UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

RAZONES SOCIOLÓGICAS DE LA CREACIÓN DE JUZGADOS Y FISCALÍAS ESPECIALIZADOS DERIVADOS DEL AUMENTO DE LA CIBERDELINCUENCIA DURANTE LOS MESES DE JUNIO A DICIEMBRE DEL AÑO 2020 EN GUATEMALA

KIMBERLY GABRIELA YAC DOMINGUEZ

GUATEMALA, JULIO DE 2023

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

RAZONES SOCIOLÓGICAS DE LA CREACIÓN DE JUZGADOS Y FISCALÍAS ESPECIALIZADOS DERIVADOS DEL AUMENTO DE LA CIBERDELINCUENCIA DURANTE LOS MESES DE JUNIO A DICIEMBRE DEL AÑO 2020 EN GUATEMALA

TESIS

Presentada a la Honorable Junta Directiva
de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

KIMBERLY GABRIELA YAC DOMINGUEZ

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

Y los títulos Profesionales de

ABOGADA Y NOTARIA

Guatemala, julio de 2023

HONORABLE JUNTA DIRECTIVA

DE LA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DE LA

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	M.Sc.	Henry Manuel Arriaga Contreras
VOCAL I:	Licda.	Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic.	Rodolfo Barahona Jácome
VOCAL III:	Lic.	Helmer Rolando Reyes García
VOCAL IV:	Br.	Javier Eduardo Sarmiento Cabrera
VOCAL V:	Br.	Gustavo Adolfo Oroxom Aguilar
SECRETARIA:	Licda.	Evelyn Johanna Chevez Juárez

TRIBUNAL QUE PRACTICÓ

EL EXAMEN TÉCNICO PROFESIONAL

Primera Fase:

Presidente:	Licda.	Paula Estefanie Osoy Chamo
Vocal:	Licda.	Ana Marce Castro
Secretaria:	Licda.	Orfa Mabely Santos Escobar

Segunda Fase:

Presidente:	Lic.	Juan Manuel Perny García
Vocal:	Lic.	Ignacio Blanco Ardón
Secretario:	Lic.	Raúl Antonio Castillo Hernández

RAZÓN: "Únicamente el autor es responsable de las Doctrinas sustentadas y contenido de la tesis". (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C.A.

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, 23 de julio de 2021.

Atentamente pase al (a) Profesional, **CARLOS EFRAÍN PERNILLA GONZÁLEZ**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **KIMBERLY GABRIELA YAC DOMÍNGUEZ**, con carné **201014279**, intitulado **ESTABLECIMIENTO DE LÍMITES EN EL USO Y FUNCIONAMIENTO DE ILÍCITOS COMETIDOS A TRAVÉS DE INTERNET.**

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

CARLOS EBERTITO HERRERA RECINOS
Jefe(a) de la Unidad de Asesoría de Tesis

Fecha de recepción 10 / 02 / 2022 f) _____
Asesor(a)
(Firma y Sello)

CARLOS EFRAÍN
CIENCIAS JURIDICAS
ABOGADO Y NOTARIO
PERNILLA

Lic. Carlos Efrain Pernilla Gonzalez
Abogado y Notario
7a.Av 9-20, zona 09, Edificio Jade, ciudad de Guatemala
Teléfonos: 54270163

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C.A.

Ciudad de Guatemala, 10 de Febrero de 2022

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
10 FEB 2022
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Licenciado
Carlos Ebertito Herrera Recinos
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala

Distinguido Licenciado Herrera Recinos:

En cumplimiento del nombramiento de fecha veintitrés de julio del año dos mil veintiuno, emitido por la Unidad de Asesoría de Tesis, procedí a **ASESORAR** el trabajo de tesis del bachiller **KIMBERLY GABRIELA YAC DOMINGUEZ**, intitulado: **"ESTABLECIMIENTOS DE LIMITES EN EL USO Y FUNCIONAMIENTO DE ILICITOS COMETIDOS A TRAVES DE INTERNET".** y que fue modificado según el desarrollo de su plan de tesis por **"RAZONES SOCIOLOGICAS DE LA CREACION DE JUZGADOS Y FISCALIAS ESPECIALIZADOS DERIVADOS DEL AUMENTO DE LA CIBERDELICUENCIA DURANTE LOS MESES DE JUNIO A DICIEMBRE DEL AÑO 2020 EN GUATEMALA"** Para el efecto me permito manifestar las siguientes opiniones:

a) En relación del contenido científico y técnico de la presente tesis, demuestra que efectivamente que cumple objetivamente con cada uno de los capítulos elaborados permitiendo un análisis concreto, así como conceptos y definiciones que puedan determinar la necesidad de establecimientos de límites en el uso y funcionamiento de ilícitos cometidos a través de internet. dándole un enfoque en el desarrollo del plan de tesis cuales pueden ser la razones sociológicas de la creación de juzgados y fiscalías especializados derivados del aumento de la ciberdelincuencia durante los meses de junio a diciembre del año 2020 en Guatemala

b) Así como la utilización de la metodología moderna concerniente al método jurídico que se utilizó para realizar un análisis respectivo cumple con los pasos necesarios en la deducción, como técnicas principales de investigación se utilización de la bibliografía de campo métodos de investigación deductiva y comparativa

c) La redacción de este trabajo reúne las condiciones exigidas en cuanto a tecnicismo, claridad y precisión adecuada jurídicamente correcto.

d) La contribución científica del trabajo de tesis en referencia, se centra en la búsqueda de encontrar establecimientos de límites en el uso y funcionamiento de ilícitos cometidos a través de internet, así mismo las razones sociológicas de la creación de juzgados y fiscalías especializados derivados del aumento de la ciberdelincuencia durante los meses de junio a diciembre del año 2020 en Guatemala

e) En mi opinión, las conclusiones y recomendaciones fueron redactadas en forma clara y sencilla, mismas que son congruentes con el tema investigado, haciendo aportaciones valiosas y propuestas concretas para su realización

f) La bibliografía empleada por el sustentante, fue adecuada, puntual moderna y acorde al tema objeto de investigación

En mi calidad de asesor, al haberse cumplido con todos los requisitos establecidos en el Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y Examen General Público referidos resulta pertinente aprobar el trabajo de investigación objeto de asesoría, por lo que para el efecto procedo a emitir el presente **DICTAMEN FAVORABLE.** a efecto se continúe el trámite, se nombre revisor y se culmine su aprobación en el examen general público.

Atentamente,

Lic. Carlos Efraín Pernilla Gonzalez
Abogado y Notario
Colegiado No. 19416

CARLOS EFRAIN PERNILLA GONZALEZ
CIENCIAS JURIDICAS Y SOCIALES
ABOGADO Y NOTARIO

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

Guatemala, 29 de abril de 2022

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
29 ABR 2022
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

DOCTOR CARLOS EBERTITO HERRERA RECINOS
JEFATURA DE LA UNIDAD DE ASESORÍA DE TESIS
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

Respetuosamente informo que procedí a revisar la tesis de la bachiller **KIMBERLY GABRIELA YAC DOMINGUEZ** cual se titula " **RAZONES SOCIOLÓGICAS DE LA CREACIÓN DE JUZGADOS Y FISCALÍAS ESPECIALIZADOS DERIVADO DEL AUMENTO DE LA CIBERDELINCUENCIA DURANTE LOS MESES DE JUNIO A DICIEMBRE DEL AÑO 2020 EN GUATEMALA".**
Le recomendé al bachiller algunos cambios en la forma, estilo, gramática y redacción de la tesis, por lo que habiendo cumplido con los mismos emito **DICTAMEN FAVORABLE** para que se le otorgue la correspondiente orden de impresión.

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
29 ABR 2022
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Atentamente,

"ID Y ENSEÑAD A TODOS"

Licda. Brenda Margarita Martínez Cerna

Docente consejera de la Comisión de Estilo

c.c. Unidad, estudiante.

Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala. Ciudad de Guatemala, diez de mayo de dos mil veintitrés.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis de la estudiante KIMBERLY GABRIELA YAC DOMÍNGUEZ, titulado RAZONES SOCIOLÓGICAS DE LA CREACIÓN DE JUZGADOS Y FISCALÍAS ESPECIALIZADOS DERIVADOS DEL AUMENTO DE LA CIBERDELINCUENCIA DURANTE LOS MESES DE JUNIO A DICIEMBRE DEL AÑO 2020 EN GUATEMALA. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

CEHR/SAQO

DEDICATORIA

A DIOS: Ser supremo que dirige mi camino por el sendero correcto.

A LA VIRGEN DE GUADALUPE: Por ser mi consuelo y compañía en este camino.

A MI PADRE: Carlos Armando Yac Guzmán por su apoyo y amor incondicional y su gran compromiso para motivarme a cumplir con mis metas, cuya satisfacción es para todos.

A MI MADRE: Laura Lilian Domínguez Gómez, quien, con su amor incondicional, por tener siempre la fortaleza de salir adelante sin importar los obstáculos, por su esfuerzo, quien me ha impulsado a ser mejor.

A MI HIJO: Antonny Matias Morales Yac, quien desde el día que supe de su existencia, ha sido el motor para superarme y pueda ofrecerle lo mejor en el mundo.

A MIS HERMANOS: Jesicka, Ethel, Manuel y Carlos, que con su apoyo, amor y presencia día con día me impulsan a salir adelante.

A MIS SOBRINOS: Michael, Diego, Nikol, Sebastián, Grecia, Natalia, Ariana, Rodrigo y Juan Pablo, con todo mi amor.

A MI ESPOSO: Antonny Morales, por su apoyo, y estar presente en toda esta etapa de mi vida.

A MIS CUÑADOS: Alex, Juan Carlos y Anabella con todo mi cariño.

A MIS ABUELAS: Juana Guzmán con cariño y María Teresa del Pilar Gómez (Q.E.P.D.) con todo mi amor.

A MIS TÍOS: Helder, Rebeca, Juan Daniel y María Elvira (Q.E.P.D.),con todo mi cariño.

A MIS PRIMOS: Juan Carlos, Dany, José, Helder, Jeimy, Rubí y Eric, con todo mi cariño.

A LOS PROFESIONALES: Carlos Efraín Pernilla González y Víctor Fernando Santizo Gómez, por su invaluable apoyo.

MIS AMIGOS: Por el apoyo y ánimos brindados para culminar este esfuerzo que sin duda es de todos. En especial a Luis, Carla, Andrea, Olga, Yessenia, Juan y Jorge Menocal (Q.E.P.D.).

A: La Tricentenaria Universidad de San Carlos de Guatemala.

A: Mi amada Facultad de Ciencias Jurídicas y Sociales, gracias

PRESENTACIÓN

La finalidad de la realización de la presente tesis intitulada "Razones Sociológicas de la Creación de Juzgados y Fiscalías Especializados, Derivado del Aumento de la Ciberdelincuencia durante los Meses de Junio a Diciembre del Año 2020 en Guatemala",es explicar los efectos sociales, jurídicos y económicos que causa el mal uso de las tecnologías de la información y comunicación, el Internet y las Redes Sociales en la actualidad, especialmente ante el incremento de su utilización por la emergencia sanitariaque afrontó el país en el año 2020 como consecuencia del COVID 19. Así como proponerla creación de juzgados especializados en el sector justicia con competencia y jurisdicción suficientes para atender los crímenes cibernéticos que atentan contra el patrimonio e integridad de los guatemaltecos. Además, promover capacitaciones especializadas a losfiscales para combatir los ciberdelitos, lo cual permitirá contrarrestar la ciberdelincuencia que impera en el país, facilitando mecanismos y medidas para detectar y perseguir a los ciberdelincuentes a nivel nacional e incluso internacional.

Por medio de la extensa investigación documental realizada, se comprobó el aumento que ha tenido este tipo de ataques cibernéticos, especialmente en el año 2020, con motivo de la pandemia COVID 19, comprobando además que Guatemala no cuenta con personal y equipo especializado para debilitar los ataques de la ciberdelincuencia. La creación de Juzgados y Fiscalías Especializados en ciberdelincuencia es una estrategia necesaria para la atención de los delitos cometidos por medios electrónicos, su ausencia hace que Guatemala sea uno de los países más vulnerable para la comisión de los ciberdelitos y que las personas no acudan a interponer las denuncias respectivas.Al no existir Juzgados Especializados en la atención de delitos informáticos se recarga eltrabajo en un solo juzgado y el personal no está altamente capacitado para ese tipo de delitos, dándole el mismo tratamiento a éstos como a los que comúnmente se atiende en ellos.

HIPÓTESIS

Es necesaria la creación de juzgados y fiscalías especializados para reducir y contrarrestar la ciberdelincuencia, en el país, la cual se ha incrementado en el año 2020, como consecuencia del necesario incremento de las tecnologías de la información y comunicación, el Internet y las Redes Sociales, como herramienta para continuar con el trabajo, estudios, negocios y demás actividades sociales necesarios para el desarrollo biopsicosocial del ser humano. Así como promover capacitaciones especializadas a los fiscales para combatir los ciberdelitos.

COMPROBACION DE LA HIPÓTESIS

La hipótesis fue comprobada por la autora, en virtud que las estrategias nacionales e internacionales que se han propuesto consideran la importante necesidad de la existencia en el país de juzgados con equipos especiales para detectar de donde proviene el ciberdelito además, Guatemala contaría con una herramienta para fortalecer la ciberseguridad y frenaría los ataques cibernéticos, motivando con ello a la población para acudir a interponer la denuncias respectivas para la pronta investigación por parte del personal especializado.

Es importante indicar que además se comprobó que los perfiles sociológicos de los ciberdelincuentes, los cuales incluyen conocimientos especializados y poder económico superior al de la población vulnerable, hacen que cada día los mismos tengan capacidades más creativas e innovadoras para modificar el modus operandi de la comisión de estos despreciables hechos delictivos.

ÍNDICE

Pág.

