UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE OCCIDENTE
DIVISION DE CIENCIAS JURIDICAS Y SOCIALES

“PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMÁTICOS”.

ANA LUCÍA SAJQUÍM JUÁREZ

QUETZALTENANGO, MAYO DE 2019

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE OCCIDENTE
DIVISION DE CIENCIAS JURIDICAS Y SOCIALES

"PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMÁTICOS".

TESIS
Presentada a las Autoridades de la División de Ciencias Jurídicas y Sociales del Centro Universitario de Occidente de la Universidad de San Carlos de Guatemala.

POR:

ANA LUCÍA SAJQUÍM JUÁREZ

Previo a conferirsele el Grado Academico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

Y los títulos profesionales de

ABOGADO Y NOTARIO

Quetzaltenango, mayo de 2019.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE OCCIDENTE
DIVISION DE CIENCIAS JURIDICAS Y SOCIALES

AUTORIDADES:

RECTOR MAGNIFICO: Ing. Murphy Olympo Paiz Recinos
SECRETARIO GENERAL: Arq. Carlos Enrique Vallladares Cerezo

CONSEJO DIRECTIVO:

DIRECTORA GENERAL: Msc. María del Rosario Paz Cabrera
SECRETARIA ADMINISTRATIVA: Msc. Silvia Recinos

REPRESENTANTE DE LOS CATEDRÁTICOS:

Ing. Arg. Hector Alvarado Quiroa
Ing. Edelman Cándido Monzón López

REPRESENTANTE DE LOS EGRESADOS:

Dr. Luis Emilio Bucaro Echeverria

REPRESENTANTE DE LOS ESTUDIANTES:

Br. Luis Angel Estrada García
Br. Edson Vitelio Amezquita Cutz

DIRECTOR DE LA DIVISIÓN DE CIENCIAS JURÍDICAS Y SOCIALES:

Dr. Carlos Abraham Calderón Paz

COORDINADOR DE LA CARRERA DE ABOGADO Y NOTARIO:

Lic. Patrocinio Bartolomé Díaz Arrivillaga.

TRIBUNAL QUE PRACTICÓ EL EXAMEN PROFESIONAL

PRIMERA FASE:

(FASE PRIVADA)

Lic. Luis Angel Ordoñez Rodriguez	Área Mercantil
Licda. Rosmery Yamilett Orozco López	Área Civil
Lic. Gabriel Estuardo Perez Delgado	Área Mercantil

SEGUNDA FASE:

(FASE PÚBLICA)

Lic. Anibal Sacor Cobaquil	Área Penal
Lic. Carlos Sacalxot Valdés	Área Laboral
Licda. Ester Elizabeth Mendez Pérez	Área Administrativa

ASESOR DE TESIS:

Lic. Erick Dario Nufio Vicente

REVISOR DE TESIS:

Lic. Fausto Roberto Reyes Sánchez

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Centro Universitario de Occidente

COORDINACIÓN DE LA CARRERA DE ABOGADO Y NOTARIO, DIVISIÓN DE CIENCIAS JURIDICAS DEL CENTRO UNIVERSITARIO DE OCCIDENTE, QUINCE DE AGOSTO DEL AÑO DOS MIL DIECIOCHO.

Se asigna como trabajo de tesis del (la) estudiante: ANA LUCIA SAJQUIM JUAREZ, Titulado: ***"PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMATICOS".***

Consecuentemente se le solicita al estudiante se sirva proponer al asesor que llene el perfil establecido en el reglamento respectivo, para que en su oportunidad rinda su dictamen.

Atentamente,

"ID Y ENSEÑAD A TODOS"

CENTRO UNIVERSITARIO DE OCCIDENTE
CARRERA ABOGADO Y NOTARIO
COORDINADOR
Quetzaltenango

Msc. Patrocinio Bartolomé Díaz Arrivillaga
Coordinador de la Carrera de Abogado y Notario

cc. Archivo
PBDA/gbtb

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Centro Universitario de Occidente

COORDINACIÓN DE LA CARRERA DE ABOGADO Y NOTARIO, DIVISIÓN DE CIENCIAS JURIDICAS DEL CENTRO UNIVERSITARIO DE OCCIDENTE, VEINTINUEVE DE AGOSTO DEL AÑO DOS MIL DIECIOCHO.

