.

Es importante mencionar que esta forma de utilización de tecnología ha abierto algunas brechas de seguridad serias, y se ha sabido de ataques masivos de parte de hackers hacia sitios donde está almacenada la información de empresas y gobiernos. El uso de cualquier tipo de tecnología lleva implícitos riesgos y, cuando se trata de tecnología sobre la cual depende el funcionamiento de un país, se debe tener consideraciones especiales de seguridad que serán tratadas más adelante.

La tecnología influye en nuestras vidas y, tal como predijo Moore, se seguirá abaratando y haciendo más rápida; nuestra forma de comunicarnos, nuestro estilo de vida, nuestro aprendizaje, la divulgación de nuestro conocimiento, nuestra salud, nuestra seguridad seguirán dependiendo de ella.

1.6.1 Retos de Ciberseguridad para los avances tecnológicos

Todo avance presenta retos, y la tecnología no es la excepción. Con cada avance de la ciencia y aplicación de los conocimientos que ella ha develado, la humanidad se ha enfrentado a nuevos problemas, consecuencias naturales de su aplicación o de la ambición. El presidente del Banco Interamericano de Desarrollo (BID) expresó las siguientes palabras en la introducción de la publicación: “¿Ciberseguridad, Estamos preparados en América Latina y el Caribe?”: “Hay Mucho en juego. Según cálculos, el cibercrimen le cuesta al mundo hasta US$575,000 millones al año, lo que representa 0,5% del PIB global. Eso es casi cuatro veces más que el monto anual de las donaciones para el desarrollo

internacional. En América Latina y el Caribe, este tipo de delitos nos cuestan alrededor de US$90,000 millones al año. Con esos recursos podríamos cuadruplicar el número de investigadores científicos en nuestra región"[35].

Después de mencionar que somos el cuarto mercado mundial en el uso de internet y las telecomunicaciones, Moreno menciona nuestra situación como región en cuanto a la ciberseguridad: **"Pero en donde nos quedamos cortos es en prevenir y mitigar los riesgos de la actividad delictiva o maliciosa en el ciberespacio**…Si vamos a sacarle la mayor ventaja posible a la llamada cuarta revolución industrial, tenemos que crear una infraestructura digital no solo moderna y robusta sino también segura. ***Proteger a nuestros ciudadanos del cibercrimen no es una mera opción: es un elemento clave para nuestro desarrollo***".

Es por ello que debemos urgentemente atender el tema de la ciberseguridad en un marco nacional y, como primeras acciones, definir un modelo nacional de ciberseguridad y una política nacional de ciberseguridad que sea el instrumento de su implementación.

John Chambers, gerente y jefe ejecutivo de CISCO, la compañía líder mundial en la fabricación de dispositivos de interconexión sobre los cuales funciona Internet, dijo: "Nunca deja de sorprenderme la velocidad de la innovación. El cambio es la única y verdadera constante, y cada año ritmo de cambio solo se acelera. Transiciones que una vez han tenido lugar durante tres o cinco años ahora suceden en 12 a 18 meses."[36]

Todo este avance de dependencia tecnológica del sector público y privado genera que las instituciones y empresas se preocupen y ocupen, en mayor o menor medida, por la seguridad de la información. Todo indica que el país tiene un reto

---

[35] *Ciberseguridad ¿estamos preparados en América Latina y el Caribe?* BID-OEA. 2016. Pág. 9 Disponible en:https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean; consultado el 21/01/2018

[36] *Reporte Global de Tecnologías de la Información 2014*. Foro Económico Mundial. Consultado en: http://reports.weforum.org/global-information-technology-report-2014/#section=foreword-cisco-systems

gigantesco; debemos avanzar en el uso de la tecnología, y debemos crecer tecnológicamente en un entorno seguro; de lo contrario, estaremos construyendo castillos de arena que serán digitalmente frágiles. Guatemala tiene instituciones, centros de servicio e infraestructura que dependen de la tecnología; es allí donde, en primera instancia, debemos trabajar para protegerla de ataques cibernéticos.

1.7 Marco Jurídico Nacional en la protección de la información

Guatemala no cuenta con alguna ley que regule la seguridad de la información de forma explícita. No existe un marco jurídico que garantice la confidencialidad, integridad y disponibilidad de la información. Se carece de la legislación mínima necesaria para construir un ciberespacio efectivo ante amenazas para la seguridad nacional.

Esto tiene como consecuencia que en el país no haya instituciones que sean los entes rectores encargados de velar por la seguridad cibernética a ninguna escala, en ninguna de las temáticas como comercio electrónico: respuesta ante políticas y estrategias, emergencias informáticas, investigación cibernética, alianzas público-privadas, desarrollo de estándares, informática forense y protección a las infraestructuras críticas del Estado.

No existe una ley que tipifique los actos de ciberdelito que comprometan la confidencialidad, la integridad y la disponibilidad de la información y sistemas informáticos tales como: acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos. Tampoco de los delitos informáticos: falsificación informática, fraude informático.[37].

A continuación, se presenta un análisis de las leyes y reglamentos que abordan el tema de la seguridad de la información y la seguridad informática.

---

[37] *Convenio sobre la Ciberdelincuencia ETS 185 (Budapest)*. Firmado por los Integrantes de la Unión Europea. Budapest. 2001. Disponible en: https://rm.coe.int/16802fa403. Consultado el 20 de diciembre 2018

1.7.1 Constitución Política de la República de Guatemala

La Constitución Política de la República de Guatemala es la ley suprema, el marco rector de todas las demás normas y leyes vigentes y por aprobarse. Establece el marco legal para la creación y ejecución de cualquier política pública, ya que sus objetivos deben empatar con los artículos que la componen y son la base para el funcionamiento correcto del Estado y la sociedad.

El marco constitucional para la implementación de políticas, estrategias, instituciones y leyes en busca de brindar ciberseguridad por parte del Estado lo respalda nuestra constitución al rezar:

Artículo 1: “El Estado de Guatemala se organiza para proteger a la persona y la familia; su fin supremo es la realización del bien común”.[38]

Artículo 2: “Deberes del Estado. Es deber del Estado garantizarles a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona.”[39]

Artículo 3. “Derecho a la vida. El Estado garantiza y protege la vida humana desde su concepción, así como la integridad y la seguridad de la persona.” [40]

Artículo 51. “Protección a menores y ancianos. El Estado protegerá la salud física, mental y moral de los menores de edad y de los ancianos. Les garantizará su derecho a la alimentación, salud, educación y seguridad y previsión social.”[41]

---

[38] *Constitución Política de la República de Guatemala. Congreso de la República de Guatemala*. 1985. Pág. 1
[39] Ídem
[40] Ídem
[41] Ibídem, pág. 10

1.7.1.1 Protección de la Información en la Constitución Política de la República de Guatemala

El primer párrafo del artículo 24 de la Constitución Política de la República de Guatemala, literalmente, dice: "Se garantiza el secreto de la correspondencia, comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna". [42]

En el año 1985 las tecnologías de información y comunicación aun no tenían el crecimiento y costos bajos de hoy en día; por ello es pertinente el párrafo que, en su parte conducente, señala: "…otros productos de la tecnología moderna". Y en el rubro de comunicaciones con tecnología moderna, se pueden considerar las redes sociales, correo electrónico y videoconferencias.

Al hablar de secreto de la correspondencia de tecnologías modernas se sobreentiende que abarca los tres aspectos que permiten una comunicación efectiva: emisor, medio de transporte y receptor, por lo que se interpreta que, sea cual sea el medio de comunicación, voz o datos, o voz y datos, queda garantizada por la Carta Magna, la no interceptación, alteración o divulgación del contenido de estas.

La protección puede comprender desde el almacenamiento, acceso, distribución, alteración, destrucción o comercialización de la información.

1.7.2 Código Penal

Muñoz Conde define el derecho penal como "un conjunto de normas jurídicas que asocian a la realización de un delito como presupuesto, la aplicación de penas y/o medidas de seguridad, como principales consecuencias jurídicas"[43]. Y como su artículo 1 dice "Nadie podrá ser penado por hechos que no estén expresamente

[42] Ibídem. Art. 24
[43] Muñoz, Conde et al. *Derecho Penal*. Tirant lo Blanch. 2010. Valencia. Pág. 33

calificados, como delitos o faltas, por ley anterior a su perpetración; ni se impondrán otras penas que no sean las previamente establecidas en la ley."[44].

Lo poco que se puede encontrar, en materia de delitos, donde la tecnología es utilizada como medio o como fin, se encuentra en el artículo 274 "A" al "H".

Artículo 274 "A" Destrucción de Registros informáticos: Quien destruya, borre o de cualquier modo inutilice, altere o dañe registros informáticos.

Artículo 274 "B" Alteración de programas: Al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan computadoras.

Artículo 274 "C" Reproducción de instrucciones o programas de computación: Sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación.

Artículo 274 "D" Registros Prohibidos: Al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Artículo 274 "E" Manipulación de información: Al que utilizare registros informáticos o programas de computación para ocultar, 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.

Artículo 274 "F" Uso de información: Al que, sin autorización utilice u obtenga para sí o para otro, datos contenidos en registros informáticos, bancos de datos o archivos electrónicos.

Artículo 274 "G" Programas destructivos: Al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.

---

[44] *Código Penal Guatemalteco*. Congreso de la República de Guatemala. Guatemala. Art. 1

Artículo 274 “H” Alteración maliciosa de número de origen: Quien mediante cualquier mecanismo altere el número proveniente de un operador extranjero de telefonía utilizado exclusivamente para tráfico internacional o altere el número de identificación del usuario que origine una llamada de telefonía.[45]

Para los delitos tipificados en los artículos 274 “A” Destrucción de Registros informáticos, 274 “B” Alteración de programas, 274 “C” Reproducción sin autorización, 274 “D” Registros prohibidos, 274 “G” Programas destructivos, el código procesal penal establece penas de prisión de 6 meses a 4 años.

Mientras tanto, para los delitos contemplados en los artículos: 274 “E” Manipulación de información: prisión de 1 a 5 años; 274 “F” Uso de información sin autorización: prisión de 6 meses a dos años; y 274 “H” Alteración maliciosa de número de origen: de 6 a 10 años de prisión

Estos artículos del código procesal penal están orientados hacia la protección de la tecnología, datos y medios de producción en los cuales se busca proteger los derechos de autor. Para una legislación que busque la protección del ciberespacio orientado a la protección del ser humano, del Estado y sus infraestructuras críticas este artículo no es suficiente, porque solo trata superficialmente algunos temas de seguridad de la información y protección de tecnología.

1.7.2.1 Protección a la Infraestructura de Servicios públicos en el código penal

El código penal, decreto 17-73, en los artículos 294 y 295 del capítulo II De los delitos contra los medios de comunicación, transporte y otros servicios públicos, presenta la tipificación de delitos que son los que más se aproximan a protección de infraestructuras críticas. El responsable será sancionado de uno a cinco años de prisión.

[45] Ibídem. Art. 274

El artículo 294. “Atentado contra la seguridad de servicios de utilidad pública. Quien ponga en peligro la seguridad, o impida o dificulte el funcionamiento de servicios de agua, luz, energía eléctrica o cualquier otro destinado al público.”[46]

Cuando se aprobó el código penal en 1973, los servicios de agua, luz y energía eléctrica eran los servicios públicos prioritarios, los cuales se citan directamente en el artículo. En la frase “cualquier otro destinado al público” se consolidaron todos los demás servicios que en esa fecha funcionaban. El espíritu de este artículo jamás fue tipificar la seguridad de las tecnologías con las cuales funcionaban estos servicios.

En esos años el país se encontraba sumido en una cruel guerra interna que inició en 1960 y finalizó con los tratados de firma de la paz en 1996. Una de las estrategias del bando que se oponía al régimen de gobierno era bombardear pozos de agua, generadores eléctricos y torres de distribución de energía eléctrica de alta tensión. Para inutilizar la infraestructura era necesario destruirla físicamente en forma total o parcial; ahora, la infraestructura puede estar intacta, pero ocasionando problemas a sus controles digitales, hacer que dejen de funcionar totalmente y causarles daño irreparable. De manera que el espíritu del artículo 294 fue la protección física de tales infraestructuras de servicio. No era importante, en ese entonces, la seguridad de información y de los sistemas de información e interconectividad de tales servicios. El ciberespacio presenta un escenario mucho más complejo en la actualidad.

Artículo 295. “Interrupción o entorpecimiento de comunicaciones. Quien, atentare contra la seguridad de telecomunicaciones o comunicaciones postales, o por cualquier medio interrumpiere o entorpeciere tales servicios.”[47]

En el año 1973 se consideraba telecomunicaciones a la escasa infraestructura de torres telefónicas, antenas parabólicas de recepción de datos,

[46] *Código Penal*, Decreto 17-73. Congreso de la República de Guatemala. Art. 294

[47] Ibídem. Art. 295

torres de transmisión de radios para uso militar; los telegramas eran transmitidos por telégrafos de un punto a otro. Nunca paso por la mente de los creadores del código penal que un día los sistemas compuestos por hardware y software constituirán una vulnerabilidad de esas plataformas de servicios. Aun con el avance de la tecnología, a la fecha en que se redacta la presente tesis el Estado no toma cartas en el asunto y no percibe que la tecnología que controla las actuales infraestructuras necesita ser jurídica, técnica y tecnológicamente protegidas para evitar un ciberataque que ocasione una catástrofe social en el país.

No se podrá mitigar las vulnerabilidades cibernéticas dependiendo únicamente de estos dos artículos. Es imprescindible como se expondrá en el capítulo tres, un marco jurídico integral. Es necesario y urgente legislar contra el ciberdelito, protección de información y datos, y una ley de protección contra las infraestructuras críticas del país.

1.7.3 Ley del Registro Nacional de Personas

La Ley del Registro Nacional de Personas, Decreto número 90-2005, faculta a la institución con el mismo nombre para recolectar, digitalizar, almacenar, analizar y proveer el documento oficial de identificación de los guatemaltecos. Esto requiere una inmensa tarea informática para cumplir con el objetivo, si analizamos que no únicamente se almacenan datos biográficos, pues también se capturan, almacenan y procesan datos biométricos como lo son las huellas dactilares de los 10 dedos y la fotografía del rostro.

Todo esto se comprime y almacena en un chip en varios niveles de información, codificada de tal forma que no sea fácil la obtención de estos datos. El artículo 2 Objetivos, menciona “El RENAP es la entidad encargada de organizar y mantener el registro único de identificación de las personas naturales, inscribir los hechos y activos relativos a su estado civil, capacidad civil y demás datos de identificación desde su nacimiento hasta la muerte, así como la emisión del Documento personal de identificación. Para tal fin implementará y desarrollará estrategias, técnicas y procedimientos automatizados que permitan un manejo

integrado y eficaz de la información, unificando los procedimientos de inscripción de las mismas."[48]

1.7.4 Sobre la Seguridad en Comunicaciones Telefónicas y Otros Medios

La tecnología de interceptación de comunicaciones telefónicas es altamente sofisticada. La evidencia muestra que en Guatemala estas tecnologías no están siendo comercializadas únicamente con entidades gubernamentales autorizadas por ley. Cualquier persona con poder adquisitivo puede violar el derecho de confidencialidad de todos los ciudadanos guatemaltecos, pues las compañías de tecnología sin escrúpulos comercializan con particulares que no tienen respaldo legal para llevar a cabo estas tareas de investigación.

Se mantiene una constante oferta de servicios de interceptación de llamadas telefónicas, mensajes de texto y la información que viaja por medio de aplicaciones de mensajería y redes sociales; esta información, luego, es utilizada para fines políticos, competencia desleal entre empresas, represión y, lo peor, para fines criminales.

El Estado de Guatemala dio legalidad a las escuchas telefónicas enfocadas a investigación criminal por medio de la Ley contra la Delincuencia Organizada, dando vida legal a los Métodos Especiales de Investigación Criminal, como herramienta tecnológica para combatir la delincuencia organizada y la delincuencia común.

1.7.5 Ley Contra la Delincuencia Organizada del Estado de Guatemala

La Ley Contra la Delincuencia organizada, decreto No 21-2006, en su artículo 15 dice literalmente: "Las comunicaciones interceptadas conforme esta ley y la información relacionada con el segundo párrafo del artículo 24 de la Constitución Política de la Republica, deberán permanecer en estricta confidencialidad para

[48] *Ley del Registro Nacional de las Personas*. Decreto número 90-2005. Congreso de la República de Guatemala. Art. 2.

terceros durante y después de todo el proceso penal. No se consideran terceros las autoridades competentes de otros países en materia de investigación penal"[49]. De esta forma, se legaliza un derecho adquirido de inviolabilidad de las comunicaciones, haciendo posible su interceptación en pro del combate de todo tipo de delincuencia.

Además, el artículo autoriza la interceptación, grabación, reproducción, de comunicaciones orales, escritas, telefónicas, radiofónicas, informáticas y similares que utilicen el espectro electromagnético, así como cualquiera que en el futuro exista[50] . El único requisito para llevarlas a cabo es presentar ante el juez, los números telefónicos, frecuencias, direcciones electrónicas, para determinar el medio informático o electrónico que se pretende interceptar para la escucha, grabación o reproducción de la comunicación respectiva.

Pero va más allá que solo la interceptación de comunicaciones del espectro electromagnético, sea cual sea su fuente. La Ley, en su artículo 14, cita las entidades del Estado obligadas a brindar información acerca del o de los sujetos bajo investigación, y cita a la Superintendencia de Bancos, la Dirección de Catastro y Avalúos Inmuebles, el Registro de la Propiedad Inmueble, el Registro Mercantil, el Registro de Marcas y Patentes, la Superintendencia de Administración Tributaria, la Intendencia de Verificación Especial y cualquiera otra entidad pública.[51] Este artículo autoriza la obtención de información financiera, contable, patrimonio de inmuebles, patentes e información de impuestos. Claramente va más allá de la interceptación telefónica y entra en otro campo más amplio de los sistemas de información de cada una de las dependencias citadas que almacenan datos de los ciudadanos.

En cuanto a los métodos especiales, esta Ley en su artículo 1, define su objeto, que es establecer las conductas delictivas atribuibles a los integrantes de

---

[49] *Ley contra la delincuencia organizada*. Decreto número 21-2006. Congreso de la República de Guatemala. Art. 15
[50] Ídem.
[51] Ibídem. Art. 14

organizaciones criminales y el establecimiento y regulación de los métodos especiales de investigación y persecución penal. Estos métodos se definen en la citada ley en los artículos del 21 al 34 las operaciones encubiertas, del artículo 35 al 47 las entregas vigiladas, y en los artículos del 48 al 71 las intervenciones telefónicas.

Las intervenciones telefónicas fueron operativizadas en el Ministerio de Gobernación mediante el Acuerdo Gubernativo 158-2009, Reglamento para la Aplicación de los Métodos Especiales de Investigación y la Orden General número 22-2009 de la Policía Nacional Civil, en los cuales se establecen procesos, funciones y organización de la Unidad de Métodos Especiales (UME).

En cuanto a seguridad de la información, vale la pena plantearnos las siguientes preguntas, que no están en el rango de investigación de la presente tesis. ¿Qué medidas de control se tienen establecidas para que las personas debidamente autorizadas por la ley cumplan con la confidencialidad de la información sensible recopilada en estas investigaciones?, ¿están únicamente las entidades autorizadas por ley realizando estas actividades de interceptación, tanto telefónicas como de otros medios de comunicación?

1.7.6 Sobre Violaciones al Principio de Confidencialidad de la Información

Si bien el artículo 24 de la Constitución Política de la República de Guatemala hace hincapié en la confidencialidad de esta información, autoriza la revisión por la autoridad competente de: “Los Libros, documentos y archivos que se relacionan con el pago de impuestos, tasas, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley”. [52]

[52] *Constitución Política de la República de Guatemala*. Congreso de la República. Art. 24

En cuanto los funcionarios que tengan acceso a la información descrita en el anterior artículo 24 de la Constitución Política de la Republica, la Ley Contra la Delincuencia Organizada, en su artículo 15 establece que la información recabada: "podrá ser utilizada exclusivamente en la investigación correspondiente, debiéndose guardar la más estricta confidencialidad para terceros durante esta fase. El servidor público que indebidamente quebrante la reserva de las actuaciones en la fase de investigación o proporcione copia de ellas o de los documentos, será responsable administrativamente; sin perjuicio de la responsabilidad penal en que pudiera incurrir". Por lo tanto, violar el principio de confidencialidad de la información, tiene consecuencias administrativas y penales sobre el funcionario implicado.

El Código Penal, Decreto número 17-73, en el capítulo V De la Violación y Revelación de Secretos, artículo 217 bajo la sección Violación de Correspondencia y Papeles Privados, reza literalmente: "Quien, de propósito o para descubrir los secretos de otro, abriere correspondencia, pliego cerrado o despachos telegráficos, telefónicos o de otra naturaleza, que no le estén dirigidos a quien, sin abrirlos, se impusiere de su contenido, será sancionado con multa de cien a un mil quetzales"[53]. Se puede observar que este artículo nuevamente sanciona contra la violación a la confidencialidad de la información, y es obvio que por el año de su redacción y aprobación habla de correspondencia en papel. La tecnología móvil, redes sociales, el correo electrónico y la internet son medios actuales que sustituyeron a las cartas y telegramas en papel, por lo que se ve la urgente necesidad de modificar estas leyes obsoletas en términos de multas y en tecnologías aplicables.

En su artículo 219, sobre la Interceptación o reproducción de comunicaciones, dice: "Quien, valiéndose de medios fraudulentos interceptare, copiare o grabare comunicaciones televisadas, radiales, telegráficas, telefónicas u otras semejantes o de igual naturaleza, o las impida o interrumpa, será sancionado con multa de cien a un mil quetzales[54]". El mismo artículo implica el respeto de los

[53] *Código Penal*. Congreso de la República de Guatemala. Decreto número 17-73. Art. 217
[54] Ibídem. Art. 219

derechos de autor y prohíbe copiar comunicaciones televisadas y radiales, así como confidencialidad de información al mencionar las comunicaciones telegráficas y telefónicas. Este artículo es más amplio en cuanto a los medios de transmisión, pues menciona “u otras semejantes o de igual naturaleza”; esto deja abierto el campo a tecnologías de comunicación que se desarrollaron después del año 1973.

En su artículo 220, bajo Agravación específica impone prisión de seis meses a tres años si quien viola la confidencialidad de la información actúa en calidad de funcionario público o empleado de la dependencia, empresa o entidad respectivas.

En cuanto divulgar información reservada como secreto profesional, el Código Penal en su artículo 223 establece prisión de seis meses a dos años y multas de cien a un mil quetzales. El espionaje industrial es una de las actividades delictivas de competencia desleal, y se puede observar que las penas y multas fijadas para estas actividades son ridículas, en esta era denominada del conocimiento, en donde lo que realmente tiene valor comercial son paquetes de *software*, algoritmos y fórmulas. También se observa que en el año 1973, debido a que la dinámica económica era la industrial y agrícola, no se le dio la priorización adecuada a la propiedad intelectual profesional y queda plasmada en nuestro Código Penal.

El artículo 183 del Código Procesal Penal garantiza el derecho a la intimidad en las comunicaciones al estipular: “no son admisibles los elementos de prueba obtenidos por un medio prohibido, tales como la tortura, la indebida intromisión en la intimidad del domicilio o residencia, la correspondencia, las comunicaciones, los papeles y los archivos privados”. De esta forma se garantiza que en un proceso penal no se aceptarán pruebas de intromisiones “ilegales” a la información de las personas. Únicamente aquellas que se hayan recabado según lo estipula la Ley en Contra de la Delincuencia Organizada, Decreto 21-2006, por lo que nuevamente observamos que no hay garantía de que este principio de privacidad se respete.

1.7.7 Sobre la Distribución Obligatoria de Información por parte del Estado

El marco jurídico de la República de Guatemala obliga, en ocasiones, al Estado a proveer información acerca de los ciudadanos o de entidades gubernamentales. Se analizan algunas de ellas, en las cuales las instituciones estatales quedan obligadas a suministrar información de naturaleza jurídica, personal, penal o financiera.

El Código Procesal Penal, Decreto 51-92, establece en su artículo 74 que el Estado de Guatemala tiene la obligación de poner a disposición pública la consulta al sistema de detenciones del Organismo Judicial, y en relación a los medios a utilizar dice: "Las oficinas de correos, telégrafos y telecomunicaciones serán agencias del servicio; sus empleados y funcionarios estarán obligados a responder a los consultantes gratuitamente, para lo cual se comunicarán con el registro del modo más rápido posible".[55] En consecuencia, el Organismo Judicial tiene la obligación de brindar información de forma rápida y gratuita sobre los registros de detenciones.

1.7.8 Ley de Acceso a la Información Pública

La Ley de Acceso a la Información Pública, Decreto Ley 57-2008, es la que más se aproxima a proteger la información considerada confidencial, aunque su interés primordial es la transparencia del quehacer del Estado.

En su artículo 2 describe su naturaleza: "establece normas y los procedimientos para garantizar a toda persona, natural o jurídica, el acceso a la información o actos de la administración pública que se encuentre en los archivos, fichas, registros, base, banco o cualquier otra forma de almacenamiento de datos que se encuentren en los organismos del Estado". Los sujetos obligados de esta ley según el artículo 2 "Organismos del estado, municipalidades, instituciones autónomas y descentralizadas y las entidades privadas que perciban, inviertan o

[55] *Código Procesal Penal*. Congreso de la República de Guatemala. Decreto 51-92. Pág. 18

administren fondos públicos". La ley de acceso a la información pública no es aplicable a empresas privadas, únicamente al sector público.

Los artículos 31 y 64 presentan sanciones a quienes atenten contra la propiedad de confidencialidad de la información.

Se define como Información Reservada los tipos enlistados en el artículo 23, tales como diplomáticos, militares, propiedad intelectual y todos aquellos considerados como de Seguridad Nacional.

Clasifica la información como confidencial, la que no se podrá suministrar a los solicitantes que se amparen bajo esta ley. Es información confidencial según el artículo 22:

1) La expresamente definida en el artículo veinticuatro de la Constitución Política de la República de Guatemala.

2) La expresamente definida como confidencial en la Ley de Bancos.

3) La calificada como secreto profesional.

4) La que por disposición expresa de una ley sea considerada como confidencial.

5) Los datos sensibles o personales sensibles, que solo podrán ser conocidos por el titular del derecho

6) La información de particulares recibida por el sujeto obligado bajo garantías de confidencia.

La información a la que se refiere el numeral 2 del artículo 22, según La Ley de Bancos y grupos financieros, es la siguiente: la identidad de los depositantes de los bancos, instituciones financieras y empresas de un grupo financiero, así como las informaciones proporcionadas por los particulares a estas entidades. Estipula el mismo artículo que deja de ser confidencial en casos de investigación de lavado de

dinero.[56]

1.7.9 Habeas Data y Protección legal de la Información

Su origen es latín y significa que el sujeto que requiera los datos pueda poseerlos y acceder a ellos. Su traducción literal podría ser “tener datos presentes”.

En dos artículos de la Constitución Política de la República de Guatemala se protege la información generada por cada persona, dentro del ámbito de la comunicación. La inviolabilidad es reconocida en el artículo 24, el cual estipula: “Inviolabilidad de correspondencia, documentos y libros. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna”.

La importancia de la información estriba en la capacidad de identificar y que sea identificable. El titular de esta es quien decide su destino final. Dentro del conjunto de datos que conforman la información, hay determinados aspectos de la vida que, si bien pueden mencionarse o se confían a cierta persona o entidad, no se pretende que el contenido de esa información llegue a un público masivo y desconocido, ya que estos “también describen aspectos más sensibles o delicados sobre el individuo, como son los datos personales sensibles que tiene que ver con la forma de pensar, estado de salud, características físicas, ideología o vida sexual, entre otros.”[57]

En el plano constitucional, únicamente se protege la información que pueda ser vulnerada en un ámbito de comunicación, pero no garantiza la protección de los datos que sean obtenidos por bases de datos privadas, las cuales utilizan esa información con propósitos mercantiles.

---

[56] *Ley de Bancos y Grupos Financieros*. Congreso de la República de Guatemala.Decreto 19-2002. Pág. 25

[57] Juárez, Rosa M et al. *Investigación sobre la Ley de Acceso a la Información Pública y Protección de Datos*. Disponible en http://www.redipd.org/actividades/talleres/La_Antigua_02_2014/common/Ponencias_Taller_La_Antigua./Guatemala.pdf. Consultado el 20 de febrero de 2016.

La Constitución Política de la República reconoce el Habeas Data en el artículo 31.

Pero esta garantía solo se refiere a archivos y registros estatales. Únicamente sobre esa información recae la autodeterminación informática del titular. Esta circunstancia es limitada frente a la amplitud que generalmente abarca el *Habeas Data* en otros países. Dicha afirmación puede corroborarse con la reciente publicación (2015) de la Agencia Española de Protección de Datos.[58]

En la Ley de Acceso a la Información Pública, Decreto número 57-2008, se coadyuva en la transparencia informativa. El ciudadano puede verificar la información que acopian todas las entidades estatales. Este cuerpo normativo cumple con su finalidad, pero se requiere distinguir los propósitos de cada conjunto preceptivo, o bien, identificar su primacía en lo que respecta al contenido normativo. Con esta ley se pretende transparentar las actividades ligadas a la información en poder del Estado, pero no así la protección de los datos.

El artículo 9, numeral 4, de la citada Ley de Acceso a la Información Pública, proporciona una definición de habeas data como: la garantía de toda persona a tener conocimiento sobre qué información de ella está en poder de las entidades gubernamentales y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización.

Los ciudadanos también cuentan con la autodeterminación informática sobre las bases de datos estatales, ya que pueden conocer, modificar o eliminar la información. Esto no se debe a la ley citada, sino por disposición del artículo 24 de la *Constitución Política de la República*.

La finalidad del habeas data es “proteger ampliamente al individuo contra la invasión de su intimidad, su privacidad y honor; conocer, rectificar, suprimir y

[58] López, Carballo et al. *Protección de datos y habeas data: una visión desde Iberoamérica. XVIII*. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Proteccion_de_datos_y_habeas_data.pdf. Consultado el 22 de febrero de 2016.

prohibir la divulgación de determinados datos, especialmente los sensibles, evitando así calificaciones discriminatorias o erróneas que puedan perjudicarlo[59]".

Es un derecho denominado de tercera generación. Y básicamente protege al individuo de información personal privada, registrada en bases de datos públicas o privadas, en cuanto a proteger su divulgación, actualización y tiempo de registro en sistemas informáticos.

La garantía del habeas data es el derecho que asiste a toda persona, identificada o identificable, a solicitar la exhibición de los registros, públicos o privados, en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimientos de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos, o que impliquen discriminación, por ejemplo, afiliación a un partido político, creencia religiosa, etcétera. [60]

1.7.9.1 Tipos De Habeas Data

Los diversos tipos de habeas data surgen de acuerdo con el objetivo que mediante la acción, se persigue. Así se distinguen:

a.) **Habeas Data informativo**: es el que tiene por objeto acceder a la información que se tiene sobre un determinado banco de datos. Pueden distinguirse tres subtipos:

1) Exhibitorio. Su finalidad es observar cuáles son los datos registrados o, dicho de otra forma que se registró.

2) Finalista. Responde a la pregunta para qué se registró.

3) Autoral. Su objeto es saber quién obtuvo los datos registrados.

---

[59] Flores D. Rubén. *Amparo, Habeas Corpus y Habeas Data*. IBDF. Montevideo. 2004. Pág. 70
[60] Ibídem. Pág. 69

b.) **Habeas Data de actualización**: Este actualiza o agrega un dato a un banco donde aquel no consta.

c.) **Habeas Data Rectificador**: Tiene por objeto corregir una información errónea.

d.) **Habeas Data Asegurativo**: asegura que determinados datos no sean divulgados.

e.) **Habeas Data de Exclusión**: es el que tiene por finalidad excluir determinados datos sensibles de un registro.[61]

1.7.10 Ley para el reconocimiento de las Comunicaciones y Firmas Electrónicas

Se cuenta con la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto número 47-2008. En esta normativa se regula la validez de los datos, rigiéndose por el "principio de no repudio". Sitúa en condiciones de igualdad los datos obtenidos por un medio electrónico con los conseguidos por un medio tradicional como es el papel. Al abordar la Seguridad de la Información el enfoque es distinto en el comercio electrónico, la firma electrónica y las comunicaciones. Por un lado, los datos e información de los contratantes, legalmente, deben ser visibles y estar disponibles para su consulta, con la advertencia de que solo las partes contratantes y el tercero de confianza tienen la potestad de acceder a esa información.

La emisión de esta ley también obliga a emitir una normativa específica para prevenir, sancionar y erradicar los delitos de naturaleza informática que pudieran afectar el objeto o materia de la legislación sobre comercio electrónico, y también todos los actos ilícitos de naturaleza informática.

---

[61] Sagues, Néstor Pedro. *El Habeas Data en Argentina*. Ius Et Praxis. Buenos Aires. 1997. Pag. 8

1.7.11 Ley de Derecho de Autor, Decreto No. 33-98

La propiedad intelectual es la forma en la que el Estado protege la fuerza creadora e innovadora de sus ciudadanos. El artículo 15 define qué es una obra: "todas las producciones en el campo literario, científico y artístico, cualquiera que sea el modo o forma de expresión siempre que constituyan una creación intelectual original.

Define derecho de autor como aquello por la cual nadie puede comercializar una obra o distribuirla sin el consentimiento del autor de esta.

Es la única ley que habla de derechos sobre programas informáticos y bases de datos, dando al autor los derechos de comercialización de estos, protegiéndolo de copias piratas y cualquier otra forma de comercialización ilícita sin su consentimiento. Para ello, el artículo 44 declara que será un plazo de protección de 75 años, contados a partir de la primera publicación.

En apoyo a esta ley se agregó el artículo 274 al código procesal penal, según el cual la alteración, robo y eliminación de información, así como la piratería, son sancionados con severas penas en prisión.

1.7.12 Iniciativas de Leyes contra el Ciberdelito en Guatemala

Se presentan a continuación las iniciativas de ley contra el ciberdelito en Guatemala. Se considera sumamente importante el conocimiento del contenido y su análisis en el marco de elaborar una propuesta integral de combate de las amenazas a que está expuesto el país en materia cibernética.

1.7.12.1 Iniciativa de Ley 4055 contra el Cibercrimen en Guatemala (2009)

En Guatemala no existe una ley de tipificación del Cibercrimen y actividades informáticas ilícitas; la primera iniciativa de ley es la 4055[62]. El Congreso de la

[62] https://congresovisible.com/wp-content/uploads/iniciativa-4055-ley-de-delitos-informticos.pdf. Consultado el 26 de enero 2020

República ha dejado de lado un aspecto fundamental para comenzar a construir un ciberespacio seguro, como lo es la tipificación de los delitos informáticos. La iniciativa 4055 toma como base el Convenio de Budapest de la Unión Europea, aunque permite que se adhieran países de todo el mundo.

La iniciativa en mención pretende establecer normas especiales que sean suficientes para prevenir y sancionar las conductas de cibercrimen que no tienen fronteras, ni poseen lenguaje específico, y que se realizan en un espacio virtual o ciberespacio. Con el contenido de dicha iniciativa se pretende brindar protección integral a la información de las personas que se almacena, opera o transmite por medio de sistemas que utilizan tecnologías de la información, así como la prevención y sanción de los delitos cometidos contra o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas físicas o jurídicas. Dicha normativa será de aplicación general y regirá en todo el territorio nacional y en cualesquiera de los lugares establecidos en el contenido de esta.[63]

La iniciativa de ley 4055 tipifica como delitos informáticos los siguientes:

Delitos contra la confidencialidad, integridad y disponibilidad de datos y tecnologías de la información: acceso ilícito, daño informático, reproducción de dispositivos de acceso, espionaje informático, violación a la disponibilidad, Interceptación ilícita, falsificación informática, delitos contra la persona; delitos de pornografía infantil, control de acceso a pornografía infantil, difusión y alteración de imágenes personales, uso de identidad ajena; delitos contra la nación y actos de terrorismo, sabotaje, espionaje o robo de información, actos de terrorismo informático.