Introducción…… i

CAPÍTULO I

1. Sociología…….. 1

1.1. Definición…… 1

1.2. Historia…… 2

1.3. Objetivos de la Sociología…… 4

1.4. Importancia de la Sociología…… 4

1.5. Relación de la Sociología con el Derecho…….. 5

1.6. Métodos de la Sociología del Derecho…… 7

CAPÍTULO II

2. Ciberdelincuencia y Ciberdelitos…… 9

2.1. Ciberdelincuencia……... 9

2.1.1. Antecedentes…… 9

2.1.2. Definición…… 11

2.1.3. Tipos de ataques cibernéticos…… 11

- Ransomware……..... 13
- Ataque a las bases de datos…… 13
- Denegación de Servicio…… 14
- Phishing…… 14

- Cross-Site Scripting…… 14
- El spyware…… 15

2.1.4. Ataques cibernéticos que hicieron historia en el Mundo…… 15

2.1.5. Cómo surgió la Ciberdelincuencia en Guatemala…… 17

2.1.6. Ciberdelincuencia y sus consecuencias jurídicas…… 25

2.2 Ciberdelitos…….. 27

2.2.1 Definición de Ciberdelitos…….. 27

2.2.2 Características de los ciberdelitos…… 28

2.2.3 Delitos informáticos más comunes en Guatemala…… 31

2.2.4 Definición de los ciberdelincuentes…… 36

CAPÍTULO III

3. Ciberseguridad…….. 41

3.1 Antecedentes…… 41

3.2 Definición…….. 43

3.3 Finalidad de la Ciberseguridad……. 44

3.4 Como se da la Ciberseguridad en Guatemala…… 45

CAPÍTULO IV

4. Razones sociológicas para la creación de Juzgados y Fiscalías Especializados…….. 47

4.1 Creación de Juzgados Especializados……. 49

4.2 Creación de Fiscalías Especializadas…….. 52

4.3 Fines Específicos de los Organismos Especializados…….. 54

4.4 Instrumentos Internacionales en el Ámbito de Delitos Informáticos…… 58

4.4.1 Convenios Internacionales en el ámbito de delitos informáticos……. 59

4.4.2 La Organización de las Naciones Unidas y la prevención del delito informático…… 60

4.4.3 La Organización de Estados Americanos OEA y los delitos informáticos…… 62

CONCLUSIÓN DISCURSIVA……. 65

BIBLIOGRAFÍA…… 67

INTRODUCCIÓN

El presente trabajo de investigación tiene como propósito evaluar la necesidad de la creación de juzgados especializados en el Organismo Judicial, así como establecer de forma periódica y constante la capacitación y especialización de las fiscalías que atiendenlos asuntos de la ciberdelincuencia en el país. Contando el sistema judicial del país con personal capacitado y especializado en la materia de delitos informáticos y cibernéticos,ayudaría a contrarrestar la ciberdelincuencia, teniendo un equipo especial para detectar de donde proviene el ciberdelito, sus causas sociológicas, así como la propuesta para fortalecer la ciberseguridad, frenando los ataques cibernéticos y motivando a la poblaciónа denunciar los delitos con la confianza de una pronta y efectiva investigación por parte del personal especializado. El estudio refleja cómo influyen los determinantes sociológicos en la comisión de los delitos informáticos y como los roles del ente investigador, del sistema policial y judicial responden ante los mismos.

La presente investigación se realizó con un alcance exploratorio, documental y sociológico, pues la abundancia de información internacional al respecto, permite determinar las deficiencias del sistema de justicia nacional, pero fundamentalmente las deficiencias en tecnología, infraestructura y recursos humanos técnicos y especializadosque integran el sistema de justicia guatemalteco, la falta de cohesión con actores clave del sector público así como del sector privado para resolver dichas falencias.

En el primer capítulo se hace un análisis sociológico; en el capítulo dos se conceptualiza y define laciberdelincuencia y el ciberdelito; el capítulo tres pretende evidenciar la necesidad de contar con la Ciberseguridad; en el capítulo cuatro se desarrolla la comprobación de la hipótesis planteada por la autora en el presente estudio de investigación, la cual se considera que fue verificada pues el estudio ofrece lineamientos oportunos para ser tomados en cuenta a la hora de especializar el sistema de justicia, se evidencia la necesidad de contar con órganos jurisdiccionales y personal especializado y con amplios conocimientos en sistemas informáticos; constituyendo un insumo esencial en la toma de decisiones del sistema

de justicia guatemalteco, para incorporar juzgados y fiscalías especializadas con personal altamente conocedor de la era tecnológica que tanto desarrollo ha logrado para la humanidad, como perjuicio para el patrimonio y la indemnidad de las personas.

CAPÍTULO I

1. Sociología

1.1 Definición

El concepto de sociología puede definirse desde varios puntos de vista el eminentementejurídico, el social y el filosófico, por la naturaleza de lo que se pretende argumentar en elpresente estudio, es importante conocer una definición social "La Sociología es el estudiode la vida social humana, de los grupos y sociedades. El ámbito de la sociología es extremadamente amplio y va desde el análisis de los encuentros efímeros entre individuos en la calle hasta la investigación de los procesos sociales globales." Anthony Giddens, 1998.

Jurídicamente, es una rama de la sociología general, que enfoca el derecho como un fenómeno social; tratando de explicar sus características, su función en la sociedad, susrelaciones y las influencias entre esos fenómenos sociales; por lo cual, García Maynez ladenomina como la Sociología del Derecho y la define como la "disciplina que tiene por objeto la explicación del fenómeno jurídico, considerado como hecho social".

La sociología centra su atención principalmente en los seres humanos y su interacción en sociedad, es decir, el comportamiento de unos a otros frente a las circunstancias o hechos sociales y fundamentalmente describe y explica el comportamiento o actitud humana frente a los conflictos sociales que dentro de su contexto religioso, cultural, político, académico se desarrollan.

1.2 Historia

Desde tiempos remotos los filósofos han buscado comprender cómo la vida en sociedadse desarrolla y cómo su contexto influye en ella. Por ejemplo, Platón planteó un funcionamiento ideal de la vida humana en grupo. Seguido por Aristóteles, cuyo fin perseguido era la felicidad.

San Agustín expuso la doble posición del individuo que se debate entre el bien y el mal. En tanto que Santo Tomás explicaba el comportamiento humano desde una perspectiva cristiana.

Esta comprensión social de hechos, comportamiento y contexto en el cual se desarrolla la humanidad, permite predecir el resultado de las acciones que se van desarrollando enel mundo con aciertos y desaciertos de los individuos y cuya naturaleza puede no necesariamente ser positiva e ideal para su desenvolvimiento.

En la historia de la sociología se pueden evidenciar grandes teóricos que desde su origenhasta el desarrollo de su concepción dieron aportes valiosos y fundamentales en la historia de la misma. Entre ellos se puede mencionar a Augusto Comte, Henri Saint-Simon, Émile Durkheim, Karl Marx y Max Weber. De quienes se referirá los aspectos más relevantes.

Augusto Comte (1798-1857), empleó por primera vez la palabra sociología, y desarrolló además todo un estudio en relación con el comportamiento humano que vive en sociedad.Henri Saint-Simon (1760-1825), quién aun cuando ostentó un título nobiliario siendo conde, irónicamente pensaba que los conflictos que vivía en aquellos momentos la sociedad se podrían resolver si se lograba reorganizar la producción. Para ello, pensaba,era necesario privar de los medios de producción a los propietarios de éstos. Saint-Simonfue también quien dio origen al socialismo utópico.

Adicionalmente Émile Durkheim (1858-1917), bautizó a la sociología como aquella ciencia cuyo objetivo es estudiar lo que él denominaba hechos sociales. Es decir, el estudio de los fenómenos sociales que había que estudiar y analizar con el apoyo de la psicología.

Desde otros puntos de vista y perspectivas se brindaron aportes al estudio de la sociología entre ellos Adam Smith (1723-1790) y Karl Marx (1818-1883) quienes sin ser sociólogos estudiaron el comportamiento humano y cómo este aportó valor en lo que respecta a sus decisiones de empleo y riqueza en sociedad.

Para Adam Smith, los productores y prestadores de servicios ofrecían al mercado satisfactores, esto es la existencia de la "mano invisible". Para Karl Marx, existían dueñosde los medios de producción que se apropiaban del plusvalor que era producido por los trabajadores que eran explotados.

Por su lado Max Weber (1864-1920) fue considerado padre de la sociología moderna y fundamento sus estudios y análisis de la misma en el método científico para quien era fundamental en sus investigaciones. Weber aportó a la sociología la interpretación de lasacciones llevadas a cabo por los individuos de una sociedad. Por un lado, la interpretacióno valoración que los individuos daban a sus propias acciones y, por otro, el contexto socialen el que eso se producía.

Por qué se considera de importancia el estudio de la historia de la sociología para el desarrollo del presente trabajo de investigación: porque ese estudio sociológico permite proponer a la autora, la posibilidad de observar desde distintas perspectivas y puntos devista el comportamiento en los individuos frente a las tecnologías de la información y comunicación, el Internet y las Redes Sociales, además de las acciones que de manerailícita se pueden generar como conocimiento de la forma que el individuo

reacciona en sociedad ante diferentes acontecimientos. Acontecimientos que en el caso de estudiose desenvuelven en un contexto económico, cultural, tecnológico, entre otros, los cualesinfluyen y confluyen en el desarrollo en sociedad.

1.3 Objetivos de la Sociología

Para el presente estudio de investigación es necesario definir los objetivos de la sociología por la complejidad de acontecimientos sociales que han surgido con el fin de siglo XX y el inicio del siglo XIX por la incorporación de las Tecnologías de la Informacióny Comunicaciones -TIC-, el Internet y las Redes Sociales, en el contexto en el cual se desarrolla el individuo, por lo que se considera que una disciplina científica como la Sociología, proporcione un conocimiento científico y racional de los cambios sociales y tecnológicos contemporáneos.

El objetivo fundamental de la Sociología es comprender, explicar y diagnosticar el entornode la vida social en todas sus manifestaciones, utilizando una combinación de datos. Dicho conocimiento permite tomar decisiones para responder a las necesidades que se presentan en todos los ámbitos de la vida cotidiana, pero además permite decidir sobre las acciones encaminadas a responder las necesidades que la población guatemalteca exige en el ámbito jurídico, especialmente en la administración de justicia.

1.4 Importancia de la Sociología

Como se indicó supra, es importante el estudio de la sociología desde sus orígenes, su evolución e historia, pero además su contexto actual para lograr establecer la diferencia en el método de estudio de la sociedad entre las ciencias naturales o físicas y las ciencias sociales. Porque en el caso de las primeras todos los métodos, experimentos,

observaciones se llevan a cabo sobre todo dentro de cuatro paredes en laboratorios noasí en el caso de las ciencias sociales, cuyo estudio científico de lo social permite la recolección de datos, mediante información de personas que en el presente caso son extensos conocedores de la materia, lo cual constituye un desafío por lo subjetivo de losresultados, pero no por ello menos importante.

La sociología permite la construcción de perspectivas holísticas de la sociedad, ya que desglosa cada uno de los componentes y lo integra para conocer el fondo del comportamiento humano, en la presente investigación el estudio de la sociedad, *per se*, será deficiente, pues la tecnología ha evolucionado tanto el comportamiento humano al extremo que se ha constituido como la principal herramienta para la comisión de hechosy actos ilícitos que afectan a una sociedad de manera inminente.

1.5 Relación de la Sociología con el Derecho

Siendo que como se definió la Sociología es la ciencia que se ocupa de las sociedades humanas, su origen, condiciones de existencia, desenvolvimiento, relaciones entre sus miembros individuales y organizaciones humanas en forma sistemática, las personas no viven aisladas sino que interactúan permanentemente y su comportamiento aprendido ensu mayoría de "la escuela" que es la sociedad, debe responder y respetar a ciertas reglasimpuestas en la sociedad para la armónica convivencia lo cual permite ser aceptado y nodiscriminado de ella.

Sin embargo, las sociedades han debido establecer, además de estas normas sociales, otras que, sin dejar de ser sociales, son impuestas también por la sociedad: las normas jurídicas que protegen intereses, valores y derechos, y cuya violación por parte de un individuo miembro de la sociedad merece ser castigada pues afecta intereses de terceros

o de la sociedad en su conjunto. Por lo tanto, las normas jurídicas, cuyo conjunto componen el Derecho, son necesarias para que la sociedad se conduzca y funcione dentro de la legalidad, que respete los derechos de todos.

El Derecho, para regular las conductas sociales, debe conocerlas, y analizar su evolucióny cambio, y por ello la Sociología le otorga ese conocimiento a través de la Estadística, encuestas de opinión, entre otros.

Por ejemplo, Alberto Hernán Saúl[1] indicó: "que desde que inició esta inesperada, trágicay dura emergencia sanitaria a nivel mundial, por un momento llegamos a creer que ninguna otra cuestión podría ser noticia de impacto en los medios de difusión masiva; pero una vez más y sin descanso ni contemplaciones, se manifiesta en su máximo esplendor el cibercrimen."

Lo cual obliga a dirigir los estudios científico-sociales en la atención de los delitos informáticos que nacen como resultado de los avances de la tecnología, delitos que atentan contra la libertad de acción, la propiedad documental de las personas, la integridad y la garantía de confidencialidad que la Constitución Política de la República de Guatemala otorga a cualquier ciudadano, a través de sistemas informáticos, vulnerando aún más la situación que se vive en el país como consecuencia de la pandemia COVID 19.

[1] HERNÁN, Saúl Alberto. **Cibercrimen, Protección de Datos y Evidencia Digital.** (UBA), profesor de Derecho Informático (Educación IT / ISTEA), y responsable Comercial de Grandes Cuentas (EDSI Trend Argentina S.A.) @AlbertoSaulIT.

1.6 Métodos de la Sociología del Derecho

Para hablar de los métodos de la sociología jurídica o Sociología del Derecho, es importante comprender los métodos de investigación.

Tal y como lo indica Jean Carbonnier[2], "la sociología jurídica ha recibido mucho de la sociología general, y sus métodos no son otra cosa que un trasplante, al concreto ámbito jurídico, de los métodos utilizados en otros campos sociológicos, por ejemplo: el histórico-comparativo, el estadístico, el de observación, entre otros. Por ello, muchos de los conceptos manejados por la sociología jurídica: coacción social, control social, conciencia colectiva, rol, no son otra cosa que conceptos de la sociología general vertidos al ámbitojurídico."

Incluso se puede admitir que algunas nociones formalmente jurídicas, *ab initio* correspondientes a fenómenos del *ius* familia conyugal, por ejemplo, fueron en un primermomento utilizadas en sociología. Es importante determinar los conceptos de sociologíageneral y de sociología jurídica para entender de mejor manera la "relación de intercambio" expresada por Carbonnier.

Recaséns Siches[3] define la sociología como "el estudio científico de los hechos sociales,de la convivencia humana, de las relaciones interhumanas, en cuanto a su realidad o serefectivo." El ilustre profesor catalán- mexicano destaca que "la sociología se ocupa, esencialmente, de la convivencia y de las relaciones interhumanas, mientras que otras ciencias sociales se consagran al conocimiento de los aspectos sociales de la vida

2 CARBONNIER, Jean. **Sociología Jurídica.** Madrid: TECNOS, 1982. 256p.
3 RECASÉNS SICHES, Luis Pedro Alejandro. Ciudad de Guatemala, 19 de junio de 1903 — Ciudad de México, 4 de julio de 1977, fue un abogado, jurista y filósofo del derecho hispano-guatemalteco.

humana. Por consiguiente, la sociología tiene como eje central la investigación de las relaciones y actividades interhumanas.