En virtud de cumplir con el perfil establecido por el reglamento de tesis de la División de Ciencias Jurídicas del Centro Universitario de Occidente se designa como *Asesor* del Trabajo de Tesis del estudiante: **ANA LUCÍA SAJQUÍM JUÁREZ,** Titulado: ***"PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMATICOS"***, al Licenciado(a): ERICK DARIO NUFIO VICENTE; consecuentemente se solicita al estudiante que juntamente con su asesor elaboren el diseño de investigación y lo sometan a consideración del Departamento de Investigaciones de la División para su aprobación correspondiente, previamente a elaborar el trabajo designado, debiendo el *asesor* nombrado oportunamente, rendir su dictamen al finalizar la labor encomendada.

"ID Y ENSEÑAD A TODOS"

Lic. Patrocinio Bartolomé Díaz Arrivillaga
Coordinador de la Carrera de Abogado y Notario

CENTRO UNIVERSITARIO DE OCCIDENTE
CARRERA ABOGADO Y NOTARIO
COORDINADOR
Quetzaltenango

cc. Archiv
PBD/gbtb

Quetzaltenango, 18 de septiembre de 2018.

Licenciado:

Patrocinio Bartolomé Díaz Arrivillaga

División de Ciencias Jurídicas y Sociales

CUNOC-USAC

Licenciado Patrocinio: Por medio de la presente me permito informar que conjuntamente con la Estudiante **ANA LUCÍA SAJQUÍM JUÁREZ**, Carné **1990 31312 0901**, de este Centro Universitario, hemos elaborado el diseño de investigación de la tesis denominada **"PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMÁTICOS"** el cual a mi criterio cumple con todos los requisitos establecidos por la Coordinación de Investigación Jurídicas y Sociales. En consecuencia considero que la misma puede continuar con el trabajo de investigación para elaboración de su tesis.

Sin otro particular, me suscribo de usted.

Deferentemente:

LICENCIADO
ERICK DARIO NUFIO VICENTE
ABOGADO Y NOTARIO

Lic. Erick Dario Nufio Vicente

Abogado y Notario

No. de colegiado 5,898

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Centro Universitario de Occidente

CIJUS-113-2018

Quetzaltenango 01 de Octubre 2018

Licenciado
Patrocinio Bartolomé Díaz Arrivillaga
Coordinador de la Carrera de Abogacía y Notariado
División de Ciencias Jurídicas
CUNOC-USAC

Licenciado Díaz:

Por medio de la presente me permito informar que el (la) estudiante: ANA LUCÍA SAJQUIM JUÁREZ, ha llenado el requisito reglamentario para la Aprobación del Diseño de Investigación denominado: ***"PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMÁTICOS"***

En Consecuencia, puede continuar con el trabajo de Investigación, para la elaboración de su Tesis.

Sin otro particular, me suscribo.

Atentamente,

"ID Y ENSEÑAD A TODOS"

CENTRO UNIVERSITARIO DE OCCIDENTE
CARRERA ABOGADO Y NOTARIO
COORDINACIÓN DE INVESTIGACIONES JURÍDICAS
Quetzaltenango

LIC. RONY ESTUARDO HIPP REYNA
Coordinación de Investigaciones Jurídicas y Sociales

Quetzaltenango, 23 de octubre de 2018.

Msc.: PATROCINIO BARTOLOMÉ DÍAZ ARRIVILLAGA

Coordinador Académico de la carrera de Abogado y Notario

División de Ciencias Jurídicas

Centro Universitario de Occidente

Universidad de San Carlos de Guatemala.

En forma atenta y respetuosa me dirijo a usted, informándole que, en cumplimiento de la respectiva resolución, he finalizado la función de asesorar la tesis denominada "PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMÁTICOS", elaborada por la estudiante ANA LUCÍA SAJQUÍM JUÁREZ, que se presenta como requisito previo para obtener el grado académico de Licenciada en Ciencias Jurídicas y Sociales y los títulos profesionales de Abogada y Notaria.

La tesis relacionada es sumamente importante, en virtud que aborda un tema de especial trascendencia, principalmente en la presente época en que el avance de la tecnología es un hecho sin precedentes y, como contrapartida, no se cuenta con regulación jurídica suficiente que proteja bienes jurídicos que tengan relación con los delitos informáticos; el objeto de estudio también es de impacto social y del cual existe poca bibliografía nacional, lo que evidencia que es un buen aporte tanto para esta casa de estudios superiores como para la comunidad jurídica y el pueblo en general. La tesista acató en todo momento las orientaciones que se le transmitieron, utilizó la metodología y técnicas de investigación adecuadas para este tipo de trabajos y arribó a conclusiones y recomendaciones valorables.