[63] www.csirt.gt. Consultado el 4 de abril de 2019

1.7.12.2 Iniciativa de Ley 5254 contra el Cibercrimen en Guatemala (2016)

A finales del año 2016, Guatemala fue invitada por el consejo de Europa a asistir a la conferencia Octupus 2016, cooperación contra el cibercrimen efectuada en Estrasburgo, Francia[64]. Se expuso la alianza del Gobierno de Guatemala con la OEA en la redacción del primer borrador de la estrategia nacional contra el cibercrimen. Una de las lecciones aprendidas durante dicha conferencia fue, que sin legislación contra el cibercrimen, es imposible combatirlo. Es necesario un modelo nacional de ciberseguridad que esté orientado a prevenir las principales formas de ataque como las de denegación de servicio, ramsomware o robo de datos.

Fue en la sede del consejo de Europa que al Sr. Alexander Seger, secretario de la convención de delitos cibernéticos se le formuló la invitación para que el consejo de Europa asistiera técnica y jurídicamente a Guatemala para elaborar una propuesta de ley contra el Cibercrimen apegada al convenio de Budapest, por medio de una visita de apoyo técnico a Guatemala.

El 20 de abril de 2016, mediante oficio No. DM-518-16-FMRL-WGF/fdl, el Ministro de Gobernación presentó la solicitud de “oficializar por medio de la cancillería el oficio dirigido al Sr. Alexander Seger secretario de la convención de delitos cibernéticos, el cual tiene el propósito de expresar el deseo de nuestro país de ser parte de la Convención de Delitos Cibernéticos del consejo de Europa (ETS 185), así como solicitar el apoyo para poder cumplir los requerimientos necesarios para poder acceder a este convenio, así mismo (sic) la invitación de una misión de asistencia técnica para desarrollar una Estrategia Nacional de Ciberseguridad, la cual será liderada por el Programa de Seguridad Cibernética del Comité

[64] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/octopus-2016-cooperation-against-cybercrime. Consultado el 18 de enero 2018

Interamericano contra el terrorismo CICTE de la Organización de los Estados Americanos (OEA)".[65] (Ver Anexo 3. Imagen 1*).*

El resultado de esta visita fue que en el mes de febrero del año 2017 se elaboró lo que se denominó el "borrador cero" (draft cero) de una propuesta de ley contra el cibercrimen en Guatemala. Esto se logró gracias a la visita al país de una comisión del consejo de Europa, los expertos Manuel de Almeida Pereira, Pedro Verdelho, procurador del Ministerio Público y jefe del comité contra el cibercrimen en Portugal; de parte de la OEA, Belisario Contreras, Bárbara Marchiori y del departamento de justicia de los Estados Unidos el asesor del fiscal general Rudy Orjales.

Se obtuvo como resultado la redacción de un documento alineado al convenio de Budapest, en formato de ley para Guatemala. El documento también se encuentra dentro del contexto del Plan Glacy + del Consejo de Europa, y consiste en suministrar apoyo tecnológico y técnico a países que necesitan ayuda en el combate contra el cibercrimen. Por medio de capacitaciones, congresos, una plataforma de cooperación y asistencia técnica, Glacy + logra que sus miembros se mantengan vigentes en el combate del cibercrimen.

Lamentablemente Guatemala, en la fecha que se redacta el presente trabajo de investigación, aún no cuenta con legislación contra el ciberdelito, lo que hace imposible que el país forme parte del convenio de Budapest y de Glacy +.

Se puede consultar en la página del Ministerio de Gobernación [66]. El documento consta de 23 páginas y es el resultado de muchas horas de discusión y consenso con el Convenio de Budapest como marco. Las instituciones que estuvieron en la creación del borrador cero de este proyecto de ley contra la ciberdelincuencia en Guatemala fueron: Ministerio Público, Ministerio de la Defensa,

---

[65] Ministerio de Gobernación. oficio No. DM-518-16-FMRL-WGF/fdl. Despacho Superior. 20 de abril 2016.

[66] http://seguridadcibernetica.mingob.gob.gt/wp-content/uploads/2016/09/Cybercrime-Law-Guatemala-Draft-Zero_FINAL.pdf. Consultado el 25 de enero del 2018

Ministerio de Gobernación, Secretaría Técnica del Consejo Nacional de Seguridad, Superintendencia de Administración Tributaria, Congreso de la República, universidades, entre otras. (*Ver Anexo 3. Imagen 2)*

El borrador elaborado con el apoyo, tanto de instituciones de peso en Guatemala, como de los rectores mundiales, del tema El Comité contra el Terrorismo de la OEA y el Consejo de Europa, fue adoptado por el Congreso de la República para ser presentado como una propuesta de ley, que luego sería la Iniciativa de Ley 5254, que reza: "Se somete a consideración del Honorable Pleno del Congreso de la República, la iniciativa de ley contra la ciberdelincuencia la cual proviene de una revisión minuciosa y detallada, a través de un estudio de antecedentes y la discusión con Ministerio de Gobernación, Consejo de Europa en virtud de haberse utilizado como referencia el convenio contra la ciberdelincuencia suscrito en Budapest, del cual Guatemala deberá en un futuro adherirse.

La iniciativa desarrolla normas necesarias para que el país se ponga al día en cuanto a lo que en el orbe se ha discutido desde hace más de 15 años entorno a la ciberdelincuencia y la necesidad de que los Estados hagan un frente común para poder proteger por medio de cooperación internacional, además de contar con normas penales y de Derecho Procesal para la persecución de este tipo de delitos."[67]

De manera que el borrador cero elaborado se convirtió en la iniciativa de Ley 5254, una iniciativa actualizada y que responde a los estándares internacionales requeridos en materia jurídica para al combate al cibercrimen.

En la exposición de motivos de la iniciativa contra la Ciberdelincuencia se lee: "*La tipificación actual de los delitos informáticos contenidos en el Código Penal, no responde a las modalidades de los ilícitos que se cometen a través de redes o sistemas informáticos*, muchos de ellos ya reconocidos en la legislación

[67] https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/Registro5254.pdf. consultado el 25 de enero de 2018

internacional como por ejemplo la interceptación ilícita, el abuso de los dispositivos, el fraude o estafa informática e incluso la pornografía infantil, por la utilización de medios informáticos para su comisión; además de que deben adecuarse al Convenio sobre la Ciberdelincuencia de Budapest suscrito en Europa en el año 2,001, al cual Guatemala debiera adherirse y ratificar para poder lograr la cooperación entre los países y así contribuir a la lucha por la persecución penal de los delitos informáticos a nivel global."[68]

El país tiene una referencia de calidad internacional en cuanto a legislación contra el cibercrimen.[69]

1.7.12.3 Iniciativa de Ley Prevención y Protección Contra la Ciberdelincuencia 5601 (2019)

En agosto de 2019, la bancada TODOS presentó una iniciativa de Ley en contra de la ciberdelincuencia. Esta propuesta se elaboró tomando como base la iniciativa de ley 5254, como se menciona en el comunicado oficial: "que dio seguimiento a la propuesta que fue socializada y analizada por distintos sectores. Autoridades del Ministerio de Gobernación, miembros del Consejo de la Carrera Judicial, Organismos Internacionales y expertos en el tema emitieron sus opiniones, las cuales fueron tomadas en cuenta al integrar la iniciativa."[70]

Los delitos que se incorporan al código penal guatemalteco son: "Acceso ilícito, Interceptación Ilícita, Ataque a la integridad de los datos, Ataque a la integridad del sistema; regula delitos considerados dentro de los delitos propiamente denominados informáticos siendo éstos: Falsificación informática, Apropiación de Identidad ajena; Abuso de Dispositivos, Fraude Informático. También se incorpora el Delito de acoso cibernético y engaño pederasta."[71] Es la

---

[68] ídem
[69] https://www.prensalibre.com/guatemala/justicia/gobernacion-elaborara-ley-para-combatir-el-cibercrimen/
[70] https://todos.gt/todos-presenta-iniciativa-contra-la-ciberdelincuencia/. Consultado el 20/01/2020
[71] *Iniciativa de ley 5601*. Congreso de la República Guatemala. 2019. Bancada Todos. Consultado en: https://www.congreso.gob.gt/assets/uploads/info_legislativo/iniciativas/748df-5601.pdf

última iniciativa de ley contra el ciberdelito presentada al Congreso de la República en el período de redacción del presente trabajo de investigación.

1.7.12.4 Ataque Sistemático a las propuestas de Ley contra la Ciberdelincuencia

Los medios de comunicación han jugado un rol determinante en la no aprobación de las distintas iniciativas legislativas contra el ciberdelito. Alegando que algunos artículos violan la libre emisión del pensamiento, han sistematizado los ataques a cualquier iniciativa de este tipo. Son los mismos medios de comunicación que siempre se quejan de que, maliciosamente, "fuerzas oscuras" han atacado sus medios digitales para evitar que la población se entere de alguna noticia importante. Cómo pueden esperar que los protejan de los supuestos ataques a sus servidores, si no existe el marco jurídico que ellos mismos se encargan de atacar.

Seguidamente, se citan algunos ejemplos de ataques hacia determinadas iniciativas de ley:

El 18 de septiembre de 2019, la periodista Carmina Valdizan se pronuncia así: "¿vuelve la burra al trigo? Por tercer año consecutivo y por tercera vez estoy escribiendo sobre un nuevo proyecto de ley de ciberseguridad y ciberdelincuencia"[72]. La periodista menciona que el fin último de esa iniciativa es la creación de un CSIRT que, por sus siglas inglés, es un Grupo de respuesta ante emergencias cibernéticas, lo cual no es cierto. Es uno de sus objetivos. El CSIRT es un grupo técnico que atendería cualquier emergencia cibernética ya sea público o privado. Los "güizaches", como ella llama a quienes hicieron esta propuesta, fueron expertos del consejo de Europa, de la Organización de Estados Americanos y de la oficina del fiscal general de los Estados Unidos, quienes, por invitación oficial del gobierno de Guatemala, redactaron el borrador cero de la iniciativa de ley contra el ciberdelito 5254, de la cual nace la iniciativa 5601.[73] Ella basó su ataque en el

[72] https://elsiglo.com.gt/2019/09/18/corre-y-va-de-nuevo-iniciativa-5601-de-ciberseguridad/ Consultado el: 20/12/2019

contenido del artículo 19, mencionando que no está claro el término acoso. En su arremetida contra la iniciativa 5254, la periodista [74]atacó el artículo 14, porque según ella "atenta contra el hacking ético". Además del artículo 18 que habla sobre el acoso.

Por su parte Plaza Pública, bajo el título "Cinco Leyes que nos amenazan", cita a la iniciativa de ley 5254 como una iniciativa de ley "antisocial", la cual, según expertos de derecho internacional, criminaliza las actividades de los usuarios en las redes sociales y dificulta la defensa de los derechos humanos. [75]

Sobre esto, Mercedes Fernández Antón menciona que "el público no piensa casi nunca por sí mismo, sino que es un dócil consumidor de las "ilusiones necesarias", que las elites gobernantes fabrican para él y que le son debidamente suministradas por unos "medios de comunicación" que no actúan como comunicadores de la realidad existente, convirtiéndose en meros propagandistas de los intereses dominantes"[76]

Nos vemos ante el escenario que menciona Jean-Jacques Rousseau en su célebre obra El Contrato Social: "Siempre se quiere el bien, pero no siempre se le ve, nunca se corrompe al pueblo, pero a menudo se le engaña y tan solo entonces parece querer lo malo"[77]. Rousseau establece la diferencia entre la voluntad de todos y la voluntad general. La voluntad de todos es la voluntad de unos cuantos que tratan de influir en la voluntad general del pueblo. Este autor advierte de la manipulación de la voluntad del pueblo cuando dice "pero cuando se desarrollan intrigas y se forman asociaciones parciales (…) entonces no hay más voluntad general, y la opinión que domina no es sino una opinión particular"[78]

---

[74] https://elsiglo.com.gt/2017/09/15/ley-bozal-ciberdelincuencia/. Consultado el 20/12/2019
[75] https://www.plazapublica.com.gt/content/cinco-leyes-que-nos-amenazan. Consultado el 17 de octubre 2019
[76] Antón, Mercedes. *Control de Pensamiento en las Sociedades*. https://dialnet.unirioja.es/descarga/articulo/5073061.pdf. Consultado el 17 de octubre 2019.
[77] Rousseau, Jean-Jacques*. El Contrato Social*. Plutón Ediciones. Barcelona. 2014. Pág. 60
[78] Ibídem. Pág. 61

Citando el ejemplo de Grocio y su traductor Barbeyrac, y la forma como habían retorcido su propio libro para quedar bien tanto con el rey Luis XIII como con Guillermo, rey de Inglaterra, respectivamente, Rousseau llega a la conclusión "Si estos dos escritores hubieran adoptado los verdaderos principios, todas las dificultades hubieran desaparecido". Y hace una sabia reflexión que, sin decirlo explícitamente, lleva al lector a concluir acerca de los motivos de escribir para grupos de poder: "ahora bien la verdad no conduce a la riqueza, y el pueblo no da embajadas, ni cátedras, ni pensiones".[79]

1.8 Marco Jurídico Internacional

Con relación a la seguridad de la información y el fortalecimiento institucional para brindar a los ciudadanos un ciberespacio seguro, Guatemala se ha adherido a diversos convenios, tratados y estatutos, los cuales pueden apoyar al país para fortalecer su sistema jurídico propio y lograr así el cometido, o sea, la construcción de un ciberespacio seguro.

1.8.1 Declaración Universal de los Derechos Humanos

La asamblea general de las Naciones Unidas, adoptó en diciembre de 1948 la Declaración Universal de los Derechos Humanos de la cual Guatemala es signatario. En su artículo 12 estipula: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley ante tales injerencias".

En su artículo 19 dice: "Nadie podrá ser molestado a causa de sus opiniones, toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideraciones ni fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".

[79] Ibídem. Pág. 60

Esta debe ser la base sobre la cual se elabore y aplique cualquier marco jurídico, institucionalidad y la aplicación de herramientas tecnológicas para construir un ciberespacio seguro.

1.8.2 Convención Americana sobre Derechos Humanos, pacto de San José (1978)

La Organización de las Naciones Unidas (OEA) hace oficial la puesta en vigor de la llamada Convención Americana de Derechos Humanos o Pacto de San José. En este pacto, los países signatarios, entre ellos Guatemala, se comprometen a que las leyes, instituciones y políticas de país velen por la garantía de derechos humanos, pronunciándose así: "la garantía de derechos de los seres humanos se basa en el establecimiento de condiciones básicas necesarias para su sustentación (alimentación, salud, libertad de organización, de participación política entre otros"[80].

Esta es la base sobre la cual debe funcionar el modelo de ciberseguridad para Guatemala. Cualquier iniciativa de ley, ya sea contra el ciberdelito, protección de la información, o protección a infraestructuras críticas, debe respetar y estar orientada acerca del respeto a los derechos humanos. Y no es solo un asunto moral, pues, al ser signatario Guatemala del Pacto de San José, es obligatorio su cumplimiento. Los artículos que se consideran relevantes para la construcción de un ciberespacio seguro son los siguientes:

"Artículo 1. Obligación de Respetar los Derechos

1) Los estados Parte en esta convención se comprometen a respetar los derechos y libertadas reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, opiniones políticas

[80] *Convención Americana sobre Derechos Humanos.* OEA. 1978. Pág. 1. Consultado en: https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf. El 18 de enero 2020.

o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social.

Artículo 2. Deber de adoptar disposiciones de derecho interno

Si el ejercicio de los derechos y libertadas mencionados en el artículo 1 no estuviere ya garantizado por disposiciones legislativas o de otro carácter, los estados parte se comprometen a adoptar, con arreglo a sus procedimientos constitucionales y a las disposiciones de esta convención, legislativas o de otro carácter que fueran necesarias para hacer efectivos tales derechos y libertades.

Artículo 5. Derecho a la integridad personal

1) Toda persona tiene derecho a que se respete su integridad física, psíquica y moral.

Artículo 11. Protección de la Honra y de la dignidad

2) Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

3) Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

4) Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Artículo 14. Derecho de Rectificación o respuesta

1) Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a

efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley".[81]

1.8.3 Declaración sobre seguridad en las Américas (2003)

Guatemala fue signatario de la declaración sobre seguridad en las Américas aprobada en la tercera sesión plenaria, celebrada el 28 de octubre de 2003 en ciudad de México. En ella se menciona: "Reconociendo que los Estados del hemisferio enfrentamos tanto amenazas tradicionales a la seguridad como nuevas amenazas, preocupaciones y otros desafíos que por sus características complejas han determinado que la seguridad tenga un carácter multidimensional"[82].

En esa declaración Guatemala se comprometió, manifestando: "Desarrollaremos una cultura de seguridad cibernética en las Américas adoptando medidas de prevención eficaces para prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas y la delincuencia cibernéticas, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas. Reafirmamos nuestro compromiso de desarrollar e implementar una estrategia integral de la OEA sobre seguridad cibernética, utilizando las contribuciones y recomendaciones elaboradas - 10 - conjuntamente por los expertos de los Estados Miembros y por el Grupo de Expertos Gubernamentales de la REMJA en Materia de Delito Cibernético, el CICTE, la Comisión Interamericana de Telecomunicaciones (CITEL) y otros órganos apropiados, teniendo en cuenta el trabajo que desarrollan los Estados Miembros coordinado con la Comisión de Seguridad Hemisférica."[83]

---

[81] Ídem
[82] *Declaración sobre seguridad de las Américas*. OEA. México. 2003. Consultado en: http://www.oas.org/36AG/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf. Consultado el 25 /01/2020
[83] Ibídem. Pág. 9

1.8.4 Declaración de Panamá sobre "La Protección de la Infraestructura Crítica en el hemisferio frente al Terrorismo" (2007)

El séptimo período ordinario de sesiones de la Organización de los Estados Americanos se celebró del 28 de febrero al 2 de marzo de 2007. Con excepción de Venezuela, todos los países miembros de la OEA, incluyendo Guatemala, firmaron la Declaración de Panamá sobre la Protección de la Infraestructura Crítica en el hemisferio frente al Terrorismo.

En ella, los países firmantes declaran: "3. Que la infraestructura crítica consiste, entre otras, en aquellas instalaciones, sistemas, y redes, así como servicios y equipos físicos y de tecnología de la información cuya inhabilitación o destrucción tendría un impacto negativo sobre la población, la salud pública, la seguridad, la actividad económica, el medio ambiente, la gobernabilidad democrática, o el eficaz funcionamiento del gobierno de un estado miembro.

4. La importancia de que los Estados miembros identifiquen su infraestructura crítica, así como los riesgos y amenazas que el terrorismo representa para ésta, de acuerdo con su ordenamiento jurídico interno y prioridades nacionales.

9. Su compromiso de cumplir y continuar cumpliendo con las normas internacionales relacionadas con la protección de la infraestructura crítica.

10. La necesidad de alentar a los Estados Miembros a estrechar vínculos con el sector privado y la sociedad civil, cuando corresponda, en sus respectivos países, para desarrollar programas de fomento de la capacidad preventiva y de protección contra las amenazas a la infraestructura crítica.

11. Se encomienda a la secretaría del CICTE a que promueva en los estados miembros actividades de educación y capacitación para crear una cultura pública de reconocimiento de la infraestructura crítica a fin de sensibilizar a la sociedad civil.

12. Su apoyo a los esfuerzos que realiza la secretaría del CICTE para colaborar y coordinar con los órganos, organismos, y entidades pertinentes de la

OEA, así como con las organizaciones subregionales e internacionales capaces de contribuir en materia de protección de la infraestructura crítica contra actos de terrorismo".[84]

1.8.5 Estrategia Interamericana Integral de Seguridad Cibernética (2011)

En 2001, en el marco de la Tercera Cumbre de las Américas celebrada en Quebec, Canadá, los estados miembros de la Organización de los Estados Americanos, incluyendo Guatemala, se comprometieron a establecer una estrategia interamericana integral de seguridad cibernética, la cual abarcaba temas como el fomento de la cultura de seguridad cibernética, identificar y evaluar normas técnicas y, prácticas para dar certeza a la seguridad de la información transmitida por internet y otras redes de comunicaciones, proporcionar información a los usuarios y operadores para ayudarles a asegurar sus computadores y redes contra amenazas y vulnerabilidades, a responder ante incidentes y a recuperarse de los mismos.

Además, promover 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. Se fomenten asociaciones públicas y privadas con el objetivo de incrementar la educación y la concientización de la seguridad cibernética. *Se trabaje con el sector privado, el cual posee y opera la mayoría de las infraestructuras de información de las que dependen las naciones para asegurar esas infraestructuras*.

La estrategia interamericana dice: "Lamentablemente, la Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de Internet. La información que transita por Internet puede ser malversada y manipulada para invadir la privacidad de los usuarios y estafar a los negocios. La destrucción de los datos que residen en las computadoras conectadas

[84] http://www.informaticalegal.com.ar/2007/03/02/declaracion-de-panama-sobre-la-proteccion-de-la-infraestructura-critica-en-el-hemisferio-frente-al-terrorismo/. Consultado el 25/01/2020

por Internet puede obstaculizar las funciones del gobierno e interrumpir el servicio público de telecomunicaciones y otras infraestructuras críticas."[85]

La estrategia interamericana de ciberseguridad es una lista de buenos deseos en los cuales los gobiernos de Latinoamérica se comprometieron a fortalecer la ciberseguridad, algo que nunca han volteado a ver y todo indica que no lo harán en el corto ni mediano plazo.

1.8.6 Declaración de protección de infraestructura crítica ante las amenazas emergentes (2015)

Durante la quinta sesión plenaria celebrada en Washington DC, Estados Unidos, el 20 de marzo de 2015, los Estados miembros del comité interamericano contra el terrorismo (CICTE) de la OEA, entre ellos Guatemala suscribió la declaración de protección de infraestructuras críticas, que reza: "Teniendo en cuenta que la infraestructura crítica consiste, entre otras, en aquellas instalaciones, sistemas y redes, así como servicios y equipos físicos y de tecnología de la información, cuya inhabilitación o destrucción tendría un impacto negativo sobre la población, la salud pública, la seguridad, la actividad económica, el medio ambiente, servicios de gobierno, o el eficaz funcionamiento de un Estado miembro y que cualquier interrupción de estos causada por actos terroristas tendría graves consecuencias para los flujos de servicios esenciales y el funcionamiento de las cadenas de suministros.

Subrayando que la protección de las infraestructuras críticas contra ataques terroristas y otras amenazas emergentes, tales como el uso del Internet para fines terroristas, entre otros, así como su normal funcionamiento, son una preocupación de los Estados Miembros; que llama a la implementación de programas de seguridad, que incluyan la resiliencia de la infraestructura crítica basada en análisis de riesgos desarrollados en cooperación con las partes interesadas, por medio del

[85] *Una estrategia interamericana integral de seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética*. OEA. 2014. Consultado en: http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf

intercambio de buenas prácticas y experiencias, a efectos de garantizar la seguridad de las mismas; todo lo cual constituye una responsabilidad compartida de actores públicos y privados y hace necesario la concienciación, cooperación y colaboración entre los mismos".[86]

Guatemala está comprometida a luchar por un ciberespacio seguro y a proteger sus infraestructuras críticas en aras de la seguridad nacional e internacional.

1.8.7 Asamblea Mundial de Normalización de las Telecomunicaciones (2016)

Como Estado miembro de las Naciones Unidas, Guatemala suscribió la resolución 50 sobre ciberseguridad el 03 de noviembre de 2016. Entre los considerandos menciona "que la seguridad es una cuestión intersectorial y que el panorama de la ciberseguridad es complejo y diverso, en el que intervienen distintos actores en los planos nacional, regional y mundial, que son responsables de identificar, examinar y reaccionar a las cuestiones relacionadas con la creación de confianza y seguridad en la utilización de las TIC; f) que las pérdidas considerables y crecientes en que han incurrido los usuarios de sistemas de telecomunicaciones/TIC, a consecuencia del problema cada vez mayor de la ciberseguridad, alarman a todos los países desarrollados y en desarrollo sin excepción; g) que debido, entre otras cosas, a que las infraestructuras esenciales de telecomunicaciones/TIC están interconectadas a escala mundial, la seguridad insuficiente de la infraestructura de un país podría aumentar la vulnerabilidad y el riesgo en otros países, por lo que la cooperación es importante; h) que el número y métodos de ciberataques y los ciberataques están aumentando, del mismo modo

[86] *Declaración Protección de Infraestructura Critica ante las amenazas emergentes*. OEA. 2015. Pág. 5. Consultado en: https://www.sites.oas.org/cyber/Documents/CICTE%20DOC%201%20DECLARACION%20CICTE00955S04.pdf

que la dependencia de Internet y otras redes que son necesarias para acceder a servicios e información"[87].

Entre las obligaciones asumidas por Guatemala como signatario de esta resolución se encuentran: a) colaborar estrechamente en el fortalecimiento de la cooperación regional e internacional…con el fin de mejorar la confianza y seguridad en la utilización de las TIC y mitigar los riesgos y las amenazas; b) cooperar y participar activamente en la aplicación de la presente Resolución y de las medidas asociadas; c) que trabajen en actividades pertinentes de Comisiones de Estudio del UIT-T para desarrollar normas y directrices de ciberseguridad a fin de crear confianza y seguridad en la utilización de las TIC".[88]

1.9 Marco Jurídico en el Modelo de Ciberseguridad Nacional

Un país que no tenga un marco jurídico para el combate del ciberdelito está condenado a convertirse en un paraíso de delitos en su ciberespacio. Y no únicamente en contra de sus infraestructuras críticas. También puede ser un paraíso para que utilicen la infraestructura informática con fines de atacar a otros países. Fácilmente nos convertiremos en puente de los ciberataques hacia terceros. Eso nos colocará en muy mala posición en nuestras relaciones internacionales. La información que el Estado tiene la obligación constitucional de proteger será una tarea imposible.

Los servicios que prestan las infraestructuras tales como telecomunicaciones, banca, energía eléctrica, están tan vulnerables que ante cualquier ataque pueden colapsar. No habrá un centro de emergencias de respuesta ante eventos cibernéticos; por lo tanto, se hace imposible la coordinación interinstitucional para hacer frente a ciberataques presentes y futuros. Nunca se podrá hablar de justicia veraz y objetiva sin procedimientos y métodos científicos aplicados a la informática

---

[87] *Asamblea Mundial de Normalización de las Telecomunicaciones*. UIT. 2016. Pág. 4 Consultado en: https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2016-PDF-S.pdf. Consultado el 26/01/2020

[88] Ibídem. Pág. 6

forense. Y la economía del país está en la balanza, pues se podría ver afectada enormemente, como ha ocurrido en otros países que han sido víctimas de la paralización económica al estar bajo ataque su infraestructura de bolsa de valores y banca.

La OEA es clara al decir “Si no cuentan con leyes y reglamentos adecuados, los Estados Miembros no pueden proteger a sus ciudadanos de los delitos cibernéticos. Además, los Estados miembros que carecen de leyes y mecanismos de cooperación internacional en materia de delito cibernético corren el riesgo de convertirse en refugios para los delincuentes que cometen estos delitos”.[89]

Considerando que la legislación es la base para formular un modelo de ciberseguridad, se estima que la legislación mínima necesaria para el combate al cibercrimen es: a) Ley contra el ciberdelito, b) Ley de Protección de la Información y c) Ley de Protección de las Infraestructuras Críticas. Esta triada de leyes, como se explicará en el capítulo tres, formará parte de un modelo integral de país para el combate del cibercrimen y la protección a las infraestructuras críticas de este.

[89] http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf. Consultado el 20/01/2020

CAPÍTULO DOS

2. Infraestructuras Críticas

En el presente capítulo luego de la definición, se pretende presentar la propuesta de un catálogo de infraestructuras críticas para Guatemala, dada la importancia de su protección para la seguridad nacional. Ello, además de exponer los riesgos sociales, económicos y tecnológicos a que está expuesta la seguridad nacional ante un ataque cibernético.

2.1 Definición de Infraestructura Crítica

La Legislación española define la Infraestructura crítica como "las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales".[90]

Peter Burnett, coordinador del proyecto Meridian, uno de los más importantes en ciberseguridad, describe cuáles son las infraestructuras críticas así: "Estos incluyen sistemas que controlan las defensas contra inundaciones, las represas, las instalaciones de generación de electricidad, los oleoductos, los controles de plantas químicas y muchos otros componentes de la infraestructura crítica. Antes de este siglo, eran controles manuales, o eran controlados por hardware y software especiales oscuros y que solo algunos ingenieros y especialistas entendían".[91]

Por su parte, la cámara de comercio internacional, organización que brinda seguridad a empresas en todo el mundo, señala que: "El término Infraestructura Crítica es empleado por los Estados para definir instalaciones y los sistemas sobre

---

[90] *Ley de Protección de Infraestructura Crítica*. 2011. BOE-A-2011-7630.Gobierno de España. Disponible en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf. Consultado el 14 de julio 2018

[91] *Reporte de Seguridad Cibernética y Protección de la Infraestructura Crítica*. OEA- Trend Micro. 2015. Pág. 17. Disponible en: https://cutt.ly/AtYpNwU. Consultado el 14 de julio 2018

los que recaen servicios esenciales cuyo funcionamiento no permite soluciones alternativas. Las infraestructuras críticas existentes en un estado se agrupan dentro de sectores estratégicos: aquellos que son esenciales para la seguridad nacional o para un conjunto de la economía de un país (defensa, energía, aeroespacial, nuclear, administración, financiero, etc.”.[92]

De manera que se consideran infraestructura crítica aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión considerable en la salud, la seguridad o el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de los gobiernos. [93]

2.2 Importancia para los países de proteger la infraestructura Crítica

Eric Schmidt, presidente de Google, en el libro El Futuro Digital anota: “Los Estados se harán cosas online los unos a los otros que podrían ser demasiado provocativas en el mundo real, lo que permite que los conflictos se desarrollen en un campo de batalla virtual mientras todo lo demás permanece en calma”.[94] Esto ha cobrado relevancia en una sociedad en la cual las infraestructuras críticas están controladas, cada vez más, por sistemas informáticos, lo que permite ataques Estado-Estado bajo el anonimato casi completo y de los cuales únicamente quedan sospechas de quien fue el autor. Recientemente se atribuyen a los Estados Unidos los ataques a las generadoras eléctricas de Venezuela, como ensayo para programar ataques a las generadoras de energía eléctrica en Rusia, a lo que los medios han llamado “Guerra Fría Digital”.

---

[92] *La protección de Infraestructuras críticas y la ciberseguridad industrial*. Primera Edición octubre 2013. Centro de Ciberseguridad Industrial. Pág. 8. Disponible en: https://www.cci-es.org/documents/10694/331476/documento+PIC+y+CI.pdf/6f4f7e57-4719-4d85-ad27-7218800ca138 . Consultado el 24 de abril 2018

[93] *Plan Nacional de Protección de Infraestructuras Criticas*. Gobierno de España. 2007. Disponble en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

[94] Schmidt, Eric. *El Futuro Digital*. Ediciones Anaya Multimedia. Madrid. 2014. Pág. 142

2.3 Protección a la infraestructura Crítica en las Américas

La estrategia de seguridad cibernética adoptada por la OEA en 2004 especifica: "Desarrollaremos una cultura de seguridad cibernética en las Américas adoptando medidas de prevención eficaces para prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, luchando contra las amenazas y la delincuencia cibernéticas, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas."[95]

Lamentablemente, doce años después de firmada esta declaración por parte de la OEA y los líderes latinoamericanos, un estudio demostró que la mayoría de los países latinoamericanos ni siquiera cuenta con una Política o una Estrategia para abordar el tema de los riesgos tecnológicos en las infraestructuras críticas. Pareciera ser que nuestros líderes quieren hacerse de oídos sordos ante una realidad, a la cual solo una crisis hará que presten atención.

Es notorio que el único organismo internacional que actualmente está reconociendo e intentando que los gobiernos de la región tomen cartas en el asunto es la OEA. Para el caso de Guatemala, fue la OEA quien coadyuvó en la elaboración de la Estrategia Nacional de Ciberseguridad, cuyo inicio de formulación se dio en el año 2016. También fue a través de la OEA que Guatemala recibió apoyo del Consejo de Europa para formular el primer borrador o borrador cero de la iniciativa de ley actualizada contra el cibercrimen.

En 2004, en la misma convención firmada por líderes de toda América Latina, dicha organización continua manifestando: "Es necesario desarrollar una estrategia integral para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario. La OEA está comprometida con el desarrollo e implementación de esta estrategia de seguridad cibernética y en

---

[95] *Una estrategia interamericana integral de seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética*. OEA. 2014. Disponible en: http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf. Pág. 4. Consultado el 20 de agosto 2018

respaldo a esto, celebró una Conferencia sobre Seguridad Cibernética que demostró la gravedad de las amenazas a la seguridad cibernética para la seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, y que una acción eficaz para abordar este problema debe contar con la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales"[96].

Ni la cooperación de los Estados Unidos (USAID), ni el Banco Mundial, ni el Banco Interamericano de Desarrollo han apoyado tan activamente al país y a la región como la OEA, en materia de Ciberseguridad para la seguridad nacional.

En 2015, la firma privada de ciberseguridad Trend Micro, junto a la Organización de los Estados Americanos público el estudio "Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas", en el cual hace un análisis detallado del estado actual del avance en cuanto al uso de la tecnología en las infraestructuras de los países de Latinoamérica.

También presenta un ejemplo de cómo sería un instante de una caída de las infraestructuras críticas: "Solo imagine una interrupción prolongada de Internet que no solo privaría de su ancho de banda, sino que también detendría la estación encargada de bombear agua, el sistema que genera la electricidad, el centro de logística para distribuir materia prima a las fábricas de alimentos y supermercados, el oleoducto que lleva el combustible a las refinerías y a las gasolineras; la pesadilla sería interminable"[97]. Las consecuencias al fallar las infraestructuras críticas pueden ser fatales.

Seguidamente, se realizará un análisis respecto de la protección de infraestructuras críticas en dos países que van a la vanguardia en la región, en

[96] Ibídem. Pág. 1
[97] *Reporte de Seguridad Cibernética y Protección de la Infraestructura Crítica*. OEA- Trend Micro. 2015. Pág. 17. Disponible en: https://cutt.ly/utYi0Oq. Consultado el 14 de enero 2018

materia de legislación, políticas e institucionalidad para la ciberseguridad de sus infraestructuras críticas, Argentina, Colombia y Uruguay.

2.3.1 Protección de las Infraestructuras Críticas en Argentina

En Argentina existe el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad, con las siglas ICIC, en donde se describe como: "El Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), creado mediante la Resolución JGM No. 580/2011, tiene como finalidad impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional."[98] A través de su sitio web, el gobierno argentino ofrece alertas de seguridad informática, capacitaciones a empleados públicos y privados, recomendaciones a todos los ciudadanos sobre el uso seguro del Internet, y la posibilidad de presentar denuncias sobre posibles delitos informáticos.[99]

Es propicio, por la índole del tema de la presente tesis, enumerar detalladamente los objetivos orientados a la protección de las infraestructuras críticas que plantea el ICID:

- Fortalecer los niveles de seguridad cibernética en el Sector Público Nacional, mediante la creación de estrategias comunes para proteger la información y las infraestructuras críticas.

- Fomentar la colaboración entre los diferentes sectores de la sociedad (empresas, industrias, organizaciones de la sociedad civil, universidades, etc.), con el objetivo de adoptar un marco común de lineamientos para fortalecer los niveles de ciberseguridad e infraestructuras de información críticas de sus organizaciones.

---

[98] http://www.icic.gob.ar/ . Consultado el 7 de febrero del 2018.

[99] Ídem

- Contribuir al mejoramiento de la ciberseguridad y la infraestructura de información crítica a escala internacional.[100]

2.3.2 Protección de la Infraestructura Crítica en Colombia

Uno de los países de la región latinoamericana con mayor avance en materia de Estrategia aplicada a la seguridad de sus Telecomunicaciones y Tecnología utilizada el Gobierno para brindar servicios a la población, es Colombia. En el Documento del Consejo Nacional de Política Económica y Social 3854 denominado Política Nacional de Seguridad Digital, justifica el desarrollo de una política de esta índole, de la siguiente forma: “El creciente uso del entorno digital en Colombia para desarrollar actividades económicas y sociales, acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno.”[101]

Con una propuesta iterativa, la política nacional de seguridad digital de Colombia propone realizar un catálogo de la infraestructura crítica, el cual busca identificación y priorizar el nivel de relevancia que cada una tenga dentro de la seguridad nacional.