Es por ello que hace uso de métodos de análisis que tienen que ver con la observación, la comparación y el análisis histórico; métodos que se aplican en el presente estudio paradeterminar cuáles son las razones sociológicas para la creación de juzgados y fiscalías especializados, por el significativo aumento de la ciberdelincuencia especialmente en el año 2020 en Guatemala, por la creciente utilización de tecnologías de la información y comunicación, el Internet y las Redes Sociales con motivo de la pandemia del COVID 19.

CAPÍTULO II

2. Ciberdelincuencia y Ciberdelitos

2.1 Ciberdelincuencia

2.1.1 Antecedentes

Actualmente se define como cibernético a todo aquello relacionado con la tecnología informática, con el Internet y las Redes Sociales, y que se usa hoy en día para la comunicación y las relaciones interpersonales, la academia, el trabajo, incluso para los ámbitos religiosos y políticos, entre otros. Por ello, el prefijo Ciber se usa para denominar a personas o actitudes que se desarrollan en este entorno como: Cibernauta, Cibercafé,Ciberbullying, *Ciberfriends*, Cibernética, y demás.

La historia y evolución del delito cibernético son fáciles de rastrear y coinciden con la evolución del propio Internet. Los primeros crímenes fueron, por supuesto, simples hackeos para robar información de las redes locales, pero a medida que el Internet se estableció más, también lo hicieron los ataques.

Mientras que el delito cibernético existía antes de esto, la primera gran ola de delitos cibernéticos llegó con la proliferación del correo electrónico a finales de los años 80. Lo cual, permitió que una gran cantidad de fraudes o *malware* se enviaran a las bandejas de entrada.

La siguiente ola en la línea de tiempo de la historia del delito cibernético llegó en los años 90 con el avance de los navegadores web. En ese momento había una multitud para elegir, muchos más que hoy, y la mayoría eran vulnerables a los virus. Los virus eran enviados a través de conexiones a Internet siempre que se visitaban sitios web cuestionables. Algunos causaban que las computadoras funcionaran lentamente,

otros causaban que la aparición de publicidad molesta invadiera las pantallas de los ordenadores o las redirigiera a los sitios pornográficos más asquerosos.

El delito cibernético realmente empezó a despegar a principios del año 2000 cuando lasredes sociales cobraron vida. La oleada de gente que, poniendo toda la información quepodía en una base de datos del perfil, creó una inundación de información personal y el aumento del robo de identidad. Los ladrones utilizaban la información de varias maneras,incluyendo el acceso a cuentas bancarias, la creación de tarjetas de crédito u otros fraudes financieros.

Mientras que puede parecer que los gobiernos hostiles son los culpables número uno cuando se trata de ataques de internet en línea, éste no es el caso. Según estimaciones de expertos en seguridad cibernética de las Naciones Unidas, aproximadamente el 80%de todos los delitos cibernéticos está siendo cometido por pandillas sofisticadas de criminales que participan en operaciones altamente organizadas. Las pandillas operaban igual que las empresas legítimas, ya que mantenían horas laborales regulares con una jerarquía de miembros, trabajando en conjunto para crear, operar y mantener cualquier fraude en el que se centraban.

El crimen se esconde justo debajo de la superficie de Internet. Es como un hongo que nose puede ver, extendiéndose a través de la web con una brecha cada vez más extensa. La razón por la que es capaz de propagarse de la manera en que lo hace se reduce a una serie de factores, en primer lugar, los criminales pueden esconderse fácilmente detrás de sus terminales lejos de los reguladores, operando con impunidad, utilizando softwares de última generación y técnicas de redes para enmascarar sus ubicaciones, y desviar cualquier mirada indiscreta. En segundo lugar, el Internet proporciona el acceso fácil a casi todos en el planeta y, cuando se encuentra el núcleo del problema, cualquier persona con el dinero o la información para robar ésta, probablemente esté desconectaday no es difícil de encontrarla.

En tercer lugar, si se ejecuta una estafa, no se necesita serun programador, todo lo que se debe saber es dónde comprar uno.

2.1.2 Definición

Según la Revista de la Universidad en Internet UNIR, "la ciberdelincuencia consiste en la comisión de actividades delictivas que se llevan a cabo a través de medios tecnológicos, los ciberdelincuentes atacan a personas, empresas, entidades de distintos tipos ygobiernos con diferentes objetivos, el primero de destruir o dañar sus sistemas informáticos y conexiones: normalmente para realizar un uso fraudulento de esos medios tecnológicos y acceder a las carteras de datos personales o confidenciales, incluso realizar una estafa económica y segundo para llevar a cabo delitos comunes (robo, extorsión, fraude, entre otros) a través de estos medios para atacar a las personas directamente y para cometer multitud de delitos a través del espacio virtual."

2.1.3 Tipos de ataques cibernéticos

Según el Instituto Nacional de Ciberseguridad de España -INCIBE- un "ataque cibernéticoes una acción delictiva y malintencionada que se realiza para acceder a información privada, bien para apropiarse de ella o bien para inutilizarla y pedir dinero a cambio de liberarla."

Detrás de estos ataques cibernéticos están delincuentes informáticos, hackers, organizaciones criminales, entre otros, cuyo objetivo es apropiarse de la información o extorsionar a la empresa o persona atacada. Cualquier empresa que almacene, manipuleo transmita datos se encuentra expuesta a un ciberataque.

Según informes de la plataforma *Threat Intelligence Insider Latin America de Fortinet*, herramienta que recopila y analiza incidentes de ciberseguridad en todo el mundo, pandemia COVID-19 y los ataques de "fuerza bruta" fueron un catalizador para el aumento de la actividad cibercriminal durante la primera mitad del 2020.

Guatemala fue objeto de 25 millones de intentos de ciberataque entre enero y junio del año 2020, sumando un total de 15 mil millones de intentos en América Latina y el Caribe durante el mismo período.

"El crecimiento del trabajo remoto y la teleducación ha reavivado el interés de los hackers en los ataques de fuerza bruta. Con la transición masiva a la oficina y el aprendizaje en casa, los ciberdelincuentes encuentran una importante cantidad de servidores de protocolo de escritorio remoto (RDP) mal configurados, lo que facilita este tipo de ataque", señala Obdelio Sierra, Country Manager de Fortinet Guatemala. "Los ataques de fuerza bruta se utilizan comúnmente para descifrar algoritmos u obtener contraseñas débiles de correo electrónico, credenciales de redes sociales y acceso a *Wi-Fi*, entre otros. El atacante realiza varios intentos casi simultáneos a través de mecanismos automáticos repetitivos hasta lograr un resultado exitoso".

Un ejemplo de un intento de ataque que reportó la compañía fue *SSH.Connection.Brute.Force*, que consta de varias solicitudes de inicio de sesión, lanzadas a una velocidad de aproximadamente 200 veces en 10 segundos. Otra detección fue *SMB.Login.Brute.Force*, con al menos 500 inicios de sesión en un minuto, lo que indica un posible ataque de fuerza bruta en los sistemas operativos Microsoft Windows.

"Es esencial que las organizaciones tomen medidas para proteger a sus empleados remotos y ayudarles a proteger sus dispositivos y redes domésticas. El primer paso para

mitigar los ataques de fuerza bruta es utilizar contraseñas seguras. También es importante que las empresas utilicen mecanismos de encriptación y limiten el número de intentos de inicio de sesión durante un período determinado, al igual que habiliten otros mecanismos de autenticación robustos, como multifactor, tokens o validación de imágenes (CAPTCHA)", agregó Sierra, según publicación del Periódico Digital, Centroamericano y del Caribe.

- **Ransomware**

El cual es un programa malicioso que encriptan y bloquean un sistema u ordenador, pidiendo un rescate económico a cambio de desbloquearlo. Las primeras variantes de ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito.

- **Ataque a las bases de datos**

Conocido como ataque de inyección SQL, tiene como objetivo inyectar código maliciosoa la base de datos para extraer su información, las Bases de Datos son el lugar donde residen generalmente los datos más valiosos relacionados a la empresa, los clientes, lasfinanzas, por lo cual, si esta es comprometida de alguna manera, las pérdidas económicas pueden ser muy elevadas, con el consecuente daño también a la imagen dela organización.

El punto de entrada más frecuentemente explotado en la actualidad hacia las bases de datos son las aplicaciones web. Aunque no se deben descartar las malas configuraciones, tener contraseñas débiles, o ser vulnerable a vulnerabilidades conocidaso desconocidas.

- **Denegación de Servicio**

Este ataque, conocidos como DoS, pretende saturar un servidor para colapsarlo e impedir su funcionamiento. Por ejemplo, el correo electrónico o un sitio web, no funciona como es debido, la denegación no se debe a un ataque planificado, sino que es accidental y se produce porque hay demasiadas peticiones legítimas. Sin embargo, los ataques DoS maliciosos contra dispositivos de red son frecuentes, y cada vez se ve más una nueva clase de ataque DoS dirigido específicamente a las aplicaciones.

- **Phishing**

Es un ataque o un delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito con una táctica de phishing común, las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita o suplanta su identidad a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.

- **Cross-Site Scripting**

En este ciberataque es importante tener en cuenta que, con esta vulnerabilidad o ataque, los atacantes explotan la confianza que un usuario tiene en un sitio en particular, de forma reflejada y de forma almacenada. Desde redirigir el sitio a otro para robar información mediante phishing, hasta hacer que se descargue alguna amenaza y se ejecute en el sistema.

- **El spyware**

Es un software malicioso que infecta los ordenadores o dispositivos móviles y recopila información sobre su usuario, su navegación y su uso habitual de Internet, así como otros datos. El spyware es un malware que infecta un sistema para obtener la información contenida en él. Los gusanos se reproducen automáticamente en todos los equipos conectados a la red, mientras que los troyanos funcionan en segundo plano de forma silenciosa, y su fin es permitir la entrada de otros malwares.

2.1.4 Ataques Cibernéticos que hicieron historia en el mundo

Cuatro son los ataques cibernéticos que revolucionaron al mundo e integraron la ciberdelincuencia a la preocupación de los sistemas de justicia:

Ataque a tiendas creadas con Magento, la cual es una de las plataformas más populares para crear y gestionar tiendas virtuales junto a PrestaShop. En septiembre de 2020 se produjo un ciberataque global con técnicas conocidas como Magecart o web skimming dirigidas especialmente a negocios online creados con esta plataforma.

El objetivo de este ciberataque era el de robar los datos de tarjetas de crédito de los clientes y el número de e-commerce afectados se acercó a los 3000. Para realizar este ataque, los ciberdelincuentes insertaron scripts (pequeños programas) en los sitios web con el objetivo de robar los datos bancarios de los clientes cuando éstos introducían su tarjeta de crédito en el momento de finalizar la compra. Este ciberataque pudo llevarse acabo porque muchas tiendas online no tenían Magento actualizado a su última versión ylos ciberdelincuentes se aprovecharon de vulnerabilidades presentes en versiones anteriores de la plataforma para poder inyectar su código malicioso para robar los datos bancarios.

para el que no está preparado, por lo que termina colapsando o funcionando de forma deficiente. Plataformas de servicios online como Netflix o Spotify sufrieron hace unos años las consecuencias de este tipo de ciberataques viendo como sus servicios online quedaban inutilizados durante horas causando unas grandes pérdidas económicas y afectando negativamente a su prestigio e imagen. Este ataque se produjo con un malware conocido como Mirai, que infectó una gran cantidad de dispositivos inteligentes que actuaban como un "ejército de zombis" formando un enorme *botnet*, que es una red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques de denegación de servicio distribuido (DDoS) sin el conocimiento o el consentimiento de los propietarios reales de los equipos, el cual, cuando se realizó el ataque fue capaz de tirar plataformas de empresas globales de gran prestigio.

Robo de datos en Redes Sociales, las tiendas en Facebook o Instagram son muy populares, y a pesar de que las medidas de Ciberseguridad de estos dos gigantes de las redes sociales son muy sofisticadas y potentes, no se han librado de recibir ataques. No hace mucho un grupo de ciberdelincuentes rusos fue capaz de comprometer los datos de millones de usuarios de Facebook e Instagram a través de un código malicioso que se insertaba en extensiones de los naveg adores. Este tipo de extensiones facilitan, automatizan y añaden funciones a los programas que utilizamos para navegar por la web (barras de herramientas, bloqueadores de spam o cambios de interfaz son algunos ejemplos).

Ataque al gigante chino Alibaba, que es el mayor centro de venta online del mundo con portales como AliExpress. Este último recibe millones de ciberataques diarios y por ello invierte una gran cantidad de dinero en medidas de Ciberseguridad avanzadas. A lo largo de su trayectoria, AliExpress ha sufrido ataques que han comprometido los datos de los usuarios de su plataforma online de compra venta. Uno de los casos más graves se presentó hace unos años con una vulnerabilidad que permitía averiguar el ID de un

usuario conectado a la plataforma con un script automatizado para rastrear su *mailing Address.* Afortunadamente, esta vulnerabilidad fue detectada a tiempo y los daños causados pudieron ser minimizados. A partir de ese momento el gigante asiático puso en el centro de sus prioridades la Ciberseguridad, convirtiéndose en una de las plataformas online más seguras del mundo, pero que a su vez es una de las que más ataques diarios recibe.

2.1.5 Cómo surgió la Ciberdelincuencia en Guatemala

Como parte de los innovadores *modus operandi* generados en los hechos delictivos en materia tecnológica en Guatemala se hizo indispensable las reformas al Código Penal para prohibir y sancionar esas conductas. El Congreso de la República introdujo modificaciones a la ley sustantiva penal mediante el Decreto 33-96 publicado el 21 de junio de 1996. En las cuales se expone: "Que los avances de la tecnología obligan al Estado a legislar en bien de la población de derechos de autor en materia informática tipos delictivos que nuestra legislación no ha desarrollado".