En tal virtud, emito dictamen FAVORABLE, a efecto la tesista en mención pueda continuar con sus trámites de revisión de tesis.

Sin otro particular:

LICENCIADO
ERICK DARIO NUFIO VICENTE
ABOGADO Y NOTARIO

MSc. ERICK DARIO NUFIO VICENTE

Asesor

Colegiado número: 5898

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Centro Universitario de Occidente

COORDINACIÓN DE LA CARRERA DE ABOGADO Y NOTARIO, DIVISIÓN DE CIENCIAS JURIDICAS DEL CENTRO UNIVERSITARIO DE OCCIDENTE, TREINTA DE OCTUBRE DEL AÑO DOS MIL DIECIOCHO.

En virtud de cumplir con el perfil establecido por el reglamento de tesis de la División de Ciencias Jurídicas del Centro Universitario de Occidente se designa como *Revisor* del Trabajo de Tesis del Estudiante: ANA LUCÍA SAJQUIM JUÁREZ, Titulado: ***"PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMÁTICOS"***, al Licenciado (a): FAUSTO ROBERTO REYES SANCHEZ; consecuentemente se solicita al *revisor* que oportunamente rinda su dictamen.

Atentamente,

"ID Y ENSEÑAD A TODOS"

CENTRO UNIVERSITARIO DE OCCIDENTE
CARRERA ABOGADO Y NOTARIO
COORDINADOR
Quetzaltenango

Msc. Patrocinio Bartolomé Díaz Arrivillaga
Coordinador de la Carrera de Abogado y Notario

Dr. Carlos Abraham Calderón Paz Director
de la Carrera de Abogado y Notario

DIVISION DE CIENCIAS JURIDICAS Y SOCIALES
DIRECCION

Quetzaltenango 3 de enero de 2019.

Licenciado :

Patrocinio Bartolomé Díaz Arrivillaga

Coordinador de la Carrera de Abogado y Notario

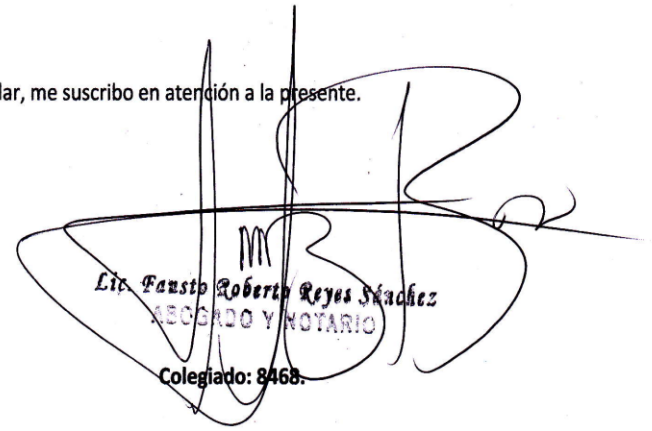
Division de Ciencias Jurídicas y Sociales

Centro Universitario de Occidente

Quetzaltenango.

En cumplimiento al cargo recaido en mi persona, he concluido la **REVISION** de Tesis de Grado Profesional de la estudiante **ANA LUCÍA SAJQUÍM JUÁREZ**, con número de Carné **200730504** titulada **"PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELLITOS INFORMÁTICOS",** habiendo atendido la ponente las directrices metodológicas que le fueran orientadas para la culminacion del presente trabajo de tésis, por lo que siendo un aporte para la academia, emito **OPINION FAVORABLE**, a efecto de que pueda continuar con los trámites administrativos correpondientes.

Sin otro particular, me suscribo en atención a la presente.



Colegiado: 8468.

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Centro Universitario de Occidente

Quetzaltenango, 25 de Febrero de 2019

Licenciado
Carlos Abraham Calderón Paz
Director de la Carrera de Abogacía y Notariado
División de Ciencias Jurídicas
CUNOC-USAC

Licenciado Calderón:

Por medio de la presente me permito informar que el (la) estudiante: **Ana Lucía Sajquím Juárez** Con carné N. 1990313120901 y Registro Académico No. 200730504 de este Centro Universitario, ha llenado los requisitos reglamentarios para la **Orden de Impresión de Tesis** denominada: **"PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMÁTICOS"** Sin otro particular, me suscribo.