Este proceso repetido una y otra vez, hará que se torne más robusto al permitir la participación a más instituciones públicas y privadas.

En su política Nacional de seguridad Digital hace hincapié en el proceso a seguir para que su seguridad nacional no se vea amenazada: “Es indispensable generar una estrategia de protección de la infraestructura crítica cibernética en el país, culminando el proceso de catalogación de dicha infraestructura bajo un

[100] Ídem
[101] *Política Nacional de Seguridad Digital*. Gobierno de Colombia. 2016. Pág. 3. Disponible en: https://bibliotecadigital.ccb.org.co/handle/11520/14856

enfoque de gestión de riesgos de seguridad digital, y vinculado activamente a las múltiples partes interesadas, especialmente al sector privado."[102]

En la conceptualización del objetivo de fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos, la Política Nacional de Seguridad Digital reza: "Este objetivo específico busca desarrollar capacidades de prevención, detección, contención, respuesta, recuperación y defensa para garantizar los fines del Estado. Al mismo tiempo que busca mejorar la protección, preservar la integridad y la resiliencia de la infraestructura crítica cibernética nacional"[103]

2.3.3 Protección de la Infraestructura Crítica en Uruguay

En el caso de Uruguay, uno de los países más avanzados en cuanto a Elaboración e Implementación de estrategia digital en el mundo, su Política de Defensa Nacional establece líneas estratégicas en cuanto a la seguridad cibernética, al expresar: "En la actualidad se da en forma reiterada el espionaje por parte de empresas, Organismos o Estados extra-regionales a los gobiernos de la región, las empresas públicas, así como a empresas privadas u organismos de la sociedad civil con el fin de captar ilícitamente información para obtener ventajas económicas y el control político, miliar o social, en el plano estratégico de los países. Como correlato de la dependencia científico-tecnológica, fruto del uso de tecnologías desarrolladas bajo licencias y patentes privativas de la influencia de las redes y medios informáticos como soporte de las tecnologías; y del aumento del soporte electrónico para las bases de datos del Estado y la digitalización de la gestión estatal, se da un incremento de la vulnerabilidad ante ataques cibernéticos capaces de generar conmoción económica, política y social". [104]

---

[102] Ibídem. Pág. 46
[103] Ibídem. Pág. 60
[104] *Política de Defensa Nacional*. Republica del Uruguay. 2014. Pág. 23. Disponible en: https://www.impo.com.uy/bases/decretos-originales/105-2014. Consultado el 20 de agosto 2014

Por ello, en sus líneas estratégicas de defensa de Uruguay la Política de Defensa Nacional manda a: “Proteger al Uruguay de ataques cibernéticos y preservar la reserva de datos producto de la gestión estatal y privada, tanto a nivel nacional como regional, en cuanto esta última corresponda.” [105]

2.4 Ataques Relevantes a la Infraestructura Crítica a Nivel Mundial

En octubre de 2012, el secretario de defensa de los Estados Unidos, León Paneta, advirtió “una nación agresora podrá usar este tipo de herramientas cibernéticas para controlar conmutadores críticos. Podrían hacer descarrilar trenes de pasajeros o incluso algo más peligroso, descarrilar trenes de pasajeros cargados con productos químicos. Podrían contaminar el suministro de agua de grandes ciudades, o cortar el suministro eléctrico en grandes zonas del país”.[106]

La situación se agrava cuando Schmidt menciona la tendencia hacia la cual se dirigen los países de convertirse en estados virtuales, en los cuales los ciudadanos utilizan servicios online, incluyendo gobierno electrónico (e-gobierno), votación electrónica (e-votación), banca electrónica (e-banca) y parking móvil (m-parking), tal es el caso de Estonia, el país más conectado del planeta [107].

Durante el ataque mundial de secuestro de información del virus WannaCry (Ramsonware, 2017): millones de usuarios de computadores leyeron "Si puedes leer este texto, tus archivos ya no están disponibles, ya que han sido encriptados. Quizá estás ocupado buscando la forma de recuperarlos, pero no pierdas el tiempo: **nadie podrá hacerlo sin nuestro servicio de desencriptación**".

Fue con ese texto que, el 27 de junio de 2017, amanecieron computadoras de farmacéuticas, empresas de transportes marítimos, empresas del sector energético, bancos, oficinas de gobierno. Los países más afectados fueron: Polonia,

[105] Ibídem. Pág. 29
[106] Schmidt, Eric et al. El Futuro Digital. Anaya Multimedia. Madrid. 2014. Pág. 138
[107] Ibídem. Pág. 143

Francia, Inglaterra, España, Holanda, Rusia, Estados Unidos, Ucrania, Suiza. Una variante del Virus Petya resurgió ahora denominado WannaCry, que encripta información del dispositivo de almacenamiento del computador infectado a un nivel que hace casi imposible su desencriptación por medios convencionales, infectó a escala mundial, causando caos y pérdidas millonarias, al grado de que el puerto de Rotterdam, en Holanda, se vio obligado a detener sus operaciones diarias. [108] Se citarán algunos casos relevantes de ataques contra infraestructuras críticas a nivel mundial.

2.4.1 Qatar (2,017)

Según inteligencia de los Estados Unidos de América, un ataque informático ordenado por los Emiratos Árabes Unidos, publicó en el sitio web de una agencia de noticias de Qatar declaraciones falsas sobre la normalización de relaciones diplomáticas con Irán, lo que ocasionó una grave crisis política, llegando a un punto que Arabia Saudita, Bahréin, Egipto, Emiratos Árabes, Libia, Yemen, Maldivas, Mauritania y Comoras rompieran relaciones Diplomáticas con Qatar y suspendieran comunicaciones terrestres, marítimas y aéreas, acusándolos de patrocinar al terrorismo. [109] Este es un ejemplo de un ciberataque de Estado a Estado.

2.4.2 Corea del Sur (2017)

El mercado más importante de criptomonedas de Corea del Sur sufrió ataques por parte de piratas informáticos y comprometió al 3% de cuentas de usuarios de dicha plataforma. Logró extraer de las “billeteras virtuales” cientos de miles de dólares en Bitcoins, la moneda criptográfica de más uso a nivel mundial. Se sospecha que Corea del Norte estuvo tras el ataque informático. En 2013,

[108] https://www.elconfidencial.com/tecnologia/2017-06-27/ataque-ransomware-dla-piper-wannacry_1405839/. Consultado el 10 de junio 2018
[109] http://www.telesurtv.net/news/EE.UU.-apunta-a-Emiratos-Arabes-como-autor-del-ciberataque-a-Qatar-20170716-0046.html. Consultado el 10 de agosto 2018

también en otro ciberataque las redes informáticas de las principales emisoras de televisión y dos de los mayores bancos de Corea del Sur quedaron inutilizados. Al menos tres cadenas de televisión y dos bancos informaron a la Agencia Nacional de Policía surcoreana que sus redes informáticas se habían interrumpido por completo.[110]

2.4.3 Estonia (2,007)

En mayo 2007, el traslado de la estatua del soldado de bronce del centro de la capital a un cementerio apartado provoca la ira del gobierno ruso, quien respondió a esta acción con un ciberataque masivo contra la banca, la prensa y páginas de oficinas oficiales del gobierno de Estonia, causando un caos a nivel nacional que el país entero se vio en la necesidad de recurrir a medios de comunicación tradicionales como llamadas telefónicas y uso de fax para trasladar información. Fue un ataque técnicamente denominado Denegación de Servicios (DDOS, por sus siglas en inglés), y consiste en saturar la capacidad de respuesta de un servidor. Durante este ataque pasaron de tener de 1,500 visitas diarias a 1,500 por segundo, sobrepasando la capacidad de respuesta. Proveedores de Internet, banca, prensa y otros se vieron afectados por este ciberataque a escala nacional.[111]

2.4.4 Irán (2,013)

Aunque nunca se tendrá la versión oficial de la casa blanca ni del primer ministerio de Israel respecto del tema, todo apunta, según medios estadounidenses, a que en conjunto con Israel se desarrolló un poderoso virus con capacidad de detener las plantas de Uranio de Irán. A esta operación se le denominó en clave "Juegos Olímpicos" y el Virus, una vez descubierto por la firma rusa de antivirus Kaspersky Labs, recibió el nombre de Stuxnet; este poderoso virus recopilaba

[110] http://archivo.elcomercio.pe/tecnologia/actualidad/corea-sur-fue-victima-ciberataque-sospecha-norcorea-noticia-1552610. Consultado el 15 de agosto 2018

[111] https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html. Consultado el 20 de septiembre de 2018

información de los ordenadores infectados y logró, según fuentes de inteligencia, retrasar de año y medio a dos años el programa nuclear de los ayatolas.

Cuando accidentalmente se filtró al internet este virus, se desarrolló otro aún más poderoso al cual se le denominó “Flame”; este ha ido evolucionando, al punto de ser la base con la que las agencias de inteligencia interceptan memorias de dispositivos móviles, activan micrófonos y llegan a utilizar las cámaras de video de computadoras portátiles. [112]

Irán se fortaleció en materia de ciberdefensa y ciberofensa después de ser víctima de uno de los ataques más sofisticados de que se tenga registros: el famoso virus Stuxnet contra sus plantas nucleares. La prensa iraní acusa a los Estados Unidos e Israel de haberlo desarrollado e implementado dentro de la central nuclear, por medio de una unidad de almacenamiento USB que un empleado descuidado empleó en la planta nuclear.

“El gusano -ahora conocido como Stuxnet- tomó el control de 1,000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse”[113]. Esto causó que las centrifugadoras usadas para enriquecer uranio fallaran y provocaran años de atraso en el desarrollo nuclear iraní.

Nuevamente, en 2019, Estados Unidos atacó las plantas nucleares de Irán con programas maliciosos dirigidos a detener la producción de uranio; esta vez, Washington se atribuyó el ciberataque, aunque Irán hizo público que el mismo no tuvo éxito.[114]

---

[112] http://www.abc.es/20120609/internacional/rc-ciberataque-obama-contra-iran-201206090744.html. Consultado el 19 de septiembre 2018

[113] http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet. Consultado el 10 de octubre 2016

[114] https://elpais.com/internacional/2019/06/24/actualidad/1561356118_942931.html.Consultado el 10 de enero 2020

2.4.5 Estados Unidos (2016)

El concepto de mente colmena, utilizado para el mal, se materializa cuando computadoras infectadas de todo el mundo aportan procesamiento que es útil para llevar ataques masivos como el que dejó fuera a la mitad del Internet de los Estados Unidos, cuando uno de los proveedores principales, Dyn, quedó fuera de línea a causa de un ataque de denegación de servicio por una botnet que causó que sitios como Twitter, Spotify y Amazon dejaran de funcionar temporalmente.[115]

La protección de las plataformas tecnológicas, de las cuales dependen las infraestructuras críticas, constituye un aspecto importante para los Estados Unidos de Norteamérica y otros países que han identificado el Ciberespacio como un dominio en su seguridad nacional. El Internet en sí se puede considerar una infraestructura crítica, el 21 de octubre de 2016, el mundo observaba cómo la mitad de los Estados Unidos se quedaba sin acceso a la plataforma Twitter y periódicos de circulación nacional, por el que ha sido uno de los peores ataques de denegación de servicio en la historia de ese país. [116]

2.5 Ciberdefensa en el Marco Internacional

El Ministerio de Defensa Nacional de Chile define la ciberdefensa como "Infraestructuras críticas como los servicios básicos, transportes y diversas industrias como la financiera y del transporte, entre muchas otras, incluidas la administración del Estado y la Defensa Nacional, son susceptibles de ser atacadas en el ciberespacio, pudiendo amenazar la estabilidad, seguridad y soberanía de los países de múltiples formas(…) En el ámbito de la defensa, hoy se considera al ciberespacio como un nuevo ambiente en el que se desenvuelven diversos conflictos de diversa naturaleza, nacionales e internacionales."[117]

---

[115] https://www.efe.com/efe/america/tecnologia/un-ataque-contra-los-servidores-en-ee-uu-ralentiza-internet-todo-el-mundo/20000036-3074810 . Consultado febrero de 2018
[116] Ídem
[117] https://www.defensa.cl/temas-de-contenido/ciberdefensa/. Consultado el 21 de enero 2020

El entonces presidente de los Estados Unidos, Barack Obama, declaró que la infraestructura digital de América debe ser considerada "un activo nacional estratégico". En mayo de 2010, el Pentágono estableció su nuevo *Cyber Command* (Cybercom), con el objetivo de proteger las redes militares estadounidenses, y dirigir y efectuar ataques cibernéticos que fueran necesarios contra otros países.[118]. En junio de 2019, este Cibercomando fue el encargado, por instrucciones del presidente Donald Trump, de realizar ataques cibernéticos a las instalaciones de misiles nucleares de Irán, dejándolos, según fuentes del Pentágono, temporalmente inservibles para operar una misión de ataque.[119]

Yendo al terreno de lo que se ha denominado Ciberdefensa, William. J. Lynn III, Deputy Secretary of Defense, publicó en la revista Foreing Affairs los cinco principios básicos de la estrategia de la guerra del futuro:[120]

- El ciberespacio debe ser reconocido como un territorio de dominio igual que la tierra, mar y aire en lo relativo a la guerra.

- Cualquier posición defensiva debe ir más allá del mero mantenimiento del ciberespacio limpio de enemigos, para incluir operaciones sofisticadas y precisas que permitan una reacción inmediata.

- La defensa del ciberespacio (ciberespacial) debe ir más allá del mundo de las redes militares –dominios.mil y.gov. del Departamento de Defensa, para llegar hasta las redes comerciales (dominios. com, .net,.info,.edu, etc.) y que deben estar subordinados al concepto de Seguridad Nacional.

- La estrategia de la Defensa Ciberespacial debe realizarse con los aliados internacionales para una política efectiva de alerta compartida. ante las

---

[118] Citado por Aguilar, Luis Joyanes. *"Introducción. Estado del arte de la ciberseguridad."* Cuadernos de estrategia, No. 149. 2011. Pag. 30. Disponible en: https://dialnet.unirioja.es/descarga/articulo/3837217.pdf

[119] https://elpais.com/internacional/2019/06/23/estados_unidos/1561302401_346950.html. Consultado el 2 de Julio 2019

[120] William J, Lyns. Foreign Affairs, vol. 89, n. 5, septiembre/octubre de 2010, pp. 97

amenazas mediante establecimiento de Ciberdefensas con países aliados.

- El Departamento de Defensa debe contribuir a mantener e incrementar el dominio tecnológico de Estados Unidos y mejorar el proceso de adquisiciones y mantenerse al día con la agilidad que evoluciona la industria de las Tecnologías de la Información.

Gran Bretaña ha respondido ante posibles ataques cibernéticos en contra de su infraestructura crítica de información, creando el *Goverment Communications Headquarters* o GCHQ (Cuartel General de Comunicaciones del Gobierno), que es el equivalente de la NSA de Estados Unidos. La finalidad de sus 4,500 empleados es proteger los sistemas de comunicaciones informáticas del gobierno británico.

China ya piensa en las guerras de la segunda mitad del siglo XXI, y recientemente anunció el Ministerio de Seguridad Chino la primera policía de Internet del mundo orientada a vigilar sitios clave para ese país. Muchos otros países están organizándose para la ciberguerra; entre ellos, Rusia, Israel, Corea del Norte, etc. Definitivamente, el Ciberespacio formará parte de cualquier guerra que se produzca en el futuro.[121]

Israel considera como dominios de defensa: aire, tierra, mar, espacio y ciberespacio. Estima que el ciberespacio es el quinto dominio y fue uno de los primeros países en tomarlo en cuenta como defensa militar, al igual que Estados Unidos, Rusia y China. Israel, por su parte considera el Ciberespacio como un espacio para guerras de baja intensidad, pero declara que muchas veces la intensidad es alta.[122]

En la edición 2017 de la Estrategia de Seguridad Nacional Española establece el *Ciberespacio*, Espacio Marítimo y el Espacio Aéreo y Ultraterrestre

---

[121] *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio*. Ministerio de la Defensa Española. 2010. Pág. 31. Disponible en: http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

[122] https://www.perfil.com/noticias/internacional/la-seguridad-tiene-cinco-dominios-aire-tierra-mar-espacio-y-ciberespacio.phtml. Consultado el 23/09/2018

como espacios globales comunes de defensa [123]. También se resalta que la transformación digital de la administración pública puede ser aprovechada por atacantes. Además, menciona puntualmente: “el robo de datos e información, los ataques ramsomware, y de denegación de servicios, el hackeo de dispositivos móviles y sistemas industriales y los ciberataques contra las infraestructuras críticas son ejemplos de ciberamenazas”.

El 13 de octubre de 2017, el presidente de los Estados Unidos, Donald Trump, en el marco de la nueva estrategia que los Estados Unidos adoptaría con Irán, de no certificar el acuerdo nuclear vigente entre los dos países, mencionó que Irán “era el principal patrocinador de terrorismo en el mundo” [124].

En esa ocasión el presidente Trump acusó a Irán de lanzar “ciberataques contra nuestra infraestructura crítica y sistema financiero y militar"[125]. Se basó en posibles ataques de un grupo de hackers iraní denominado APT33 Advanced Persistent Threat (amenaza persistente avanzada). Entre 2011 y 2013 se supone que este grupo atacó a instituciones financieras de Europa y los Estados Unidos, incluida una represa cerca de New York.

El citado artículo de la BBC menciona que un grupo de hackers iraní tiene interés en el ciberespionaje en temas de aviación militar, comercial y energético, lo que nos hace observar un tablero mundial donde las condiciones favorecen las constantes ofensas cibernéticas de un país a otro. Y el panorama se hace más complejo cuando analizamos los ataques, que ahora no se realizan únicamente con fines de espionaje financiero o industrial, sino también con fines políticos y manipulación de masas.

---

[123] *Estrategia Nacional de Seguridad Nacional*. Gobierno de España. ESN-2017. Pág. 66

[124] http://www.elnuevodiario.com.ni/internacionales/443220-trump-lanza-nueva-estrategia-iran-no-certificar-ac/. Consultado el 20 de octubre 2019

[125] http://www.bbc.com/mundo/noticias-41637526. Consultado el 20 de diciembre 2017

2.6 Ciberdefensa en Guatemala

Por medio del acuerdo gubernativo 65-2019, se creó en Guatemala el "comando de informática y tecnología como un comando militar especial con jurisdicción en todo el territorio nacional"; también fue creado el "Comando de Comunicaciones del Ejército de Guatemala", como parte de un proceso de modernización de dicha institución. Citando al referido decreto, la razón de la creación de los comandos es: "atendiendo a la necesidad de integrarse con organismos internacionales que coadyuvan a la defensa del ciberespacio ante cualquier amenaza o violación de naturaleza diversa y alcance multidimensional en defensa de la infraestructura crítica, medios y sistemas de comunicaciones e información, en atención a la seguridad interior y exterior del territorio nacional"[126]

Es un paso sumamente importante en materia de ciberseguridad, por lo que es imprescindible que el ejército de Guatemala tome cartas en el asunto. El objetivo de proteger el ciberespacio y las infraestructuras críticas en los ámbitos interno y externo responde a las necesidades planteadas en la política nacional de seguridad. El acuerdo gubernativo en mención no contiene mayor información acerca de funciones y objetivos. Esa falta de información, tanto en el acuerdo gubernativo como por parte de las autoridades del ejército, dio lugar a que la prensa nacional atacara su creación como un posible centro de inteligencia y espionaje.[127]

Si cumple con los objetivos planteados de proteger el ciberespacio e infraestructuras críticas, el comando de informática y tecnología del ejército de Guatemala será un pilar fundamental en la construcción de un país más seguro. Es la primera dependencia del Estado que se crea específicamente para garantizar la ciberseguridad. Llama la atención que los considerandos de su creación mencionen que se integrará a organismos internacionales para cumplir su función. No

---

[126] *Acuerdo gubernativo número 65-2019*. Presidencia de la República de Guatemala. Pág. 1 consultado en: https://sgp.gob.gt/wp-content/uploads/2019/05/AG-065-2019.pdf el 21 de enero 2020

[127] https://elperiodico.com.gt/nacion/2019/06/02/nueva-comandancia-del-ejercito-despierta-desconfianza/. Consultado el 21 de enero 2020

especifica cooperación interinstitucional. Es de resaltar que su creación constituye un gran avance y puede llegar a ser una pieza importante en la búsqueda de la seguridad integral del ciberespacio en Guatemala.

Existe una delgada y difusa línea en los conceptos de Ciberdefensa y Ciberseguridad; incluso, algunos autores hacen una mezcla de ellos.

Una crítica constructiva es que, si bien es loable la creación de unidades y el fortalecimiento institucional en la ciberseguridad, primero debe existir un marco jurídico sólido y políticas públicas contra el ciberdelito. Luego, es preciso fortalecer las instituciones, ya que de lo contrario, se estarían realizando esfuerzos aislados y sin cooperación interinstitucional y/o internacional, tornándose en esfuerzos estériles.

2.7 Infraestructuras Críticas Bajo Ataque

Las infraestructuras críticas dependen de la tecnológica informática para funcionar, y la tendencia es que estén interconectadas con centrales de monitoreo, con sucursales de operaciones remotas o administraciones tecnológicas remotas. Ello obliga a que permanezcan conectadas a otras redes informáticas y, en muchos casos, que utilicen el Internet para su interconexión. Este modelo de interconexión las hace más vulnerables que antes a sufrir ataques informáticos, aunque, como veremos en uno de los casos más relevantes de la historia de ataques a infraestructuras críticas, no es del todo necesaria su conexión a Internet para un ataque sofisticado.

El escenario de infraestructuras críticas conectado a Internet no es el único en el cual pueden estar bajo ataque. El ataque a la infraestructura crítica de las plantas nucleares en Irán empleando el virus Stuxnet se realizó utilizando un dispositivo de memoria USB. Resalta que los ciberataques es posible efectuarlos, aunque los sistemas no se encuentren conectados a Internet.

El embajador de la OEA, Albert Ramdim, manifiesta: “Los Estados Miembro dependen de su infraestructura crítica para brindar servicios y productos imprescindibles, y gracias a que los países de América han experimentado un crecimiento del número de infraestructuras que operan sobre las redes de Internet, también ha aumentado el número de ataques cibernéticos a dichas infraestructuras, lo que podría comprometer la infraestructura crítica de un país así como su capacidad de proveer servicios imprescindibles para sus ciudadanos”.[128]

Guatemala ha avanzado, al punto de ofrecer servicios en línea a los ciudadanos, lo que conlleva riesgos de ataques a la infraestructura. Algunas municipalidades del país están en proceso de implementación de proyectos de ciudades inteligentes, concepto que utiliza la tecnología para mejorar los servicios públicos y la calidad de vida de los habitantes. Aprovecha al máximo el uso de Internet de las cosas (IOT por sus siglas en inglés), y requiere un ambiente hiperconectado. Esto constituye también un nicho de vulnerabilidad, en materia de ciberseguridad, en el corto plazo, susceptible de ser explotado por ciberdelincuentes.

La eventual llegada de la tecnología 5G, dada su velocidad, causará una revolución en la conectividad de dispositivos. Con ello las vulnerabilidades también aumentan exponencialmente.

Ya han ocurrido ciberataques a lo que podríamos considerar infraestructura crítica en Guatemala. A continuación se analizará el caso de ataque a la infraestructura tecnológica de la Superintendencia de Administración Tributaria de Guatemala (SAT).

---

[128] *Reporte de Seguridad Cibernética y Protección de la Infraestructura Crítica*. OEA-Trend Micro. 2015. Página 4. Consultado en: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-120/15. Consultado el 20 de junio 2018

El 27 de junio de 2017 la SAT hizo público que estaba siendo blanco de un ataque dirigido a sus sitios web, lo que impedía el pago de impuestos en línea.[129] Algunos usuarios se quejaron de que por un término de cinco días no fue posible realizar pagos en los sistemas. El superintendente, en su cuenta de Twitter, el 27 de junio 2017 publicó: "Estamos sufriendo ataques cibernéticos constantes durante las dos últimas semanas. Esperamos levantar pronto los sistemas."[130] Nunca se hizo pública la estimación del costo financiero que representaron las pérdidas para el Estado de Guatemala durante el tiempo en que las páginas Declaraguate y otros sitios de la SAT estuvieron fuera de línea. Se sospecha se trató de un ataque dirigido de denegación de servicios (DDoS), el provoca saturación en el servidor encargado de responder peticiones sobre un servicio digital.

El marco jurídico utilizado para denunciar dichos ataques ante el Ministerio Público fueron los artículos 294 y 295 del código penal. Este fue el comunicado: "La SAT informó que denunciará el caso del ataque informático ante el Ministerio Público. La denuncia será por los delitos de atentado contra la seguridad de servicios de utilidad pública e Interrupción o entorpecimiento de comunicación (artículos 294 y 295 del Código Penal)."[131]

Lo anterior evidencia que en Guatemala es necesario echar mano de figuras de delitos "coincidentes" para ciberataques, ya que se usa legislación cuyo espíritu de creación fue proteger únicamente la seguridad física, cuando se lucha contra otros más sofisticados como lo son los delitos en el ciberespacio. En Guatemala es urgente legislar en contra del ciberdelito.

Un mes después de este incidente, volvía a suscitarse un posible ataque cibernético a la infraestructura tecnológica de la SAT. Con el título "SAT denuncia ataque cibernético y complica trámites en línea", el 27 de julio 2017 el

---

[129] http://www.prensalibre.com/economia/sat-denuncia-por-ataques-a-enlaces-de-internet. Consultado el 20 de agosto 2017
[130] https://twitter.com/foppaguate/status/879781977343365121. Consultado el 28 diciembre 2019
[131] http://www.prensalibre.com/economia/sat-denuncia-por-ataques-a-enlaces-de-internet. Consultado el 20 de agosto 2017

superintendente volvía a denunciar que sufrían ataques de sabotaje a los servicios en línea. El nuevo incidente fue denunciado públicamente, siempre a través de su cuenta de Twitter; esta vez publicó: “Seguimos con problemas en los servidores a causa de ataques cibernéticos. Están saboteando la red @SATGT desde el lunes”. Este supuestamente sabotaje a la infraestructura crítica de la SAT coincidió con la cercanía del vencimiento del pago de impuestos de circulación.

Por ello, el titular del Periódico, en su edición del mismo día, decía: “Sigue sabotaje cibernético a la SAT”[132] y mostraba las plataformas que eran afectadas y las acciones que tomó la superintendencia para sobrellevar la situación:

“Como los ataques al sistema electrónico de la entidad comenzaron la mañana del pasado lunes, la Superintendencia de Administración Tributaria emitió la Resolución 570-2017 a través de la que declaró día inhábil el 24 de julio para el cumplimiento de las siguientes obligaciones y corrió el plazo para el 25 la presentación y pago, pero sigue sin web: Informe de Constancias de Exención emitidas a través del sistema ExenIVA correspondiente al trimestre abril-junio 2017. Aviso de legalización de firmas en certificados de propiedad de vehículos terrestres, realizadas durante junio último. Declaración jurada y pago de retenciones efectuadas el mes pasado”.[133]

De estos actos nunca se dio a conocer a los responsables; ni siquiera se pronunció el Ministerio Público respecto de qué líneas tomaría la investigación en este caso que paralizó la economía del país. Ni el Ministerio Público, ni el Instituto Nacional de Ciencias Forenses, ni la Policía Nacional Civil poseen personal capacitado ni equipo técnico adecuado para llevar a cabo este tipo de investigaciones. No son capaces de realizar investigaciones de alto nivel informático. Cuando se analiza el fondo del problema acerca de la razón por la que las instituciones guatemaltecas no están preparadas para este y otros casos, no hay

---

[132] https://elperiodico.com.gt/nacion/2017/07/27/sigue-sabotaje-cibernetico-al-sitio-web-de-la-sat/. Consultado el 10 de octubre 2017.
[133] Ídem

que ir muy lejos para conocer la respuesta: No existe un modelo de ciberseguridad, ni las condiciones para aplicarlo en la actualidad.

2.8 El modelo español de identificación de infraestructura crítica y su protección

La ley 8/2011 de España, por la que se establecen medidas para la protección de infraestructuras críticas,[134] menciona en su preámbulo: "Para su protección se hace imprescindible, por un lado, catalogar el conjunto de aquellas que prestan servicios esenciales a nuestra sociedad y, por otro, diseñar un planteamiento que contenga medidas de prevención y protección eficaces con las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente en medios de información y de comunicación de carácter público y abierto".

El reglamento de la ley de protección de infraestructuras críticas, en el artículo 5. Gestión y actualización del catálogo, párrafo 2, estipula: "El ministerio del Interior, a través, de la Secretaría de Estado de Seguridad, será responsable de clasificar una infraestructura como estratégica y, en su caso, como infraestructura crítica o infraestructura crítica europea, así como de incluirla por vez primera en el Catálogo, previa comprobación de que cumple uno o varios de los criterios horizontales de criticidad previstos en el artículo 2, apartado h) de la ley 8/2011".[135]

---

[134] *Ley de Protección de Infraestructura Crítica*. BOE-A-2011-7630. Gobierno de España. 2011. Consultado en https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

[135] *Reglamento de ley de Protección de Infraestructura Crítica*. BOE-A-2011-8849. Gobierno de España. Consultado en https://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf. Consultado el 20 de junio 2017

La citada ley 8/2011 española define algunos criterios para que se considere a las infraestructuras como críticas: número de personas afectadas, impacto económico, impacto medio ambiental, impacto público y social. (*Ver tabla 1.Anexo 7)*

El IEEE subraya que muchas fortalezas de los Estados en donde aplica tecnología a servicios críticos a la población podrían convertirse también en una debilidad; es decir, las sociedades desarrolladas y altamente tecnificadas dependen en extremo de una serie de servicios esenciales, sin los cuales no hay capacidad de subsistencia. Pensemos en servicios tales como el sistema de transportes, el agua, la electricidad, las telecomunicaciones, etc. Por este motivo, hace unos años se acuñó la frase ***infraestructura crítica*** para referirse a la prestación de estos servicios básicos imprescindibles, junto a la necesidad de su protección.

El Instituto Español de Asuntos Estratégicos define el nivel de implicación de la protección de las infraestructuras críticas dentro de la seguridad nacional, al decir: "Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, expuestas a una serie de amenazas, para cuya protección se hace imprescindible, por un lado, catalogarlas y, por otro, diseñar un plan con medidas eficaces de prevención y protección contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones". [136]

En esta tesis se presenta una propuesta de catálogo de infraestructura crítica. Aunque se debe recurrir a medios rigurosos para su catalogación oficial, hay que comenzar con una lista de infraestructura que provee servicios críticos para la población y para la seguridad nacional. Siguiendo estas premisas, en el modelo de

[136] M. Caro Bejarano. *Protección a las Infraestructuras Críticas*. Instituto Español de Asuntos Estratégicos. 2011. Disponible en: http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf

ciberseguridad planteado en el presente trabajo se pretende catalogar y proponer un plan de protección de infraestructuras críticas.

La Estrategia Nacional de Seguridad del Gobierno Español de 2013, remarca la necesidad de incluir la seguridad del ciberespacio, al manifestar: “La dependencia de la sociedad del ciberespacio y su fácil accesibilidad hacen que cada vez sean más comunes y preocupantes las intromisiones en ese espacio”. [137]

Además, menciona que está documentado que estos ataques proceden de grupos terroristas, redes del crimen organizado, empresas, Estados o individuos aislados. Y que la Ciberseguridad también puede verse vulnerada por causas técnicas o fenómenos naturales.

Por ello, el objetivo primario de una Política Nacional de Seguridad, en cuanto a las infraestructuras críticas, debería ser: “Robustecer las infraestructuras que proporcionan servicios esenciales para la sociedad”.[138] Este plan fue activado en febrero de 2014, a raíz de los atentados sufridos en París. Por lo anterior, cabe asegurar que el uso de tecnologías en infraestructuras que prestan servicios indispensables para el funcionamiento de un país es inminente.

El objetivo general de un país, al proteger sus infraestructuras críticas de servicios, debe ser: “Fortalecer las infraestructuras que proporcionan los servicios esenciales para la sociedad”.

2.9 Infraestructura esencial en Guatemala

La Asociación Guatemalteca de Ingeniería Estructural y Sísmica presenta una clasificación de infraestructuras y las divide en: utilitarias, ordinarias, importantes y esenciales. Para efectos del presente estudio, son útiles las que se encuentran categorizadas como esenciales, en virtud de que las define como: son

[137] *Estrategia Nacional de Seguridad de España*. Gobierno de España. 2013. Disponible en: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional
[138] Plan Nacional para la Protección de las Infraestructuras Criticas. Gobierno de España. 2010

las que deben permanecer en operación continua durante y después de un siniestro. Incluyendo obras, tanto estatales como privadas, se mencionan:

1) Instalaciones de salud con servicios de emergencia, de cuidado intensivo, salas de neonatología o quirófanos.

2) Instalaciones de defensa civil, bomberos, policía y de comunicaciones asociadas con la atención a desastres.

3) Centrales telefónicas, de telecomunicación y de radiodifusión.

4) Aeropuertos, hangares de aeronaves, estaciones ferroviarias y sistemas masivos de transporte.

5) Plantas de energía e instalaciones para la operación continua de las obras que clasifiquen como esenciales.

6) Líneas troncales de transmisión eléctrica y sus centrales de operación y control

7) Instalaciones de captación y tratamiento de agua y sus centrales de operación y control.

8) Estructuras que formen parte de sistemas contra incendio en obras esenciales.

9) Estructuras que contengan agentes explosivos, tóxicos o dañinos al público.

10) Puentes sobre rutas centroamericanas y aquellas que la autoridad competente considere.

11) Instalaciones específicamente diseñadas como refugios para emergencias.

12) Instalaciones de importancia estratégica para la seguridad nacional.

13) Aquellas obras que las autoridades estatales o municipales específicamente declaren como esenciales.[139]

Aunque la clasificación está orientada a la protección física de infraestructura, es útil porque presenta el nivel de importancia que estas tienen para el funcionamiento del país. Para una clasificación oficial de infraestructura crítica, se debe tomar como punto de partida esta clasificación.

2.10 Propuesta de Catálogo de Infraestructura Crítica en Guatemala

Según los conceptos analizados acerca de infraestructura crítica en Guatemala, se podría catalogar en una primera aproximación a la banca, las telecomunicaciones, la emisión de documentos de identidad nacional, el control aéreo, los puertos y aeropuertos, centrales de control de monitoreo de energía eléctrica, tribunal supremo electoral según los últimos acontecimientos con relación a la tecnología utilizada en las elecciones generales de 2019, las plataformas de sistemas para pago de impuestos, la producción agropecuaria que sostiene el PIB nacional como el café y azúcar, lo cual también tiene un alto grado de automatización y sistematización. Y cada año se sumará a esta lista más infraestructura que depende de la tecnología para su funcionamiento.

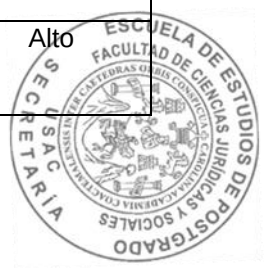
La única vez que se menciona responsables de catalogar infraestructura crítica es en la agenda estratégica de seguridad de la nación, en el Proyecto: Fortalecimiento del Sistema de Prevención, Mitigación y Recuperación a Desastres Naturales. Está en la acción programática Desarrollar infraestructura crítica para la prevención, planeamiento, gestión, reducción, intervención y recuperación de eventos y desastres naturales. Entre las acciones específicas se encuentra caracterizar la infraestructura crítica del país de acuerdo con su vulnerabilidad y riesgo. La asignación institucional para realizar esta acción fue la CONRED. Para

[139] *Normas de Seguridad Estructural para Guatemala*. Asociación Guatemalteca de Ingeniería Estructural y sísmica. 2018. Página 3-3. Disponbile en: https://www.agies.org/wp-content/uploads/2018/08/NSE-1-2018-Edicion-Beta-Generalidades-administracion-y-supervision.pdf. consultado el 25/01/2020

fines de este trabajo no se encontró el estudio que la agenda de seguridad mandataba a la CONRED realizar.

Siguiendo los criterios establecidos por la legislación española, (*Ver anexo 6*) se presenta este catálogo preliminar de Infraestructura Crítica Nacional candidata a una evaluación a fondo, para ser estimada como infraestructura crítica. Se propone la primera aproximación de lo que debería considerarse como infraestructura crítica.