Para fines del presente estudio se detallan los delitos informáticos que su comisión afecta el patrimonio y la propiedad intelectual y que fueron adicionados en el Capítulo VII, de los Delitos contra el Derecho de Autor, la Propiedad Industrial y Delitos Informáticos, del Código Penal, a través del Decreto Número 33-96 del Congreso de la República de Guatemala en los Artículos 274 literales de la A a la H respectivamente, y los cuales se transcriben literalmente a continuación:

"ARTÍCULO 274. Violación a derechos de autor y derechos conexos. Salvo los casos contemplados expresamente en leyes o tratados sobre la materia de los que la República de Guatemala sea parte, será sancionado con prisión de uno a seis años y una multa de cincuenta mil a setecientos cincuenta mil quetzales quien realice

cualquiera de los actossiguientes:

a) Identificar falsamente la calidad de titular de un derecho de autor, artista intérprete o ejecutante, productor de fonogramas o un organismo de radiodifusión;

b) La deformación, mutilación, modificación u otro daño causado a la integridad de laobra o al honor y la reputación de su autor;

c) La reproducción de una obra, interpretación o ejecución, fonograma o difusión sinla autorización del autor o titular del derecho correspondiente;

d) La adaptación, arreglo o transformación de todo o parte de una obra protegida sinla autorización del autor o del titular del derecho;

e) La comunicación al público por cualquier medio o proceso, de una obra protegida o un fonograma sin la autorización del titular del derecho correspondiente;

f) La distribución no autorizada de reproducciones de toda o parte de una obra o fonograma por medio de su venta, arrendamiento de largo plazo, arrendamiento, arrendamiento con opción a compra, préstamo o cualquier otra modalidad;

g) La fijación, reproducción o comunicación al público por cualquier medio o procedimiento, de una interpretación o ejecución artística sin la autorización del intérprete o ejecutante o del titular del derecho;

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

i) La comunicación al público de una difusión o transmisión en un sitio al que el público pueda tener acceso pagando una cuota de admisión, o con el fin de consumir o adquirir productos o servicios, sin la autorización del titular del derecho correspondiente;

j) La publicación de una obra protegida que tiene un título que se cambió o retiró,

con o sin alteración de la obra;

k) Manufacture, ensamble, modifique, importe, exporte, venda, arrende o de cualquier forma distribuya un dispositivo o sistema tangible o intangible, sabiendoo teniendo razón para saber que el dispositivo o sistema sirve o asiste principalmente para decodificar una señal de satélite codificada, que tenga un programa sin la autorización del distribuidor legal de dicha señal, o la recepción ydistribución intencionada de una señal que lleva un programa que se originó como señal satelital codificada, sabiendo que fue decodificada, sin la autorización del distribuidor legal de la señal;

l) Con respecto a las medidas tecnológicas efectivas, la realización de lo siguiente:

l.1) Acto que eluda o intente eludir una medida tecnológica efectiva que impida o controle el acceso o el uso no autorizado a toda obra, interpretación o ejecución ofonograma protegido; o

l.2) Fabrique, Importe, distribuya, ofrezca al público, provea, venda, ofrezca para la venta o de otra manera comercialice dispositivos, productos o componentes, u ofrezca al público o brinde servicios que:

l.2.1) Se promuevan, anuncien, o comercialicen con el propósito de eludir una medida tecnológica efectiva;

l.2.2 Tengan únicamente un propósito o uso comercialmente significativo limitado que no sea eludir una medida tecnológica efectiva; o

l.2.3) Estén diseñados, producidos, o interpretados o ejecutados principalmente con el propósito de permitir o facilitar la elusión de una medida tecnológica efectiva;

m) La realización de todo acto que induzca, permita, facilite u oculte la infracción de cualquiera de los derechos exclusivos de autores, titulares de derecho de autor, intérpretes o ejecutantes, productores de fonogramas u organismos de difusión;

n) El retiro o alteración, sin autorización, de información de gestión de los derechos;

o) La distribución o importación, para su distribución, de información de gestión de derechos, sabiendo que la información de gestión de derechos fue suprimida o alterada sin autorización para hacerlo;

p) La distribución, comercialización, promoción, importación, difusión o comunicacióno puesta a disposición del público, sin autorización, de copia de obras, interpretaciones o ejecuciones, fonogramas o difusiones, sabiendo que la información de gestión de los derechos fue retirada o alterada sin autorización;

q) La transportación, almacenamiento u ocultamiento de reproducciones o copias o cualquier tipo de medio tangible de obras, fonogramas, interpretaciones o ejecuciones o difusiones protegidas que se hayan hecho sin el consentimiento delautor o titular del derecho correspondiente;

r) El cobro de utilidades del uso de obras, interpretaciones o ejecuciones, fonogramas o difusiones protegidas o la realización de cualquier otra actividad típica de una empresa de gestión colectiva sin autorización para ello;

s) La divulgación de una obra nueva sin el consentimiento del autor o del titular del derecho correspondiente;

t) La traducción de una obra total o parcialmente sin la autorización del autor o titulardel derecho correspondiente;

u) La distribución, sin autorización, de una obra o fonograma original protegido o desus reproducciones legales, para su venta, arrendamiento de largo plazo, arrendamiento, arrendamiento con opción a compra, préstamo o cualquier otra modalidad; y

v) La importación o exportación de una obra original protegida o sus reproducciones,para comerciarlas, en cualquier tipo de medio o fonograma sin la autorización deltitular del derecho correspondiente.

Las disposiciones n), o) y p) no serán aplicables a actividades legalmente autorizadas, realizadas por empleados, funcionarios, o contratistas del gobierno, para la aplicación de la ley, así como la realización de actividades de inteligencia, defensa nacional, seguridad u otros propósitos gubernamentales similares.

Las excepciones contenidas en el artículo 133 sexties del Decreto Número 33-98 del Congreso de la República, Ley de Derecho de Autor y Derechos Conexos y sus reformas, también serán aplicables a la literal l) que antecede.

El diseño, o el diseño y selección, de piezas y componentes para productos electrónicos de consumo, telecomunicaciones o productos de computación no necesitan responder auna medida tecnológica específica si el producto no infringe la literal l) del presente artículo.

Se entenderá por información para la gestión de derechos, cuando lo descrito en las literales siguientes esté adherido a una copia de la obra, interpretación o ejecución o fonograma, o aparezca en relación con la comunicación o puesta a disposición del público

de una obra, interpretación o ejecución, o fonograma:

1. Información que identifique una obra, interpretación o ejecución, o fonograma, al autor de la obra, al intérprete o ejecutante de la interpretación o ejecución o al productor del fonograma o a cualquier otro titular de un derecho protegido en la obra, interpretación o ejecución, o fonograma;
2. Información sobre los términos y condiciones de uso de la obra, interpretación o ejecución, o fonograma; o
3. Cualquier número o código que represente dicha información.

Medida tecnológica efectiva: tecnología, dispositivo o componente que, en el giro normal de su funcionamiento, controla el acceso a obras protegidas, interpretaciones o ejecuciones y fonogramas protegidos o cualquier otro material protegido, o proteja un derecho de autor o un derecho relacionado con el derecho de autor.

Los supuestos contenidos en esta disposición se determinarán con base en las disposiciones aplicables de la Ley de Derecho de Autor y Derechos Conexos."
"ARTICULO 274. "A". Destrucción de registros informáticos. Será sancionado con prisión de seis meses a cuatro años y multa de dos mil a diez mil Quetzales, quien destruya, borre o de cualquier modo inutilice, altere o dañe registros informáticos.

Si la acción contemplada en el párrafo anterior estuviere destinada a obstaculizar una investigación o procesamiento de carácter penal, el responsable será sancionado conforme al artículo 458 Bis del presente Código."

"ARTÍCULO 274. "B". Alteración de Programas. La misma pena del artículo anterior se aplicará al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras."

"ARTÍCULO 274. "C". Reproducción de instrucciones o programas de computación. Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación."

"ARTÍCULO 274. "D". Registros prohibidos. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, 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. Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, 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 alterar los estados contables o la situación patrimonial de una persona física o jurídica."

"ARTÍCULO 274. "F". Uso de información. Se impondrá prisión de seis meses a dos años, y multa de dos mil a diez mil Quetzales 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. Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación."

"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, será sancionado con pena de prisión de seis (6) a diez (10) años."

Además, el 21 de noviembre de dos mil ocho mediante Decreto Número 64-2008 del Congreso de la República de Guatemala se adicionó el delito de Pánico Financiero contenido en el Artículo 342 "B" del Código Penal citado.

"ARTÍCULO 342 "B". Pánico financiero. Comete delito de pánico financiero quien elabore, divulgue o reproduzca por cualquier medio o sistema de comunicación, información falsa o inexacta que menoscabe la confianza de los clientes, usuarios, depositantes o inversionistas de una institución sujeta a la vigilancia e inspección de la Superintendencia de Bancos. Se entenderá que se menoscaba la confianza de los clientes, usuarios, depositantes o inversionistas de una institución cuando, como consecuencia de los referidos actos, se atente contra su reputación o prestigio financiero o que la misma sea objeto de retiro masivo de depósitos o inversiones, mayores o superiores a su flujo normal u ordinario. El responsable de la comisión de este delito será sancionado con prisión de uno a tres años y con multa de cinco mil a cincuenta mil Quetzales.

Si el delito fuere cometido conociendo o previendo los daños o perjuicios a causar a la institución, el responsable será sancionado con prisión de cinco a diez años inconmutables y con una multa de cien mil a ochocientos mil Quetzales. En este caso, no se podrá otorgar cualquiera de las medidas sustitutivas contempladas en el Código Procesal Penal.

Las sanciones a que se refiere el presente artículo serán aumentadas en una tercera parte cuando el responsable del delito sea accionista, director, administrador, gerente, representante, funcionario o empleado de institución sujeta a la vigilancia e inspección de la Superintendencia de Bancos, o autoridad, funcionario o empleado del Banco de

Guatemala o de la Superintendencia de Bancos.

Se excluyen del alcance del presente artículo, a los autores de los estudios, análisis y opiniones de carácter científico o académico que, con base a Información auténtica y verificable, estén orientados a evaluar o calificar el sistema financiero o sus actores, buscando maximizar su eficiencia y desarrollo."

El contenido de los Artículos citados supra, permite establecer que la legislación guatemalteca sí ha sido enfática en integrar a través de reformas legislativas la protección de la integridad de las personas, su patrimonio y su información tanto personal como patrimonial, como consecuencia de la proliferación de la ciberdelincuencia que cada día es más evidente en este país. Además, otras leyes ordinarias y reglamentarias también han incluido reformas que tienden a la protección de la integridad de las personas su patrimonio y a la protección de los datos y registros de las mismas, lo cual justifica la necesidad de crear juzgados especializados y fiscalías especializadas en la atención de los ciberdelitos que se han proliferado en los últimos años en Guatemala, especialmente como consecuencia de la pandemia COVID 19.

2.1.6 Ciberdelincuencia y sus consecuencias jurídicas

Una de las partes más importantes sobre este tema de la ciberdelincuencia y sus consecuencias es conocer las causas. A lo largo de los años se han llevado a cabo incontables estudios acerca de este tema. Los profesionales dedicados a las nuevas tecnologías, Internet y Redes Sociales, junto con criminólogos de todo el mundo se han centrado en buscar y entender las razones por las que las personas recurren a estos comportamientos delictivos.

Aunque los ciberdelitos no siempre son iguales, tampoco tienen el mismo alcance o daño. Pero las causas por las que se cometen suelen ser más similares de lo que la mayoría de las personas cree.

Una de las principales causas de este tipo de delincuencia comienza con la crisis, las

dificultades económicas son uno de los elementos por los que se producen los ciberdelitos.

Los criminólogos y los juristas centran sus estudios e investigación sociológica en la población juvenil, es decir en la ciberdelincuencia juvenil. Este es un problema que va en aumento con el paso de los años. Conocer bien las causas y consecuencias jurídicas de la ciberdelincuencia puede ser la clave para mantener a los ciberdelincuentes alejados de ella .Muchos expertos coinciden en que cada vez existen más ataques informáticos a manosde hackers, crackers y piratas informáticos. Estos buscan atentar y alterar los intereses,tanto económicos como sociales, político, jurídicos, entre otros.

El problema central es que no existe suficiente legislación a nivel nacional e incluso regional para enfrentar la problemática, no existe un ordenamiento especializado en el cual queden tipificados dichos delitos con drásticas sanciones para los responsables, y es que, la tecnología a ese respecto, avanza a pasos mucho más agigantados que las legislaciones donde queden tipificados esos hechos criminales.

Además, se dan casos específicos en los cuales los ataques cibernéticos se dan entre empresas, como consecuencia de una competencia desleal, constituyéndose en prácticas muy abusivas y muy perjudiciales para las víctimas que quedan en estado de indefensión por no saber a quién acudir inmediatamente antes de perder o perjudicar sus patrimonios.

Actualmente, existe una notoria falla en los medios y en el conocimiento jurídico de los sistemas tecnológicos e informáticos y sus alcances. La expansión de la ciberdelincuencia es preocupante, incluso hasta los delincuentes comunes usan la tecnología como herramienta para la comisión de hechos ilícitos y no necesariamente por la vía tecnológica sino como el medio idóneo de comunicación y vigilancia.

Cuando se realizan acciones tendientes a fortalecer los conocimientos jurídicos y sociales sobre la seguridad informática se aborda siempre el mismo tema desde hace años: los

ataques a los objetos inteligentes. También conocido como el "Internet de las cosas". Porque la tecnología no deja de avanzar, pero la ciberseguridad se está quedando siempre un paso por detrás.

2.2 Ciberdelitos

2.2.1 Definición de Ciberdelitos

El ciberdelito o delito informático es todo aquel acto ilegal realizado por un ciberdelincuente en el espacio digital a través de las redes informáticas y diversos dispositivos electrónicos. Dichos actos ilegales atentan contra la integridad y confidencialidad de los datos y de los sistemas informáticos, y tienen el objetivo de estafar y robar datos.

Estos ciberdelitos se realizan a través de programas maliciosos, también llamados malwares, desarrollados para dañar, deteriorar, borrar, hacer inaccesibles, suprimir o alterar datos informáticos sin la autorización del propietario y con fines monetarios y de daño.

Rodríguez Flores (2013) señala que el término "cibercrimen o ciberdelito carecería de una definición universalmente homogénea y aceptada por los especialistas jurídicos, existiendo acuerdo entre los investigadores en que sería una actividad ilegal realizada

[4] Rifkin, Jeremy, **La Sociedad del Coste Marginal, El Internet de las Cosas, el Procomún Colaborativo y el Eclipse del Capitalismo**, pág. 24

mediante el computador o un sistema informático". Sin embargo, continúa el autor, "habría desacuerdo sobre el lugar en que se ejecuta tal actividad, y tales diferencias se evidenciarían en las definiciones del señalado delito".

-Chung (2004) lo define como "actividades ilegales realizadas a través de computadores que a menudo tienen lugar en las redes electrónicas globales".

-Parker (1998) afirma que "es el sistema de información que sirve de canal".

-Philippsohn (2001) considera que "se realizan a través de Internet".

-Power (2002) lo define como "la intromisión sin autorización de un computador".

-Chawki (2005) indica que "el computador tiene varios roles en el cibercrimen, pues sirve de objeto, sujeto, herramienta y símbolo". A su vez, sostiene que "se diferencia en cuatro formas de los llamados crímenes territoriales: permiten un fácil aprendizaje de cómo realizarlos, requieren pocos recursos en comparación con el daño potencial que pueden ocasionar, pueden ser cometidos en una jurisdicción sin necesidad de estar físicamente presente y frecuentemente no son claramente identificados como ilegales"[5].

2.2.2 Características de los ciberdelitos

Es importante indicar que los ciberdelitos o delitos informáticos son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas, pues se llevan a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

[5] Cavada Herrera, Juan Pablo, **Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera.** Julio 2020. Pág. 2.