Atentamente,

"ID Y ENSEÑAD A TODOS"

LIC. RONY ESTUARDO HIPP REYNA
Coordinación de Investigaciones Jurídicas y Sociales
Investigador

CENTRO UNIVERSITARIO DE OCCIDENTE
CARRERA ABOGADO Y NOTARIO
COORDINACION DE INVESTIGACIONES JURIDICAS
Quetzaltenango

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Centro Universitario de Occidente

El infrascrito **DIRECTOR DE LA DIVISIÓN DE CIENCIAS JURÍDICAS.** Del Centro Universitario de Occidente ha tenido a la vista la **CERTIFICACIÓN DEL ACTA DE GRADUACIÓN** No. **CC.JJ Y S. 11-2019-AN** de fecha 25 de Febrero del año **2019** del (la) estudiante: **Ana Lucía Sajquím Juárez** Con carné N. 1990313120901 y Registro Académico No. 200730504, emitido por el Coordinador de la Carrera de Abogado y Notario, por lo que se **AUTORIZA LA IMPRESIÓN DEL TRABAJO DE GRADUACIÓN** titulado **"PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMÁTICOS"**

Quetzaltenango 25 de Febrero de 2019.

"ID Y ENSEÑAD A TODOS"

Dr. Carlos Abraham Calderón Paz
Director División de Ciencias Jurídicas

DIVISION DE CIENCIAS JURICAS Y SOCIALES
DIRECCION

DEDICATORIA

A DIOS:

Por haberme dado la vida, llenarme de sus dones, ser el forjador de mi camino y brindarme la fortaleza necesaria ante las adversidades en el logro de mis metas.

A MIS PADRES:

Wotsbely Enrique Sajquím López y Aura Marina Juárez Cojulún por su apoyo, consejos, comprensión, amor en los buenos y malos momentos, por darme todo necesario y más para ser la persona que ahora soy. Gracias a ustedes por su dedicación y coraje he logrado conseguir mis objetivos.

A MI HERMANO:

Mario Enrique Sajquím Juarez quien es uno de los pilares más importantes en mi vida, gracias por su compañía y apoyo incondicional en todo momento.

A MIS TIOS:

Con respeto y admiración por sus enseñanzas , guía y compañía que me han brindado a lo largo y en la culminación de mi carrera. En especial a Victor, Mario, Germán, Rosa y Blanca Juárez Cojulún

A MIS PRIMOS:

Por todo el cariño que me brindan.

A MIS AMIGOS:

Por todos los buenos momentos que hemos pasado juntos en especial a Harly Lilibeth Menchú por su amistad, cariño, compañía y comprensión incondicional.

A MIS PADRINOS:

Lic. Erick Dario Nufio Vicente y Lic. Rony Paz con toda mi admiración por sus enseñanzas y apoyo en el camino a mi meta, quienes se han convertido en un ejemplo en mi vida.

A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, en especial al CENTRO UNIVERSITARIO DE OCCIDENTE, donde forje mi camino para alcanzar mi tan anhelada meta.

INDICE

CAPITULO III

DELITOS INFORMÁTICOS

CAPITULO IV

DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL GUATEMALTECA

CAPITULO V

PROCESO LEGISLATIVO EN GUATEMALA

CAPITULO VI

BENEFICIOS JURÍDICOS Y SOCIALES

CAPITULO VII

PRESENTACIÓN DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN DE CAMPO

INTRODUCCIÓN

El nacimiento de los delitos informáticos es resultante de la masificación del fenómeno de la tecnología, en la actualidad las computadoras en su mayoría y la gran diversidad de instrumentos tecnológicos que se utilizan como herramientas de apoyo en las actividades cotidianas de la sociedad actual, no solo ofrecen beneficios sino también han contribuido a la aparición de nuevas formas de delinquir.

La implicación de la informática en el ámbito delictivo ha dado origen a una serie de comportamientos ilícitos antes impensables, que constituyen una de las principales debilidades del ordenamiento jurídico al tratar de establecer una correcta tipificación en las normas penales.

En nuestro país los delitos informáticos en los últimos tiempos han tenido un avance significativo, sin embargo no se les ha dado la atención que estos necesitan, la realidad actual demuestra que la sociedad en general, se encuentra vulnerable frente a este tipo de conductas ilícitas. La única forma de contrarrestar estos efectos es a través de la creación de la Ley que regule los delitos informáticos, el establecimiento de un marco jurídico trae consigo el control y la prevención de la ciberdelincuencia.