Catalogo Preliminar de Infraestructura Crítica Nacional						
No.	Infraestructura	Institución/Empresa Responsable	Daño Físico a personas	Impacto Económico	Impacto Medioambiental	Impacto Público y Social
1.	Sistemas en línea de pago de impuestos	Superintendencia de Administración Tributaria (SAT)	Bajo	Alto	Bajo	Alto
2.	Infraestructura tecnológica de pago de nóminas del Estado	Ministerio de Finanzas Públicas	Bajo	Alto	Bajo	Alto
3.	Sistemas tecnológicos bancarios	Banca Privada/Superintendencia de Bancos (SIB)	Bajo	Alto	Bajo	Alto
4.	Sistemas de telecomunicaciones	Empresas de Telefonía Privada/ Superintendencia de Telecomunicaciones	Bajo	Alto	Bajo	Alto
5.	Internet	Empresas privadas proveedoras de Internet	Bajo	Alto	Bajo	Alto
6.	Energía eléctrica	Empresas privadas generadoras y portadoras de energía/Instituto Nacional de Electrificación	Medio	Alto	Alto	Alto
7.	Sistemas de semáforos en ciudad de Guatemala	Municipalidad de Guatemala	Alto	Alto	Medio	Alto
8.	Puertos	Empresas Portuarias	Alto	Alto	Alto	Alto
9.	Aeropuertos	Dirección General de Aeronáutica Civil (DGAC)	Alto	Alto	Medio	Alto



10.	Registro Nacional de las Personas	RENAP	Bajo	Bajo	Bajo	Alto
11.	Registro de Dominios .gt	Universidad del Valle. Guatemala	Bajo	Alto	Bajo	Alto
12.	Sistemas de control de 33 hidroeléctricas	INDE/Empresas privadas	Alto	Alto	Alto	Alto
13.	Sistema de conteo de votos para elecciones generales	Tribunal Supremo Electoral	Medio	Alto	Bajo	Alto
Fuente: Elaboración propia, con criterios de clasificación del Reglamento de protección de Infraestructuras críticas del gobierno español.[140]						

[140] *Reglamento de ley de Protección de Infraestructura Crítica*.BOE-A-2011-8849. Gobierno de España. Consultado en https://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf. Consultado el 14 de junio 2017

En el capítulo tres, en el contexto del modelo nacional de ciberseguridad, se plantea la creación de una comisión cuya responsabilidad sea la de catalogar la infraestructura crítica. La mesa de catalogación de infraestructura crítica debe estar conformada por el sector gobierno y el sector privado, así: Sector gobierno, con sector justicia; Secretaria Nacional de Ciencia y Tecnología; Consejo Nacional de Ciencia y Tecnología; Ministerio de la Defensa Nacional; Consejo Nacional de Seguridad; Secretaría Técnica del Consejo Nacional de Seguridad, Registro Nacional de las Personas, Ministerio de Comunicaciones, Infraestructura y Vivienda; universidad. Del sector privado: telecomunicaciones, generación y distribución de energía, puertos y universidades.

2.11 Infraestructuras Críticas como Elementos de la Seguridad Nacional

Matt Dixon, experto en ciberseguridad y director de la empresa Point86, escribe para Harvard Business Review: “De los 3 mil millones de cuentas de correo electrónico de Yahoo! comprometidas en 2013 a los datos de identidad y crédito de 143 millones de estadounidenses robados de la agencia de crédito Equifax (y una miríada de otros ataques), las infracciones masivas de datos se han vuelto demasiado familiares. La frecuencia y severidad de estos ataques, combinados con el alto nivel de seguridad y sofisticación tecnológica de sus víctimas, ha provocado indignación pública y preguntas sobre si es posible incluso una protección suficiente contra infracciones futuras. Gemalto, una compañía internacional de seguridad de datos resumió este sentimiento en su Informe de índice de nivel de incumplimiento del primer semestre de 2017: Cada vez más organizaciones aceptan el hecho de que, a pesar de sus mejores esfuerzos, las infracciones de seguridad son inevitables.[141]

[141] https://www.toptal.com/insights/innovation/blockchain-identity-management . Consultado el 7 de febrero 2018

Incluso en países como los Estados Unidos se puede observar un panorama no muy alentador por parte de expertos quienes dudan que los ataques algún día dejarán de traer consecuencias severas financiera como socialmente. Es por eso por lo que la protección a infraestructuras críticas y la ciberdefensa ahora es un dominio más de su seguridad nacional.

En Guatemala, “La Agenda Nacional de Riesgos y Amenazas -ANRA- es la base para la elaboración de la Política Nacional de Seguridad, a cargo del Consejo Nacional de Seguridad, y constituye una herramienta para desarrollar el conjunto de lineamientos y cursos de acción necesarios para reducir los riesgos y mitigar las amenazas a la Seguridad de la Nación.”[142]

En su edición del año 2018, la ANRA incluye entre las amenazas a la Seguridad Nacional los ciberataques, junto a la Violación a la soberanía, Lavado de Dinero y otros activos, Transito y tráfico ilegal de armas de fuego, municiones y explosivos y la narcoactividad.

El mismo documento define la Seguridad a la Nación como “el conjunto de principios, políticas, objetivos, estrategias, procedimientos, organismos, funciones y responsabilidades de los componentes del Estado en materia de seguridad, que garantizan la independencia, soberanía e integridad y los derechos fundamentales de la población establecidos en la Constitución Política de la República de Guatemala, que consolidan la paz, el desarrollo, (la justicia y el respeto de los derechos humanos. Citando a la Ley marco del Sistema Nacional de Seguridad, Decreto 18-2008, Capítulo II, Definiciones. Artículo 2, inciso a.)”[143].

---

[142] *Agenda Nacional de Riesgos y Amenazas*. Sistema Nacional de Inteligencia. Secretaria de Inteligencia de Guatemala. 2018. Consultado en: https://www.sie.gob.gt/portal/images/DocumentosVarios/anra/2018_ANRA.pdf. Consultado el 18 de enero 2018

[143] Ídem

Es impostergable que se comience a ver el tema cibernético a la par de las amenazas tradicionales a la seguridad nacional. Es tiempo que nuestro gobierno establezca las bases para la prevención y la lucha contra el cibercrimen; de lo contrario, es un mal que inevitablemente crecerá conforme avance la era digital.

Ahora se pasara a analizar las herramientas que utilizan grupos organizados para dañar la información de la población, las empresas y las instituciones públicas.

2.12 Virus, Troyanos y Gusanos utilizados en Ataques Tecnológicos Dirigidos a la Infraestructura Crítica

El informe anual de la firma de seguridad cibernética Symantec para el 2018, denominado Informe sobre las Amenazas para la seguridad en Internet, volumen 23, manifestó que, según Symantec, el concepto de ataques dirigidos es "trabajo de grupos organizados. La mayoría de esos grupos son patrocinados por naciones, y generalmente se enfocan en un número limitado de objetivos, número limitado de intereses: recopilación de información, interrupción de actividades, sabotaje o intereses financieros. En términos generales "ataques dirigidos" corresponden a actos de espionaje, a pesar de que los límites de estas definiciones están comenzando a cambiar y, en los últimos tiempos, hemos observado a varios grupos propagarse más allá del espionaje". [144]

Por otro lado el estudio realizado por la OEA en 2015 titulado "Reporte de Seguridad Cibernética e Infraestructura Critica de las Américas"[145], presenta el alcance de las vulnerabilidades en las infraestructuras críticas de los países miembros de la OEA: en un 60%, la información de la región latinoamericana está expuesta a caer en manos no autorizadas, el 30% está vulnerable a ser alterada y

---

[144] *Informe Sobre las Amenazas para la Seguridad en Internet*. Symantec. 2018. https://www.symantec.com/es/mx/security-center/threat-report . consultado el 2 de mayo 2018

[145] https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf. Consultado el 5 de mayo 2018

el otro 10% puede ser secuestrada para fines de extorciones. (*Ver anexo 1. Gráfica 1)*

Según el citado reporte, los ataques han aumentado un 53% en relación con el año 2014 a sistemas críticos computacionales de los Estados miembros, mientras que el 40% reporta niveles de ataque similares al de 2014, y solo el 10% reporta que los niveles han disminuido con relación al año 2014[146] en mención. Esto hace que nos cuestionemos ¿cuáles son los motivos?, ¿son personas individuales, organizaciones o gobiernos los que están detrás de estos ataques?

El reporte indica que 46% ha sido actividad del Gusano Botnet Conficker. Este tipo de programa maligno infecta equipo de cómputo sigilosamente burlando las defensas de antivirus; (*Ver anexo 1. Gráfica 2)* permanece dormido hasta que desde una central se le ordena ser parte de miles o millones de otros equipos infectados en un ataque sincronizado a algún servidor o servicio público o privado en Internet. Por ello, a los equipos infectados con este tipo de malware se les denomina Equipo Zombie[147].

Este malware impactó tanto a los sistemas operativos Windows, que el 12 de febrero de 2019 Microsoft publicó que daría una recompensa de US$250,000 (dólares americanos) a quien suministrara información que llevara al arresto de las personas responsables de haber creado el código del gusano Conficker, pues mencionó que la empresa lo consideraba un acto criminal y prestaría toda su colaboración a las autoridades para dar con los responsables.[148].

Según el Equipo de respuesta de emergencias informáticas (CERT, por sus siglas en inglés) de la Universidad Nacional Autónoma de México, se estima que

---

[146] Ídem. Pág. 19
[147] https://es.wikipedia.org/wiki/Zombi_(inform%C3%A1tica). Consultado febrero de 2018
[148] https://technet.microsoft.com/en-us/security/dd452420.aspx. Microsoft. Consultado febrero de 2018

hay más de diez millones de computadoras infectadas en todo el mundo con alguna de las variantes de este gusano.[149]

El código B106 pertenece a una familia de malware, y va dirigido a robo de identidad, fraude financiero e invasión de la privacidad. El que tenga un 30% de los ataques dirigidos hacia estas actividades nos indica que los mismos aumentan año con año, siendo el principal motivo las ganancias financieras de los atacantes. Microsoft, en su sitio dirigido para Asia, hizo el siguiente comunicado de ciberseguridad: "Las amenazas cibernéticas son reales y una preocupación creciente tanto para las personas como para las organizaciones, especialmente con la propagación de software malicioso. De hecho, según el Índice de infecciones de malware de Microsoft para el primer trimestre de 2015, la principal amenaza de malware en la ASEAN era la familia de malware Bladabindi / Jenxcus (B106).

Esto permite a los piratas informáticos robar información sensible; también tiene la capacidad de descargar otro malware y dar acceso no autorizado a su PC. Algunas variantes de la familia de malware B106 también pueden controlar la cámara de una PC para grabar y realizar funciones de captura de teclas."[150]

El código B68 o Zero Access identifica a un grupo de malware que explota vulnerabilidades de los equipos para cometer fraudes de clic falsos. Los anunciantes como Google, Yahoo! o Microsoft tienen el modelo de pago de publicidad contabilizada por el número de clics que potenciales clientes dan para ir a los sitios web de los anunciantes[151]. Por medio de malware, como la familia B68, se puede inflar de manera falsa los clics y de esta forma cobrar fraudulentamente cantidades de dinero de clics que realmente nunca ocurrieron.

---

[149] https://www.cert.org.mx/historico/documento/index.html-id=20 . UNAM. Consultado febrero de 2018

[150] Microsoft. https://news.microsoft.com/apac/2015/05/15/flight-to-quality-and-trust/ . Consultado febrero 2018

[151] Margaret Rouse. http://searchdatacenter.techtarget.com/es/definicion/Fraude-de-clic-fraude-de-pago-por-clic . Consultado en febrero de 2018

La propagación de malware de este tipo ha sido tan alarmante, debido a que los grandes del internet como Google, Microsoft y Yahoo! han tenido que devolver sumas considerables de dinero a sus anunciantes cuando se ha descubierto que miles o millones de clics, supuestamente de clientes reales, han sido una estafa. Microsoft publicó el siguiente comunicado en su sitio Microsoft Active Response for Security (por sus siglas en inglés, MARS), y lo llamó operación B68: "Microsoft estima que estas botnets han dañado más de dos millones de personas, con algunos de los mayores números de infecciones que aparecen en los EE. UU., India, Italia, Turquía, Reino Unido y España. Sirefef/Zero Access es responsable de más de 2,7 millones de dólares (USD) cada año en pérdidas de los particulares y empresas de todo el mundo. "[152]

La vulnerabilidad B54 es la base de la Botnet o red de computadoras zombis denominada Citadel, que alrededor del mundo causó la pérdida de aproximadamente quinientos millones de dólares a entidades financieras como American Express, Bank of América, PayPal, HSBC, Royal Bank of Canadá y Wells Fargo.

Los ciberdelincuentes creadores de Citadel, cobran a los bancos montos de dinero utilizando el usuario y contraseñas de las cuentas bancarias en línea robadas de las computadoras infectadas.

La colaboración de Microsoft y el FBI en una operación conjunta realizada en 80 países permitió que se desmantelara parte de esta red, pero se estima que aún existen cinco millones de equipo infectados en todo el mundo.[153]

En cuanto a Waledac, se estima que unas 70,000 a 90,000 computadoras están infectadas con esta variante de malware tipo gusano. Este gusano es capaz de enviar 1.5 billones de correo basura (spam) diariamente y lo hace por medio de

---

[152] Microsoft. https://blogs.technet.microsoft.com/seguridad/2013/12/06/alerta-microsoft-active-response-for-security-mars-operacin-b68-sirefefzeroaccess/. Consultado en febrero 2018
[153] http://www.bbc.com/news/technology-22795074 . Consultado en febrero 2018

robar contraseñas de correo en las computadoras infectadas; luego, utiliza las cuentas de correo para enviar el correo basura. Según la firma de ciberseguridad Symantec, una computadora puede infectarse con tan solo visitar un sitio web infectado. Utiliza como medio de infección sitios de envío de tarjetas navideñas, sitios para mandar tarjetas en el Día de San Valentín, por medio de SMS.

El gusano se descarga de forma automática y se autoinstala en la computadora, convirtiéndola en una computadora de la red zombie Waledac. Envía correos basura de productos de dudosa procedencia, ofertas de trabajo, juegos en casinos y otros.[154]

Podemos, entonces, concluir que los ataques aumentan cada año y su principal motivo son las ganancias financieras, contrario a otros años que lo primordial era ganar un nombre o la fama por medio de burlar las medidas de seguridad informáticas. Ahora es obtener ganancia por medio de estafas, robo de identidad, ciber-robos bancarios, fraude en publicidad.

Pero hay un patrón en este esquema de ataque. Los atacantes cometen los mismos delitos de antes; no obstante el modelo es más ambicioso porque agrupan equipos informáticos infectados; ya no se enfocan en ataques a computadoras aisladas, pues ahora lo hacen dejando una semilla que, en su momento, cuando los ciberdelincuentes desean esta germina, convirtiendo a esa computadora en un arma más en su red de ataque hacia un objetivo más grande.

---

[154] *W32.Waledac treat analysis*. Symantec. Consultado en: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/W32_Waledac.pdf . consultado el 18 de marzo 2018

2.13 Estado Tecnológico de Guatemala según el Foro Económico Mundial

En el prefacio del Reporte Global de Tecnologías de la Información del año 2015, Barth Eide menciona lo siguiente: “El Foro Económico Mundial aborda estos temas a través de su futuro de Internet Global Reto. Este esfuerzo tiene como objetivo garantizar que la Internet sigue siendo un motor central del progreso humano y para salvaguardar su integración global, altamente distribuida, y la naturaleza de múltiples partes interesadas. Incluye el Cyber Iniciativa de resiliencia, cuyo objetivo es aumentar la conciencia de riesgo cibernético y para construir compromiso con respecto a la necesidad para enfoques más rigurosos para la mitigación del riesgo cibernético. En dicho informe se evalúan todos los países del mundo en su madurez y avances en el uso de la tecnología.

Esperamos que, a través de este Informe y sus iniciativas, El Foro Económico Mundial contribuya a hacer que la revolución de las TIC sea verdaderamente global, crecimiento favorable e inclusivo”.[155]

El nivel superior del índice de tecnología es, para Singapur, con un punteo de 6, lugar que comparte con Finlandia (6), Suecia, Noruega, Holanda; Suiza y los Estados Unidos comparten el segundo lugar con 5.8, mientras que el tercer lugar lo comparten Inglaterra y Luxemburgo con un índice de 5.7. En 2016 ostentamos un 3.5, lo que nos sitúa en el puesto 103 de 139 países evaluados.

La mala noticia no es únicamente que nos sobrepasan en la calificación mundial países como Vietnam en el ranking 79, Ruanda 80, Trinidad y Tobago 67, o Islas Mauricio en el lugar 49. La peor noticia es que hemos retrocedido con los años en el índice de tecnología global. (*Ver anexo 2. Gráfica No. 1)*

Ha sido un sube y baja en el índice Global de Tecnología, logrando nuestro máximo punteo como país en el año 2014 con un 3.52; esto se debió a que en ese

[155] *Reporte Global de Tecnologías de Información 2015*. Foro Económico Mundial. Consultado en http://www3.weforum.org/docs/WEF_GITR_Preface_2015.pdf. Consultado el 12 de febrero 2018

año Guatemala logró un punteo alto para el subíndice preparación que mide las habilidades, infraestructura digital y la accesibilidad al Internet con un 3.9 ese año, para, luego, bajar en 2015 con 3.34 y subir un poco en 2016.

El mejor lugar en que ha estado posicionado nuestro país fue en 2012; después de eso, nunca ha vuelto a recuperar terreno del puesto 98 que tuvimos. Han sido recuperaciones en el 2014 y el 2016 que muestra el lugar 103 actual. ¿Cómo ayudaría una política nacional de ciberseguridad para que el país pueda optar a una mejor posición en el índice global de tecnología? (*Ver anexo 2. Gráfica No. 2).* Nuestro lugar 106 a nivel mundial responde a los siguientes valores en los respectivos índices evaluados por el Foro Económico Mundial. (*Ver anexo 2. Gráfica No. 3)*

Nos queda un largo camino por recorrer en el uso y aplicaciones de tecnologías, para que el país aproveche la coyuntura de la era de la información. ¿Cómo estamos protegiendo la tecnología que tenemos?

2.14 Estado de la Ciberseguridad en Guatemala Según la Organización de los Estados Americanos

El informe Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? la Organización de los Estados Americanos, el Banco Interamericano de Desarrollo y la Universidad de Oxford, analizan el estado del País a partir de 49 indicadores que se agrupan en cinco dimensiones, las cuales nos muestran en qué ejes estratégicos debemos fortalecer el país: 1) Política y Estrategia; 2) Cultura y Sociedad;3) Educación; 4) Marcos Legales; y 5) Tecnologías.

Según el informe de la OEA y el Banco Interamericano de Desarrollo, estamos en los niveles de madurez que el gráfico representa, debido a los factores que se exponen en el anexo 6. (*Ver anexo 5. Tabla No.1).* Los resultados son alarmantes: de 5 puntos máximo posibles, en cada índice tenemos, como país, en

política y estrategia 1 punto; en tecnologías 1.1 puntos; sociedad y cultura 1.44 puntos; educación 1.8 puntos; marcos legales 1.5 puntos. El resultado general como país es deficiente en todos los índices de ciberseguridad evaluados. (*Ver anexo 1. Gráfica 3)*

Otro estudio realizado en el año 2015, la Organización de los Estados Americanos (OEA) y la firma mundial de Ciberseguridad Trend Micro publicaron un informe sobre el estado de las infraestructuras críticas en Latinoamérica, y el nivel de esfuerzo de los gobiernos en turno por protegerlas. El citado informe resume la situación de vulnerabilidad de las infraestructuras críticas de la región, al decir: "el 60% de las vulnerabilidades que dejan al descubierto los agujeros podrían afectar a la confidencialidad de la información. En tanto, 30% de las vulnerabilidades representan una amenaza para la integridad, mientras que 10% de las vulnerabilidades son debilidades que pueden aprovechar los ataques contra la disponibilidad de la información de los servicios". [156]. Son cifras alarmantes; podríamos decir con esas conclusiones que la región latinoamericana es un caldo de cultivo listo para convertirse en un paraíso para los ciberdelincuentes.

Es seguro que mucha información catalogada como confidencial se está filtrando a manos que no deberían tener acceso. También es casi seguro que existe manipulación a sistemas críticos para que fallen o se detengan completamente. La pobreza tecnológica de protección es evidente; el recurso humano semicapacitado, y los sistemas los soportan infraestructuras físicas y de hardware en pésimas condiciones.

El estudio en mención arrojó resultados que sorprenden tanto del lado del avance tecnológico en la región, como el nivel de protección a estas plataformas,

---

[156] *Reporte de Seguridad Cibernética y Protección de la Infraestructura Crítica*. OEA- Trend Micro. 2015. Pág. 18. Disponible en: https://cutt.ly/utYi0Oq

que son las que permiten que un Estado funcione adecuadamente sin interrumpir servicios vitales tales como energía eléctrica, agua potable, el sector financiero, seguridad e impuestos.

Dicho estudio indica que los incidentes cibernéticos están aumentando y se están volviendo más sofisticados. Además identifica la necesidad de mejorar el nivel protección y los procesos de respuesta a incidentes, para garantizar el adecuado funcionamiento de las tecnologías críticas. El 76% de los encuestados indicó que perciben que los ataques a infraestructuras críticas han aumentado con relación al 2014. (*Ver anexo 1. Gráfica 4)*

El 52% de los encuestados reconoció contar con un plan de respuesta a incidentes cibernéticos. Estas cifras no son un buen indicador en caso ocurriera un ciberataque. Además únicamente el 37% de las organizaciones que participaron en el estudio declararon haber adoptado estándares de ciberseguridad. Este escenario pone en evidencia el inminente riesgo de ciberseguridad de las infraestructuras críticas en la región. (*Ver anexo 1. Gráfica 5*)

De acuerdo con los resultados de dicho estudio, los sectores gobierno y energía son las dos principales industrias que sufren mas ciberataques. Seguidos por los sectores de comunicaciones, banca y finanzas. (*Ver anexo 1. Gráfica 6*).

Se identificó al *phishing* como la principal amenaza que utilizan los atacantes que intentan vulnerar los sistemas tecnológicos de las infraestructuras críticas. El phising (no existe traducción técnica, el equivalente al español seria “pescar”) es un tipo de ataque, el cual mediante correos electrónicos, se dirige al usuario a sitios que simulan ser de empresas o corporaciones confiables. Si el usuario no se percata que es un sitio falso, corre el riesgo de suministrar información sensible para él o para la organización que trabaja, como por ejemplo: nombre de usuario, contraseña, número de tarjeta de crédito o cualquier otro dato confidencial. Esta información obtenida por ciberdelincuentes mediante engaños la utilizan para realizar estafas financieras o para conseguir acceso no autorizado a sistemas informáticos que

controlan las infraestructuras críticas. (*Ver anexo 1. Gráfica 7*)

Una de las conclusiones de dicho informe contempla algo que es de interés para nuestro país y refleja cuál es la situación política y tecnológica del mismo, cuando dice: “Si bien las organizaciones de América han hecho un buen trabajo para proteger la infraestructura crítica contra los ataques, se acerca un punto crítico. Debido a que la frecuencia y la sofisticación de los ataques continuarán o se agravarán y se enfocarán no sólo en afectar a la infraestructura crítica sino también en comprometer la información vital que pudiera usarse en el futuro, los defensores pronto podrían no tener el apoyo necesario para prevenirlos. La falta de financiamiento y de liderazgo gubernamental en esta área deja a los defensores sintiéndose cada vez más solos. Más que eso, los gobiernos de la región necesitan tender la mano a los encargados de la infraestructura crítica que buscan ayuda y guiarlos para ofrecer mejor protección contra los crecientes ataques a este sector crucial”.[157]

Este es el panorama ante el cual se enfrenta la región; no es muy alentador.

En materia presupuestaria existe un abandono total en fortalecer el ciberespacio. (*Ver anexo 1. Gráfica 8*). Esto explica por qué las instituciones encargadas de administrar infraestructura criticas el 40% considera estar “algo preparadas”; y que el 34% exprese que se encuentran “no preparada” para afrontar un incidente cibernético (*Ver anexo 1. Gráfica 9*). A esto se suma la falta de confianza generalizada de las instituciones privadas e incluso públicas a los esfuerzos del gobierno de abordar el tema de ciberseguridad. Esta situación explica por qué el 60% expresó que su organización “no participa” en los esfuerzos de gobierno por fortalecer la seguridad de infraestructuras críticas. (*Ver anexo 1. Gráfica 10*)

---

[157] Ídem.

Un marco legal contra el ciberdelito, políticas y estrategias de ciberseguridad, fortalecer la institucionalidad, adherirse a convenios internacionales contra el cibercrimen, realizar alianzas público-privadas y ejecutar proyectos tecnológicos estratégicos de país; son los ejes que se proponen en el siguiente capítulo como parte de un modelo de ciberseguridad nacional para protección de infraestructuras críticas, que pretende cambiar la realidad actual en la que los ciberataques representan una amenaza real a la seguridad nacional de Guatemala.

CAPÍTULO TRES

3. Modelo de Ciberseguridad Nacional para la Protección de Infraestructuras Críticas

Este modelo se refiere al conjunto de leyes, convenios internacionales, políticas, estrategias, planes, estándares e instituciones que el país debe poseer para garantizar la ciberseguridad de sus infraestructuras críticas. El presente capítulo desarrolla el modelo nacional de ciberseguridad para Guatemala, el cual consiste en los ejes: a) Legislación, Institucionalidad, Políticas y estrategias, cooperación internacional, proyectos tecnológicos estratégicos y alianzas público-privado. El objetivo principal de este modelo es reducir el riesgo de ciberseguridad en las infraestructuras críticas a un nivel aceptable. En el capítulo dos se analizó la creación del comando de informática y tecnología del Ministerio de la Defensa, por lo que hace referencia al mismo en términos de ciberdefensa.

El modelo de ciberseguridad nacional debe ser el marco común técnico-jurídico que sirva como base para dotar al país de herramientas en el combate al ciberdelito.

En este trabajo se expone un modelo basado en la legislación guatemalteca, identifica brechas de alta prioridad y propone implementación de nueva legislación, institucionalidad, políticas, estrategias y proyectos especialmente dirigidos a desarrollar recurso humano, estándares, buenas prácticas enfocadas a fortalecer el ciberespacio para garantizar la protección de las infraestructuras críticas del país. Por ello, es un modelo con un costo admisible y que es factible de implementar.

Como se ha expuesto en el capítulo dos, las consecuencias económicas para el país cuando se han explotado las vulnerabilidades de las plataformas informáticas de las entidades encargadas de recaudar impuestos han sido desastrosas.

La seguridad democrática se ha visto comprometida con el caso reciente del sistema informático del tribunal supremo electoral.

La agenda nacional de riesgos y amenazas menciona que los ciberataques ya constituyen una amenaza a la seguridad nacional.

El modelo utiliza la institucionalidad actual, vinculada con funciones específicas de institucionalidad propuesta, que se complementa y fortalece mutuamente.

La Organización de los Estados Americanos menciona: “Los programas de ciberseguridad más exitosos son aquellos que no se basan simplemente en la aplicación de controles técnicos, sino que definen una estrategia, un marco, para abordar cada una de las funciones esenciales de ciberseguridad: identificar el contexto, proteger los sistemas y activos, detectar los desvíos, responder ante incidentes y recuperar las operaciones del negocio” [158]

El presente capítulo pretende exponer cuáles deberían ser las herramientas para que el país atienda integralmente las amenazas cibernéticas a su seguridad nacional.

3.1 Marco jurídico en el modelo de ciberseguridad Nacional

Como se analizó en el capítulo uno del presente trabajo, Guatemala carece de un marco jurídico adecuado para el combate al ciberdelito. Únicamente aparecen figuras coincidentes de delitos en el Código Penal, en los artículos 274, 294 y 295 y algunas leyes que mencionan la obligación del Estado de recolectar, resguardar y

[158] *Ciberseguridad Marco NIST Edición 5.* Organización de los Estados Americanos. 2019. Consultado en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf. Consultado el 26 de enero 2020.

distribuir información. Es claro que el Estado guatemalteco no está preparado en el marco jurídico para garantizar la ciberseguridad de las infraestructuras críticas.

Es urgente que se realice un consenso entre los tres poderes del Estado: Ejecutivo, Legislativo y Judicial, sector empresarial privado, academia y sociedad civil, para que se apruebe una ley en contra del ciberdelito. Como se especificó en el capítulo uno, existen las propuestas 4055, 5254 y, recientemente, la 5601. Las tres propuestas basan su contenido en el convenio de Budapest, el convenio internacional más efectivo en contra del ciberdelito. Unas resaltan algunos temas más que otras, pero el tiempo ha demostrado que cualquiera de dichas propuestas está vigente y sería un buen inicio para que constituya la piedra angular sobre la cual el país desarrolle capacidades de defensa y combate al ciberdelito.

Este trabajo ha demostrado la profunda necesidad de contar con legislación orientada a proteger los sistemas informáticos de las infraestructuras críticas. En el marco de un modelo de ciberseguridad nacional se le considera la base, sin la cual todo esfuerzo por parte de los tres poderes del Estado, iniciativa privada nacional o internacional está condenado al fracaso.

Por esa razón en la presente propuesta se prioriza el marco jurídico. A continuación, se presenta la tríada de leyes que se estima básica para garantizar la seguridad tecnológica en las infraestructuras críticas.

3.1.1 Ley contra el ciberdelito

El primer paso es tipificar el ciberdelito en Guatemala. Las tres propuestas de leyes contra el ciberdelito mencionadas anteriormente adicionan tipos de delitos que aún no se encuentran tipificados en el código penal guatemalteco; algunos de ellos son: Acceso ilícito, Interceptación Ilícita, Ataque a la integridad de los datos, Ataque a la integridad del sistema; regulan delitos considerados dentro de los delitos propiamente denominados informáticos, siendo éstos: Falsificación informática,

Apropiación de Identidad ajena; Abuso de dispositivos, Fraude informático. También se incorporan el Delito de acoso cibernético y engaño pederasta.

El principio de derecho penal *Nullum crimen, nulla poena sine praevia lege,* es un aforismo en latín que se traduce como "Ningún delito, ninguna pena sin ley previa". Al no existir lineamientos en materia procesal, las instituciones encargadas de la seguridad nacional, de investigación criminal y las de impartir justicia no pueden invertir tiempo y presupuesto en fortalecer su capacidad por medio de procesos, personal y tecnología orientado a combatir el ciberdelito.

Es urgente, tal como la iniciativa de ley 5601 menciona en sus considerandos, “En vista de que los delitos informáticos han tenido mayor incidencia en los últimos años y se han convertido en ilícitos transnacionales, se hace necesario contar con un instrumento jurídico penal que contenga las figuras penales necesarias para encuadrar los hechos ilícitos además de lograr la persecución penal de manera coordinada a nivel internacional y contar con el apoyo de las entidades de carácter internacional para lograr una respuesta inmediata, así como el monitoreo constante para protección de los usuarios ante los delitos informáticos”.[159]

En este sentido, Guatemala tiene un camino bastante avanzado con las tres propuestas que han sido presentadas al Congreso de la República. Ninguna ley es perfecta y siempre será necesario realizarle algún ajuste, según la dinámica social y tecnológica cambie y avance. La urgencia de la aprobación de alguna iniciativa es más sentida que nunca. Guatemala está atrasada en el combate al cibercrimen, y de postergarse más la aprobación de esta ley, las consecuencias negativas para la

[159] *Iniciativa de Ley de Prevención y Protección contra la Ciberdelincuencia 5601*. Congreso de la Republica. consultada en: https://www.congreso.gob.gt/detalle_pdf/iniciativas/5614. Consultada el 16/01/2020

seguridad nacional y la cooperación en mantener la seguridad internacional podrán verse en corto plazo.

Esta ley deberá aportar lo siguiente:

1) Instituciones responsables de la ciberseguridad en Guatemala.
2) Creación de un Equipo de respuesta ante emergencias informáticas (CSIRT, por sus siglas en inglés).
3) Tipificación del ciberdelito y su clasificación según sus medios y sus fines.
4) Ajustarse a las Normas penales y derecho procesal vigentes en el país.
5) Cumplir con las tipificaciones de ciberdelitos contenidos en el convenio de Budapest.
6) Orientada a cooperación nacional e internacional.
7) Protección de datos personales en Internet.
8) Definir tiempos de respuesta de operadores de telecomunicaciones para suministrar información relevante solicitada en procesos de investigación de ciberdelitos.
9) Creación del Instituto Guatemalteco de Ciberseguridad.
10) Definir el ámbito de cooperación público-privada en el marco del combate al ciberdelito.

3.1.2 Ley de protección a las infraestructuras críticas

Después de dar el primer paso de tipificar el ciberdelito, es necesario proponer, analizar, presentar y aprobar una Ley orientada a la protección de las

infraestructuras críticas. El espíritu de esta ley deberá ser la conservación y funcionamiento de las infraestructuras críticas, física y tecnológicamente.

Esta ley deberá realizar los siguientes aportes:

1) Creación de una comisión nacional para la protección de infraestructuras críticas como un órgano adscrito al consejo nacional de seguridad
2) Sistema de documentos que definan las políticas, estrategias, planes y agendas que especifiquen las medidas para la protección de infraestructuras críticas.
3) Catálogo nacional de infraestructuras críticas. Debe definir los entes encargados de efectuarlo tomando en cuenta las características de las infraestructuras existentes. (Este documento es confidencial)
4) Gestión de incidentes informáticos. Para ello es indispensable la creación del CSIRT-gt como centro de respuesta ante incidentes cibernéticos.
5) Definir el ámbito de cooperación público-privada en el marco de la protección de las infraestructuras críticas.
6) Orientada al cumplimiento de las obligaciones adquiridas en tratados y convenios internacionales de los cuales el país ha sido signatario en materia de ciberseguridad a infraestructuras críticas.
7) Orientada a definir una cultura de ciberseguridad basada en estándares que deberán cumplir operadores privados e instituciones estatales.

Esta ley deberá proteger lo que la comisión de catalogación de infraestructura crítica defina como tal. El capítulo dos presentó un catálogo preliminar que enlista los siguientes temas: sector telecomunicaciones, energético, transportes, administración, salud.

3.2 Institucionalidad clave propuesta

El marco jurídico debe dar paso a fortalecer y crear institucionalidad. En el modelo de ciberseguridad propuesto se contempla un marco institucional robusto y apegado a la legislación de la Ley marco del consejo nacional de seguridad.

3.2.1 Comisión nacional de ciberseguridad

Esta comisión sería la responsable de atender el tema de ciberseguridad a alto nivel dentro del consejo nacional de seguridad, el cual está facultado para promover la creación de la comisión nacional de ciberseguridad. Dentro de sus funciones se encuentra "conocer y recomendar sobre aquellos asuntos de carácter estratégico para la seguridad del país"[160], también, "promover la actualización del marco normativo e institucional aplicable a las actividades de seguridad" [161]. Desarrollará sus funciones dentro del ámbito de la secretaría técnica, quien será la responsable del apoyo logístico y administrativo.

La creación de la comisión de ciberseguridad está plenamente justificada por los convenios internacionales de los que el país ha sido signatario, expuestos en el capítulo uno. En cada uno de ellos el país se ha comprometido a proteger las infraestructuras críticas mediante el fortalecimiento de su ciberespacio, en búsqueda de garantizar su seguridad nacional y cooperar con la seguridad internacional.

La agenda nacional de riesgos y amenazas coloca los ciberataques como una de las principales amenazas para el país.

---

[160] *Ley marco del Sistema Nacional de Seguridad.* Congreso de la República. 2008. Art. 10. Literal e

[161] Ibídem. Literal f

Al igual que otras comisiones, el objetivo de su creación será el de "Asesorar al Consejo Nacional de Seguridad".[162]

Las principales funciones de la comisión serán:

1) Formular y proponer la Política Nacional de Ciberseguridad y protección a las infraestructuras críticas.
2) Formular y proponer la Estrategia Nacional de Ciberseguridad y protección a las infraestructuras críticas.
3) Asesorar a la Secretaría Técnica del Consejo Nacional de Seguridad en materia de Ciberseguridad. Según el artículo 17, literal c, una de las funciones de la secretaría técnica es: "Dar seguimiento a aquellas políticas, planes y directivas que se determinen por el consejo nacional de seguridad"[163].
4) Formular y proponer el libro blanco de alianza-público privado en materia de ciberseguridad.
5) Formular y proponer el plan nacional de ciberseguridad de infraestructuras críticas.
6) Creación y definición de un marco nacional de ciberseguridad integral.
7) Asesorar al Consejo Nacional de Seguridad sobre propuestas de creación y actualización de leyes en materia de ciberdelito y ciberseguridad para el país.
8) Crear mesas de trabajo para catalogar y actualizar el listado de la Infraestructura Crítica del país.