Los ciberdelitos o delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los delincuentes. Estos delitos informáticos han sido denominados conductas criminales de cuello blanco, es decir, que solo un determinado número de personas con ciertos conocimientos técnicos puede llegar a cometerlas, teniendo la oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico para lograrlo.

Otra característica común en estos delitos es que los mismos provocan serias pérdidas económicas, debido a que casi siempre producen grandes "beneficios" a aquellos que las realizan y ofrecen posibilidades de tiempo y espacio, ya que se producen en pocos segundos y sin necesidad de presencia física lo cual dificulta su inmediata intervención oaprehensión de los responsables.

Es importante recordar y señalar que el 27 de junio de 2017 el sistema tributario guatemalteco reportó una caída en su operación provocada por constantes ataques cibernéticos para interrumpir los servicios hacia la ciudadanía. En ese entonces las autoridades de la Superintendencia de Administración Tributaria (SAT), confirmaron que el portal web en donde se suministran los servicios de tributación había sido blanco de esos ataques cibernéticos durante dos semanas de forma recurrente.

Situación similar vivió el Congreso de la República el 12 de febrero de 2017, un domingo en el cual en dos ocasiones ciberdelincuentes o cibercriminales lograron ingresar a la red de ese organismo de Estado y hackear su sitio web. En esa ocasión el colectivo de hackers Anonymous se atribuyó los hechos justificando la caída del sistema como una represalia en contra de la institución por actos de corrupción. Sin embargo, aun cuando se asumió la responsabilidad del ataque no se pudo individualizar a los ciberdelincuentes.

Además, las nuevas tecnologías son utilizadas por delincuentes comunes como medios para cometer delitos como las extorsiones, secuestros, captación de menores para trata de personas y sobre todo pornografía infantil. Solo durante 2018 fueron capturadas más de 15 personas por delitos relacionados a pornografía infantil y se realizaron en el país al menos dos operativos a gran escala apoyados por investigaciones internacionales en donde el país figura como parte de redes mundiales en estos delitos.

En el pasado fueron capturados dos guatemaltecos a quienes la Agencia Federal de Investigación e Inteligencia, FBI por sus siglas en inglés, relacionó a una organización criminal detectada en Yakarta, Indonesia. Según investigadores, hasta un 40% del material distribuido por esa red de pornografía infantil podría haber sido de víctimas nacionales y esta estructura apoyada por ciberdelincuentes que facilitan sus operaciones. Cuando se habla de las características de los ciberdelitos no debe desatenderse principalmente el conocimiento de cuál es el bien jurídico tutelado que se vulnera en la comisión de los mismos. El bien jurídico tutelado lo constituyen todos aquellos derechos, valores o atributos de la persona que el Estado encuentra merecedores de protección a través del Derecho Penal, se puede afirmar que en el caso de los delitos informáticos existe una pluralidad de bienes que son afectados o puestos en peligro.

Por un lado, las acciones que van dirigidas al sabotaje, el daño, la destrucción o pérdida de equipos de computación afectan, lesionan o ponen en peligro el bien jurídico patrimonial. Por otro lado, los delitos que se sirven o utilizan de un equipo informático para su realización pueden de igual manera afectar diversos bienes, como lo serían la indemnidad sexual (caso de la pornografía infantil), la privacidad o el mismo patrimonio en los casos de fraudes informáticos cometidos por Internet.

También debe tomarse en cuenta que el uso de ordenadores para la reproducción no autorizada de libros, películas, música, entre otros también, afecta valores de propiedad intelectual pero implícitamente estas acciones tienen una motivación económica, por lo

que a su vez redundan en la afectación al bien jurídico patrimonial.

Es por ello, que al hablar de delitos informáticos es válida la afirmación que los mismos afectan una diversidad de bienes legalmente tutelados por lo que puede considerarse pluriofensivo[6].

2.2.3 Delitos informáticos más comunes en Guatemala

Durante el transcurso de 2018[7] se plantearon 1,100 denuncias por ciberdelitos en el país, con lo cual se superó tres veces las 338 que se contabilizaron en el 2017, según consta en los registros del Observatorio Guatemalteco de Delitos Informáticos (OGDI). Entre los hechos más denunciados se encontraban, el acoso a personas por parte de grupos criminales, robo de identidad en cuentas de redes sociales, difamación; y recientemente, se ha evidenciado un repunte sobre casos de jóvenes que consumen drogas digitales[8], que son "dosis auditivas diseñadas para recrear sensaciones de tridimensionalidad en el cerebro o, lo que es lo mismo, para imitar los efectos de las drogas tradicionales. Su efectividad, no obstante, ha sido puesta en entredicho por expertos".

José Leonett, director del OGDI, explicó que "las denuncias fueron recibidas por la Sección Contra Delitos Informáticos de la Policía Nacional Civil (PNC), en donde se estableció los hechos ilícitos en los que se incurrió, quienes fueron los denunciados y luego se inició una investigación".

[6] NORIEGA Salazar, Hans Aarón, **Delitos Informáticos.** Defensa Pública Penal 2011. Pág. 36

[7] El Periódico Soy 502, 10 de noviembre de 2016

[8] PINZÓN Mayorga, IC. MORA Ardila, MM. **Drogas Digitales**. Universidad Piloto de Colombia. Pág. 4.

Leonett indicó que "existe preocupación porque cada año se aumentan los casos sobre hackeo de cuentas de Facebook y Twitter, principalmente. Pero preocupa aún más el incremento de descargas de audios que al escucharlos producen la misma sensación que al consumir alguna sustancia como marihuana, cocaína o éxtasis; se les llama "drogas digitales" y las consumen en mayor cantidad adolescentes en edad escolar", sostiene el director del OGDI.

Javier Lainfiesta del medio escrito Soy 502 @JavierLSoy502 (9 de noviembre de 2016), publicó una entrevista al viceministro de Tecnología del Ministerio de Gobernación Walter Francisco Girón, quien manifestó: "No podemos permitir que Guatemala se convierta en un paraíso de delitos informáticos", dice preocupado. "En Guatemala, se reportan cientos de crímenes informáticos; no obstante, muchos no pueden ser investigados porque no son tipificados como delitos."

Guatemala es sede de una iniciativa a nivel regional organizada por la ONU para visibilizar los ciberdelitos contra niños, comentó Girón que: "No tener una ley de delitos informáticos impide la maduración de las instituciones en el tema de informática forense, es decir la investigación de estos crímenes". En el marco del Congreso Regional "Unidos por una infancia protegida en las TIC", organizado por Naciones Unidas, el viceministro habló con Soy502 sobre los ciberdelitos más comunes en los que pueden caer los guatemaltecos y que con la legislación vigente probablemente queden en la impunidad. "Hay comportamientos criminales en Internet que ponen en peligro la seguridad nacional. Empezando por el robo de información hasta secuestro de la misma." La autoridad de Gobernación ejemplifica los siguientes casos como los más frecuente.

"Entrar a un servidor: en la actualidad no está tipificado como delito "hackear" un servidor para tener acceso a información sensible o privada. Esta puede ser vendida a interesados o utilizada para cualquier propósito.

Phishing: es el intento de obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito (y veces, indirectamente, dinero), a menudo por razones maliciosas, haciéndose pasar por una entidad confiable en una comunicación electrónica.

Spoofing: este se refiere a que una persona se hace pasar por otra en el mundo virtual para solicitar servicios o utilizar su nombre para obtener un beneficio. Las consecuencias van desde cobros por servicios no consumidos, hasta llegar a ser acusado por cometer un delito.

Extortion: es cuando un ciberdelincuente secuestra información sensible o importante de un computador de otra persona. Para que pueda recuperarla se debe pagar una cierta cantidad de dinero.

Sexting: es la práctica de un chat con contenido sexual, incluso enviando fotos íntimas. No es un delito en sí, pero si uno de los interlocutores es menor de edad e interactúa con alguien mayor que aparenta ser adolescente, podría incluirse dentro del delito de acoso sexual.

Ciberbullying: es el acoso masivo a través de las redes sociales. Aún no hay tipificación de este delito; ni el bullying escolar está tipificado aún, pero ya el Ministerio de Educación y la Procuraduría de los Derechos Humanos instan a los colegios a implementar prácticas para evitarlo. Del mismo modo, el ciberbullying es difícil de perseguir, pero las redes

sociales tienen mecanismos de denuncia de los perfiles, que pueden ser cancelados en caso de que las quejas sean constantes y recurrentes."

Otros ciberdelitos como: el robo de identidad en el cual los delincuentes obtienen información personal como contraseñas, números de identificación, números de tarjetas de crédito, datos de seguridad social, con la intención de actuar de manera fraudulenta en nombre de la víctima. Esta información puede ser usada para varios propósitos ilegales, como solicitar préstamos, realizar compras online o acceder a los datos médicos y financieros de la víctima. Cuando en un robo de identidad se recopila suficiente información, ésta se puede utilizarpara realizar compras, tomar el control de las cuentas online de las víctimas o emprenderacciones legales en su nombre. A corto plazo, las personas afectadas pueden sufrir pérdidas financieras debido a retiros de dinero no autorizados y compras realizadas a su nombre.

Otro delito cibernético común es la estafa que se comete a través del robo de identidad. Los criminales utilizan técnicas como el spam, webs falsas o softwares ilegales para engañar a las víctimas y robarles las contraseñas o claves personales, de esta manera, acceden a información confidencial.

Por último, la extorsión que sucede cuando alguien utiliza Internet para extorsionar dinero a una persona o empresa. La extorsión se comete de distintas formas. Por ejemplo, el criminal puede tener acceso a información personal y amenazar con exponerla a menos que pague cierta cantidad de dinero a cambio. Los delincuentes también pueden llevar acabo algún tipo de ataque cibernético para luego exigir un pago para detenerlo. Por estemotivo, es muy importante tener un antivirus y proteger las cuentas bancarias y personales con contraseñas de alta dificultad.

Guatemala, ha intentado integrar importantes herramientas contra el ciberdelito, porque aun cuando la tecnología ha logrado mejorar y dar saltos cualitativos en las relaciones de los individuos frente a sus compromisos laborales, comerciales y sociales, incluso como

fuente de aprendizaje todo de manera virtual, también el Internet, la tecnología y las Redes Sociales exponen a peligros o delitos a los usuarios, sean menores de edad o adultos, pues las plataformas virtuales son una forma de exposición a la violencia, la explotación sexual y al acoso en línea.

El uso del Internet se ha convertido en un aliado estratégico para las actividades y el Gobierno de Guatemala por medio del Ministerio de Gobernación y la Secretaría Contra la Violencia Sexual, Explotación y Trata de Personas (SVET), entre otras instancias, han impulsado estrategias para contrarrestar los ciberdelitos que día con día aumentan más y diversifican su *modus operandi*. El objetivo de incorporar herramientas, estrategias y políticas públicas debe ser siempre proteger los derechos constitucionales de los niños, niñas y adolescentes así como de los adultos mayores quienes en este tema son la población más vulnerable por los riesgos que corren en las redes sociales, pues es de conocimiento público que estos medios son utilizados por bandas ilegales o ciberdelincuentes quienes aprovechan la ingenuidad o inocencia de los menores para promover la explotación sexual y el acoso.

Estos comportamientos delictivos han expuesto las condiciones biopsicosociales de los actores, así como sus condiciones económicas, las cuales los obligan a buscar las formas más innovadoras de delinquir y obtener fácilmente mejores condiciones socioeconómicas.

Con el fin de promover las líneas de protección para los grupos vulnerables, y avanzar en la erradicación de los citados delitos informáticos, la SVET[9] presentó tres

[9] https://svet.gob.gt/. meconectosinclavos.net.gt. Consultada el 30 de octubre de 2021.

Ciberherramientas, que se convierten en un paso más para garantizar el derecho de la niñez y adolescencia a estar protegidas. Se trata de **Me conecto sin clavos web**, que provee información a niños y padres de familia para minimizar los riesgos del Internet; **Me conecto sin clavos App**, ligada a la página web, con la que niños y adolescentes pueden informarse de manera divertida, y **Tú amig@ SVET**, una línea de consulta juvenil a través de las redes sociales, en la que se puede conversar con personas capacitadas sobre violencia sexual, explotación y trata de personas.

Este esfuerzo interinstitucional, que cuenta con el apoyo del Fondo de las Naciones Unidas para la Infancia (UNICEF) y la Fundación Sobrevivientes, es pionero en América Latina y ayudará a mitigar los posibles riesgos y garantizará que las experiencias en línea de niños y adolescentes sean más seguras y positivas.

2.2.4 Definición de los ciberdelincuentes

Así como en la sociedad existen los delincuentes, así, en el mundo informático existen los ciberdelincuentes, que en líneas generales son personas que realizan actividades delictivas en Internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.

Los ciberdelincuentes están identificados como amenazas humanas y se clasifican en:
Hacker: persona curiosa, inconformista y paciente que busca su superación continua aprovechando sus conocimientos y las posibilidades que le brindan los sistemas informáticos.

Cracker: hacker dañino.

Phreaker: persona que engaña a las compañías o empresas telefónicas para su beneficio propio.

Pirata Informático: persona que vende software protegido por las leyes de Copyright.

Insider: personal interno de una organización o empresa que amenaza de cualquierforma al sistema de la misma, en beneficio propio o de terceros.

Creador o Diseminador de Virus: Persona que crea o distribuye programas que modifican, alteran o dañan los sistemas de información o hardware afectados.

Las actividades frecuentes de los ciberdelincuentes son:

a. Ataques a sistemas informáticos y piratería.
b. Fraude o falsificación.
c. Publicación de contenidos ilegales.

Es importante conocer la diferencia entre un ciberdelincuente y un *hacker*[10], *("persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora),* porque no siempre un hacker puede realizar una actividad delictiva, hay muchos hackers que no realizan actividades ilegales o tan agresivas como los ciberdelincuentes. El objetivo del ciberdelincuente es netamente una actividad delictiva, en cambio un hacker puede ser un investigador, un profesional, un estudiante, con altos conocimientos informáticos.

Actualmente hay varios concursos de hackers que se realizan anualmente como el 'Pwn2Own', en los cuales estos ayudan a las empresas a encontrar errores (bugs) en sus sistemas y como consecuencia repararlos a cambio de un incentivo económico. Viéndolo desde este punto un hacker correcto, indirectamente, puede ayudar a luchar contra la ciberdelincuencia. También se sabe que hay hackers que se han convertido en consultores informáticos o están trabajando en prestigiosas empresas, en el área de seguridad informática.

[10] **Diccionario de la Real Academia Española (RAE)** 23ª actualización. Diccionario de la LenguaEspañola. https://dpej.rae.es/lema/hacker consultado el 28 de octubre de 2021.