Por ello el presente trabajo responde a una inquietud largamente analizada de **"Principales Beneficios Jurídicos y Sociales de la Creación de la Ley que Regule los Delitos Informáticos"**, mismo que se desarrolla de la siguiente manera: al inicio podrá encontrarse el pertinente diseño de investigación, en donde afirmo las bases sobre las que fundamento mi trabajo de investigación. Así mismo se desarrollan siete capítulos que se desglosan de la siguiente forma: el Capítulo I se denomina "La Informática" en donde se encuentran generalidades acerca de la informática, su definición, clasificación y aspectos legislativos entorno a esta. El Capítulo II se denomina "El Delito", en el cual se establece su definición, elementos, objeto y su clasificación. El Capítulo III se denomina "Delitos informáticos", en donde se establecen aspectos relevantes en cuanto a antecedentes, definición, sujetos, los bienes jurídicos tutelados. El Capítulo IV se denomina "Delitos Informáticos en la Legislación Penal

Guatemalteca", en el cual se realiza un análisis en cuanto a los tipos penales en la legislación vigente, leyes guatemaltecas que regulan aspectos tecnológicos, convenios internacionales y las iniciativas a la fecha presentadas. El Capítulo V se denomina "El Proceso Legislativo en Guatemala", en el cual se desentraña la serie de pasos necesarios para la creación de una ley, así como una propuesta de tipos penales que debería contener la ley de delitos informáticos. El Capítulo VI se denomina "Beneficios Jurídicos y Sociales", en este se hace alusión a los diferentes beneficios que trae consigo la creación de la ley de delitos informáticos tanto a nivel jurídico como social. El Capítulo VII se denomina "Presentación de Análisis e Interpretación de Resultados de la Investigación de Campo", en este se efectúa la discusión de los resultados obtenidos con la investigación, así como la comprobación de la hipótesis. Para finalizar se presentan las conclusiones, recomendaciones y bibliografía.

Con el presente trabajo de investigación intento aproximarme al conocimiento de los beneficios de crear un marco jurídico eficaz en materia penal, con lo cual considero que puede ayudar y fortalecer futuras investigaciones respecto al objeto de estudio acá desarrollado, en aporte a la literatura jurídica y en cumplimiento de los fines constitucionales de la Universidad de San Carlos de Guatemala, me permito presentar la siguiente investigación.

DISEÑO DE INVESTIGACIÓN

OBJETO DE ESTUDIO:

Principales Beneficios Jurídicos y Sociales de la Creación de la Ley que Regule los Delitos Informáticos.

DEFINICIÓN DEL OBJETO DE ESTUDIO:

El presente estudio se pretende realizar con trabajo de campo utilizando como unidad de análisis el método de encuestas realizadas a Profesionales en Ingeniería en Sistemas, Informática y Ciencias de la Computación con preguntas prácticas y entrevistas realizadas a informantes claves, así también verificando la ausencia de un marco jurídico penal vigente que regule ilícitos penales en materia informática, con el fin de investigar y establecer a fondo los principales beneficios jurídicos y sociales de la creación de la Ley que regule los delitos informáticos. La muestra será tomada con personas que dentro del ámbito de las tecnologías de la informática, desarrollen actividades que puedan ser objeto de conductas ilícitas o que se vean afectadas por la falta de una regulación específica hacia las mismas. Se pondrán a prueba algunos factores tales como la necesidad de la protección de bienes jurídicos que anteriormente no eran objeto de ataques, seguridad en la información personal garantizando de esta manera el derecho a la privacidad, así como la protección de datos contenidos en los equipos tecnológicos, nuevos métodos de investigación, la prevención y sanción de delitos informáticos y la actualización del Sistema de Justicia ante conductas que actualmente no se establecen en materia penal.

DEFINICION DE LAS UNIDADES DE ANÁLISIS:

- UNIDADES DE ANÁLISIS INSTITUCIONALES:
  - Juzgado de Primera Instancia Penal, Narcoactividad y delitos contra el Ambiente.
  - Tribunal de Sentencia Penal, Narcoactividad y Delitos contra el Ambiente
  - Procuraduría de Derechos Humanos.
  - Ministerio Público.

- ∧ Instituto de la Defensa Pública Penal.
- ∧ Policía Nacional Civil.
- ∧ Colegio de Ingenieros de Guatemala, sede Quetzaltenango.
- ∧ Dirección de Atención y Asistencia al Consumidor.