[162] Ibídem. Art. 13
[163] *Reglamento de la Ley marco del Sistema Nacional de Seguridad*. Congreso de la República de Guatemala. 2008. Art. 17

9) Promover megaproyectos de implementación tecnológica que fortalezcan la ciberseguridad en el país.

Esta comisión deberá diseñar una estrategia de país para la adhesión de Guatemala al convenio de Budapest.

Los miembros de esta comisión serán los miembros mencionados en el artículo 9 de la ley marco del sistema nacional de seguridad: Vicepresidencia de la República, Ministerio de Relaciones Exteriores, Ministerio de Gobernación, Ministerio de la Defensa Nacional, Secretaría de inteligencia Estratégica del Estado y Procurador General de la Nación.[164] Adicionalmente, se deberá invitar a un representante de la comisión de seguridad del Congreso de la República, un representante nombrado por el Organismo Judicial, la academia, sector privado y el Instituto Guatemalteco de Ciberseguridad.

3.2.2 Instituto Guatemalteco de Ciberseguridad

Su misión deberá ser promover la seguridad del ciberespacio de Guatemala, en todos sus niveles. Ello, por medio de: brindar servicios, educación, alianzas público-privadas, crear estándares de ciberseguridad que cumplan las instituciones y sean aplicables al sector privado, así como ser el eje sobre el cual se le dé seguimiento y cumplimiento a los compromisos internacionales adquiridos.

Será el responsable de la implementación del Centro de respuesta ante eventos cibernéticos (CSIRT-gt), el cual deberá operar 24 horas los 7 días de la semana, operativizando protocolos definidos en los entes encargados internacionales. Actuará como enlace oficial de los programas internacionales, 24/7, First, y si el país se adhiere al convenio de Budapest, será el punto de contacto del programa Glacy +.

[164] Ibídem. Art. 9

Actuará como ente de monitoreo y seguimiento en el cumplimiento de políticas, estrategias y planes de ciberseguridad, junto a la secretaría técnica.

Deberá ser una entidad que promueva la ciberseguridad a nivel técnico, jurídico e institucional, en los ámbitos público, privado e internacional.

Sus principales funciones deberán ser:

1) Brindar servicios de ciberseguridad a nivel institucional y al sector privado.

2) Fomentar la cultura de ciberseguridad a los guatemaltecos, sin importar su edad.

3) Diseñar, implementar y operativizar el Centro de respuesta ante eventos cibernéticos (CSIRT-gt).

4) Fomentar la cooperación internacional en materia de ciberseguridad, con los distintos organismos internacionales rectores del tema, como, por ejemplo: Comisión Interamericana de Telecomunicaciones (OEA), Comité Interamericano contra el Terrorismo (OEA), Unión internacional de Telecomunicaciones de Naciones Unidas (ONU), Consejo de Europa y entidades rectoras de la comunidad internacional.

5) Promover alianzas público-privadas a niveles de: sector telecomunicaciones, empresas que ofrecen servicios de ciberseguridad, sector académico, empresas productoras de hardware y software de seguridad digital.

6) Apoyar técnicamente iniciativas de legislación para la ciberseguridad.

7) Operativizar políticas, estrategias, estándares, buenas prácticas en materia de ciberseguridad en el Estado, sector privado y comunidad internacional.

8) Brindar capacitaciones a distintos niveles, en ciberseguridad, al sector público y privado.

9) Implementar el marco nacional de ciberseguridad a nivel institucional, privado e internacional.

10) Orientar a la academia en cuanto a su oferta de educación en ciberseguridad.

11) Orientar al Estado en lo referente a la capacitación en distintos niveles de ciberseguridad al recurso humano de las instituciones.

12) Participar en las mesas de trabajo de la comisión nacional de ciberseguridad, para la catalogación de infraestructuras críticas del país.

13) Elaborar análisis que contenga posibles actualizaciones a las leyes contra el ciberdelito y de protección a las infraestructuras críticas.

14) Actualización constante del modelo integrado de ciberseguridad nacional.

El Instituto Nacional de Ciberseguridad deberá implementar una unidad o dirección de investigación y desarrollo para explorar modelos, estándares, buenas prácticas y tecnologías innovadoras para la protección de la información y sistemas informáticos en el país.

Puede estar adscrito al Ministerio de Gobernación, si el enfoque principal que se le dé a este instituto es el de seguridad nacional. Pero en la era digital actual, también puede ser fuente de reactivación económica, mediante generación de recurso humano, así como en el desarrollo de estándares y metodologías de seguridad de la información y ciberseguridad, por lo que también podría ser adscrito al Ministerio de Economía. La temática nos llevaría a una decisión obvia: que debería ser adscrito a la Secretaría Nacional de Ciencia y Tecnología (SENACYT), que es una instancia creada y está en funciones. Lamentablemente, el abandono

presupuestario, el poco interés político y el escaso protagonismo de los últimos años de la SENACYT no la hacen recomendable para una tarea tan crítica como lo es la ciberseguridad del país.

Es conocida la realidad de la Secretaría Nacional de Ciencia y Tecnología (SENACYT) en Guatemala. Su presupuesto para el año 2017 fue de Q.33 millones, y en el año 2018 Q. 28 millones. [165] Esto la hace una secretaría limitada de acciones. Aún con la baja asignación de recursos que actualmente tiene, la SENACYT debería ser más proactiva en temas de coordinación interinstitucional y en proponer proyectos estratégicos tecnológicos.

3.2.3 CSIRT-gt

Un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés) se define como un equipo o una entidad dentro de una agencia que proporciona servicios y apoyo a un grupo particular (la comunidad de destino), con el fin de prevenir, manejar y responder a los incidentes de seguridad de la información. Estos equipos están compuestos, generalmente, por especialistas multidisciplinarios que actúan de acuerdo con los procedimientos y políticas predefinidos para responder rápida y eficazmente a los incidentes de seguridad y para reducir el riesgo de ataques cibernéticos. Hay cientos de CSIRT en el mundo, que varían en su misión y alcance. Una de las principales formas de clasificar a los CSIRT es agruparlos por el sector o la comunidad a los que sirven[166].

En Guatemala han existido iniciativas desde el Estado, específicamente del Ministerio de la Defensa, de implementar grupos de este tipo. Se ha fallado en el intento y lo único que tenemos es, según dice el informe de Ciberseguridad de la

---

[165] *Sistema de Contabilidad Integrada Ministerio de Finanzas*. Disponible en: http://www.minfin.gob.gt/index.php/?option=com_content&view=article&id=98&Itemid=697. Consultado el 12 de marzo 2019

[166] Ciberseguridad, ¿Estamos preparados en América Latina y el Caribe? OEA/BID. Pág. 13. Disponible en: https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe. Consultado el 14 de agosto 2018

Organización de los Estados Americanos del año 2016: “Aunque entidades gubernamentales líderes han comenzado a darle prioridad a los asuntos de seguridad cibernética y evaluar los riesgos nacionales, … su principal entidad de seguridad cibernética es el equipo de respuesta a incidentes de seguridad informática nacional, el Csirt-gt, un equipo ad hoc que históricamente ha operado bajo el Ministerio de la Defensa.

El CSIRT-gt ha recibido capacitación de la OEA y otras instituciones internacionales. Recientemente, el Ministerio de Gobernación también ha mostrado interés en ir avanzando en los temas de seguridad cibernética en Guatemala.[167]”.

Existen empresas que suministran el servicio de CSIRT a la iniciativa privada guatemalteca, como: Ciberseg[168], Develsecurity[169] y Widefedense[170].

Como manifiesta el informe de la OEA, el Ministerio de Gobernación también ha hecho esfuerzos en este tema. Estableció en 2018, un grupo de expertos en ciberseguridad que suministran soporte a las instituciones.[171] También realizan monitoreo de actividades sospechosas en las redes de las instituciones que solicitan la instalación de un dispositivo que analiza el tráfico. La falta de institucionalidad y de respaldo legal hace que estas excelentes iniciativas dejen de existir; como muestra, la lección aprendida del CSIRT-gt implementado en el Ministerio de la Defensa.

Según el Instituto de Ingeniería de Software de la Carnegie Mellon University, los servicios que debe prestar un CSIRT, se pueden agrupar en tres categorías: los reactivos, los proactivos y los de gestión de calidad de la seguridad.

---

[167] Ibídem pág. 76
[168] https://www.cyberseg.com/. Consultado el 27 de enero 2020
[169] https://devel.group/. Consultado el 27 de enero 2020
[170] https://www.widefense.com/. Consultado el 27 de enero 2020
[171] https://mingob.gob.gt/inauguaran-centro-de-respuesta-a-incidentes-ciberneticos/. Consultado el 27 de enero 2020

- **Los servicios reactivos**. Estos servicios son activados por un evento o solicitud, como un informe acerca de un host comprometido, código malicioso generalizado, la vulnerabilidad de software, o algo que fue identificado por un sistema de detección de intrusos o sistema de registro. Los servicios reactivos son el componente principal de trabajo CSIRT.

- **Los servicios proactivos**. Proporcionan asistencia e información para ayudar a preparar, proteger y asegurar los sistemas constituyentes en previsión de ataques, problemas o eventos. El rendimiento de estos servicios se enfoca directamente a reducir el número de incidentes en el futuro.

- **Servicios de gestión de calidad de la seguridad**. Estos servicios aumentan los servicios existentes y bien establecidos, que son independientes de gestión de incidentes y se llevan a cabo tradicionalmente por otras áreas de la organización, tales como los departamentos de TI, auditoría o formación. Si el CSIRT realiza o coadyuva con estos servicios, su punto de vista y la experiencia pueden proporcionar información para ayudar a mejorar la seguridad general de la organización e identificar los riesgos, las amenazas y las debilidades del sistema. Estos servicios no son generalmente proactivos, sino que contribuyen indirectamente a reducir el número de incidentes.[172]

3.2.4 Fortalecimiento a la Sección contra el ciberdelito en PNC

En el año 2016 inició sus funciones la sección contra el ciberdelito en la policía nacional civil. Es excelente iniciativa el que una institución cuyo mandato es la seguridad interna cuente con una unidad que investigue casos y delitos en los cuales la tecnología ha sido el medio. Se ha fortalecido a través de alianzas con la

[172] http://www.cert.org/incident-management/services.cfm. Consultado 18 de julio 2018

iniciativa privada, que ha provisto de plataformas de investigación. Microsoft firmó una alianza con la PNC para proveer acceso a su “unidad de crimen digital” con sede en Washington, EE. UU.[173]

En su primer año, esta sección recibió 190 denuncias e investigaba 25 casos de ciberdelitos. La legislación actual no tipifica muchos de los delitos cibernéticos, lo que limita su actuación. Esto tiene efecto de contar con un acceso limitado a las entidades y herramientas de cooperación internacional en la materia. En el marco nacional de ciberseguridad, esta unidad se deberá apoyar tecnológicamente y con estándares establecidos por el Instituto Guatemalteco de Ciberseguridad.

3.2.5 Fortalecimiento a la Unidad contra la pornografía infantil del Ministerio Público

La fiscalía contra la trata de personas cuenta con una unidad de investigación de delitos sexuales y pornografía infantil. Los medios electrónicos y redes sociales son los utilizados para distribuir pornografía infantil, por lo que esta unidad tiene tareas de informática forense, y utiliza el sistema 24/7 para investigaciones en casos en los que las redes sociales fueron el medio para contactar a las víctimas.

En el marco de implementación del modelo nacional de ciberseguridad, las leyes y el Instituto Guatemalteco de Ciberseguridad serán quienes suministren las herramientas técnicas y jurídicas para su mejor funcionamiento.

3.2.6 Creación de un Ministerio de Tecnología

Es sumamente necesaria la creación de una institución que marque las políticas y estrategias del desarrollo económico del país en materia tecnológica. En el país, a raíz de que la SENACYT no ha cumplido con los objetivos de su creación, ello ha provocado que la investigación y desarrollo, educación, generación de

[173] https://www.prensalibre.com/guatemala/justicia/pnc-se-alia-a-microsoft-contra-el-ciberdelito/. Consultado el 26 de enero 2020

empleos, gestión de la cooperación internacional, cumplimiento de obligaciones internacionales adquiridas, consolidación y crecimiento de la economía digital, estén totalmente dispersos en cuanto al tema de tecnología.

En la era digital o del conocimiento, Guatemala no tiene un rumbo tecnológico, por lo que, bajo la premisa de que es imposible proteger lo que no está ordenado, es indispensable y estratégico que exista una institución que marque ese rumbo del país.

Este es el complemento perfecto para que Guatemala aproveche las tecnologías actuales, y así mejorar la calidad de vida de sus ciudadanos.

Será el ente rector de orientar, ampliar y mejorar la oferta académica respecto de y tecnología en el país, así como el punto de contacto para la comunidad internacional que desee cooperar con proyectos tecnológicos.

La tecnología tendría una voz en el gabinete de gobierno. Este Ministerio deberá ser el responsable de implementar la digitalización del Estado e impulsar leyes de gobierno electrónico.

Deberá ser, también, el encargado de impulsar los megaproyectos estratégicos tecnológicos prioritarios para el país, los cuales serán orientados a la modernización y reducción de costos de las instituciones de gobierno.

Las funciones que se plantea que deberá cumplir el Ministerio de Tecnología son las siguientes:

a) Promover iniciativas de leyes referentes a investigación y desarrollo, inversión e integración tecnológica.

b) Implementar un centro nacional de datos, el cual sea utilizado por todos los ministerios del Estado de Guatemala, que cuente con servidores, medios de almacenamiento masivos, conectividad vía fibra óptica, redundancia de

energía eléctrica, Firewalls, aire frío, piso elevado. Esto reducirá las grandes inversiones que cada uno de los ministerios realiza para construir y mantener sus propios Centros de Datos para resguardar su información.

c) Impulsar el cumplimiento de las Políticas Nacionales de Seguridad Digital, entre las cuales deberá estar la Política Nacional de Ciberseguridad orientada a la protección de infraestructura crítica de Guatemala.

d) Liderar, junto al Ministerio de Economía, iniciativas para el desarrollo económico del país, mediante el impulso de desarrollo tecnológico, a través del apoyo a empresas y emprendedores tecnológicos.

e) Liderar la implementación de gobierno electrónico en Guatemala. Coordinar acciones, proveer capacitaciones de tecnología y buenas prácticas a instituciones estatales, promover las alianzas público-privadas, facilitar el acceso a servicios públicos de la población por medio de la tecnología.

f) Trabajar, en materia de ciberseguridad, estrechamente con el Instituto Guatemalteco de Ciberseguridad.

g) Promover la interconectividad de los sistemas de las instituciones del país, para facilitar trámites y consultas realizados por instituciones y personas.

Andrés Oppenheimer, en su libro *Crear o Morir,* menciona que vivimos en la economía global del conocimiento, en donde las naciones que más crecen o más reducen la pobreza, son las que producen innovaciones tecnológicas.[174]

También menciona que, hoy en día, la prosperidad de los países depende cada vez menos de sus recursos naturales y cada vez más de sus sistemas

[174] Oppenheimer, Andrés. *Crear o Morir. La esperanza de América Latina y las Cinco Claves de la Innovación*. Editorial Debate. Madrid.2014.

educativos, sus científicos, sus innovadores. Los países más exitosos no son los que tienen más petróleo, o más reservas de agua. O más cobre o más soja, sino los que desarrollan las mejores mentes y exportan productos con mayor valor agregado. Un programa de computación exitoso, o un nuevo medicamento, o un diseño de ropa novedoso valen más que toneladas de materia prima.[175]

Algunos beneficios de contar con un Ministerio de Tecnología son: a) servicios públicos informáticos eficientes y ágiles a disposición del usuario, b) incrementar los beneficios sociales y económicos que derivan de la incorporación de las TICs seguras a la vida cotidiana, c) priorización de la eficiencia de las TICs utilizadas por la ciudadanía, empresas y gobierno, d) beneficiar a la población en general con el despliegue de redes y servicios que garantizan la conectividad digital, e) estimular el uso educativo de las TICs, permitiendo una mayor calidad en la evaluación y monitoreo de resultados, f) consolidar la inserción del país en el ámbito de la integración regional e internacional, necesario para el comercio digital e intercambio electrónico de información.

3.3 Políticas y Estrategias de Ciberseguridad

Las políticas públicas y estrategias son los instrumentos estatales que exponen cómo el Estado dará solución a un problema público. En el marco de seguridad nacional, la ciberseguridad requiere de un abordaje integral. La implementación de un modelo nacional de ciberseguridad requiere de estas herramientas para garantizar que se cumplan los objetivos trazados. Se plantea la creación y fortalecimiento de políticas públicas y estratégicas.

[175] Ídem

3.3.1 Estrategia Nacional de Ciberseguridad

El uno de marzo de 2016, el Ministerio de Gobernación solicitó, en oficio Ref. DM-256-16 /FMRL-fdl, al Ministerio de Relaciones Exteriores, el apoyo de la Organización de los Estados Americanos (OEA) por medio de una Misión de Asistencia Técnica Legislativa con funcionarios Gubernamentales de nivel superior, de la cual debería derivarse la elaboración e implementación de una Estrategia de Ciberseguridad Nacional.

Anteriormente Guatemala había participado en el Decimosexto Período Ordinario de Sesiones del Comité Interamericano Contra el Terrorismo (CICTE), en Washington, D.C, Estados Unidos de América, para darle seguimiento a las actividades propuestas. (*Ver Anexo 3. Imagen 3)*

El 25 de mayo, en oficio SMS/DPS/118-16, Paulina Duarte, Secretaria Interina de la Secretaría de Seguridad Multidimensional, responde a dicha solicitud: “Específicamente el Gobierno de Guatemala solicita la cooperación de la Secretaría de Seguridad Multidimensional en organizar una Misión de Asistencia Técnica para apoyar a la elaboración de la Política nacional sobre la materia y elaboración e implementación de la Estrategia Nacional. Me alegra mucho confirmarle el interés y disponibilidad de la Secretaría de Seguridad Multidimensional, a través del Programa de seguridad Cibernética de la secretaría del Comité Interamericano contra el Terrorismo (CICTE), para apoyar los esfuerzos de Guatemala en este sentido”. (*Ver Anexo 3. Imagen 4)*

Con la respuesta oficial de parte de la Organización de los Estados Americanos, Guatemala se garantizaba el apoyo técnico-jurídico en la elaboración de la Estrategia Nacional de Ciberseguridad. De esto se derivaron las siguientes tres misiones que la OEA ha realizado al país, hasta la fecha que se redacta la presente tesis.

También se conformó el Comité Nacional de la Estrategia Nacional de Ciberseguridad, estando compuesto por: la Secretaría Técnica Nacional de Seguridad, Ministerio de Defensa, Ministerio de Gobernación, Policía Nacional Civil, Ministerio de Relaciones Exteriores, Ministerio de Finanzas y Ministerio Público.

Estas instituciones formarían el grupo encargado de encausar y darle seguimiento a la Estrategia Nacional. Se giraron cartas en las cuales se explicaba el motivo de la conformación del comité, y que cada institución debería nombrar un representante; la respuesta fue afirmativa por parte de todas las instituciones invitadas.

En reuniones llevadas a cabo entre el Ministerio de Gobernación y la Secretaría Técnica, dicho ministerio propuso verbalmente que la estrategia nacional de Ciberseguridad pasara a formar parte de un capítulo de la Política Nacional de Seguridad. Con ello se fortalecería, a nivel nacional, la Seguridad Cibernética, en virtud de que la actual versión de la Política Nacional no cubre los aspectos tecnológicos para la seguridad nacional. La propuesta no fue aceptada por parte de la Secretaría Técnica del Consejo Nacional de Seguridad.

Durante la segunda visita de los represented del CICTE de la OEA al país, la embajada de España, el gobierno de Canadá y la embajada de la OEA en Guatemala fueron actores principales como apoyo técnico y financiero en el proceso de construcción de la estrategia nacional de ciberseguridad, en el marco de la construcción del primer borrador de esta. La actividad se desarrolló en la Antigua Guatemala, en el Centro de Cooperación Española.

La nota de prensa de la Red de gobierno electrónico de América Latina y el Caribe (Red GEALC) señaló en esa ocasión: “El taller para el Desarrollo de la Estrategia Nacional de Ciberseguridad de Guatemala, coordinado con el apoyo del Ministerio de Gobernación (MINGOB) y el Ministerio de Relación Exterior (MINEX) de Guatemala, se centró en la organización de mesas de trabajo temáticas con el objetivo de reunir representantes de diferentes sectores para dialogar e identificar

las prioridades del país en materia de ciberseguridad en el país. Cabe señalar que el Gobierno de Guatemala conformó un Comité Ejecutivo interministerial para liderar este proceso."

En ese evento estuvieron representadas las empresas privadas, representantes de la banca, empresas del sector energético, instituciones estatales, sociedad civil y universidades.

Se definieron líneas estratégicas sobre las cuales se desarrollaría la Estrategia Nacional de Ciberseguridad de Guatemala. El artículo de la RED GEALC sigue diciendo: "El Viceministro de Gobernación de Guatemala, Walter Girón, concluyó la ceremonia de apertura enfatizando que la ciberseguridad debe ser tratada como un asunto estratégico para la nación, el cual requiere el involucramiento de múltiples partes interesadas. El Viceministro de Gobernación destacó que es fundamental que la metodología para el desarrollo de la estrategia nacional de ciberseguridad tenga en cuenta aspectos tan importantes como lo son el desarrollo de la economía digital y los derechos humanos.

Débora Chatsis, embajadora de Canadá en Guatemala, comentó que han apoyado las propuestas y se ve muy bien el avance en tema de seguridad cibernética.[176] En el proceso se llevaron a cabo seis mesas de trabajo para conocer las opiniones y necesidades para combatir los delitos cibernéticos[177]

La Embajadora de la OEA en Guatemala Milagro Martínez señaló que la Secretaría General de la OEA y la Secretaría del CICTE continuarán acompañando los esfuerzos que se requieran para adoptar la Estrategia Nacional de Ciberseguridad en el país, e instó a todos los actores nacionales a tener una activa

[176] http://mingob.gob.gt/realizan-primer-borrador-de-la-estrategia-nacional-de-ciberseguridad/. Consultado el 25 de enero de 2018
[177] Ídem

participación en un tema que es fundamental tanto para la seguridad, como para el desarrollo socioeconómico del país."[178] *(Ver Anexo 3. Imagen 5)*

En el año 2019, el gobierno de Guatemala, por medio del Ministerio de Gobernación, hizo público el lanzamiento de la estrategia nacional de ciberseguridad, con el acompañamiento de la Organización de los Estados Americanos (OEA). Ese esfuerzo fue la culminación de lo iniciado en 2016 desde el viceministerio de tecnología del Ministerio de Gobernación. La estrategia de Ciberseguridad se enfoca en los ejes: Marcos legales, Educación, Cultura y Sociedad y Tecnologías de la Información.

Es un gran avance y Guatemala debe poner el tema de ciberseguridad en los reflectores de la seguridad nacional. Estamos a tiempo de iniciar con buen pie el combate al cibercrimen. Nuestras deficiencias que, como país, tenemos de penetración del Internet y digitalización del Estado, deben ser vistas como una oportunidad para colocar cimientos sólidos contra el cibercrimen. Es el primer paso que como país hemos dado hacia la implementación de lo que debería ser un modelo de ciberseguridad en Guatemala.

3.3.2 Plan de protección de infraestructuras críticas

Este plan busca proteger integralmente de ataques físicos y/o cibernéticos a las infraestructuras críticas. Los planes de protección se deben realizar según la categorización de su sector: Sector energético, Telecomunicaciones, Administración pública, además de los que se clasifiquen en el catálogo.

Debe contener las acciones, metas, indicadores, responsables y cronogramas que se utilizarán para cada sector, para los distintos tipos de amenaza,

[178] http://www.redgealc.net/oea-apoya-a-guatemala-en-el-desarrollo-de-su-estrategia-nacional-de-ciberseguridad/contenido/6934/es/, consultado el 14 de nov. 2017

ya sean físicas o cibernéticas, con los responsables directos en caso ocurra un incidente.

El plan debe contener los niveles de seguridad en contra de intromisión física, como cámaras de video vigilancia, sensores de movimiento, sistemas de admisión según el nivel de acceso otorgado al personal y/o visitantes. Los sistemas podrán ser biométricos empleando huella digital o lectura de iris para la verificación de la identidad y otorgar los permisos de ingreso físico autorizados. También se puede considerar sistemas de altavoces generales para avisos a todos los presentes en el edifico o anunciar alguna alerta o alarma.

Las infraestructuras han de contar con un sistema de monitoreo de comunicación, comando, control y computación para analizar información recopilada en los sistemas de control de acceso, cámaras de vigilancia y sensores de movimiento. La inteligencia en la videovigilancia ayuda a los encargados de la seguridad a identificar situaciones que pueden ser posibles problemas de seguridad, como por ejemplo objetos olvidados en sectores sensibles o personas caminando en áreas catalogadas como restringidas o en horarios no permitidos.

Los ataques cibernéticos a las infraestructuras críticas se describieron en el capítulo dos del presente trabajo. Al respecto, los planes de protección deben contener: a) políticas de uso de memorias USB, políticas de uso de contraseñas, políticas de actualización de antivirus, uso de dispositivos para detección de actividad sospechosa dentro de la red, así como información externa como firewalls e ips, política de manejo de contraseñas de los dispositivos de red.

El plan ha de contener protocolos de defensa, identificación, protección y recuperación ante eventos cibernéticos.

Se debe contar con una línea de emergencia destinada para comunicarse con el CSIRT-gt, en caso ocurra una emergencia cibernética.

3.4 Cooperación Internacional

Dada la naturaleza transnacional de los ciberdelitos, lamentablemente ningún país puede afrontar solo el problema. Los ciberdelitos borran las fronteras. Se hacen necesarias alianzas para lograr un combate efectivo. La cooperación puede ser técnica o jurídica.

Se exponen a continuación los instrumentos por medio de convenios o programas candidatos a formar parte del modelo de ciberseguridad nacional.

3.4.1 Convenio de Budapest

Aunque Guatemala no ha suscrito el convenio de Budapest, precisamente por no contar con legislación contra el ciberdelito, se incluye este convenio por ser el más utilizado y efectivo en el combate del Cibercrimen a nivel mundial. Su creador es el Consejo de Europa. Se incluye, también, en virtud de que la Unión Europea ha estado anuente a los llamados de apoyo técnico-jurídico hacia Guatemala. Es necesario resaltar la importancia que reviste el hecho de que Guatemala suscriba el convenio, pues le brindaría herramientas vitales en materia de cooperación internacional, capacitación a personal especializado en ciberseguridad, herramientas tecnológicas, bases de datos actualizadas acerca de posibles ataques y armas cibernéticas utilizadas en territorio de países miembros.

Los países firmantes en América son: Panamá, República Dominicana, Argentina, Canadá, Chile, Costa rica, Paraguay y Estados Unidos; como país invitado está Colombia[179].

El convenio de Budapest ofrece un marco común para el combate del ciberdelito. Esto, por medio de una “política penal común, con objeto de proteger a

---

179 https://es.wikipedia.org/wiki/Anexo:Pa%C3%ADses_firmantes_del_Convenio_de_Cibercrimen#Am%C3%A9rica. Consultado el 5 de enero del 2020

la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional"[180]. Algunos detractores de este convenio alegan que es un convenio muy vago en sus definiciones respecto de los ciberdelitos, y Estados poco transparentes pueden utilizarlo en contra de la población o tipificando como delitos algunas actividades que se consideran de libre emisión del pensamiento.

3.4.2 Guatemala Solicita aprobación para adherirse al Convenio de Budapest

En el año 2017, el Ministerio de Gobernación dirigió un oficio al Ministerio de Relaciones Exteriores solicitando la adhesión de Guatemala al convenio de Budapest. *Ver anexo de 4. Imagen* 4. UNICEF, verbalmente, hizo referencia a que también habían solicitado la adhesión del país, por los beneficios en la protección a niños del Internet y sus peligros, aunque no pasó de ser un oficio de buenas intenciones, pues la adhesión a un convenio internacional debe pasar por la aprobación del Congreso de la República. *(Ver Anexo 4. Contenido del convenio de Budapest)*

3.4.3 Glacy +

Es un proyecto de la Comisión Europea y el Consejo de Europa, de apoyo a los países signatarios del convenio de Budapest, para su implementación. Consiste en apoyo por medio de consultores internaciones que visitan los países que han firmado el convenio. Los tres grandes sectores de apoyo son:

1) Política y estrategias;

2) Capacidades de las instituciones policiales; y

[180] *Convenio sobre la ciberdelincuencia ETS 185*. Preámbulo. Consejo de Europa. 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf. Consultado el 17 de octubre 2019

3) Capacidades de la justicia penal.

- **El Área 1**. Consiste en una revisión, actualización o creación de políticas y estrategias en materia de ciberseguridad para el país.

- **El Área 2**. Se apoya al país signatario por medio de la INTERPOL, Singapur, y se especializa a las fuerzas policiales en materia de manejo de evidencia electrónica, herramientas para detectar pornografía infantil, en línea y responder ante amenazas digitales a la infraestructura de la policía.

- **El Área 3**. Brinda apoyo consistente en capacitación acerca de la aplicación de las leyes nacionales a jueces, abogados, fiscales en toda el área del sector justicia. El organismo judicial y el colegio de abogados serían el público meta de las capacitaciones que se imparten en estos talleres.

Además, suministran acceso a sistemas y bases de datos clasificados para que el país identifique rápidamente las fuentes de pornografía infantil, ataques a infraestructuras críticas, y credenciales para el centro de respuesta cibernética de la INTERPOL.

3.4.4 Programa 24/7

Se trata de una entidad del departamento de justicia de los Estados Unidos que sirve de enlace para entidades de investigación de todo el mundo. Una de sus funciones consiste en gestionar las solicitudes que hacen los organismos de justicia a los grandes de la industria tecnológica como Microsoft, Google, Facebook, Twitter, entre otros.

En Guatemala, el punto de enlace de este programa es el Ministerio Público, quien, por orden de juez competente y por nivel de urgencia, envían solicitudes de información de correos electrónicos, cuentas de redes sociales, historial de conexiones y otros temas. En entrevista con la fiscal general del Ministerio Público

en el año 2016, ella menciona que el nivel de respuesta es muy bajo. Únicamente cuando una vida corre peligro o en casos de secuestro, tienen en ocaciones alguna respuesta.

3.4.5 FIRST

Es una organización que busca la certificación de los CSIRT a nivel mundial. Las empresas o instituciones que se afilian tienen muchas ventajas como: acceder a una amplia base de datos, de atacantes, amenazas y buenas prácticas, bases de datos de conocimiento sobre cómo otros países o empresas han solucionado con éxito determinados casos de ataques a su ciberseguridad. Incluye también foros, talleres y seminarios por Internet dirigidos a los profesionales de ciberseguridad que forman parte de los equipos de respuesta.

El CSIRT-gt debe formar parte de este club internacional para estar actualizado en materia de amenazas y riesgos cibernéticos.

3.5 Proyectos Tecnológicos Estratégicos

Los proyectos tecnológicos presentados a continuación responden a la necesidad del Estado guatemalteco de optimizar los recursos invertidos en las plataformas informáticas en las diferentes instituciones que lo conforman. El Estado adolece de muchas necesidades tecnológicas y pocas son las que se logran satisfacer. Los megaproyectos tienen la ventaja de que se realizará en todos los casos una única inversión, gestión y mantenimiento. Las instituciones no tendrían que invertir de su escaso presupuesto en subsanar las necesidades que los megaproyectos cubren.

En el campo de la seguridad informática serían equipos de personal altamente calificado quienes velen por la implementación de estándares de seguridad de la información para resguardar el almacenamiento, tránsito y procesamiento de la información.

3.5.1 Centro Nacional de Datos

Este proyecto podría recibir el nombre de la "nube" del gobierno de Guatemala. Consiste en un centro nacional de datos que albergue los datos de las instituciones del país. De esa forma se evitaría duplicar la inversión en infraestructura física, seguridad física y lógica, administración de sistemas, sistemas de aire acondicionado, plantas generadoras de energía, piso elevado, sistemas de respaldo de energía (UPS, por sus siglas en inglés). La seguridad física y lógica del centro de datos será administrada por un equipo de expertos en seguridad de la información. Deberá contemplar normas internacionales para garantizar la confidencialidad, integridad y disponibilidad de los datos.

3.5.2 Prestador de Servicios de Certificación de Firmas Electrónicas para el Estado

La firma electrónica es un concepto jurídico, es un equivalente electrónico a la firma manuscrita, que permite garantizar la identidad de la persona que realiza una gestión, así como la integridad del contenido de los mensajes que envía. La autoridad certificadora del Estado de Guerrero, México, define firma electrónica como: "En términos prácticos, la firma electrónica consiste en un conjunto de datos asociados a un mensaje o documento electrónico, que permite garantizar con total seguridad la identidad del firmante y la integridad del texto o mensaje enviado".[181]

La Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto número 47-2008 del Congreso de la República de Guatemala, en su artículo 1, faculta a las instituciones a usar este instrumento tecnológico: "El Estado y sus instituciones quedan expresamente facultados para la utilización de las comunicaciones y firmas electrónicas", pero no se están utilizando, debido a dos razones 1) el alto costo financiero que representa para una institución la

[181] http://autoridadcertificadora.guerrero.gob.mx/fec/que-es-la-fec.html#quees. Consultado el 20 de junio 2017

implementación de la firma electrónica avanzada, y 2) la poca cultura de nuestro país en la confianza de este tipo de elementos de certificación electrónica de documentos.

La implementación de un certificador nacional de firma electrónica eliminaría el primer obstáculo, porque la reducción de costos sería significativa. Para superar el segundo obstáculo es necesario que el Ministerio de Economía continúe realizando capacitaciones, para que las instituciones adopten la firma electrónica.

La firma electrónica avanzada es como el fax o el teléfono; si no hay un receptor, de nada sirve tenerla.

Para usar una firma electrónica es indispensable haber obtenido un certificado emitido por una autoridad certificadora. La misma contiene una llave pública y una llave privada. La llave pública se distribuye con el mensaje o el documento firmado y la llave privada se encuentra encriptada en un dispositivo de uso privado, que puede ser una tarjeta, un dispositivo de almacenamiento USB o el disco duro de nuestra computadora.

En el artículo 2, la precitada Ley define a los prestadores de servicios de la siguiente manera: “Prestador de Servicios de Certificación: Se entenderá la entidad que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas”.

Actualmente, las instituciones en Guatemala deben pagar los servicios de un certificador para usar la firma electrónica avanzada. Un proyecto tecnológico de país es crear un certificador de firmas electrónicas nacional. De esa forma se ahorraría el costo de pago a terceros por el servicio. El Estado se convertiría totalmente abierto y digital, sin importar el formato en que se publiquen los datos, porque el respaldo será la firma electrónica avanzada.

3.5.3 Gobierno Electrónico

Los altos niveles de penetración de la tecnología en la vida diaria, comercio, comunicaciones, percepción y emisión de opiniones de una población han hecho que los gobiernos volteen a ver a la tecnología como una aliada en la actividad de ejercer gobierno. Al hecho de usar la tecnología como herramienta en el arte de gobernar se le denomina gobierno electrónico.

La Organización de los Estados Americanos, OEA, define el Gobierno Electrónico como: "la aplicación de las tecnologías de la información y la comunicación (TIC) al funcionamiento del sector público, con el objetivo de incrementar la eficiencia, la transparencia y la participación ciudadana."[182]

La AGESIC es la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento de Uruguay. Divide la implementación del Gobierno Electrónico en cuatro etapas o niveles[183] y define la madurez de un Estado en cuanto al uso de las tecnologías de la información y comunicación en la gestión pública. Las etapas o niveles en referencia son:

a) **Presencia**: se coloca información a la que los ciudadanos puedan acceder, pero sin interacción. Esto, por medio de portales web, a través de una sola vía se comunica la información que la institución quiere hacer pública.

b) **Interacción**: en este nivel, las instituciones colocan en sus portales web correos electrónicos en donde los ciudadanos pueden escribir para recibir información o información adicional. También hay formularios que se pueden llenar; la persona debe proporcionar su correo electrónico para que, de esa manera exista comunicación de ambas vías ciudadano-institución.