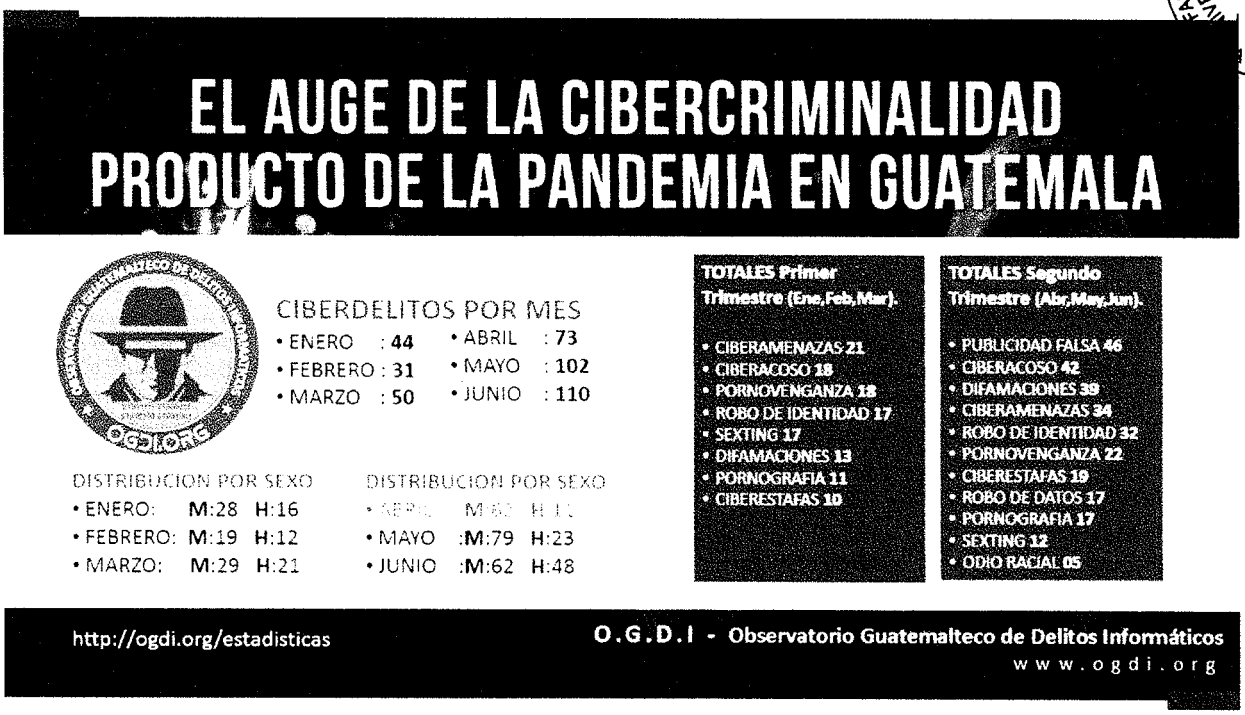
Pero no se puede negar que también existen otros grupos de hackers que sobrepasan la línea de la legalidad y utilizan sus conocimientos para actos delincuenciales, convirtiéndose en ciberdelincuentes.

Actualmente en Guatemala existe una organización sin fines de lucro, con personaría jurídica ante el Ministerio de Gobernación -MINGOB- independiente, apolítica y conformada por un grupo de expertos en seguridad cibernética e Informática Forense denominada Observatorio Guatemalteco de Delitos Informáticos (OGDI) que ha sido la pionera en Guatemala y Centroamérica en la búsqueda de crear culturas e iniciativas de paz e inclusión cibernética, para construir resiliencia colectiva contra los delitos cibernéticos y las amenazas globales de la guerra cibernética en la región.

Sin embargo, en casi todos los países de la región centroamericana y Guatemala no es la excepción, los vacíos legales y la falta de capacitación de las fuerzas policiales en esa materia permiten que los ciberdelincuentes tengan amplia ventaja y puedan incrementar constantemente la delincuencia cibernética.

A continuación, se integra una imagen[11] que refleja la estadística obtenida por la OGDI en el año 2020:

[11] https://ogdi.org/estadisticas



Fuente: Observatorio Guatemalteco de Delitos Informáticos (OGDI).

Lo que sí es necesario tomar en cuenta es que, para los ciberdelincuentes en Guatemala, no contar con legislación específica y con órganos jurisdiccionales especializados se puede convertir en una paraíso de delitos informáticos y que como tal, sea un objetivo social codiciado, pues es de resaltar que una de las dificultades para perseguir estos delitos radica en que mucha veces son personas que se encuentran fuera del país o que utilizan medios digitales del país para atacar otros objetivos, pero que su localización es imposible de detectar a corto plazo.

Es fundamental impulsar alianzas interinstitucionales para hacerle frente a la cibercriminalidad en el país, en donde tengan participación no solo el sector justicia sino además el sector privado y la academia, pues las estrategias para garantizar la seguridad informática a nivel mundial deben ser integrales tanto a nivel nacional como internacional.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C.A.

CAPÍTULO II

3. Ciberseguridad

3.1 Antecedentes

El 30 de noviembre se celebra el Día Mundial de la Ciberseguridad o Seguridad de la Información, esta fecha, que se comenzó a celebrar en la década del 80, fue instituida por la Association for Computing Machinery (ACM), una entidad que nació en Estados Unidos, en 1947, con el objetivo de concientizar sobre los riesgos que pueden causar los ciberataques.

"El primer hacker de la historia fue el mago Nevil Maskelyne[12], que en 1903 logró interceptar la primera transmisión del telégrafo inalámbrico".

El primer ciberdelincuente (o cracker) de la historia fue John Draper, también conocido como *Captain Crunch*, quien recibió ese nombre porque descubrió que modificando un silbato que se regalaba en las cajas de cereales *Cap'n Crunch* emitía un tono a 2600 Hz con el que se podía engañar a la central telefónica y realizar llamadas gratis.

En los mismos inicios de la informática moderna ya aparecieron los primeros ciberdelincuentes y el malware. A principios de los años 70, apareció Creeper, el primer malware el cual llegaba a las computadoras a través de ARPANET, la antecesora de Internet, la cual se auto ejecutaba y comenzaba a mostrar el mensaje I'm the Creeper, ¡catch me if you can! [Soy el Creeper,¡atrápame si puedes!]

---

[12] Nuevas Tendencias. **La breve historia de la ciberseguridad**. 30/Nov/2019

Debido a los estragos causados por ese malware, y para solucionarlo surgió el primer antivirus llamado Reaper, el cual básicamente era otro virus que se propagaba a través de la red en busca de computadoras infectadas con Creeper para eliminarlo.

La evolución de la tecnología hizo que cada vez existieran más aplicaciones, más datos almacenados y, por tanto, más riesgos de seguridad debido a que era información muy jugosa para los ciberdelincuentes.

En los años 80 se produjo un auge del malware y aunque con el tiempo han ido apareciendo antivirus que protegen de las amenazas, el malware ha evolucionado hasta el nivel de que hoy en día existe malware creado específicamente para evitar la protección del antivirus normal, por lo que este se vuelve totalmente ineficaz.

Aunque la "ingeniería social"[13] empezó a utilizarse a una escala mayor a finales de los años 80, hoy en día todavía sigue siendo una de las formas más eficaces para vulnerar una empresa, algo que solo se puede solucionar realizando en primer lugar, una auditoría de ingeniería social para saber hasta qué punto las personas de la empresa son vulnerables, y en segundo lugar mediante una formación y establecimiento de protocolos para hacer conciencia en lo seres humanos de los perjuicios que se ocasionan y tratar de solucionar dichos fallos.

"La ingeniería social se aprovecha de los sesgos cognitivos de las personas, que son como fallos en el hardware humano. Por desgracia para los seres humanos, hay muchos sesgos cognitivos que las personas malintencionadas pueden aprovechar para obtener datos personales y financieros de las víctimas delante de sus narices. Por ejemplo, la tendencia humana de confiar en personas percibidas

13 MORALES, Jose André PhD. **Ingeniería Social.** Instituto Nacional de Ciberseguridad. Gobierno deEspaña, 2014. Pág. 7.

como amables, atractivas o con alguna autoridad puede usarse para los ataques de ingeniería social".

3.2 Definición

La seguridad informática, también conocida como ciberseguridad, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y a la propia información.

La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras, por lo cual al hablar de seguridad de la información no debe ser confundida con la de seguridad informática, ya que esta última solamente se encarga de la seguridad en el medio informático, pero, por cierto, la información puede encontrarse en diferentes medios o formas, y no exclusivamente en medios informáticos.

La seguridad informática también se refiere a la práctica de prevenir los ataques maliciosos, a las computadoras y los servidores, a los dispositivos móviles, a los sistemas electrónicos, a las redes y los datos. En resumen, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Por lo general, estas vulnerabilidades que incluyen los ciberataques apuntan a acceder, modificar o destruir la información confidencial; extorsionar a los usuarios o interrumpir la continuidad de un negocio. Actualmente, la implementación de medidas de seguridad digital son el

resultado de que cada vez hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos.

3.3 Finalidad de la Ciberseguridad

Su objetivo y finalidad es principalmente la protección de los datos, muchos de ellos confidenciales, de las empresas evitando el robo de los mismos, los ataques cibernéticos y las usurpaciones de identidad.

Las empresas más grandes y con mayores sistemas informáticos son más propensas a ser víctimas de un ataque cibernético, los cuales cada vez son más frecuentes y se producen a un ritmo más acelerado.

Es por eso que la inversión en ciberseguridad es un aspecto clave que todas las empresas deben considerar. La tecnología se ha vuelto una pieza fundamental de todos los negocios a nivel mundial lo que hace que seamos más propensos a los ataques y es precisamente por ello que protegerlas no es algo que deba tomarse a la ligera.

Hay una gran variedad de maneras para protegerse de los ataques cibernéticos. Algunas de ellas son:

Actualizar constantemente el software y sistema operativo que utiliza con el fin de tener lo más reciente en seguridad y un mayor nivel de protección.

Configurar filtros de spam para evitar recibir correos electrónicos de remitentes desconocidos que puedan tratarse de casos de phishing.

Utilizar contraseñas diferentes para cada dispositivo y asegurar que las mismas tengan características específicas para no ser detectas rápidamente por los ciberdelincuentes.
Mantener copias remotas (sin conexión a Internet) de los archivos confidenciales y más importantes del negocio y la compañía.

Capacitar y educar permanentemente a los usuarios de sistemas informáticos, su importancia y las principales amenazas, también de las señales de alerta más comunes pueden ayudar, en gran medida, a evitar ataques cibernéticos.

La ciberseguridad ayuda a proteger los sistemas de las diversas amenazas como el ransomware, malware, entre otros. El buen uso de las herramientas de seguridad informática aumentará la confianza del uso de los sistemas informáticos, así como protección para los usuarios finales, que como se ha manifestado en el presente trabajo de investigación cada vez se incrementan más.

3.4 Como se da la Ciberseguridad en Guatemala

Según publicación realizada en el año 2016 por el Banco Interamericano de Desarrollo[14] se indica que, "aunque entidades gubernamentales líderes han comenzado a darle prioridad a los asuntos de seguridad cibernética y evaluar los riesgos nacionales, Guatemala no tiene una estrategia nacional de seguridad cibernética expresa. Su principal entidad de seguridad cibernética es el Equipo de Respuesta a Incidentes de Seguridad Informática Nacional, un equipo ad hoc que históricamente ha operado bajo el Ministerio de Defensa. El -CSIRT-gt- ha recibido capacitación de la Organización de los Estados Americanos -OEA- y otras instituciones internacionales."

El Ministerio de Gobernación también ha mostrado interés en ir avanzando en los temas de seguridad cibernética en Guatemala. Con la asistencia ofrecida por el CSIRT-gt, las fuerzas del orden tienen una cierta capacidad para investigar ataques y delincuencia cibernéticos, pero las autoridades manifiestan que hasta que no se cuente con una legislación integral sobre delincuencia, el sistema judicial tendrá dificultades para procesar los casos eficazmente.

14 BID. **Observatorio de la Ciberseguridad en América Latina y el Caribe**. Pág. 76

Por otra parte, no existe una política de divulgación y aparte de ciertas instituciones financieras, el sector privado rara vez informa al gobierno de eventos cibernéticos. Los operadores de la Infraestructura Crítica Nacional han desplegado algunas medidas de seguridad y software que cumplen con la norma ISO 27000 y otras normas internacionales. La infraestructura de tecnología suele tercerizarse y el gobierno tiene un control mínimo de la misma. Teniendo en cuenta que la tasa de penetración de Internet en el país es del 23% y que su población es en gran parte rural, es inconsistente la asimilación de una mentalidad de seguridad cibernética en la sociedad.

Al mismo tiempo, el gobierno electrónico y los servicios de comercio electrónico en Guatemala han crecido considerablemente en los últimos años, especialmente en el año 2020 como consecuencia de la Pandemia COVID 19.

Los miembros del Congreso han trabajado para abordar este tema mediante la formación del Frente Parlamentario de las Tecnologías de la Información y la Comunicación, que además de promover la legislación contra la delincuencia cibernética, tiene como objetivo promover la conciencia de seguridad cibernética y mejorar las normas y mejores prácticas en el sector privado y la sociedad civil.

Aunque Guatemala no cuenta con una estrategia a nivel nacional para el desarrollo de la educación de seguridad cibernética, los próximos pasos incluyen la implementación de un programa de capacitación conjunto público-privado para los empleados del gobierno y del sector privado, que será administrado por el CSIRT-gt en asociación con un proveedor de servicios.

CAPÍTULO IV

4. Razones sociológicas para la creación de Juzgados y Fiscalías Especializadas

Para los efectos del presente estudio de investigación y luego de la amplia investigacióndocumental realizada, así como del análisis de los órganos especializados en el sistemajudicial, policial y de investigación que atienden esta materia en el país, se puededeterminar que existe una necesidad imperante para la creación de juzgadosespecializados en ciberdelincuencia y que el personal de las fiscalías periódica yconstantemente debe recibir capacitaciones sobre la ciberdelincuencia y las tendenciasde la evolución tecnológica para enfrentar asertivamente los ataques cibernéticos y lacomisión de hechos delictivos en materia informática que proliferan en el país y quedañan la integridad y el patrimonio de las víctimas de tan despreciable actitud humana. Además, la autora presenta los resultados de la presente investigación en cuanto a cuálesson las razones sociológicas más recurrentes o comunes para la comisión de hechosdelictivos a través del uso de las tecnologías de la información y comunicación para sustentar la creación dentro del sistema de justicia guatemalteco de órganosespecializados, pero además la justificación idónea para la promoción de legislación yestrategias concretas para atender el tema central: la Ciberdelincuencia en Guatemala.

El informe del Observatorio de Redes Sociales[15] presenta un estudio de usuarios denumerosas Redes Sociales -RSO- según su edad y sexo, esta distribución depende,generalmente, de la red, estando muy igualados en casi todas. Evidenciando que, en 10de las 17 redes estudiadas, predominan como usuarios el género masculino.