- UNIDADES DE ANÁLISIS PERSONALES:

- ∧ Todas los Ingenieros en sistemas, informática y ciencias de la computación.
- ∧ Abogados Litigantes.
- ∧ Docentes Universitarios.

- UNIDADES DE ANÁLISIS DOCUMENTALES:

- ∧ Constitución Política de la República de Guatemala.
- ∧ Código Penal.
- ∧ Código Procesal Penal.
- ∧ Convenios Internacionales en el ámbito de delitos informáticos.
- ∧ Doctrina atinente con el objeto de estudio, contenida en libros, folletos, revistas, periódicos, enciclopedias e internet.

DELIMITACIÓN:

- DELIMITACIÓN TEÓRICA:

  La presente investigación será de carácter jurídico-social, porque abarcará el ámbito meramente legal y tendrá el uso de la sociología como parte del problema.

- DELIMITACIÓN ESPACIAL:

  Esta investigación se realizara en forma micro espacial delimitando la misma en el municipio de Quetzaltenango.

- DELIMITACIÓN TEMPORAL:
  Será de carácter sincrónico, es decir se analizará el fenómeno jurídico en la actualidad.

JUSTIFICACIÓN:

El artículo dos de la Constitución Política de la República de Guatemala consagra que es deber del Estado garantizarle a los habitantes de la República la vida, la libertad, la justicia, la seguridad, la paz y el desarrollo integral de la persona, siendo uno de los Derechos Humanos inherentes a la persona humana la seguridad jurídica a través de todos los medios y formas necesarias que el Estado debe implementar para el correcto cumplimiento de la norma constitucional.

Cada día más, la tecnología es parte de la vida cotidiana del guatemalteco, el ingreso a sitios electrónicos, páginas web, almacenamiento digital de información pública y privada, entre otros; por lo que el Estado como ente responsable de la seguridad jurídica debe de implementar los mecanismos electrónicos adecuados para brindar dicha seguridad informática y así mismo sancionar penalmente a quien en forma ilícita lesione los intereses, derechos y actos de quienes hacen uso de los sitios electrónicos aludidos.

Existe ahora la necesidad de conocer más sobre las distintas modalidades transgresiones informáticas, que se dan día a día, no solo en las redes sociales sino también dentro del ciberespacio de nuestro país y la manera de cómo contrarrestarlos bajo el ámbito jurídico y de investigación digital.

En la actualidad el Estado de Guatemala ha incumplido con la norma constitucional y en cierta forma con los convenios y tratados ratificados por nuestro país, por la falta de cumplimento exacto a lo preceptuado, ya que la problemática actual subyace que en Guatemala no existe un cuerpo normativo especifico que regule los tipos penales o transgresiones informáticas que se adapte a nuestra realidad nacional y al avance tecnológico actual, si bien es cierto el Código Penal Guatemalteco decreto diecisiete guion setenta y tres regula dentro de su parte especial, en el titulo sexto, específicamente en el capítulo séptimo los delitos informáticos, asignándole tan solo

ocho tipos penales, mismos que fueron creados desde el año mil novecientos noventa y seis, pero que a la fecha ya no responden a la realidad nacional, ni al contexto y avance tecnológico, siendo un problema social que cada vez va en aumento y que necesita de su estudio e investigación para proponer una solución,

En virtud de las reflexiones expuestas, el módulo elaborado se justifica por la necesidad de desarrollar dicha investigación, que contribuya a determinar desde un punto de vista jurídico y social los Principales Beneficios de la creación de la Ley que regule los Delitos informáticos en Guatemala.

Esperando que con la elaboración de la presente investigación contribuya en parte a la solución de la problemática planteada en dicha investigación, y que al mismo tiempo, pueda servir de fuente de consulta a estudiantes, profesionales y para todas aquellas personas que de una u otra forma, se interesen por profundizar y contribuir con la seguridad informática y la lucha contra las trasgresiones informáticas.