---

[182] http://portal.oas.org/Portal/Sector/SAP/DepartamentoparalaGesti%C3%B3nP%C3%BAblicaEfectiva/NPA/SobreProgramadeeGobierno/tabid/811/Default.aspx. Consultado 18 de agosto 2018

[183] https://www.agesic.gub.uy/innovaportal/v/163/1/agesic/gobierno_electronico_.html. Consultado el 3 de marzo 2017

c) **Transacción**: esta etapa o nivel comprende la realización de trámites por medios electrónicos. Los ciudadanos pueden efectuar trámites que antes únicamente podían hacerlos en persona.

d) **Transformación**: Es cuando el Estado incluso hace modificaciones presupuestarias, para cumplir sus obligaciones de forma electrónica. Pone énfasis en la capacitación de recursos humanos altamente eficiente en materia de tecnología para suplir las obligaciones de prestar servicios utilizando la tecnología. Surgen los ministerios de ciencia y/o tecnología y los viceministerios orientados a atender el tema de tecnología en cada nivel gubernamental.

En Guatemala hemos avanzado en los niveles de presencia e interacción; existen muchos portales donde una institución coloca información y también es posible tener cierto nivel de interacción por medio de correo electrónico. En el nivel “transacción”, en donde mediante servicios electrónicos los ciudadanos pueden gestionar documentos, solo hay un par de instituciones que han avanzado en el tema: una es la SAT, con la implementación de la Banca Virtual para el pago de impuestos, la denominada Banca SAT, y el pago del impuesto de circulación que es posible realizarlo de forma electrónica.

La otra institución que ha avanzado en brindar servicios electrónicos es el Registro Nacional de las Personas (RENAP). Ahora es posible solicitar, a través de una aplicación móvil o en la web, una partida de nacimiento o un documento de identidad; incluso, eliminó la barrera del pago en agencias bancarias, pues permite pagar con tarjeta de crédito, implementando sus propios switches de pago que se comunican directamente con VISA y MasterCard, información recabada en entrevista con el director de informática del RENAP en el año 2016.

3.6 Implementación del modelo nacional de ciberseguridad

Cada elemento de este modelo nacional de ciberseguridad es clave. Su implementación es imposible si falta alguno. Un ejemplo de esto son los esfuerzos de la Policía Nacional Civil y del Ministerio Público, a quienes la falta de legislación contra el ciberdelito hace que no puedan cumplir a cabalidad el objetivo para lo cual fueron creados.

Este modelo toma la legislación actual, el mandato institucional no solo del Sistema Nacional de Seguridad, sino que también del Ministerio Público y del Organismo Judicial.

La ciberseguridad en un país depende de los pilares de legislación, institucionalidad, políticas y estrategias y cooperación internacional. Si falta alguno de ellos, el combate al cibercrimen está condenado al fracaso. Haciendo un resumen del modelo, tenemos:

1) Legislación

    a) Propuesta de creación de ley contra el delito cibernético.

    b) Propuesta de creación de ley de protección de infraestructuras críticas.

2) Institucionalidad

    a) Propuesta de creación del Instituto Guatemalteco de Ciberseguridad.

    b) Creación de la comisión de ciberseguridad del Consejo Nacional de Seguridad

    c) Propuesta de creación del Ministerio de Tecnología, como ente rector del desarrollo tecnológico del país.

    d) Creación del CSIRT-gt para prevenir y responder ante eventos cibernéticos.

e) Fortalecer la actual unidad contra el ciberdelito en la Policía Nacional Civil.

f) Fortalecer la unidad contra la pornografía infantil del Ministerio Público.

g) En el capítulo tres se analizó la creación del comando de informática y tecnología del Ministerio de la Defensa. Es un actor clave en la ciberseguridad y ciberdefensa del país.

3) Políticas y Estrategias

a) Creación de la Política Nacional de ciberseguridad, que se desarrolla en el capítulo 4 del presente trabajo.

b) Creación del Plan de Protección de infraestructuras críticas.

c) Actualización de la Estrategia Nacional de Ciberseguridad del Ministerio de Gobernación.

4) Cooperación Internacional

a) Se propone que, después de que el país cuente con una legislación contra el ciberdelito, se suscriba el convenio de Budapest.

b) Luego de suscribir el convenio de Budapest, el país se adhiera al programa Glacy +.

c) Se continúe utilizando y fortaleciendo la participación del país en el programa 24/7 para investigaciones de casos de ciberdelito.

d) El CSIRT-gt se enrole en el programa FIRST, para estar actualizado tecnológicamente.

5) Proyectos nacionales estratégicos de tecnología

a) Centro Nacional de Datos.

b) Gobierno Electrónico.

c) El Estado como prestador de firma electrónica.

Con ello se cumple el objetivo general del presente trabajo de investigación, el cual es Formular un modelo nacional de ciberseguridad que garantice la disponibilidad, integridad y confidencialidad de los sistemas informáticos que controlan las infraestructuras críticas del país ante la amenaza del ciberdelito a la seguridad de la nación.

La implementación de este modelo deberá ser por medio de una política pública nacional de ciberseguridad que exponga sus elementos, defina responsables, defina el objetivo general, los objetivos específicos y le dé seguimiento y monitoreo de su cumplimiento. La política pública de ciberseguridad se expone en el capítulo cuatro siguiente.

CAPÍTULO CUATRO

4. Política Nacional de Ciberseguridad para la protección de infraestructuras Críticas en Guatemala

En este capítulo se expone la necesidad de una política nacional para la protección de infraestructuras críticas que operativice el modelo nacional de ciberseguridad planteado en el capítulo tres, clasificando la ciberseguridad de las infraestructuras críticas como un problema de seguridad nacional. Debe definir metas, objetivos y responsables en la implementación de ciberseguridad a las infraestructuras críticas del país.

En la Política Nacional de Seguridad 2017 se menciona por primera vez la necesidad de abordar la Ciberseguridad como en eje nacional de seguridad. Pone de manifiesto la relevancia de la tecnología en la coordinación y colaboración de los entes encargados de la seguridad del país, y menciona la importancia de que la información se mantenga confiable, íntegra y disponible.

Expresa claramente que “Los ciberataques se han constituido en una amenaza a la seguridad y comprometen la disponibilidad, integridad y confidencialidad de la información, dañan e interfieren parcial y totalmente los sistemas informáticos, telecomunicaciones o infraestructura de carácter público o privado.

La atención a este tema es trascendental para evitar que el ciberespacio se constituya en un escenario de conflictos que desestabilicen la institucionalidad del Estado, afecten o alteren información sustancial de carácter político, económico-financiero o social; y, obstruyan el flujo de los bienes, servicios e información,

especialmente a los sectores de seguridad, defensa, comunicaciones e infraestructura, energía y otros."[184]

De esta manera, el Sistema Nacional de Seguridad pone los ciberataques en primer plano, ante el peligro que representan para la seguridad nacional, y aunque no use directamente las palabras infraestructuras críticas, los servicios e información, seguridad, defensa, comunicaciones, infraestructura y energía son la prioridad de la política nacional para protegerlas de ataques, por considerárseles de alta prioridad para mantener la paz social y democrática.

La Política Nacional de Seguridad también hace alusión a la tecnología en breves momentos, y de forma superficial, en la sección seguridad del eje energético, dice: "La disponibilidad y seguridad energética en armonía con el ambiente, es de vital importancia para garantizar el funcionamiento de los sistemas sociales, económicos, y tecnológicos, así como para el desarrollo competitivo y sostenido de la producción nacional."[185]

En cuanto al uso de la tecnología, para lograr los objetivos la Política Nacional de Seguridad menciona que existe una brecha entre el aspecto político y la creación de indicadores medibles, y se refiere a esto cuando menciona lo siguiente: "Esta brecha, reafirma la necesidad de una política de seguridad interior consistente e integrada con la Política Nacional de Seguridad y otras políticas funcionales de la seguridad, para cubrir los vacíos de definición, organización e integración de aspectos operativos, tácticos y tecnológicos, en el empleo de recursos de las fuerzas de seguridad; y atender de manera preventiva y enfrentar el conjunto de riesgos y amenazas provenientes de la delincuencia común y organizada"[186]

---

[184] *Política Nacional de Seguridad de Guatemala*. Secretaria Técnica Nacional de Seguridad. 2017. Pág. 16. Disponible en: https://stcns.gob.gt/docs/2017/Reportes_DMC/Politica_Nacional_de_Seguridad_2017.pdf
[185] Ibídem Pág. 15
[186] Ibídem. Pág. 19

En la sección de Lineamientos Estratégicos se vuelve a abordar lo concerniente a la tecnología, con el enfoque de mejorar su uso hacia una forma más efectiva en el combate a la delincuencia común y crimen organizado, cuando cita en la sección b: “Promover el desarrollo e implementación de mecanismos de coordinación, colaboración y cooperación que articulen aspectos políticos, estratégicos, operativos, tácticos y tecnológicos para la gestión integral de la Seguridad de la Nación”[187].

Además, en la sección g menciona un concepto militar cuyas siglas son C4i, para “Desarrollar e implementar un Centro Nacional de Inteligencia para ejercer el Comando, Control, Computación, Comunicaciones e Inteligencia como mecanismo de coordinación del Sistema Nacional de Inteligencia que facilite la elaboración de productos estratégicos y coadyuve a la toma de decisiones para la consecución de los objetivos nacionales”[188].

Aunque de forma muy superficial, es un gran avance el que la política 2017 priorice el tema de ciberseguridad y lo coloque como un eje estratégico de seguridad nacional. Falta aún la institucionalidad, marco jurídico, cooperación internacional y otros aspectos importantes que se trataron en el capítulo tres, en la definición del modelo de ciberseguridad nacional.

4.1 Definición de Política

La Real Academia Española define política como: “Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado” [189]

[187] Ibídem. Pág. 21
[188] Ibídem. Pág. 22
[189] https://dle.rae.es/?id=Ta2HMYR. Consultado el 2 de junio 2018

4.2 Definición de Política Pública

La Secretaría de Planificación y Programación de la Presidencia aporta la siguiente definición de Política Pública: "constituyen cursos de acción estratégica del Estado y del Gobierno basadas en la participación y legitimidad ciudadana, los marcos jurídicos y políticos nacionales e internacionales. Orientadas a propiciar el bienestar y el goce de los derechos humanos de la población guatemalteca"[190].

Una Política Pública debe estar debidamente consensuada y dirigida a resolver un problema dentro del marco jurídico, y orientada a garantizar los derechos humanos. La política nacional de ciberseguridad para las infraestructuras críticas cumple esos criterios. Será el vehículo sobre el cual se debe implementar el modelo nacional de ciberseguridad planteado en el capítulo tres.

4.2.1 Ciclo de la política pública

Diseñar políticas públicas no es tarea fácil. Requiere de conocimientos acerca de economía, política, estadística, administración pública, derecho, sociología, antropología, psicología y comunicación. Por lo tanto, se necesita de un equipo multidisciplinario, de coordinadores capaces que obtengan la información precisa de cada especialista, así como de tomar en cuenta la opinión de todos los sectores sociales involucrados.

4.2.2 Origen

Una de las características básicas de las políticas públicas es que deben responder a un problema claro y delimitado. Una acción de gobierno o del Estado sin un diagnóstico adecuado no es política pública, es simplemente una acción gubernamental.

---

[190] Guía para la formulación de Políticas Públicas. SEGEPLAN. 2015. Pág. 16. Disponible en: http://www.segeplan.gob.gt/nportal/index.php/normativas-metodologias-politicas-publicas?download=450:guia-para-formulacion-politicas-publicas. Consultado el 20 de enero 2017

El origen de la política comienza, entonces, con la delimitación de un problema público que se desea atender, cuantificando el número de afectados, las zonas geográficas donde residen y los costos sociales que el problema ha generado.

Seguidamente, se realiza un análisis causal que nos permita conocer cuáles son las causas principales que generan el problema que se desea atender. Este análisis constituye un paso crucial en esta etapa, en virtud de que las soluciones deben estar enfocadas en atacar las causas del problema y no las consecuencias.

Corzo anota: "Las soluciones de política pública son cursos de acción alternativos para mitigar las causas de un problema público. Sugiero iniciar estableciendo claramente el objetivo de las potenciales soluciones, así como la población potencial que se desea atender. Posteriormente, propongo que se lleve a cabo una sesión de lluvia de ideas para proponer soluciones creativas con un grupo pequeño de personas involucradas en el proyecto."[191]

4.2.3 Diseño

Después del análisis de ideas, es preciso saber qué soluciones se han implementado para problemas similares. Se puede proponer a los equipos realizar dos análisis: uno de prácticas actuales y otro de mejores prácticas de política pública, según los problemas que se busque atender.

Luego, se pueden seleccionar las mejores soluciones, cuantificar sus costos y hacer que parezca tarea fácil, aunque no lo sea. Requiere de un análisis serio donde se deben calcular los costos de inversión, así como los costos de operación y mantenimiento según los resultados y la evaluación que proyecte la implementación de la política pública.

---

[191] Corzo, Julio Franco. ¿Cómo diseñar una política pública? 2014. Consultado en: https://www.iexe.edu.mx/blog/como-disenar-una-politica-publica.html.

En la mayoría de los casos, una política pública no puede atender a todos los afectados por el problema público (población potencial), debido a restricciones presupuestales, cuestiones geográficas o tiempo. En vista de lo anterior, hay que seleccionar una población objetivo, que es aquella a la que la política pública estará en condiciones de atender.

4.2.4 Gestión

Definidos los objetivos y las estrategias, será imprescindible definir los mecanismos jurídicos y administrativos requeridos para poner en marcha la política pública. Estos varían y dependen de las características de la política y de sus componentes. La gestión depende, entonces, de dos aspectos fundamentales:

- Planes, programas y proyectos: los planes de desarrollo constituyen un excelente medio para poner en marcha políticas públicas, con la ventaja de que pueden articular esfuerzos y resolver problemáticas aisladas.

- Dispositivos de vigilancia y control: en la medida en que diferentes actores participen en la ejecución de la política y tengan responsabilidades, serán necesarios sistemas de vigilancia y control que garanticen el cumplimiento de la directriz y la protección del interés público.

- Las políticas y sus estrategias deberán soportarse adecuadamente en un plan y en un marco jurídico y legal.

- "En cada país pueden existir diferentes opciones para garantizar el cumplimiento de las políticas; y los sistemas de rendición de cuentas (accountability) constituyen herramientas propias de la democracia que deberían fortalecerse." [192]

---

[192] Gómez, Rubén D. *Gestión de políticas públicas: aspectos operativos*. Universidad de Antioquia 2013. Pág. 234. Disponible en: http://www.scielo.org.co/pdf/rfnsp/v30n2/v30n2a11.pdf

También debe preverse la efectividad de medidas anticorrupción que aseguren la transparencia de las acciones involucradas en la ejecución de la política; entre ellas, el fortalecimiento institucional y administrativo de las agencias de control como el MP, Contraloría, PGN, etc.

4.2.5 Evaluación

Es la apreciación objetiva de un programa, proyecto o política en ejecución o concluida; evalúa su diseño, su puesta en práctica y los resultados. Determina el logro de los objetivos, así como la eficacia, la eficiencia, el impacto y la sostenibilidad de la política.

"Una evaluación deberá proporcionar información creíble y útil, que permita incorporar las enseñanzas aprendidas en el proceso de toma de decisiones de beneficiarios y donantes. La evaluación también se refiere al proceso de determinar el valor o la significación de una actividad, política o programa. Se trata de una apreciación, tan sistemática y objetiva como sea posible, de una intervención para el desarrollo planeada, en curso o concluida." [193]

Un proceso de evaluación puede aplicarse a programas, proyectos o políticas en general, de cuyo funcionamiento, rendimiento, desarrollo o resultados finales se quiera conocer algún aspecto.

4.3 Definición de Política de Ciberseguridad

Para Colombia, país sudamericano que presentó su política nacional de seguridad digital en el año 2016, la definición es: "La política nacional de seguridad digital debe involucrar activamente a todas las partes interesadas, y asegurar una

---

[193] *Guía de Evaluación de Políticas Públicas del Gobierno Vasco*. Gobierno Vasco. 2011. pág. 8. Disponible en: http://www.euskadi.eus/contenidos/informacion/evaluacion_coordinacion/es_def/adjuntos/guia_evaluacion_gv_pip.pdf

responsabilidad compartida entre las mismas. Principios que se reflejan en las dimensiones en las que esta política actuará, las cuales determinan las estrategias para alcanzar su objetivo principal: fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital"[194].

4.4 Política Nacional de Ciberseguridad en Guatemala

Al construir una Política de Ciberseguridad para Guatemala, se debe tener en cuenta lo mencionado en la Política de Ciberseguridad de los Estados Unidos de América: "Estrategias, políticas y normas relativas a la seguridad de las operaciones en el ciberespacio, y abarca todos los tipos de reducción de amenazas, la reducción de las vulnerabilidades, la disuasión, la participación internacional, la respuesta a incidentes, resiliencia, las políticas y actividades de recuperación, incluidas las operaciones de redes informáticas, integridad de la información, aplicación de la ley, la diplomacia, militares y misiones de inteligencia con respecto a su relación con la seguridad y la estabilidad de la infraestructura mundial de la información y las comunicaciones"[195].

Los objetivos generales de la seguridad cibernética son: Disponibilidad, Integridad y Confidencialidad de la Información, y es hacia donde se deben orientar los esfuerzos institucionales, legislativos y de cooperación internacional.

En cuanto a una política pública de ciberseguridad, hay que tener en cuenta que las amenazas cibernéticas tienen una naturaleza diferente a otras amenazas de seguridad nacional, pues pueden ser ejecutadas y planificadas por diferentes tipos de actores: crimen organizado, grupos terroristas, pero también personas

---

[194] *Política Nacional de Seguridad Digital*. Gobierno de Colombia. CONPES 3854. 2016. Pág. 3. Disponible en: https://bibliotecadigital.ccb.org.co/handle/11520/14856

[195] CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; *White House Cyberspace Policy Review*. Disponible en: https://www.sec.gov/rules/interp/2018/33-10459.pdf. Consultado el 2 mayo 2016

individuales con mucho conocimiento y pocos recursos, ya que su costo es mínimo y su trazabilidad es sumamente compleja. El espionaje, el robo de información, la vulnerabilidad de los datos o la falta de capacidad de almacenamiento centralizado, son parte de los ataques cibernéticos que se pueden organizar y ejecutar de parte de muchos tipos de actores.

Guatemala es un país con una profunda crisis institucional, con una democracia joven y débil y con un Estado ausente en muchas formas. Tener tan alta vulnerabilidad en las estructuras informáticas y de telecomunicaciones supone un riesgo altísimo para la población en general y la seguridad democrática. Se han registrado casos críticos por tener un nivel bajo de ciberseguridad en Guatemala. El Registro Nacional de las Personas, RENAP, a inicios del año 2019, es una de las instituciones que reportan problemas de naturaleza tecnológica, por no contar con un sistema avanzado de almacenamiento y protección de datos sensibles de toda la población.

4.4.1 Pilares para una Política Nacional de Ciberseguridad

La Ciberseguridad en el marco de Seguridad nacional de un país debe ir orientada hacia estos grandes temas, en los cuales resalta la protección a las infraestructuras críticas:

1) Capacidad de prevención, detección, investigación y respuesta antes las Ciberamenazas, con apoyo de un marco jurídico operativo y eficaz.

2) Garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las administraciones públicas. Se fortalecerá la seguridad de los sistemas de información y las redes de comunicaciones que soportan las *infraestructuras críticas*. Se impulsará la normativa sobre la protección de infraestructuras críticas con el desarrollo de las capacidades necesarias para la protección de los servicios esenciales.

3) Mejora de la seguridad y resiliencia de las Tecnologías de la Información y la Comunicación (TIC). En el sector privado por medio del uso de las capacidades de los poderes públicos. Por medio de alianzas público-privadas.

4) Promoción de la capacitación de profesionales en Ciberseguridad.

5) Implantación de una cultura de Ciberseguridad sólida. Se concienciará a los ciudadanos, profesionales y empresas acerca de la importancia que reviste la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.

6) Intensificación de la colaboración internacional. Se promoverán los esfuerzos tendentes a conseguir un ciberespacio internacional donde se alineen las iniciativas de todos los países que persiguen un entorno seguro y fiable. En todo momento se salvaguardarán los intereses nacionales.[196]

Están mencionados anteriormente los pilares sobre los cuales se debería construir una Política Nacional de Ciberseguridad sobre los hombros de países que han recorrido un importante camino en la implementación de tecnología y protección de la infraestructura que soporta los servicios indispensables.

4.4.2 Temporalidad para la Política Nacional de Ciberseguridad

La temporalidad y espacialidad (territorio de aplicación) son elementos por analizar previo a iniciar la planificación de creación de una política pública. Depende primero del problema que se desea solucionar y de los actores sociales involucrados en su creación, ejecución y participación. Las políticas públicas son instrumentos de planificación y gestión estratégica, que contemplan un esfuerzo de largo plazo para

[196] *Estrategia Nacional de Seguridad*. Gobierno de España. ESN-2013. Disponible en: https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional

incidir en los problemas complejos y estructurales de la población en general, un segmento o sector de esta desde las instituciones públicas.

En este caso, la ciberseguridad constituye un problema relacionado directamente con el avance de la tecnología, la constante evolución de la era digital y la masificación del uso de tecnologías de información y telecomunicaciones (TIC).

Entonces, por su naturaleza, es muy probable que esta política nacional se planifique con una aplicación permanente y evolutiva, adaptándose a los cambios de la era digital; no solo debe prever las amenazas actuales en el ciberespacio, sino cambiar en paralelo con su contexto de aplicación, ya que con el avance de la tecnología surgen nuevos escenarios y vulnerabilidades en el ambiente digital. El que deba tener una temporalidad indefinida no implica que su monitoreo, evaluación y seguimiento no cumplan con los requisitos mínimos y rigurosos de toda política pública; mayormente en el contexto digital, donde todo es medible y cuantificable.

4.4.3 Evaluación de la Política Nacional de Ciberseguridad

La evaluación de las políticas públicas es una fase importante para el seguimiento y la aplicación efectiva y constante de las acciones que enmarca. Rafael Bañón señala tres funciones en la evaluación: perfeccionamiento o mejora (improvement), recapitulación, rendimiento de cuentas o responsabilidad (accountability) y ejemplificación o iluminación para acciones futuras (enlightenment). (Bañón, 2003).

La primera (improvement) se refiere a la retroalimentación y propio aprendizaje del proceso evaluado; en el caso de una política nacional de ciberseguridad, consistiría en revisar todas las acciones de la política, por ejemplo, el marco legal mínimo para su adecuada aplicación y revisar cuántos de esos decretos o leyes sugeridas en la política han avanzado o se han aprobado en los organismos correspondientes. Revisar el avance de conformación de consejos o esfuerzos interinstitucionales y multisectoriales que la política proponga. Cada

revisión debe contener un proceso de retroalimentación enfocado en la eficacia del impacto de las acciones.

El rendimiento de cuentas (accountability) es la segunda función de la evaluación que, como su nombre lo explica, consiste en informar en diferentes niveles el uso, gestión, asignación y eficacia de los fondos o recursos que usa la política pública. La ciudadanía, las instituciones, la clase política y los distintos sectores de la sociedad tienen derecho a informes detallados sobre el uso de los fondos y recursos, así como a evaluar si la asignación de esos fondos ha sido la más correcta y si es congruente con los resultados de la implementación de la política.

El tercer componente de la evaluación se refiere a dar luz o iluminar acciones futuras (enlightenment). Las evaluaciones arrojan información sistemática que contribuye al “acervo científico”, no solo de ese programa, servicio o política concreta, sino también del abordaje de otros problemas públicos. No es más que la unificación de evaluaciones de diferentes programas, proyectos o políticas que se interrelacionan para hacer un análisis más profundo, desde el Estado, acerca de cómo se correlaciona esa política con otros programas de nación y cuál es el impacto de esa correlación.

4.4.4 ¿Es la ciberseguridad algo de carácter público?

Según la SEGEPLAN, antes de atender un tema como política pública se debe fundamentar si el problema es de carácter público, y uno de los criterios para definir lo público es, cuanto afecta o beneficia a una mayoría, cuánto afecta o beneficia a los más vulnerables; ha de estar reconocido y validado por aquellos que tienen representatividad. Deben tomarse como base estos dos aspectos:

1) “Muestra carencias objetivas en la sociedad.

2) Cuando los actores con poder califican a esa situación como problema público.” [197]

En ese sentido, la ciberseguridad es un asunto público, no solo porque las tecnologías están presentes en la vida diaria de toda la población guatemalteca, sino porque las infraestructuras críticas, como se anotó en el capítulo tres, dependen de la tecnología, y si de alguna forma fueran comprometidas, esto afectaría a un gran número de población.

Además de ello, el enfoque de la presente tesis en cuanto a la ciberseguridad de la infraestructura crítica es la Seguridad Nacional, la cual se vería comprometida, como ha ocurrido en otros países del mundo, si falla la tecnología que la soporta.

El presente trabajo de tesis enlista, previamente, un catálogo no oficial de lo que se podría calificar como infraestructura crítica. La lista incluye Puertos, Aeropuertos, Telecomunicaciones, Registro Nacional de las Personas, sector Bancario, sector de Energía, entre otros. De manera, pues, que cumple con los requisitos para ser catalogado un tema público, no solo porque abarca una gran cantidad de personas, sino porque automáticamente se convierte en una amenaza a la seguridad pública si hubiese algún fallo en el servicio que se presta.

Los líderes mundiales de China, Estados Unidos e Inglaterra, por citar algunos, han dado declaraciones y, de hecho, han convertido la ciberseguridad en un tema de agenda de seguridad nacional. En el capítulo dos se expuso cómo algunos líderes mundiales han creado comandos no convencionales de guerra denominados “de cuarta generación”. Uno de los objetivos de los cibercomandos es crear tácticas, protocolos y tecnología para atacar y detener el funcionamiento

[197] *Guía para la formulación de Políticas Públicas*. SEGEPLAN. 2015. Pág. 30. Disponible en: http://www.segeplan.gob.gt/downloads/2015/Politicas_Publicas/GpFPP.pdf. Consultado el 14 de agosto 2019

normal de las infraestructuras críticas que dependen de la tecnología digital de países enemigos, antes de iniciar una guerra convencional.

De esa forma, el tema de ciberseguridad se convierte en un tema de interés público, además de un tema de seguridad nacional. Guatemala, con carácter urgente, debe urgentemente elaborar una política pública para proteger tecnológicamente sus infraestructuras críticas, y no únicamente una estrategia que trate superficialmente el tema de ciberseguridad en el país.

4.4.5 El actor más pertinente para intervenir

Aunque el Estado no debe ser el único actor en participar en el planteamiento y ejecución de una política pública de ciberseguridad, sí es quien debe dirigir, coordinar y ejecutar las acciones de esa política.

En este caso, es fundamental la participación de todos los sectores del país y la articulación de todos los instrumentos estratégicos, para gestionar de forma adecuada la correcta ejecución de una política pública de ciberseguridad. El sector privado posee amplia experiencia y adelantos en la construcción de sistemas de defensa cibernética y protección de datos, por lo que es preciso y oportuno aprovechar esas capacidades instaladas para el desarrollo de los principales ejes de la política.

Respecto de la creación de políticas públicas y la real política en acción, Cardoso señala: “La democracia tiene un método propio para la definición de políticas públicas. Las decisiones resultan de una adaptación negociada de intereses, de acuerdo con normas transparentes definidas en el espacio público… Las políticas no reflejan la supuesta omnisciencia de tecnócratas esclarecidos, sino que representan la depuración de intereses legítimos, un concierto de voluntades, entre ellas las del propio gobierno.”[198]

[198] Cardoso, Fernando H. Discurso pronunciado en la en CEPAL en agosto 2003

4.5 Fases para la elaboración de una Política, según SEGEPLAN

4.5.1 Fase I: Identificación del Problema

Los ataques y amenazas a los sistemas de información de instituciones vitales para el Estado ponen en peligro la integridad, confidencialidad y disponibilidad de los datos, incidiendo de tal forma en la vulnerabilidad de las personas, la competitividad de sus economías y su estabilidad, razón por la cual Guatemala debe contar con una Política Nacional de Seguridad Cibernética, que disminuya las amenazas del ciberespacio, sin perder todas las ventajas que suponen las tecnologías de la información.

Los daños provocados por los ataques cibernéticos obligan a establecer acciones que fortalezcan las normativas y a la adopción de estándares en seguridad cibernética, con el fin de proteger los bienes jurídicos de las personas, instituciones y sistemas informáticos. En el caso de los ciberataques, estos han sido identificados como amenaza a la seguridad nacional por parte del sistema de inteligencia, lo cual queda registrado en la agenda nacional de riesgos y amenazas 2018[199]. También, la ciberseguridad es un eje en la Política Nacional de Seguridad 2017.[200]

4.5.2 Fase II: Identificación y formulación de soluciones

Las primeras acciones pueden establecer la formulación de un marco legal regulatorio para la correcta aplicación de la política, es decir, qué leyes, reglamentos, acuerdos gubernativos y decretos se necesitan, aprobados o en vigencia, para que la política sea aplicada de forma adecuada.

Es impostergable la conformación de una Comisión de Ciberseguridad en el marco del Consejo Nacional de Seguridad, definir qué funcionarios e instituciones

---

[199] Agenda Nacional de Riesgos y Amenazas. Secretaria de Inteligencia Estratégica 2018. Consultado en: https://www.sie.gob.gt/portal/images/DocumentosVarios/anra/2018_ANRA.pdf.
[200] Política Nacional de seguridad 2018. STNS. Consultado en: https://stcns.gob.gt/docs/2017/Reportes_DMC/Politica_Nacional_de_Seguridad_2017.pdf

la conformarían y cuál sería su correlación con otros sectores sociales. Idealmente, debería estar conformada por el Ministerio de la Defensa, Ministerio de Gobernación, Ministerio de Relaciones Exteriores, la Superintendencia de Telecomunicaciones, Secretaría Técnica del Consejo Nacional de Seguridad, Secretaría Nacional de Ciencia y Tecnología, y SEGEPLAN.

4.5.3 Fase III: Toma de decisión (Política efectiva de acción)

El Consejo puede definir ejes de trabajo de la política nacional y desarrollar la metodología más adecuada para abordar cada eje. El primero, como ya se ha mencionado, debería ser: establecer el marco legal regulatorio del funcionamiento de la política; allí se definirá qué otros actores sociales pueden integrarse en la implementación y ejecución de la política, el nivel de participación ciudadana que debe tener y de dónde se financiará su funcionamiento, entre otros detalles.

4.5.4 Fase IV: Implementación (trabajo sobre el terreno)

En esta fase se implementará el Modelo nacional de ciberseguridad que se plantea en el capítulo tres de este trabajo. Las acciones que resaltan son:

- Crear una ley contra el ciberdelito, con base en estándares internacionales aplicados a la realidad guatemalteca.
- Crear la ley de privacidad y protección de datos con base en convenios internacionales de derechos humanos.
- Crear la ley de infraestructuras críticas, para identificar y catalogar a las que prestan servicios esenciales al país y el establecimiento de medidas de prevención, protección y recuperación contra riesgos y amenazas.
- Elaborar el plan de protección a infraestructuras críticas.
- Actualizar la estrategia nacional de ciberseguridad.

- Modernizar y capacitar a todos los actores del sector justicia, sobre los delitos cibernéticos e informática forense.

- Crear e implementar la comisión de ciberseguridad para asesorar al Consejo Nacional de Seguridad, en temas relacionados con la seguridad cibernética.

- Crear el Instituto Guatemalteco de Ciberseguridad. Este será el brazo tecnológico en materia de ciberseguridad de las instituciones del Estado.

- Diseñar programas de concienciación, sobre seguridad cibernética, a los distintos sectores de la sociedad guatemalteca.

- Promover el incremento de los servicios electrónicos gubernamentales fiables y seguros, por medio de programas de gobierno electrónico.

- Ejecución de proyectos tecnológicos estratégicos.

- Adhesión al convenio de Budapest.

- Elaborar el libro blanco de alianzas público-privadas en materia de ciberseguridad.

4.5.5 FASE V: Evaluación

Deberán ser el Consejo de Ciberseguridad y la Secretaría Técnica del Consejo Nacional de Seguridad quienes funcionen como enlace entre la Política Nacional de Ciberseguridad y la planificación institucional del Sistema Nacional de Seguridad, por lo que los planes de acción que contemplan los mecanismos de monitoreo y evaluación se incorporarán en dicho instrumento, para desarrollar los programas que den seguimiento y evaluación al cumplimiento efectivo de las acciones planteadas en la política, incluidas la rendición de cuentas y la ejecución presupuestaria.

CONCLUSIONES

Se demostró la Hipótesis principal de la investigación, que el Estado de Guatemala puede garantizar la disponibilidad, integridad y confidencialidad de la información de sus infraestructuras críticas. Para lograr esa protección integral, requiere la implementación de un modelo nacional de ciberseguridad que con los ejes de: a) Legislación contra el ciberdelito, Fortalecimiento institucional, Políticas y estrategias, cooperación internacional, proyectos tecnológicos estratégicos y alianzas público-privadas. El modelo propuesto se ajusta a la realidad legislativa e institucional del país, por lo que es factible su implementación por medio de una política pública de ciberseguridad orientada a proteger las infraestructuras críticas. Durante el desarrollo del presente estudio se comprobó la Hipótesis secundaria La falta de institucionalidad, marco jurídico y alianzas público-privadas generan que el país sea vulnerable al ciberdelito. Se demostró como la falta de legislación crea una parálisis institucional respecto al combate del ciberdelito, a la vez que no permite que existan condiciones para establecer alianzas público-privadas sólidas para lograr el objetivo de ciberseguridad.

Se cumplieron todos los objetivos específicos de la investigación debido a que: a) se analizó el marco jurídico actual en materia de ciberseguridad demostrado en el capítulo uno, b) se definió un marco jurídico mínimo necesario para el combate al ciberdelito en el capítulo tres, c) se realizó una propuesta de definición y clasificación de infraestructuras críticas en el capítulo dos, d) los niveles y medios para una cooperación internacional efectiva en materia de seguridad en el ciberespacio, se definieron en el capítulo tres, e) se planteó la creación de un modelo institucional para la respuesta ante emergencias cibernéticas, al proponer el CSIRT-gt y el Instituto Guatemalteco de Ciberseguridad.

1. En vista de a que Guatemala no dispone aún de una capacidad sólida que permita realizar una dirección y gestión, eficaces y eficientes, de la ciberseguridad, es necesario que el gobierno asuma el liderazgo en esta materia, y proteger el ciberespacio del que dependen los servicios básicos, infraestructuras críticas, economía, las libertades y derechos individuales y progreso como sociedad.

2. El gobierno de Guatemala debe identificar la seguridad de su ciberespacio, especialmente de sus infraestructuras críticas, por medios estratégicos y prospectivos, ya que la materialización de las amenazas sobre dicho ciberespacio puede afectar muy negativamente al desarrollo social, económico y cultural de nuestro país.

3. Se requiere plantear una Política Nacional de Ciberseguridad orientada a proteger las infraestructuras críticas de Guatemala, que incluya la protección de bienes, activos, servicios, derechos y libertades dependientes de la jurisdicción estatal, y la responsabilidad compartida con otros Estados, bilateralmente o por medio de organismos supranacionales, sobre la ciberseguridad.

4. El modelo nacional de Ciberseguridad proporcionará un marco normativo específico que regule el ciberespacio y su seguridad. La reciente formulación de la Política Nacional de Seguridad y el Libro Blanco de Seguridad son un buen punto de partida, pero será necesario adecuar la legislación vigente, en especial la relacionada con la persecución penal de los delitos informáticos y cubrir los distintos escenarios de ataques informáticos o la rápida evolución de las técnicas o métodos de *hacking*.