[15] COCKTAIL ANALYSIS, THE. **Informe de resultados. Observatorio de Redes Sociales.** 3ª oleada. http://www.tcanalysis.com/uploads/2011/02/Observatorio-RedesSociales2011.pdf

Si se habla de las redes para el ocio y especializadas en información audiovisual ocurre lo mismo, la mayoría de los usuarios son hombres, con una diferencia de porcentaje que en ocasiones puede sobrepasar el 10%. Sin embargo, es el género femenino el que más abunda en las dos redes más utilizadas, que son Facebook y Messenger, estando, no obstante, los dos muy igualados.

Otro elemento social que se logra evidencias es que una gran parte de las RSO los usuarios principales son los más jóvenes (de 16 a 18 años) seguidos muy de cerca por aquellos con edades comprendidas entre los 19 y los 25 años. Los menos interesados en las RSO, en ocasiones de forma dramática, son los más mayores, sobre todo en aquellas que su temática es de uso profesional o laboral.

Otro punto de evidente importancia es que las RSO destinadas al uso profesional son las menos utilizadas frente a aquellas más actuales utilizadas para el ocio y la entretención. La aparición y evolución de las RSO se ha dado en muy poco tiempo, por ello las características sociológicas de sus usuarios y por consiguiente de los que cometen hechos delictivos a través de ellas es muy cambiante y se modifican con mucha frecuencia y entorno a la actualización de la propia RSO o tecnología de la información ycomunicación de que se trate.

Por lo cual, la capacidad para evolucionar de forma tan vertiginosa hace que cada día surjan nuevas aplicaciones y formas innovadoras de llevar a cabo actos ilícitos, por lo que es complicado identificarlos, seguirlos y estar alerta.

Durante la elaboración de este trabajo se ha descubierto que existen tantos tipos de RSO y tecnologías como perfiles sociológicos de sus usuarios (profesionales, deporte, entretenimiento, académicos entre otros).

Por último, es evidente que existen razones sociológicas para la comisión de delitos cibernéticos, pero la mayoría concentrados en vulnerar los derechos esenciales de la persona cuyos bienes jurídicos tutelados más recurrentes son los pertenecientes a la intimidad, a la integridad de la persona, su patrimonio y sus bienes, realizados siempre de una manera anónima y evidentemente más perjudicial.

4.1 Creación de Juzgados Especializados

La evidente ausencia de mecanismos legales, así como de órganos jurisdiccionales competentes y especializados para la oportuna administración de justicia en los casos de delitos cometidos por medio de las Tecnologías de la Información y Comunicación, el Internet y las Redes Sociales, ha generado una innumerable cantidad de puestas en marcha para resolver esta problemática, la cual no sólo afecta el Sistema de Justicia guatemalteco, sino otros sistemas de la región.

La iniciativa de Ley 4055[16], fue recibida en la Dirección Legislativa el 15 de mayo de dosmil nueve y el 10 de enero de dos mil once, recibió dictamen favorable de la Comisión deLegislación y Puntos Constitucionales del Congreso de la República, dicha iniciativa disponía aprobar la Ley de Delitos Informáticos y además crear en el Ministerio Público una unidad de investigación especializada para estos delitos.

La competencia jurisdiccional, que es la facultad que tiene el Estado para administrar justicia en un caso concreto por medio de sus órganos jurisdiccionales, cuando existe la violación de un derecho que se posee, queda en total vulnerabilidad, al no existir una norma que regule y sancione determinado hecho punible, la violación simplemente queda impune. El problema también se presenta con los delitos de índole informática, ya que en ocasiones sus efectos nocivos tienden a ser no identificables a primera vista y sus efectos

[16] www.congreso.gob.gt

en otros casos son transnacionales. Este es un elemento de suma importancia en la determinación del órgano competente para la administración de la justicia, en virtud de lainvestigación que debe realizarse por la comisión de un hecho delictivo denunciado por la parte afectada.

De conformidad con lo establecido en el Artículo 62 de la Ley del Organismo Judicial, "Competencia. Los tribunales sólo podrán ejercer su potestad en los negocios y dentro de la materia y el territorio que se les hubiese asignado...", en Guatemala se adolece de competencia jurisdiccional para conocer de los delitos cibernéticos que no están tipificados en el ordenamiento jurídico nacional, no hay juzgados especializados para conocer lo referente a los delitos de carácter cibernético.

Estos delitos se caracterizan como se ha demostrado en el contenido de la presente investigación, por cometerse por medios tecnológicos y que no necesariamente se cometen dentro del territorio nacional, sin embargo, según el Artículo de la Ley citada supra "...lo cual no impide que en los asuntos que conozcan puedan dictar providencias que hayan de llevarse a efecto en otro territorio." Pero, sin respaldo de la legislación penal que indica: "Artículo 4. Territorialidad de la ley penal. Salvo lo establecido en tratados internacionales, este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción."

En aquellos juzgados en los que se presentan denuncias de delitos de carácter cibernético, se resuelven conforme a lo que la ley dispone para los asuntos que no tienen una regulación específica, sin embargo, al no estar tipificados, en caso de haber un proceso, no hay equidad en la sanción impuesta.

En el mismo cuerpo normativo citado en la parte conducente del Artículo 57 se establece que: "Toda persona tiene libre acceso a los tribunales para ejercer sus acciones y hacer valer sus derechos de conformidad con la ley." No obstante, nuevamente, al no existir una norma específica que regule los diferentes hechos ilícitos como punibles, ese derecho es violentado. Es decir, al no existir una norma especial en materia de delitos informáticos o cibernéticos que tipifiquen como delito los hechos perpetrados a través delas tecnologías de la Información y Comunicación, el Internet y las Redes Sociales no puede haber persecución penal.

Lo manifestado anteriormente, entonces deja sin cumplimiento, lo establecido expresamente en el Artículo 22 de la Ley del Organismo Judicial que establece: "Primacíadel interés social. El interés social prevalece sobre el interés particular."

Con la existencia de estos vacíos legales, en el ordenamiento jurídico guatemalteco, se observa una inestabilidad futura, respecto de los efectos derivados de la comisión de losdelitos informáticos, lo cual hace una tarea difícil para el juzgador, al tener que adecuar el derecho violentado, al ejercicio judicial, sin una figura punible. Dentro de un ordenamiento jurídico que no prevé las herramientas jurídicas necesarias para evitar o contrarrestar la comisión de un hecho delictivo determinado y nuevo en su género, es una tarea titánica para el juzgador, el tener que aplicar una determinada sanción que sea congruente al derecho violentado, siendo que como en el caso de los delitos cometidos por medios tecnológicos, la norma vigente no se adecua a las necesidades que se presentan en el ejercicio de la aplicación del derecho a casos concretos.

Es necesario que el Estado como garante, evalúe el impacto social que se ejerce por la falta de regulación de delitos relacionados con alta tecnología, así como la falta de órganos jurisdiccionales competentes y especializados y determine que es una

Obligación imperante y necesariamente urgente para proteger a la población guatemalteca de los embates tecnológicos que el ciberespacio está ocasionando con énfasis en la vulneración de los menores de edad y adultos mayores, que al final constituyen la población más vulnerable en el país[17].

4.2 Creación de Fiscalías Especializadas

Según publicaciones del Ministerio de Gobernación, el uso de la tecnología ha cambiado la vida de los adolescentes y adultos, siendo aprovechado por presuntos pandilleros, estafadores y pedófilos que buscan en redes sociales víctimas para dañarles la vida, ante esto, elementos de la Unidad de Cibercrimen de la Policía Nacional Civil (PNC) brindan apoyo de manera trasversal a las Fiscalías del Ministerio Público y de otras unidades policiales. Desde el 2018 a la fecha, han contribuido en 4 mil 024 casos a nivel nacional. En 2018 fueron 713 casos. En 2019 hubo un aumento de 757, en el 2020 apoyaron con 809 procesos y en 2021 van hasta el momento 275.

Autoridades de la cartera del interior informaron que año con año se reportaron aumentos, puesto que la población guatemalteca constata que la Unidad de Cibercrimen ha dado resultados en temas donde las víctimas son menores, adolescentes y mujeres que han sufrido robo de fotografías, bullying, acoso, estafa y hasta promociones en páginas privadas de pornografía.

Cuando el delito se esté cometiendo en internet, los especialistas policiales podrán identificar y perfilar a los usuarios a través de la Web.

[17] Centro de reportes de información de Guatemala. https://www.youtu be. (24 de mayo de 2015).

Los análisis en línea son realizados para localizar a personas desaparecidas, estafadores, entre otros, una vez involucre el uso de las Tecnologías de la Información y la Comunicación, el Internet y las Redes Sociales. Dentro de las recomendaciones policiales esta: No permitir que los niños descarguen o agreguen a personas desconocidas, no intercambiar fotografías, verificar con quien platican en línea y sobre todo temporalizar el uso de los móviles o computadoras.

Es importante que el Ministerio Público guatemalteco emule las buenas prácticas de otros países como Perú, Argentina, Paraguay entre otros, en los cuales se ha determinado la especialización de las Fiscalía para la atención de la ciberdelincuencia y los delitos informáticos, quienes tienen a su cargo la investigación y procesamiento de toda infracción penal que utilice las tecnologías de la información y comunicación, el Internet y las Redes Sociales como medio o herramienta clave para la comisión de un delito, siempre y cuando aquella fuera determinante en la actividad delictiva, generando una especial complejidad técnica en la investigación del delito.

En estos países, estos órganos realizan investigaciones de fraudes cometidos mediante el uso de una tarjeta de compra, crédito o débito; fraudes informáticos, siempre y cuando la tecnología informática fuera determinante en la actividad delictiva; extorsión online bajo las modalidades denominadas "ransomware", "sextorsión" o cualquier otra que apareciere en el futuro; daños y sabotajes informáticos, así como la venta, distribución, circulación o introducción en un sistema informático, de cualquier programa destinado a causar daños; incitación a cometer delitos, intimidación pública y apología del delito; falsificación de documentos y firmas electrónicas; revelación de secretos cuando se realizan por medios de comunicación electrónica con capacidad de ser difundidos a través de redes sociales a un grupo indeterminado de personas; explotación, administración u organización de juegos de azar,

cuando fueren cometidos y ofrecidos através de plataformas online; infracciones a la ley de propiedad intelectual cuando fuerencometidos y ofrecidos a través de plataformas online.

Asimismo, se ha definido que el ámbito material de actuación para estas Fiscalía Especializadas en el Cibercrimen será de excepción, la recepción de las denuncias corresponderá a las Unidades Judiciales y fiscalías de instrucción no especializadas, y sidel contenido de la causa o del resultado de la investigación surgieran hechos que reúnanlas características consignadas, deberán ser remitidas a la Fiscalía especializada en Cibercrimen.

1.3 Fines Específicos de los Organismos Especializados

La evolución y aparición de nuevas tecnologías y herramientas informáticas en las últimas décadas ha sido una ventaja para la sociedad, pero también ha posibilitado nuevas formas delictivas como el fenómeno de la ciberdelincuencia, la misma que quebranta la protección de la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como de los derechos de las personas frente el abuso de los mismos.

Por lo cual, el presente estudio de investigación propone algunos fines específicos que es importante atender por organismos especializados si se pretende su incorporación al sistema de administración de justicia en el país, con el propósito de hacer frente a esta nueva forma de delincuencia, la cual acecha a toda la población vulnerando principalmente a los menos de edad y adultos mayores a quienes de diversas formas con ardid y engaños logran que se consumen los delitos violentando principalmente su patrimonio y su integridad e indemnidad sexual.

La creación de Juzgados y Fiscalías Especializados en Delitos Informáticos deben tener por objeto principalmente la prevención de las conductas delictivas cometidas mediante los sistemas y datos informáticos. Además, deben sancionar dichas conductas garantizando los bienes jurídicos tutelados y que son vulnerados mediante la utilización de tecnologías de la información o comunicación, el Internet y las Redes Sociales.

Es por ello que con el propósito de contar con magistrados, funcionarios y empleados judiciales y de investigación idóneos para combatir los ciberdelitos, se debe dotar al Organismo Judicial y al Ministerio Público de estructuras dedicadas a enfrentar los desafíos y dificultades que la complejidad de los ciberdelitos demanda, poniendo énfasis en la capacitación de sus integrantes y la permanente actualización técnica y tecnológica en la materia de investigaciones en el ciberespacio.

Dado que, la ciberdelincuencia se ha visto incrementada con motivo del Estado de Emergencia a causa de la pandemia por el COVID-19, por el incremento necesario del uso de la tecnología, de las redes sociales, y del Internet en general, situación que ha sido aprovechada por los denominados ciberdelincuentes para innovar los modus operandi y perpetrar los ciberdelitos señalados en el presente estudio, se hace necesario crear Juzgados y Fiscalías Especializados en Ciberdelincuencia cuya con competencia yjurisdicción sea a nivel nacional y que dependan del Organismo Judicial y del Fiscal General de la Nación respectivamente.

En una publicación internacional del El País se indicó que: En 2017, España sufrió 122.000 ciberataques, en contradicción con los 18.000 que se produjeron en el 2014, en virtud de las oportunidades que brindan las nuevas tecnologías en manos de los criminales lo cual, se ha convertido en un gran desafío para los tribunales, que no pueden competir con la velocidad y los medios con los que dispone una ciberdelincuencia cada

vez más sofisticada y globalizada. La realidad de los juzgados a nivel mundial, en los que aún se amontonan los expedientes en papel, y una legislación pensada para la era analógica, minan la eficacia del combate de las nuevas formas de criminalidad. "Los delincuentes están en el siglo XXI y la justicia, en el XIX", retrata Juan Gonzalo Ospina[18], abogado penalista y socio de Ospina Abogados. Opinión que comparten los que, día a día, ven cómo la lenta tramitación de los procedimientos judiciales favorece la destrucción de pruebas y facilita la impunidad.

La actividad delictiva en Internet es amplia y está en continua reinvención. Se suplantan identidades, se asaltan sistemas informáticos o se blanquea dinero. Otras fechorías muy de moda son las estafas en la red, las botnet y los keyloggers, el hacking, el cracking, el Phishing, el fraude con tarjetas de crédito o el espionaje. A esto hay que añadir el fenómeno de la encriptación, la computación en la nube o la inteligencia artificial. Entonces, surge la interrogante: ¿Está preparado el sistema judicial para combatir todo ello? El problema no es menor, porque estos casos son cada vez más numerosos en los juzgados de muchos países. Más aún cuando uno de los objetivos principales de la justicia es resarcir esos daños, y muchas veces es prácticamente imposible.