MARCO TEÓRICO:

El marco teórico de la presente investigación, estará integrado por el conjunto de conceptos, definiciones, principios y categorías apropiadas al tema, utilizándose para el efecto los siguientes aspectos:

La parte teórica de la presente investigación nos lleva a conocer algunos conceptos básicos que deben ser tomados en cuenta por el lector para su mejor interpretación tal es el caso de nuestro tema Principales Beneficios Jurídicos y Sociales de la creación de la Ley que regule los Delitos Informáticos, analizaremos como génesis de nuestro marco teórico la Ley, en este sentido el autor Manuel Osorio, en el Diccionario de Ciencias Jurídicas Políticas y Sociales hace la siguiente definición "**Ley**: Toda norma jurídica reguladora de los actos y de las relaciones humanas, aplicable en determinado tiempo y lugar. Dentro de esa idea, seria ley todo precepto dictado por autoridad competente, mandando o prohibiendo una cosa en consonancia con la justicia y para el bien de los gobernados. Así, entraría dentro del concepto no solo la ley en sentido restringido o propio, como norma jurídica elaborada por los órganos estatales con

potestad legislativa, sino también los reglamentos, ordenanzas, órdenes, decretos, etc."[1]

En el mismo orden de ideas es importante establecer quienes tienen iniciativa de ley, como lo preceptúa la Constitución Política de la República de Guatemala, la cual determina: "Para la formación de las leyes tienen iniciativa los diputados al Congreso, el Organismo Ejecutivo, la Corte Suprema de Justicia, la Universidad de San Carlos de Guatemala y el Tribunal Supremo Electoral."[2] En el entendido que cualquiera de los sujetos antes mencionados tiene la facultad para promover una iniciativa de ley que regule los delitos informáticos, tomando en consideración el objeto de esta investigación, pero debe tenerse en cuenta que para la creación y existencia de una ley se debe seguir un **Proceso Legislativo**, el cual se encuentra determinado en la Ley Orgánica del Organismo Legislativo, y se desarrolla conforme a lo siguientes pasos: 1. Toda iniciativa de ley deberá presentarse redactada en forma de decreto, debe ser presentada por escrito en hojas numeradas, rubricadas y en digital. 2. Conoce del proyecto la comisión correspondiente, la cual podrá proponer enmiendas parcial o totalmente y le concederá audiencia al proponente del mismo para discutir dichas enmiendas. 3. Finalizado el trámite ante la comisión el proyecto se entregará a la Dirección Legislativa para su registro y difusión. 4. El proyecto de ley se pondrá a discusión junto con el dictamen emitido por la comisión correspondiente, el debate se efectuara en tres sesiones, discutiendo artículo por artículo. 5. Suficientemente discutido el proyecto se someterá a votación sobre el mismo y si es aprobado se leerá en la misma sesión. 5. Agotada la lectura se someterá a votación la redacción final del proyecto de ley, si la misma es favorable queda aprobado el texto, entregándose una copia a los diputados, el proyecto posteriormente será enviado al Organismo Ejecutivo para su Sanción, Publicación y por último la entrada en vigencia.[3]

Para tener claro nuestro objeto de estudio no podemos pasar por alto y dejar de definir lo que es el Delito, sus elementos y clasificación, pues al comprender dichas

[1] Ossorio Manuel, Diccionario de Ciencias Jurídicas Políticas y Sociales, 1era. Edición Electrónica Realizada por Dastacan, S.A., Guatemala 1999 Pag.547.
[2] Artículo 174 Constitución Política de la República de Guatemala, Asamblea Nacional Constituyente, 1986.
[3] Artículos 109 al 133 Ley Orgánica del Organismo Legislativo. Decreto 63-94.

definiciones las mismas nos podrán proporcionar de manera más general, una mejor comprensión de la investigación. A continuación se presentan algunas definiciones: el autor Eugenio Cuello Calón hace la siguiente definición: **Delito**: "Es la acción humana, antijurídica, típica, culpable, sancionada por la ley".[4] En cuanto a los **Elementos del Delito** se establece la siguiente clasificación: **Elementos Positivos**: 1.Acción: comportamiento derivado de la voluntad del hombre. 2. Tipicidad: Es la especial característica de hallarse el hecho descrito en la ley como delito. 3. Antijuricidad: Es la relación de contradicción con el orden jurídico. 4. La culpabilidad: Juicio de reproche a quien ha optado por comportarse antijurídicamente.[5] **Elementos Negativos**: 1. Ausencia de Acción: cuando el sujeto activo efectúa un movimiento corporal en forma involuntaria, produce un hecho delictivo, dicho movimiento aparece como una condición causal, pero no como la causa jurídicamente eficaz. 2. Atipicidad: Significa que en el ordenamiento jurídico-penal no existe la descripción típica de una conducta determinada. 3. Causas de justificación: razones que en determinadas circunstancias, llevan a valorar en forma positiva la lesión de un bien. 4. Causas de inculpabilidad: Falta de reprobabilidad ante el derecho penal, por falta de voluntad o el conocimiento del hecho.[6]