5. Es indispensable la creación del Instituto Guatemalteco de Ciberseguridad, cuyo objetivo será desarrollar y promover el uso de mecanismos avanzados de seguridad, como la criptografía, y otras normas y estándares que permitan al país lograr la independencia

tecnológica en cuanto al resguardo de información sensible y de seguridad de Estado.

6. Las TIC no son el problema, son parte de la solución. Su protección y empleo seguro no son solo responsabilidad del gobierno, sino de las municipalidades junto con el sector privado, empresarial y doméstico. Todos son corresponsables, pero le corresponde al gobierno el liderazgo y la dirección de la gestión nacional de la ciberseguridad. Estas responsabilidades no pueden delegarse y deben traducirse en proporcionar el impulso, las ideas y la dirección que Guatemala necesita.

7. El gobierno de Guatemala debe fomentar y reforzar la cooperación internacional en materia de ciberseguridad. Las alianzas multinacionales y bilaterales en este sentido son indispensables. En el caso guatemalteco, se tiene una oportunidad de cooperación responsable con los países centroamericanos y se deberán alcanzar acuerdos con los países que, aunque no se encuentren dentro de este entorno geopolítico más próximo, son relevantes para controlar las amenazas sobre nuestro ciberespacio.

8. La falta de personal calificado en instituciones del Estado hace que áreas sensibles como Seguridad Interior, Ministerio Público, Relaciones Exteriores e industrias corran el riesgo de quedar inoperativas, parcial o permanentemente, ante la materialización de una amenaza tecnológica o un ataque informático real. Por tal motivo, se hace necesario desarrollar el capital humano en las instituciones del Estado para lograr la excelencia operativa en distintas áreas estratégicas.

9. En las administraciones del Estado deberá promoverse una cultura de la ciberresponsabilidad, basada en la sensibilización y formación continua en ciberseguridad. Para lograr este objetivo, los planes de estudio de las enseñanzas primaria, secundaria y universitaria deben incluir en sus

planes de estudio asignaturas relacionadas con el manejo responsable del ciberespacio.

10. La alta penetración tecnológica en Guatemala hace que, cada vez más, los ciudadanos estén conectados y el uso de nuevos dispositivos es algo casi obligatorio en las nuevas generaciones. Esto representa un riesgo, especialmente para los niños, debido a que a través de cualquier dispositivo se puede ver afectada la integridad personal mediante delitos como la pornografía, pedofilia, pornovenganza, entre otros riesgos. Ante esto, es imprescindible promover una cultura de seguridad de la información, que pueda ser transmitida y enseñada en las aulas de clase de todo el país.

Anexos

Anexo 1. Gráficas de la situación de la infraestructura crítica en América Latina.

Anexo 2. Gráficas del Estado de Madurez tecnológica en Guatemala Según el Foro Económico Mundial

Anexo 3. Imágenes

Anexo 4. Convenio de Budapest.

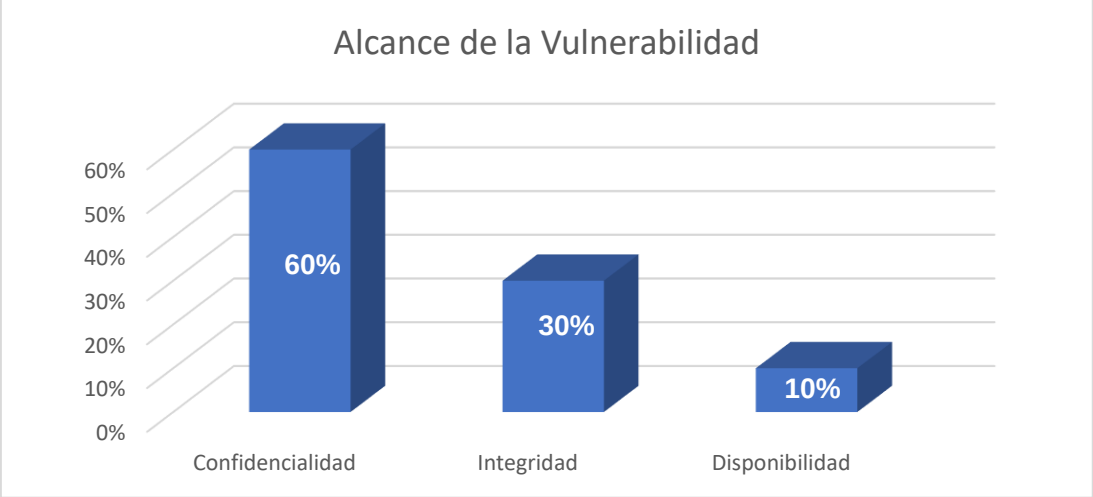
Anexo 5. Tabla de variables en materia de ciberseguridad de la OEA.

Anexo 6. Criterios para clasificar infraestructura crítica en España.

Anexo 1. Gráficas de la Situación de la Infraestructura Crítica en América Latina

En el año 2015[201] la organización de los Estados Americanos junto a Trend Micro una de las más grandes empresas privadas de seguridad digital, realizaron el estudio denominado Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas. En el estudio participaron más de veinte Estados Miembros de la OEA, la academia, sociedad civil y el sector privado. Los resultados del estudio se sintetizan en la presentación de las gráficas que muestran datos relevantes para la presente tesis. Las gráficas presentadas están orientadas al estado de la ciberseguridad y la infraestructura crítica de los más de veinte estados participantes.

Gráfica 1

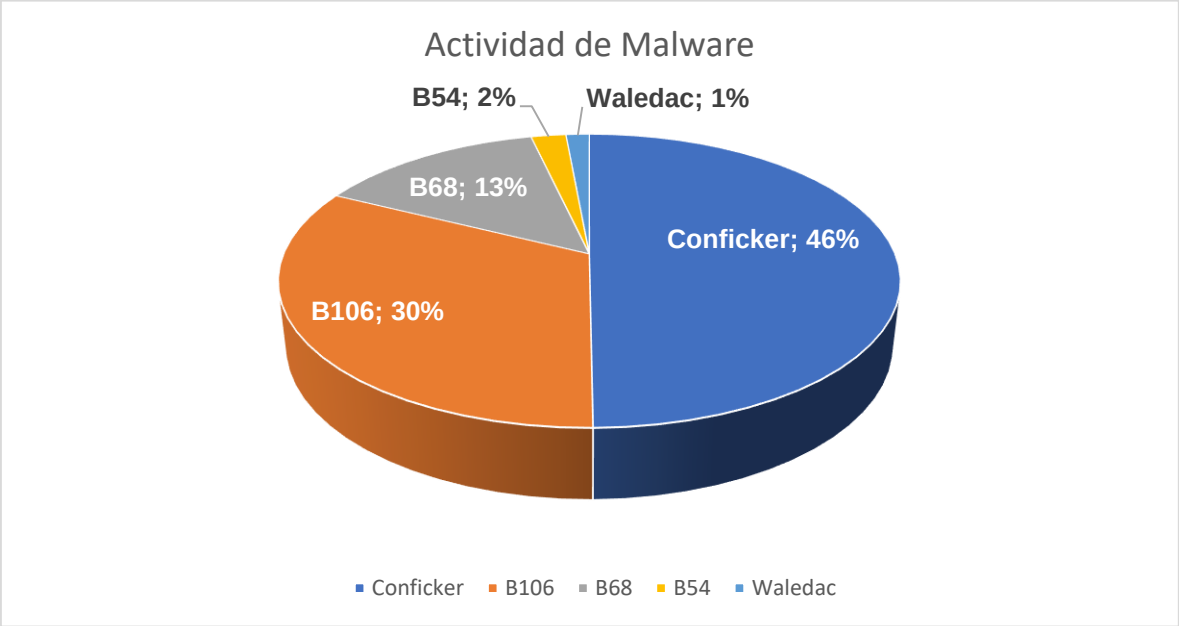


Fuente: Elaboración propia con datos de "Reporte de Seguridad Cibernética y Protección de las Infraestructuras Críticas en las Américas"[202]. OEA 2015

[201] *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*. OEA-Trend Micro. Consultado en. Consultado en: http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-120/15

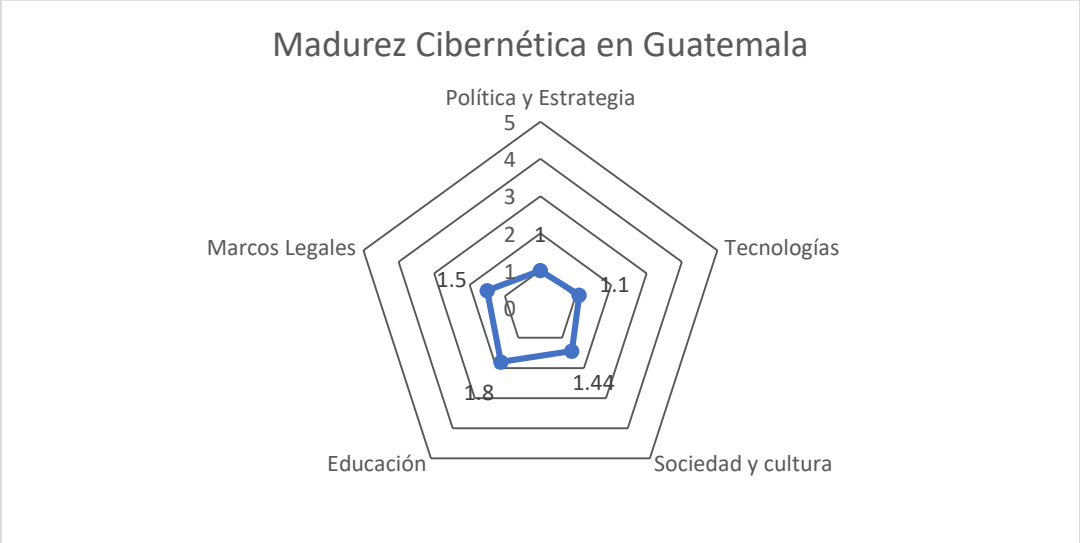
[202] *Ídem*

Gráfica 2



Fuente: Elaboración propia con datos de "Reporte de Seguridad Cibernética y Protección de las Infraestructuras Críticas en las Américas"[203]. OEA 2015

Gráfica 3

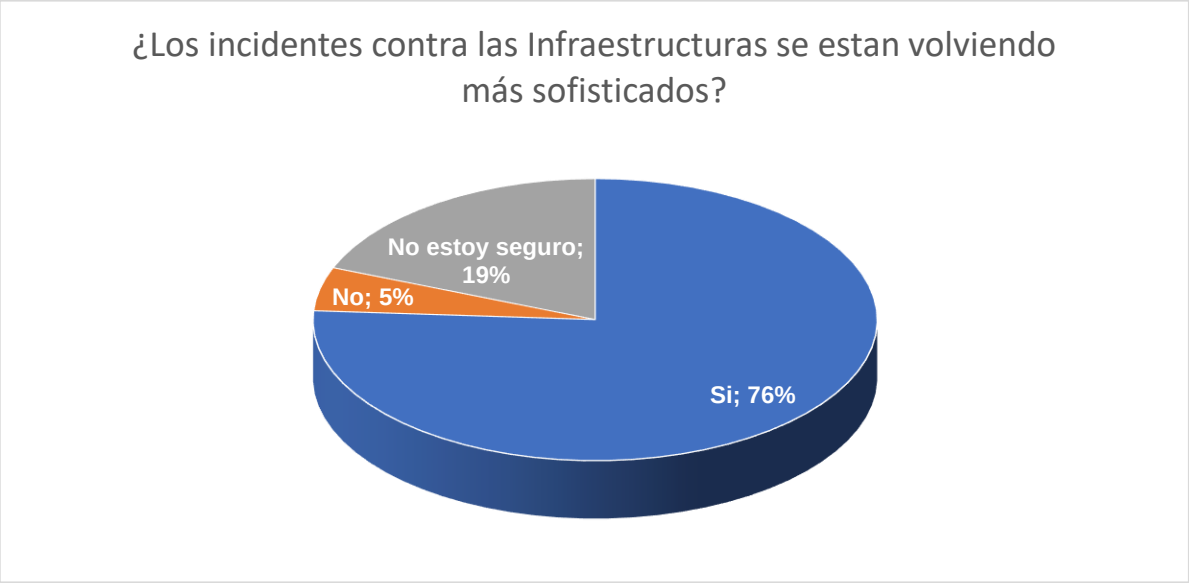


Fuente: Elaboración propia según "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?"[204]. OEA 2016

[203] Ídem

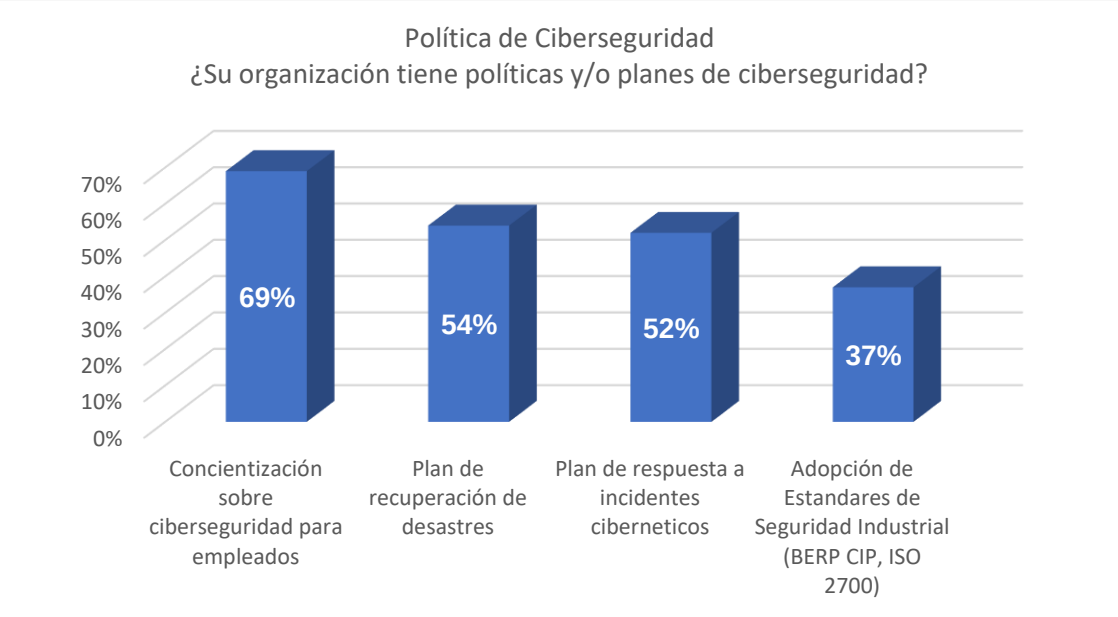
[204] Ciberseguridad Estamos preparados en América Latina y el Caribe. OEA-BID. 2016. Pág. 76

Gráfica 4



Fuente: Elaboración propia con datos de "Reporte de Seguridad Cibernética y Protección de las Infraestructuras Críticas en las Américas"[205]

Gráfica 5



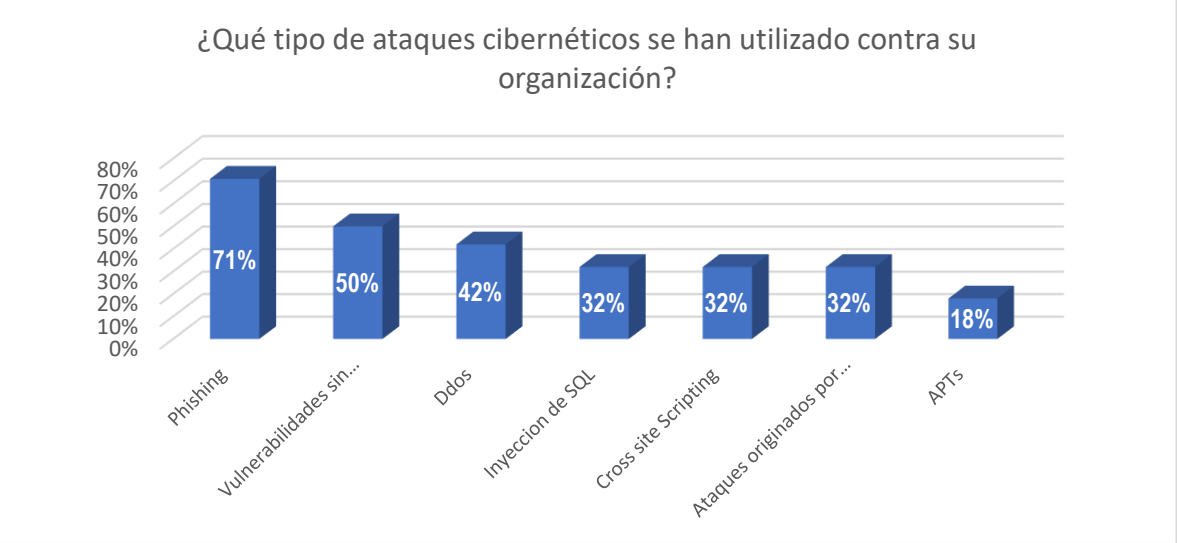
Fuente: Elaboración propia con datos de "Reporte de Seguridad Cibernética y Protección de las Infraestructuras Críticas en las Américas"[206]

[205] Ídem
[206] Ídem

Gráfica 6

Fuente: Elaboración propia con datos de "Reporte de Seguridad Cibernética y Protección de las Infraestructuras Críticas en las Américas"[207]

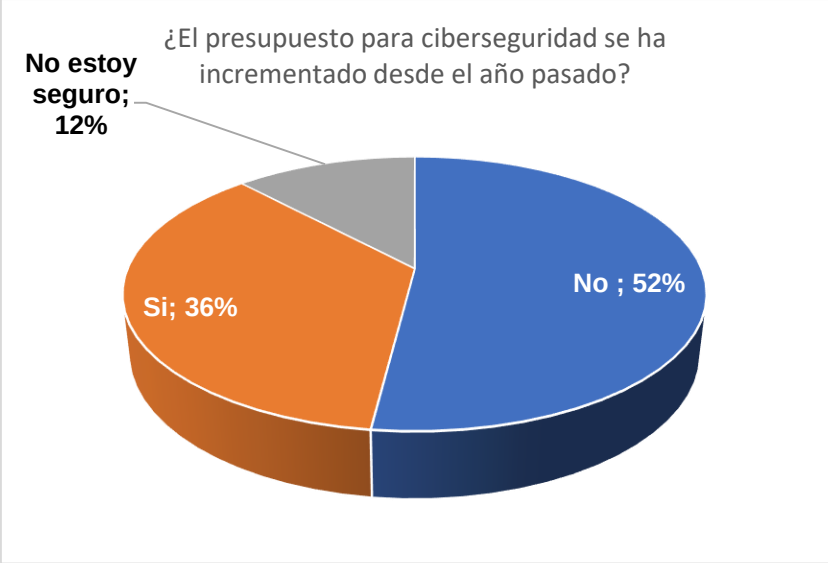
Gráfica 7



Fuente: Ídem

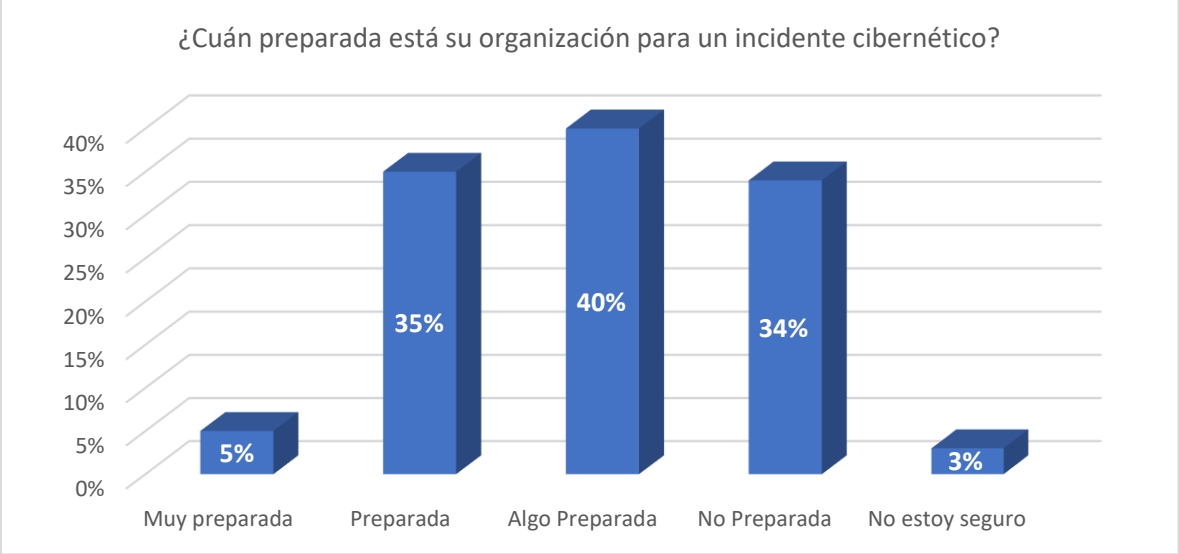
[207] Ídem

Gráfica 8



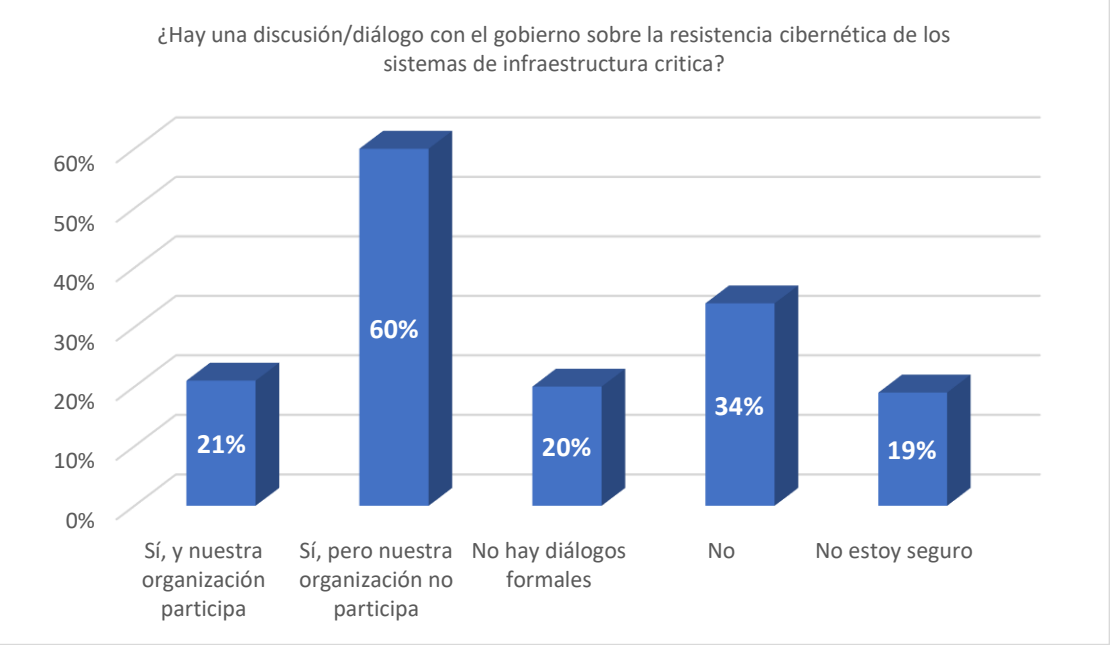
Fuente: Ídem

Gráfica 9



Fuente: Elaboración propia con datos de “Reporte de Seguridad Cibernética y Protección de las Infraestructuras Críticas en las Américas”. OEA. 2015

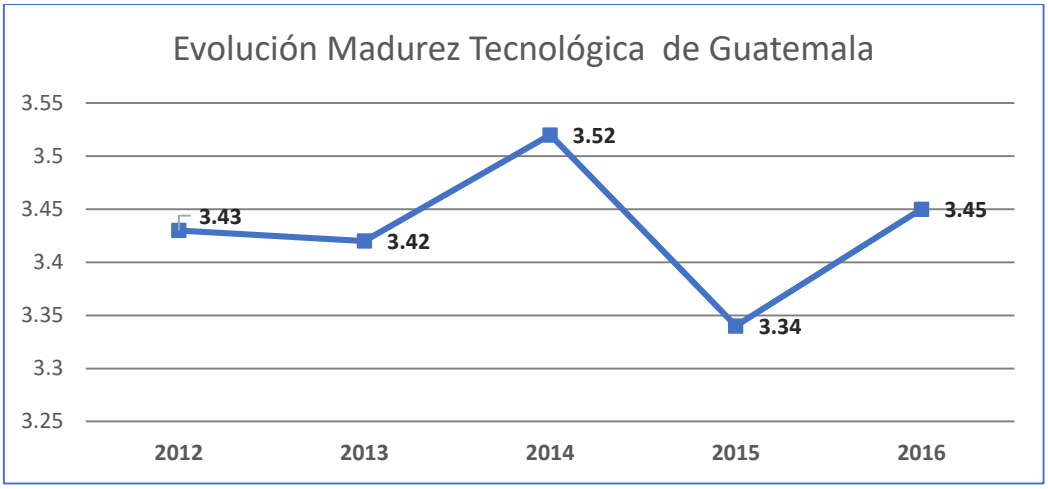
Gráfica 10



Fuente: Elaboración propia con datos de “Reporte de Seguridad Cibernética y Protección de las Infraestructuras Críticas en las Américas”. OEA. 2015

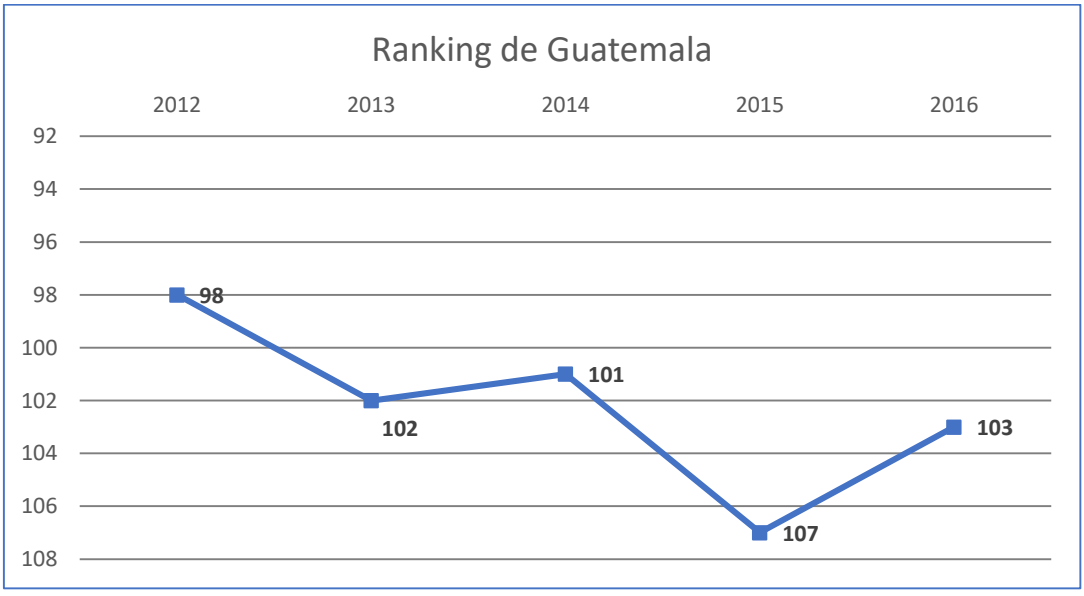
Anexo 2. Gráficas del Estado de Madurez tecnológica en Guatemala Según el Foro Económico Mundial

Gráfica 1



Fuente: Elaboración Propia con Datos de Foro Económico Mundial. Reporte GITR 2016[208]

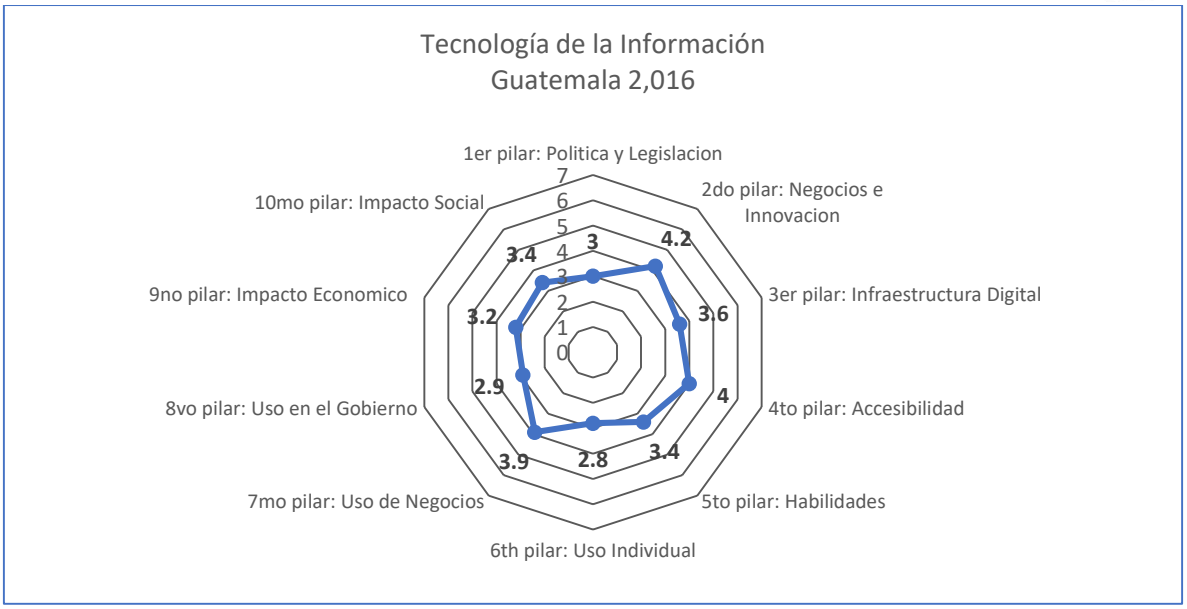
Gráfica 2



[208] http://reports.weforum.org/global-information-technology-report-2016/economies/#economy=GTM. Consultado el 10 de junio 2018

Fuente: Elaboración Propia con Datos de Foro Económico Mundial. Reporte GITR. 2012, 2013, 2014, 2015, 2016[209]

Gráfica 3



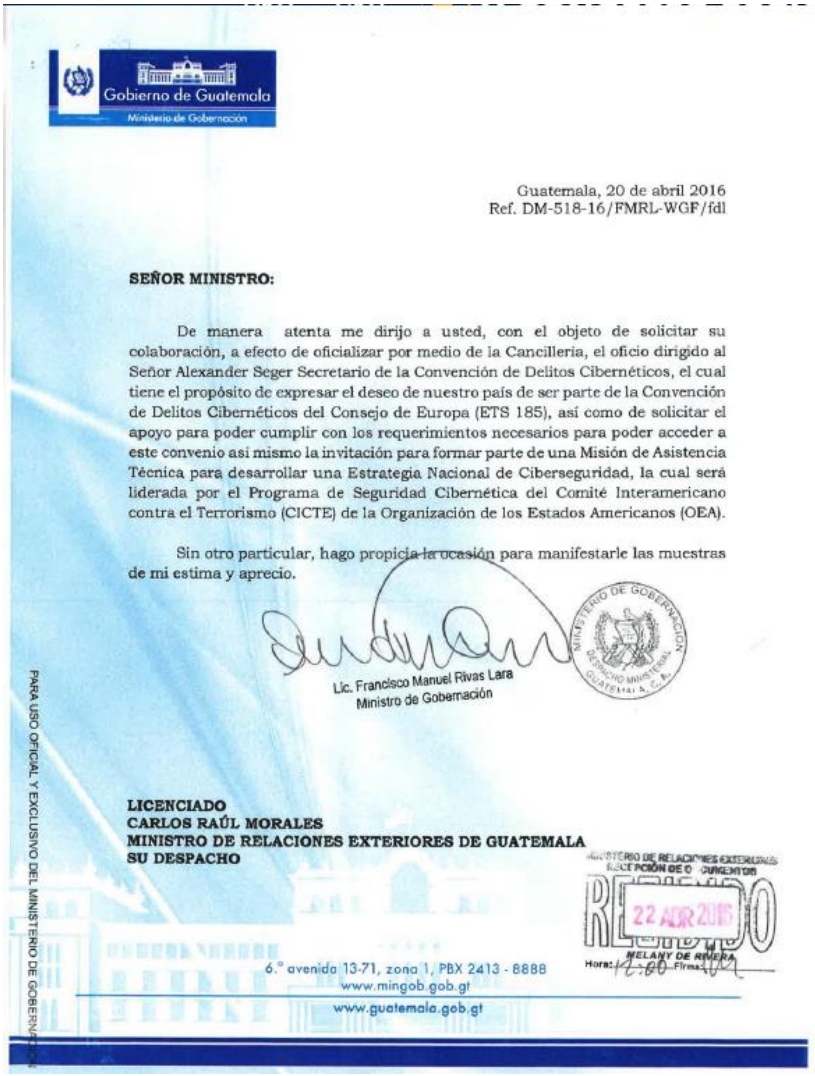
Fuente: Elaboración Propia con Datos de Foro Económico Mundial. Reporte GITR.2016[210]

[209] Reporte Global de Tecnologías de la Información (2012, 2013, 2014, 2015,2016). Foro Económico Mundial. Consultados en: https://www.weforum.org/reports. Consultado el 11 de junio 2018

[210] http://reports.weforum.org/global-information-technology-report-2016/economies/#economy=GTM. Consultado el 25 de enero de 2018

Anexo 3. Imágenes

Imagen 1



Gobierno de Guatemala
Ministerio de Gobernación

Guatemala, 20 de abril 2016
Ref. DM-518-16/FMRL-WGF/fdl

SEÑOR MINISTRO:

De manera atenta me dirijo a usted, con el objeto de solicitar su colaboración, a efecto de oficializar por medio de la Cancillería, el oficio dirigido al Señor Alexander Seger Secretario de la Convención de Delitos Cibernéticos, el cual tiene el propósito de expresar el deseo de nuestro país de ser parte de la Convención de Delitos Cibernéticos del Consejo de Europa (ETS 185), así como de solicitar el apoyo para poder cumplir con los requerimientos necesarios para poder acceder a este convenio así mismo la invitación para formar parte de una Misión de Asistencia Técnica para desarrollar una Estrategia Nacional de Ciberseguridad, la cual será liderada por el Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA).

Sin otro particular, hago propicia la ocasión para manifestarle las muestras de mi estima y aprecio.

Lic. Francisco Manuel Rivas Lara
Ministro de Gobernación

MINISTERIO DE GOBERNACIÓN
DESPACHO MINISTERIAL
GUATEMALA, C. A.