Según Moisés Barrio Andrés, letrado del Consejo de Estado en España y autor del libro Delitos 2.0[19], "el impacto económico de los ilícitos relacionados con el Internet fue del 0,8% del PIB mundial". En España, explica, "hemos pasado de unos 18.000 ciberataques en 2014 a más de 122.000 en 2017, de los cuales el 95% afectó a empresas y ciudadanos". Por ello, el experto incide en la importancia de sus consecuencias y de ponerle freno.

---

18 https://cincodias.elpais.com/cincodias/2019/03/15/legal. Madrid, 18 de marzo de 2019.

19 Barrio Andrés, Moisés. **Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos**.2018

"El impacto económico del Cibercrimen supera al narcotráfico", asevera. Por su parte, Ospina pone el foco en la Ley de Enjuiciamiento Criminal, que data de 1882, ya que produce disfuncionalidades para las víctimas y fortalece la impunidad deldelincuente. A su juicio, reformas como la de 2015 para fortalecer la investigación deestos ilícitos, "no valen de nada porque los mecanismos para salvaguardar a losciudadanos del delito llegan tarde". ¿El motivo? "Un mecanismo de denuncia arcaico",explica el abogado.

Por ello, es importante que al plantear propuestas o reformas al sistema de justicia guatemalteco se tome en cuenta que es importante establecer funciones sustantivas y específicas a los órganos jurisdiccionales y fiscalías para que en el ámbito de sus respectivas competencias y jurisdicciones puedan entre otras funciones:

1. Brindar acompañamiento técnico y especializado a todos los funcionarios del sistema de justicia: los fiscales en la realización de la investigación y a los jueces para que mediante la aplicación de la sana crítica razonada y de acuerdo a su lealsaber y entender puedan administrar justicia, con capacidades para la obtencióny diligenciamiento de pruebas digitales que sean determinantes para la investigación y desarrollo del proceso penal respectivo.

2. Unificar criterios en procedimientos y métodos de investigación en materia de ciberdelincuencia.

3. Elaborar directivas, lineamientos, instructivos y guías, en el ámbito de su competencia, que orienten las investigaciones de las Fiscalías Especializadas enCiberdelincuencia y a los Juzgados que se creen a nivel nacional.

4. Coordinar con los organismos nacionales e internacionales el adecuado y eficientetrabajo para el debido cumplimiento de las funciones asignadas a los OrganismosEspecializados en Ciberdelincuencia.

5. Promover la articulación entre el Organismo Judicial, Ministerio Público y la PolicíaNacional Civil, con el fin de hacer más eficiente la administración de justicia para la población guatemalteca en esa materia.

6. Coordinar con las diversas redes internacionales, capacitaciones periódicas y permanentes, para jueces, fiscales, peritos y para los que investigan casos en losque la tecnología es un medio para cometer los delitos, a fin de poder brindar respuesta inmediata y oportuna a los casos relacionados en materia de ciberdelincuencia.

7. Proponer políticas públicas que permitan hacer frente a la ciberdelincuencia en elpaís, garantizando la protección de la integridad de sus habitantes quienes constantemente sufren los ataques que mediante las tecnologías de la Información y Comunicación, el Internet y las Redes Sociales realizan a su patrimonio, seguridad e integridad personal.

4.4 Instrumentos Internacionales en el Ámbito de Delitos Informáticos

Es importante indicar que los delitos informáticos no solo son un problema a nivel nacional como se ha indicado en todo el contenido del presente estudio, y que existe un innumerable respaldo jurídico de instrumentos internacionales que fundamentan su atención y las formas de administrar justicia pronta y cumplida.

4.4.1 Convenios Internacionales en el ámbito de delitos informáticos

4.4.1.1 Convenio sobre cibercriminalidad: El Convenio sobre delitos cibernéticos, Convenio de Budapest sobre delitos cibernéticos o Convenio de Budapest es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes. Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de Canadá, Japón y China como estados observadores. El convenio y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001. El 23 de noviembre de 2001 se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004. A partir del 28 de octubre de 2010, 30estados firmaron, ratificaron y se adhirieron a la convención, mientras que otros 16 estados firmaron la convención, pero no la ratificaron. El 1 de marzo de 2006 entró en vigor el Protocolo Adicional a la Convención sobre el delito cibernético. Los estados quelo han ratificado deben penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como amenazas racistas y xenófobas e insultos.

4.4.1.2 Convenio Número 108 del Consejo de Europa: El Convenio 108 del Consejo de Europa, de fecha 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protecciónde datos. Tiene como fin garantizar a cualquier persona física el respeto de sus derechosy libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona. Con el protocolo que ha modificado el Convenio se pretende ampliar su ámbito de aplicación, aumentar el nivel de protección de los datos y mejorar su eficacia.

4.4.1.3 Decisión marco 2005/222/JAI del Consejo de Europa: Decisión marco 2005/222/JAI del Consejo, de fecha 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, tiene por objeto reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, incluida la policía y los demás servicios represivos especializados de los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información. Se ha comprobado la existencia de ataques contra los sistemas de información, en particular como consecuencia de la amenaza de la delincuencia organizada, y crece la inquietud ante la posibilidad de ataques terroristas contra sistemas de información que forman parte de las infraestructuras vitales de los Estados miembros. Esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia, y por tanto exige una respuesta por parte de la Unión Europea.

4.4.2 La Organización de las Naciones Unidas y la prevención del delito informático

4.4.2.1 Duodécimo Congreso de Naciones Unidas para la prevención del delito y la justicia penal: El 12º Congreso aprobó la Declaración de Salvador, que, entre otras cosas, abrió la puerta a los debates sobre nuevas respuestas nacionales e internacionales a la delincuencia cibernética.

4.4.2.2 Declaración de Viena sobre la delincuencia y la justicia frente a los retos del siglo XXI: Resolución de la Asamblea General de Naciones Unidas con fecha4 de Diciembrede 2000. La cual se formuló por el impacto en nuestras sociedades de los delitos gravesde carácter mundial y convencidos de la necesidad de cooperación en materia de prevención del delito y justicia penal en los planos bilateral, regional e internacional, se decidió en ella formular recomendaciones de política orientadas a la acción para la prevención y el control de los delitos relacionados con la informática

y se invitó a la Comisión de Prevención del Delito y Justicia Penal a que emprenda trabajos a este respecto, teniendo en cuenta la labor en curso en otros foros. Comprometiéndose al esfuerzo para aumentar la capacidad de prevenir, investigar y enjuiciar los delitos de alta tecnología y relacionados con la informática.

4.4.2.3 Resolución 57/239 sobre los elementos para la creación de una cultura mundial de seguridad cibernética: Esta resolución fue aprobada en la cuarta sesión plenaria, celebrada el 10 de junio de 2003, sobre los elementos para la Creación de una Cultura Mundial de Seguridad Cibernética para Sistemas y Redes de Información, sobre la base del informe de la Segunda Comisión (A/57/529/Add.3).

La Asamblea General observando que los gobiernos, las empresas, otras organizaciones y los usuarios individuales dependen cada vez más de las tecnologías de la información para el suministro de bienes y servicios esenciales, la gestión de sus asuntos y el intercambio de información, reconoció la necesidad de aumentar la seguridad cibernética que no es sólo cuestión de prácticas de gobierno o de orden público, sino que debe alcanzarse promedio de la prevención y con el apoyo de toda la sociedad.

Además de reconociendo que las disparidades entre los países en el acceso a las tecnologías de la información y en su utilización pueden reducir la eficacia de la cooperación internacional en la lucha contra la utilización de las tecnologías de la información con fines delictivos y en la creación de una cultura mundial de la seguridad cibernética, y teniendo en cuenta la necesidad de facilitar la transferencia de las tecnologías de la información, en particular a los países en desarrollo.

4.4.2.4 El manual de las Naciones Unidas para la prevención y control de delitos informáticos: En 1994, en el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos se señaló que el potencial de la delincuencia informática es tan amplio como el de los propios sistemas internacionales de telecomunicaciones. Como era de esperar, la palabra "Internet" aparecía solo una vez en el Manual y la palabra "ciberdelincuencia" no se utilizó; sin embargo, las conclusiones demostraron una gran visión de futuro. Si bien el Manual centró su atención en el concepto de "delito informático", es bien sabido que hoy en día la "ciberdelincuencia" recurre efectivamente a las tecnologías globalizadas de la información y las comunicaciones, en particular a Internet y Redes Sociales, para la comisión de actos delictivos de alcance transnacional.

4.4.2.5Tratado de la Organización Mundial de la Propiedad Intelectual sobre el derecho de autor: El Tratado de la OMPI sobre Derecho de Autor (WCT) es un arreglo particular adoptado en virtud del Convenio de Berna que trata de la protección de las obras y los derechos de sus autores en el entorno digital. Además de los derechos reconocidos en el Convenio de Berna, se conceden determinados derechos económicos. El Tratado también se ocupa de dos objetos de protección por derecho de autor: i) los programas de computadora, con independencia de su modo o forma de expresión, y ii) las compilaciones de datos u otros materiales ("bases de datos").

4.4.3 La Organización de Estados Americanos OEA y los delitos informáticos

4.4.3.1 Estrategia de la OEA sobre seguridad informática: La Estrategia Interamericana Integral de Seguridad Cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA).

La Estrategia reconoce la necesidad de que todos los participantes en las redes y

sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad a fin de crear una cultura de seguridad cibernética.

La Estrategia también reconoce que un marco eficaz para la protección de las redes y sistemas de información que integran la Internet y para responder a incidentes y recuperarse de los mismos dependerá en igual medida de que: Se proporcione información a los usuarios y operadores para ayudarles a asegurar sus computadoras y redes contra amenazas y vulnerabilidades, y a responder ante incidentes y a recuperarse de los mismos; Se fomenten asociaciones públicas y privadas con el objetivo de incrementar la educación y la concientización, y 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; Se identifiquen y evalúen normas técnicas y prácticas óptimas para asegurar la seguridad de la información transmitida por Internet y otras redes de comunicaciones.

Y se promueva la adopción de las mismas; y Se promueva la adopción de políticas y legislación sobre delito cibernético que protejan a los usuarios de Internet y prevengan y disuadan el uso indebido e ilícito de computadoras y redes informáticas, respetando a su vez la privacidad de los derechos individuales de los usuarios de Interne


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C.A.

CONCLUSIÓN DISCURSIVA

La existencia y el uso de las nuevas tecnologías de la información y la comunicación, el Internet y las Redes Sociales han provocado el surgimiento de una nueva forma de delinquir, en Guatemala no existe aún suficientes normas aprobadas que tipifiquen y regulen todos los tipos de delitos informáticos que mediante estas tecnologías se cometen de una forma desmedida, sobre todo en la actualidad como consecuencia de la virtualidad a que obligó la pandemia del COVID 19.

Es evidente que los factores sociales son causa de esta criminalidad como se demostró en el contenido del presente estudio de investigación lo social incide sobre la forma y frecuencia en la comisión de los delitos informáticos. Las causas sociológicas, dan importancia absoluta o predominante a factores externos, por esto se consideran las condiciones económicas, académicas, culturales y sociales en las cuales destacan sus amistades, trabajo, centros de diversión, organización social, su economía y su influencia ambiental.

La legislación guatemalteca no contempla aún la garantía de la protección del patrimonio de las personas como consecuencia de los ataques cibernéticos, por lo cual, la privacidad y protección de datos personales en Internet y Redes Sociales es deficiente.

Los órganos jurisdiccionales y fiscalías en Guatemala resultan insuficientes ante las nuevas formas del Cibercrimen no existen órganos jurisdiccionales especializados en la materiay el ente investigador compuesto por el Ministerio Público y la Policía Nacional Civil, aúnno cuentan con capacitaciones y especializaciones periódicas para garantizar la seguridad cibernética, la inoperancia del sistema de justicia que no responde oportunamente ante estos hechos delictivos. Por lo cual, se considera que la creación de juzgados y fiscalías especializadas será una herramienta necesaria para el estudio y resolución de los casos que se presenten por los delitos cometidos por medios electrónicos, y la capacitación permanente para tratar dichos delitos permitirá contar con un equipo estatal para enfrentar los ataques cibernéticos con una estrategianacional de seguridad cibernética.

BIBLIOGRAFIA

BARRIO ANDRÉS, Moisés. **Delitos 2.0 Aspectos penales, procesales y de seguridad de los ciberdelitos.** EDITORIAL. Wolters Kluwer, Madrid, 1ª Edición, 2018.

BID. **Observatorio de la Ciberseguridad en América Latina y el Caribe**. Pág. 76

CARBONNIER, Jean. **Sociología Jurídica**. Madrid: TECNOS, 1982. 256p.

CAVADA HERRERA, Juan Pablo. **Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera**. Julio 2020. Pág. 2.

Centro de reportes de información de Guatemala. https://www.youtube. 24 de mayo de 2015.

COCKTAIL ANALYSIS, THE. **Informe de resultados**. Observatorio de Redes Sociales. 3ª oleada.

http://www.tcanalysis.com/uploads/2011/02/Observatorio-RedesSociales2011.pdf

El País, **Cinco Días,** Madrid 18 de marzo de 2019.

El Periódico, **Soy 502**, Guatemala, 10 de noviembre de 2016. https://drive.google.com/file/d/1PSvsnucnLG25lhBYt5D-t-Vg7KviRsuA/view

https://es.ryte.com/wiki/Hacker

https://forbescentroamerica.com/2020/07/13/cibercrimen-maximo-esplendor

https://lam.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

https://ogdi.org/estadisticas

https://svet.gob.gt/

https://www.congreso.gob.gt

https://www.lawebdelprogramador.com/diccionario/Botnet/

https://www.unodc.org/documents/congress//About/information/65-years-brochure_es.pdf

MARTÍNEZ, Fátima. **4 Casos de Ciberdelincuencia en Internet | Luces y sombras de las marcas**. fatimamartinez.es

NORIEGA SALAZAR, Hans Aarón, **Delitos Informáticos. Defensa Pública Penal 2011.** Pág. 36

NUEVAS TENDENCIAS. **La breve historia de la Ciberseguridad**. 30/Nov/2019.

RECASÉNS SICHES, Luis Pedro Alejandro. **Direcciones contemporáneas del pensamiento jurídico: la filosofía del derecho en el siglo XX**. 1936.

RIFKIN, Jeremy. **La Sociedad del Coste Marginal, El Internet de las Cosas, el Procomún Colaborativo y el Eclipse del Capitalismo**, pág. 24.

PINZÓN MAYORGA, Ivonne Caterine, Maryere Mildred Mora Ardila. **Especialización en Seguridad Informática.** http://repository.unipiloto.edu.co/ Colombia.

Legislación

Constitución Política de la República de Guatemala. Asamblea NacionalConstituyente. Guatemala, 1986.

Ley del Organismo Judicial. Decreto 2-89 del Congreso de la República, Guatemala, 1989.

Código Penal de Guatemala. Decreto Número 17-73, del Congreso de la República de Guatemala, 1973.