LICENCIADO
CARLOS RAÚL MORALES
MINISTRO DE RELACIONES EXTERIORES DE GUATEMALA
SU DESPACHO

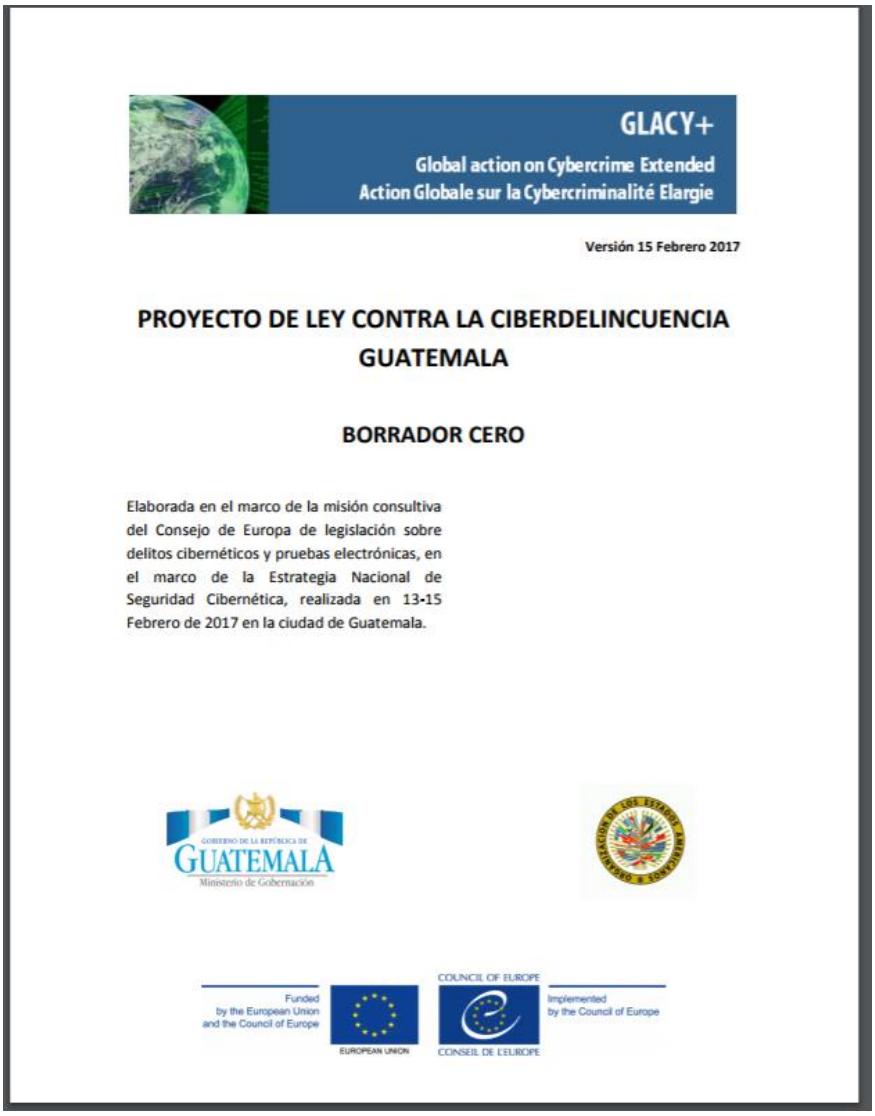
MINISTERIO DE RELACIONES EXTERIORES
RECEPCIÓN DE DOCUMENTOS
RECIBIDO
22 ABR 2016
Hora: 12:00 Firma:
MELANY DE RIVERA

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

PARA USO OFICIAL Y EXCLUSIVO DEL MINISTERIO DE GOBERNACIÓN

Fuente: Ministerio de Gobernación

Imagen 2



GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Versión 15 Febrero 2017

PROYECTO DE LEY CONTRA LA CIBERDELINCUENCIA
GUATEMALA

BORRADOR CERO

Elaborada en el marco de la misión consultiva del Consejo de Europa de legislación sobre delitos cibernéticos y pruebas electrónicas, en el marco de la Estrategia Nacional de Seguridad Cibernética, realizada en 13-15 Febrero de 2017 en la ciudad de Guatemala.

GUATEMALA
Ministerio de Gobernación

Funded by the European Union and the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Implemented by the Council of Europe

Fuente: Borrador Cero presentado ante el congreso como propuesta de Ley contra la Ciberdelincuencia en Guatemala

Imagen 3

Gobierno de Guatemala
Ministerio de Gobernación

Guatemala, 1 de marzo de 2016
Ref. DM-256-16/FMRL-fdl

SEÑOR MINISTRO:

De manera atenta me dirijo a usted, para hacer de su conocimiento que el Ministerio de Gobernación participó en el **Decimosexto Periodo Ordinario de Sesiones del Comité Interamericano Contra el Terrorismo (CICTE)** el cual se llevó a cabo los días del 24 al 27 de febrero de 2016 en la Ciudad de Washington, D.C. Estados Unidos de América.

En dicho evento se hizo contacto con la Secretaría Técnica de la Organización de Estados Americanos –OEA-, quienes han sido un enlace importante para los avances en materia de combate del Cibercrimen y del Ciberterrorismo en Guatemala y quienes ofrecen diferentes actividades que son de interés al Ministerio de Gobernación en materia de Seguridad Cibernética.

Derivado de lo anterior, me permito solicitar se gestione el apoyo de una **Misión de Asistencia Técnica Legislativa** con funcionarios gubernamentales de nivel superior sobre la ratificación e implementación de la Convención Interamericana contra el Terrorismo y los instrumentos jurídicos universales contra el terrorismo, la cual deberá derivarse la elaboración e implementación de una **Estrategia de Ciberseguridad Nacional**. Esta Estrategia podrá ser la base para la promoción de una iniciativa de Ley contra el Cibercrimen y el Ciberterrorismo.

Este Despacho Superior, designa al Licenciado Walter Girón Figueroa, Cuarto Viceministro de Gobernación, para dar seguimiento a las actividades propuestas, así como para ampliar cualquier información al respecto.

Sin otro particular aprovecho la ocasión para suscribirme de usted, con las muestras de mi estima y aprecio.

Lic. Francisco Manuel Rivas Lara
Ministro de Gobernación

MINISTERIO DE GOBERNACIÓN
DESPACHO MINISTERIAL
GUATEMALA, C. A.

LICENCIADO
CARLOS RAÚL MORALES MOSCOSO
MINISTRO DE RELACIONES EXTERIORES
SU DESPACHO

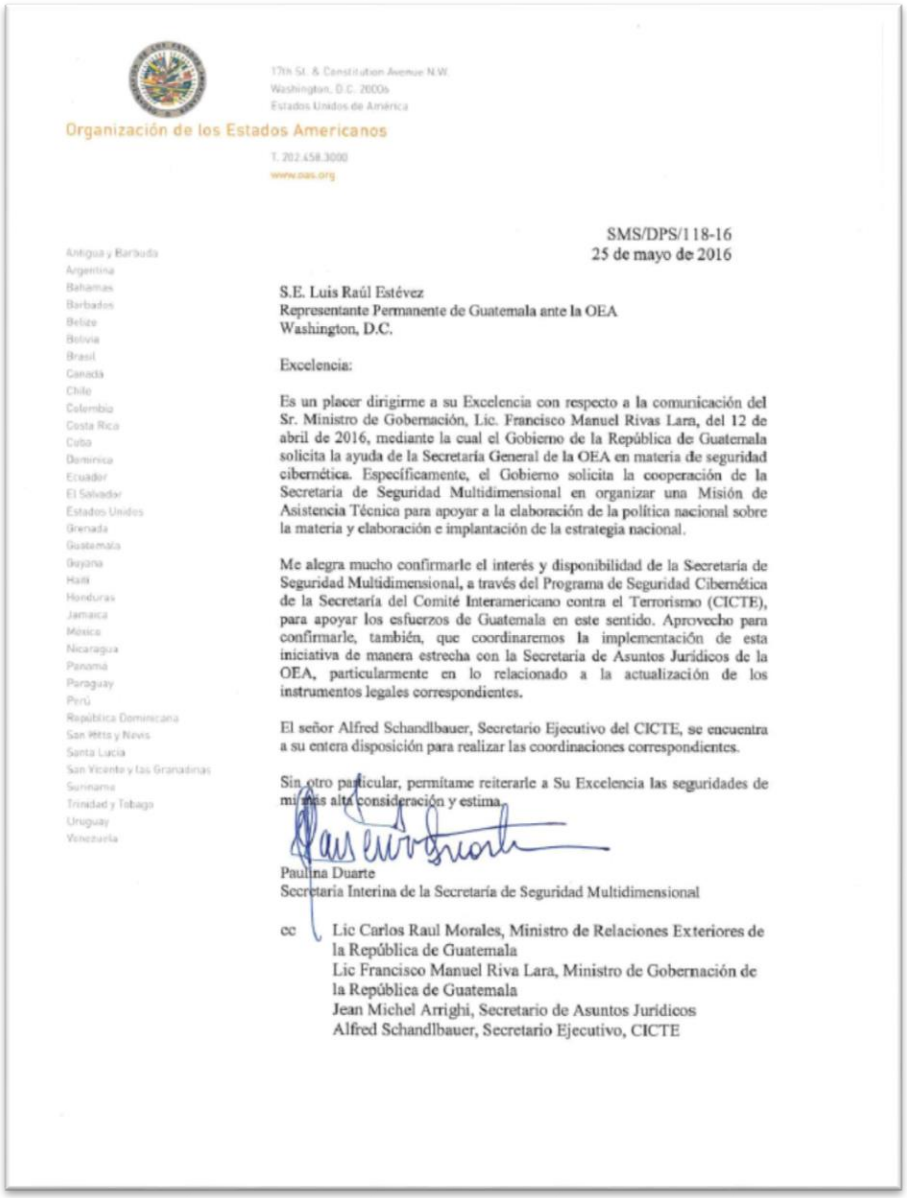
c.c. Cuarto Viceministro de Gobernación

MINISTERIO DE GOBERNACIÓN
CUARTO VICEMINISTERIO
RECEPCION
08 MAR 2016
Hora: 4:31 Firma:

6ta. Avenida 13-71 zona 1, Teléfonos PBX: 2412 - 0800
www.mingob.gob.gt
www.guatemala.gob.gt

Fuente: Archivo Ministerio de Gobernación

Imagen 4



17th St. & Constitution Avenue N.W.
Washington, D.C. 20006
Estados Unidos de América

Organización de los Estados Americanos

T. 202.458.3000
www.oas.org

Antigua y Barbuda
Argentina
Bahamas
Barbados
Belize
Bolivia
Brasil
Canadá
Chile
Colombia
Costa Rica
Cuba
Dominica
Ecuador
El Salvador
Estados Unidos
Grenada
Guatemala
Guyana
Haití
Honduras
Jamaica
México
Nicaragua
Panamá
Paraguay
Perú
República Dominicana
San Kitts y Nevis
Santa Lucía
San Vicente y las Granadinas
Suriname
Trinidad y Tobago
Uruguay
Venezuela

SMS/DPS/118-16
25 de mayo de 2016

S.E. Luis Raúl Estévez
Representante Permanente de Guatemala ante la OEA
Washington, D.C.

Excelencia:

Es un placer dirigirme a su Excelencia con respecto a la comunicación del Sr. Ministro de Gobernación, Lic. Francisco Manuel Rivas Lara, del 12 de abril de 2016, mediante la cual el Gobierno de la República de Guatemala solicita la ayuda de la Secretaría General de la OEA en materia de seguridad cibernética. Específicamente, el Gobierno solicita la cooperación de la Secretaría de Seguridad Multidimensional en organizar una Misión de Asistencia Técnica para apoyar a la elaboración de la política nacional sobre la materia y elaboración e implantación de la estrategia nacional.

Me alegra mucho confirmarle el interés y disponibilidad de la Secretaría de Seguridad Multidimensional, a través del Programa de Seguridad Cibernética de la Secretaría del Comité Interamericano contra el Terrorismo (CICTE), para apoyar los esfuerzos de Guatemala en este sentido. Aprovecho para confirmarle, también, que coordinaremos la implementación de esta iniciativa de manera estrecha con la Secretaría de Asuntos Jurídicos de la OEA, particularmente en lo relacionado a la actualización de los instrumentos legales correspondientes.

El señor Alfred Schandlbauer, Secretario Ejecutivo del CICTE, se encuentra a su entera disposición para realizar las coordinaciones correspondientes.

Sin otro particular, permítame reiterarle a Su Excelencia las seguridades de mi más alta consideración y estima.

Paulina Duarte
Secretaria Interina de la Secretaría de Seguridad Multidimensional

cc Lic Carlos Raul Morales, Ministro de Relaciones Exteriores de la República de Guatemala
Lic Francisco Manuel Riva Lara, Ministro de Gobernación de la República de Guatemala
Jean Michel Arrighi, Secretario de Asuntos Jurídicos
Alfred Schandlbauer, Secretario Ejecutivo, CICTE

Fuente: Archivo Ministerio de Gobernación/OEA

Imagen 5

Fuente: Ministerio de Gobernación. Evento de definición de la estrategia de ciberseguridad para Guatemala. De izquierda a derecha en la mesa principal. Sra. Milagros Martínez, embajadora de la OEA, Sra. Devora Chatsey, embajadora de Canadá, Sr. Alfonso Portabales, embajador de España, Walter Giron, viceministro de Tecnologías, Ministerio de Gobernación[211]

[211] http://mingob.gob.gt/realizan-primer-borrador-de-la-estrategia-nacional-de-ciberseguridad/. Consultado el 25 de enero del 2,018.

Anexo 4. Convenio de Budapest

La estructura del convenio de Budapest es la siguiente:

Capítulo I. Terminología: Presenta las definiciones formales sobre que es dato informático, sistema informático, proveedor de servicios y datos relativos al tráfico.

Capitulo II. Medidas que deberán adoptarse a Nivel Nacional. En donde sección 1 aborda El Derecho Penal Sustantivo. En el Titulo 1 tipifica delitos como Acceso Ilícito, Interceptación Ilícita, Ataques a la integridad de los datos y el sistema. En el titulo 2, delitos informáticos, aborda los temas de falsificación informática y fraude informático. El título 3 menciona los delitos relacionados con el contenido y tipifica los delitos relacionados con la pornografía infantil, entre otros. El título 4 trata sobre delitos relacionados con infracciones a la propiedad intelectual y de derechos afines. El título 5 menciona otras formas de responsabilidad y sanción, como la tentativa y la complicidad, la responsabilidad de las personas jurídicas y las sanciones y medidas.

En la sección 2 se refiere al Derecho Procesal. En el Título 1, Disposiciones comunes, se aborda el ámbito de aplicación de las disposiciones de procedimiento, condiciones y salvaguardias. El título 2 trata la conservación rápida de datos informáticos almacenados. El Título 3, se ocupa de lo referido a la Orden de presentación. El título 4 es sobre el Registro y confiscación de datos informáticos almacenados. El Título 5, Obtención en tiempo real de datos informáticos relativos al tráfico, contempla “obligar a cualquier proveedor de servicios en la medida de sus capacidades técnicas a obtener o grabar con medios técnicos existentes en su territorio o a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al tráfico asociados o

comunicaciones especificas transmitidas en su territorio por medio de un sistema informático"[212], también se contempla la interceptación de datos.

En la sección 3 se aborda la jurisdicción, el artículo 22 dice "cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos del 2 al 11 del presente convenio, cuando el delito se haya cometido a.) en su territorio; o b.) a bordo de un buque que enarbole su pabellón o c.) a bordo de una aeronave matriculada según sus leyes o d.) por uno de sus nacionales, si el delito es susceptible a sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto de este. " [213]

Capítulo 3. Cooperación Internacional: Sección 1 Principios Generales. El título 1, Principios Generales relativos a la cooperación internacional. Título 2, Principios Relativos a la Extradición. Título 3, Principios Generales a la asistencia mutua. Título 4, Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

Sección 2, Disposiciones específicas. Título 1, Asistencia Mutua en materia de medidas provisionales. Trata de la asistencia entre países sobre la conservación de rápida de datos informáticos almacenados. La revelación rápida de los datos conservados. Título 2, Asistencia mutua en relación con el acceso a datos almacenados. El título 3 se refiera al sistema de Red 24/7 y se menciona "cada parte designará 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 a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda

[212] *Convenio sobre la ciberdelincuencia ETS 185*. Concejo de Europa. Budapest 23 nov. 2001. Pág. 16. Consultado en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
[213] Convenio sobre la ciberdelincuencia ETS 185, Consejo de Europa. Budapest 23 nov. 2001. Pág. 14. Consultado en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

acción que facilite las medidas que figuran a continuación o su aplicación directa si lo permite el derecho y la práctica internos a.) asesoramiento técnico; b.) conservación de datos, de conformidad con los artículos 29 y 30; y c.) obtención de pruebas, suministro de información de carácter jurídico y la localización de sospechosos.

Capitulo IV. Cláusulas finales: Trata la adhesión al convenio por parte de los Estados interesados, la aplicación territorial, Efectos del convenio, Reservas del convenio, Enmiendas, Solución de controversias, Denuncias, Notificaciones

Anexo 5. Tabla de variables en materia de ciberseguridad de la OEA

Tabla 1

Eje	Subeje	Punteo para Guatemala
Política y Estrategia		**1 (5 el más alto)**
Estrategia Nacional de Seguridad Cibernética Oficial y Documentada	Desarrollo de la Estrategia	Inicial (1 de 5)
	Organización	Inicial (1 de 5)
	Contenido	Inicial (1 de 5)
Defensa Cibernética	Estrategia	Inicial (1 de 5)
	Organización	Inicial (1 de 5)
	Coordinación	Inicial (1 de 5)
Cultura y Sociedad		**1.44 (5 el más alto)**
Mentalidad de Seguridad cibernética	En el gobierno	Inicial (1 de 5)
	En el Sector Privado	Formativo (2 de 5)
	En la Sociedad	Inicial (1 de 5)
Conciencia de seguridad cibernética	Sensibilización	Inicial (1 de 5)
Confianza en el uso de Internet	En los servicios en línea	Formativo (2 de 5)
	En el gobierno electrónico	Inicial (1 de 5)
	En el comercio electrónico	Formativo (2 de 5)
Privacidad en Línea	Normas de Privacidad	Formativo (2 de 5)
	Privacidad del Empleado	Inicial (1 de 5)
Educación		**1.8 (5 el más alto)**
	Educación	Formativo (2 de 5)

Disponibilidad nacional de la educación y formación cibernéticas	Formación	Formativo (2 de 5)
Desarrollo nacional de la educación de seguridad cibernética	Desarrollo nacional de la educación de seguridad cibernética	Inicial (1 de 5)
Formación e iniciativas educativas públicas y privadas	Capacitación de empleados	Formativo (2 de 5)
Gobernanza corporativa, conocimiento y normas	En las empresas estatales y privadas	Formativo (2 de 5)
Marcos Legales		**1.5 (5 el más alto)**
Marcos jurídicos de seguridad cibernética	Para la seguridad de las TIC	Inicial (1 de 5)
	Privacidad, protección de datos y otros derechos humanos	Formativo (2 de 5)
	Derecho sustantivo de delincuencia cibernética	Formativo (2 de 5)
	Derecho procesal de delincuencia cibernética	Inicial (1 de 5)
Investigación Jurídica	Cumplimiento de la ley	Formativo (2 de 5)
	Fiscalía	Inicial (1 de 5)
	Tribunales	Formativo (2 de 5)
Divulgación responsable de la información	Divulgación responsable de la información	Inicial (1 de 5)
Tecnologías		**1.10 (5 el más alto)**

Adhesión a las normas	Aplicación de las normas y practicas mínimas aceptables	Inicial (1 de 5)
	Adquisiciones	Inicial (1 de 5)
	Desarrollo de Software	Inicial (1 de 5)
Organizaciones de coordinación de seguridad cibernética	Centro de mando y control	Inicial (1 de 5)
	Capacidad de respuesta a incidentes	Inicial (1 de 5)
Respuesta a incidentes	Identificación y designación	Formativo (2 de 5)
	Organización	Inicial (1 de 5)
	Coordinación	Inicial (1 de 5)
Resiliencia de la infraestructura nacional	Infraestructura tecnológica	Formativo (2 de 5)
	Resiliencia nacional	Inicial (1 de 5)
Protección de la Infraestructura Crítica Nacional	Identificación	Inicial (1 de 5)
	Organización	Inicial (1 de 5)
	Planeación de respuesta	Inicial (1 de 5)
	Coordinación	Inicial (1 de 5)
	Gestión de Riesgos	Inicial (1 de 5)
Gestión de Crisis	Planeación	Inicial (1 de 5)
	Organización	Inicial (1 de 5)
Mercado de la ciberseguridad	Tecnologías de seguridad cibernética	Inicial (1 de 5)
	Seguros de delincuencia cibernética	Inicial (1 de 5)

Fuente: Elaboración propia según "Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?"[214]

[214] *Ciberseguridad: "Estamos preparados en América Latina y el Caribe?"*, OEA-BID. 2016. Pág. 123

Anexo 6. Criterios para catalogar infraestructura crítica en España

Tabla 1

Criterios Horizontales			
Número de Personas Afectadas	Víctimas Mortales	Heridos con Lesiones Graves	Consecuencias para la Salud Pública
Impacto Económico	Magnitud de las pérdidas económicas	Deterioro de Productos y Servicios	
Impacto Medioambiental	Degradación del lugar y sus alrededores		
Impacto público y social	Confianza de la población en la capacidad de las Administraciones públicas	Sufrimiento Físico y la alteración de la vida cotidiana	Pérdida y el grave deterioro de servicios esenciales

Fuente: Elaboración propia con información de BOE-A-2011-7630. Ley de Protección de Infraestructura Crítica. España[215]

[215] Ley de Protección de Infraestructura Crítica. BOE-A-2011-7630.2011. Gobierno de España. Consultado en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf. Consultado el 21 de junio 2017

Bibliografía

AGIES. (2018). *Normas de Seguridad Estructural para Guatemala.* Guatemala.

Aguayo, S. (2002). *En busca de la Seguridad Perdida.* México: Siglo Veintuno Editores.

al, J. M. (1994). *Seguridad y Protección de la Información.* Madrid: Centro de Estudios Ramón Areces.

al, S. O. (2012). *Seguridad Informatica Contribuciones a las Ciencias Sociales.*

Armando, L. F. (2014). *Los Sistemas de Apoyo en la Toma de Decisiones.*

Bauman, Z. (2001). *En Busca de la Política.* Argentina: Fondo de Cultura Económica.

BBVA, O. (2016). *Los Big Data y el Futuro de los Negocios.*

Caro, M. (2011). *Proteccion a la Infraestructuras Criticas.* España: Instituto Español de Asuntos Estrategicos.

Claria, J. (1998). *Derecho Procesal Penal.* Santa Fé: Rubinzal-Culzoni.

Colombia, G. d. (2016). *Política Nacional de Seguridad Digital.* Bogotá.

Conde, M. (2010). *Derecho Penal.* Valencia: Tirant lo Blanch.

Corzo, J. F. (2014). *¿Cómo diseñar una política pública?* Mexico.

Elguea, J. (1993). *Seguridad Internacional y el Desarrollo Nacional.* Alianza Editorial.

España, G. d. (2007). *Plan Nacional de Protección de Infraestructuras Críticas.* España.

España, G. d. (2010). *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio.* España.

España, G. d. (2010). *Plan Nacional para la Protección de las Infraestructuras Criticas.*

España, G. d. (2011). *Ley de Protección de Infraestructura Crítica.* Madrid: Gobierno de España.

España, G. d. (2011). *Reglamento de Ley de Protección de Infraestructura Critica.*

España, G. d. (2013). *Estrategia Nacional de Seguridad Nacional.*

Europea, U. (2001). *Convenio sobre la Ciberdelincuencia.* Bruselas.

Evans, P. (2015). *Reconstruir la empresa en la Era Digital.* Madrid: BBVA Press.

Fernandez, C. (2012). *La norma ISO:27001 del Sistema de Gestión de la Seguridad de la Información.* España.

Flores, R. D. (2004). *Amparo, Habeas Corpus y Habeas Data.* Montevideo.

Gomez, R. (2013). *Gestión de políticas públicas: aspectos operativos.* Antioquia: Universidad de Antioquia.

Guatemala, G. d. (1985). *Constitución Politica de la República de Guatemala.* Guatemala.

Guatemala, G. d. (1992). *Código Procesal Penal.* Guatemala.

Guatemala, G. d. (1993). *Código Penal.* Guatemala.

Guatemala, G. d. (2002). *Ley de Bancos y Grupos Financieros.* Guatemala.

Guatemala, G. d. (2005). *Ley del Registro Nacional de Personas.* Guatemala.

Guatemala, G. d. (2006). *Ley Contra la Delincuencia Organizada de la República de Guatemala.* Guatemala.

Guatemala, G. d. (2008). *Ley Marco del Consejo Nacional de Seguridad.* Guatemala: Gobierno de Guatemala.

Guatemala, G. d. (2008). *Reglamento de la Ley Marco del Sistema Nacional de Seguridad.* Guatemala.

Guatemala, G. d. (2009). *Iniciativa de Ley de Delitos Informáticos.* Guatemala: Congreso de la República.

Guatemala, G. D. (2012). *Política Nacional de Seguridad.* Guatemala: Gobierno de Guatemala.

Guatemala, G. d. (2017). *Iniciativa de ley contra la Ciberdelincuencia.* Guatemala: Congreso de la República.

Guatemala, G. d. (2017). *Política Nacional de Seguridad.* Guatemala.

Guatemala, G. d. (2019). *Acuerdo Gubernativo 65-2019.* Guatemala.

Guatemala, G. d. (2019). *Iniciativa de Ley de Prevención y Protección contra la Ciberdelincuencia.* Guatemala: Congreso de la República.

Guatemala, S. d. (2018). *Agenda Nacional de Riesgos y Amenazas.*

Hobbes, T. (1993). *Leviatán.* Madrid: Alianza Editorial.

Joyanes, L. (2011). *Introducción. Estado del arte de la ciberseguridad.* España.

Lanier, J. (2014). *Quien Controla El Futuro.* Debate.

Lyns, W. J. (2010). *Foreing Affairs.*

Mexico, G. d. (2017). *Estrategia Nacional de Ciberseguridad.*

Moore, G. (1965). *Cramming more components into integrated circuits.* Florida, Estados Unidos: Universidad de Florida.

Mundial, F. E. (2012). *Reporte Global de Tecnologías de la Información.* Washington: Foro Económico Mundial.

Mundial, F. E. (2015). *Reporte Global de Tecnologías de la Información.* Washington: Foro Económico Mundial.

Mundial, F. E. (2016). *Reporte Global de Tecnologías de la Información.* Washington: Foro Económico Mundial.

Naim, M. (2013). *El Fin del Poder.* Argentina: Debate.

OEA. (1978). *Convención Americana sobre Derechos Humanos.* San José: OEA.

OEA. (2003). *Declaración sobre Seguridad de las Américas.* Mexico: OEA.

OEA. (2014). *Una estrategia interamericana integral de seguridad cibérnetica.*

OEA. (2015). *Declaración Protección de Infraestructura Crítica ante las amenazas emergentes.* Washington: OEA.

OEA. (2019). *Ciberseguridad Marco NIST.* Washington: OEA.

OEA-BID. (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* Washington, EUU: OEA.

OEA-TRENDMICRO. (2015). *Reporte de Seguridad Cibernética y Protección de la Infraestructura Crítica.* Washington: OEA.

Oppenheimer, A. (2010). *Basta de Historias. La obsesión latinoamericana con el pasado y las 12 claves del futuro.* Randon House.

Oppenheimer, A. (2014). *Crear o Morir.* Debate.

Oren, A. (2010). *IDF Dependence on Technology Spawns Whole New Battlefield.*

Rica, G. d. (2017). *Estrategia Nacional de Ciberseguridad de Costa Rica.*

Rousseau, J.-J. (2014). *El Contrato Social.* Barcelona: Pluton Ediciones.

Sagues, N. (1997). *El Habeas Data en Argentina.* Buenos Aires.

Schmidt, E. (2014). *El Futuro Digital.* Ediciones Anaya Multimedia.

SEGEPLAN. (2015). *Guía para la formulación de Políticas Públicas.* Gobierno de Guatemala.

STNS. (2012). *Política Nacional de Seguridad.* Guatemala: Gobierno de Guatemala.

Symantec. (2018). *Informe sobre las Amenazas para la Seguridad en Internet.*

Uruguay, G. d. (2014). *Política de Defensa Nacional.* Montevideo.

Vasco, G. (2011). *Guía de Evaluación de Políticas Públicas del Gobierno Vasco.* Navarra.

Vásquez, O. (2016). *Guerras de cuarta generacion y sus efectos en la Seguridad Estratégica de Guatemala.* Guatemala: Universidad San Carlos.

Wolff, J. (2012). *Filosofía Política.* Buenos Aires: Ariel.

Bibliografía por Internet

- http://revistasumma.com/30309/. Consultado el 15/04/2019
- http://meconectosinclavos.net.gt/. Consultado el 18/01/2020
- https://leyes.infile.com/index.php?id=198&id_iniciativa=925 . consultado el 15/04/2019
- http://mingob.gob.gt/realizan-primer-borrador-de-la-estrategia-nacional-de-ciberseguridad/ . consultado el 15/04/2019
- https://www.prensalibre.com/guatemala/justicia/gobierno-busca-protegerse-de-los-ciberdelitos/ .consultado el 15/04/2019
- https://www.merriam-webster.com/dictionary/security. Consultado el 15 de enero 2020
- https://dle.rae.es/seguridad%20?m=form2. Consultado el 15 de enero 2020
- http://www.ieee.es/Galerias/fichero/docs_marco/2011/DIEEEM05-2011EvolucionConceptoSeguridad.pdf. Consultado el 17 de enero 2020
- https://www.un.org/es/sections/un-charter/chapter-ix/index.html
- https://preyproject.com/blog/es/ciberamenazas-que-son-como-te-afectan-y-que-puedes-hacer-al-respecto/. Consultado el 29/01/2020
- Rosa María Juárez et al. Investigación sobre la Ley de Acceso a la Información Pública y Protección de Datos. Disponible en: http://www.redipd.org/actividades/talleres/La_Antigua_02_2014/common/Ponencias_Taller_La_Antigua./Guatemala.pdf. Consultado el 20 de febrero de 2016.
- López Carballo et al. Protección de datos y habeas data: una visión desde Iberoamérica. XVIII. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Proteccion_de_datos_y_habeas_data.pdf. Consultado el 22 de febrero de 2016.
- www.csirt.gt. Consultado el 4 de abril de 2019

- https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/octopus-2016-cooperation-against-cybercrime. Consultado el 18 de enero 2018
- http://seguridadcibernetica.mingob.gob.gt/wp-content/uploads/2016/09/Cybercrime-Law-Guatemala-Draft-Zero_FINAL.pdf. Consultado el 25 de enero del 2018
- https://www.prensalibre.com/guatemala/justicia/gobernacion-elaborara-ley-para-combatir-el-cibercrimen/ . consultado el 15/04/2019
- https://todos.gt/todos-presenta-iniciativa-contra-la-ciberdelincuencia/. Consultado el 20/01/2020
- https://elsiglo.com.gt/2019/09/18/corre-y-va-de-nuevo-iniciativa-5601-de-ciberseguridad/. Consultado el: 20/12/2019
- https://elsiglo.com.gt/2017/09/15/ley-bozal-ciberdelincuencia/. Consultado el 20/12/2019
- https://www.plazapublica.com.gt/content/cinco-leyes-que-nos-amenazan. Consultado el 17 de octubre 2019
- Mercedes Anton. Control de Pensamiento en las Sociedades.https://dialnet.unirioja.es/descarga/articulo/5073061.pdf. Consultado el 17 de octubre 2019.
- http://www.informaticalegal.com.ar/2007/03/02/declaracion-de-panama-sobre-la-proteccion-de-la-infraestructura-critica-en-el-hemisferio-frente-al-terrorismo/. Consultado el 25/01/2020
- Asamblea Mundial de Normalización de las Telecomunicaciones. UIT. 2016. Pág. 4 Consultado en: https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2016-PDF-S.pdf. Consultado el 26/01/2020
- http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf. Consultado el 20/01/2020
- La protección de Infraestructuras críticas y la ciberseguridad industrial". Primera Edición octubre 2013. Centro de Ciberseguridad Industrial. Página 8. Consultado en: https://www.cci-

es.org/documents/10694/331476/documento+PIC+y+CI.pdf/6f4f7e57-4719-4d85-ad27-7218800ca138 . Consultado el 24 de abril 2018

- http://www.icic.gob.ar/ . Consultado el 7 de febrero del 2018.
- https://www.elconfidencial.com/tecnologia/2017-06-27/ataque-ransomware-dla-piper-wannacry_1405839/. Consultado el 10 de junio 2018
- http://www.telesurtv.net/news/EE.UU.-apunta-a-Emiratos-Arabes-como-autor-del-ciberataque-a-Qatar-20170716-0046.html. Consultado el 10 de agosto 2018
- http://archivo.elcomercio.pe/tecnologia/actualidad/corea-sur-fue-victima-ciberataque-sospecha-norcorea-noticia-1552610. Consultado el 15 de agosto 2018
- https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html .Consultado el 20 de septiembre de 2018
- http://www.abc.es/20120609/internacional/rc-ciberataque-obama-contra-iran-201206090744.html. Consultado el 19 de septiembre 2018
- http://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet. Consultado el 10 de octubre 2016
- https://elpais.com/internacional/2019/06/24/actualidad/1561356118_942931.html. Consultado el 10 de enero 2020
- https://www.efe.com/efe/america/tecnologia/un-ataque-contra-los-servidores-en-ee-uu-ralentiza-internet-todo-el-mundo/20000036-3074810 . Consultado el 23/04/2018
- https://elpais.com/internacional/2019/06/23/estados_unidos/1561302401_346950.html. Consultado el 2 de Julio 2019
- https://www.perfil.com/noticias/internacional/la-seguridad-tiene-cinco-dominios-aire-tierra-mar-espacio-y-ciberespacio.phtml. Consultado el 23/09/2018
- http://www.bbc.com/mundo/noticias-41637526. Consultado el 20 de diciembre 2017

- https://elperiodico.com.gt/nacion/2019/06/02/nueva-comandancia-del-ejercito-despierta-desconfianza/. Consultado el 21 de enero 2020
- http://www.prensalibre.com/economia/sat-denuncia-por-ataques-a-enlaces-de-internet. Consultado el 20 de agosto 2017
- https://elperiodico.com.gt/nacion/2017/07/27/sigue-sabotaje-cibernetico-al-sitio-web-de-la-sat/. Consultado el 28 de diciembre 2017
- https://www.toptal.com/insights/innovation/blockchain-identity-management . Consultado el 7 de febrero 2018
- Informe Sobre las Amenazas para la Seguridad en Internet. Symantec. 2018. https://www.symantec.com/es/mx/security-center/threat-report . consultado el 2 de mayo 2018
- https://es.wikipedia.org/wiki/Zombi_(inform%C3%A1tica). Consultado febrero de 2018
- Microsoft. https://technet.microsoft.com/en-us/security/dd452420.aspx . Consultado febrero de 2018
- UNAM. https://www.cert.org.mx/historico/documento/index.html-id=20 . Consultado febrero de 2018
- Microsoft. https://news.microsoft.com/apac/2015/05/15/flight-to-quality-and-trust/ . Consultado febrero 2018
- Margaret Rouse. http://searchdatacenter.techtarget.com/es/definicion/Fraude-de-clic-fraude-de-pago-por-clic . Consultado en febrero de 2018
- Microsoft. https://blogs.technet.microsoft.com/seguridad/2013/12/06/alerta-microsoft-active-response-for-security-mars-operacin-b68-sirefefzeroaccess/. Consultado en febrero 2018
- http://www.bbc.com/news/technology-22795074 . Consultado en febrero 2018

- W32.Waledac treat analysis. Symantec. Consultado en: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/W32_Waledac.pdf . consultado el 18 de marzo 2018
- Sistema de Contabilidad Integrada Ministerio de Finanzas. Disponible en: http://www.minfin.gob.gt/index.php/?option=com_content&view=article&id=98&Itemid=697. Consultado el 12 de marzo 2019
- https://www.cyberseg.com/. Consultado el 27 de enero 2020
- https://devel.group/. Consultado el 27 de enero 2020
- https://www.widefense.com/. Consultado el 27 de enero 2020
- https://mingob.gob.gt/inauguaran-centro-de-respuesta-a-incidentes-ciberneticos/. Consultado el 20 de enero 2020
- http://www.cert.org/incident-management/services.cfm. Consultado 18 de julio 2018
- https://www.prensalibre.com/guatemala/justicia/pnc-se-alia-a-microsoft-contra-el-ciberdelito/. Consultado el 26 de enero 2020
- http://mingob.gob.gt/realizan-primer-borrador-de-la-estrategia-nacional-de-ciberseguridad/. Consultado el 25 de enero de 2018.
- http://www.redgealc.net/oea-apoya-a-guatemala-en-el-desarrollo-de-su-estrategia-nacional-de-ciberseguridad/contenido/6934/es/, consultado el 14 de nov. 2017
- https://es.wikipedia.org/wiki/Anexo:Pa%C3%ADses_firmantes_del_Convenio_de_Cibercrimen#Am%C3%A9rica. Consultado el 5 de enero del 2020
- http://autoridadcertificadora.guerrero.gob.mx/fec/que-es-la-fec.html#quees. Consultado el 20 de junio 2017
- http://portal.oas.org/Portal/Sector/SAP/DepartamentoparalaGesti%C3%B3nP%C3%BAblicaEfectiva/NPA/SobreProgramadeeGobierno/tabid/811/Default.aspx. Consultado 18 de agosto 2018
- https://dle.rae.es/?id=Ta2HMYR. Consultado el 2 de junio 2018

- https://www.agesic.gub.uy/innovaportal/v/163/1/agesic/gobierno_electronico_.html. Consultado el 3 de marzo 2017