Dentro del estudio del delito Eduardo López Betancourt, citado por el autor Fredy Escobar Cárdenas, establece la siguiente **Clasificación de los Delitos**: 1. En función de su gravedad. 2. Según la conducta del agente 3. Por el Resultado 4. Por el daño que causan. 5. Por su duración. 6. Por su elemento interno o culpabilidad [7]

Establecida la definición de delito, en forma más específica en cuanto al objeto de la investigación, es importante determinar aspectos relevantes en cuanto a los Delitos informáticos, que son en esencia las figuras ilícitas que debe regular una ley específica y cuya creación y como consecuencia sus beneficios jurídicos y sociales son los elementos centrales de la presente investigación.

---

[4] Cuello Calón, Eugenio. Derecho Penal, Parte General, Volumen I. Editorial Bosch, España 1975. Pág. 296.
[5] De León Velasco, Héctor Aníbal, y varios autores, coordinados por Diéz Ripollés, José Luis y Giménez Sallinas i Colomer, Esther. Manual de Derecho Penal Guatemalteco, Parte General, Impresos Industriales S.A. Guatemala, 2001Págs. 143 a 146.
[6] Escobar Cárdenas, Fredy Enrique. Compilaciones de Derecho Penal, Parte General, Novena Edición, Guatemala 2018 Págs. 175, 234,282.
[7] Escobar Cárdenas, Fredy Enrique Ibid.,Págs. 291,292

En ese sentido Hans Aarón Noriega Salazar define el "**Delito Informático** como toda aquella acción típica y antijurídica, que se sirve o utiliza de una computadora para su realización, o bien va dirigida a obtener el acceso no autorizado a registros o programas de un sistema informático, o a producir un resultado de daño en ésta o de los sistemas que la misma hace operar"[8].

Como se puede analizar, el ámbito de actuación en este tipo de conductas implica el ataque o intencionalidad de daño a el sistema operativo de una computadora, la intromisión o acceso a bases de datos o archivos que la misma contenga, o bien la utilización de este aparato tecnológico como medio o instrumento para la realización de delitos.

Dentro de los delitos informáticos se debe tener en consideración la protección a los bienes jurídicos, lo que da como resultado la penalización de las conductas contrarias a las normas jurídicas, en general el bien jurídico protegido es la información, la cual se debe considerar por medio de sus diversas manifestaciones, por ejemplo a través de un valor económico o un valor intrínseco de la persona y los sistemas encargados de procesarla. De esta manera Santiago Acurio Del Pino establece una clasificación de los "**Bienes Jurídicos Protegidos**: 1. El Patrimonio: en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar. 2. La Reserva, La Intimidad y Confidencialidad de los Datos: en el caso de las agresiones informáticas a la esfera de la intimidad en forma general. 3. La Seguridad o Fiabilidad del Tráfico Jurídico y Probatorio: en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos. 4. El Derecho de Propiedad: en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los daños y el llamado terrorismo informático." [9]

Esta clase de delitos no afectan a un solo bien jurídico determinado si no que la multiplicidad de conductas que los componen afectan a una diversidad de bienes que ponen en relieve intereses colectivos, de allí la imperiosa necesidad de crear un cuerpo

[8] Noriega Salazar, Hans Aarón. Instituto de la Defensa Pública Penal, Delitos Informáticos. 1ª Edición 2011 Guatemala

[9] Acurio Del Pino, Santiago. Delitos Informáticos Generalidades, Pontificia Universidad Católica del Ecuador, Quito, Ecuador 2008 Pág.21.

normativo capaz de regular estas conductas ilícitas y como consecuencia los beneficios jurídicos y sociales que se deriven de la misma.

Del nacimiento de la diversidad de conductas constitutivas de esta clase de delitos informáticos se puede establecer una clasificación, tomando en consideración que en el Código Penal guatemalteco Decreto 17-73 se establecen muy precariamente algunos tipos penales siendo estos: Violación a derechos de autor y derechos conexos, Destrucción de registros informáticos, alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos, manipulación de información, uso de información, programas destructivos, alteración de número de origen.

Santiago Acurio brinda una clasificación de "Delitos Informáticos que desde el punto de vista objetivo que sea lo más didáctica posible al momento de tratar esta clase de conductas delictivas, estableciendo: 1. Los Fraudes. 2. El Sabotaje Informático. 3. El espionaje informático y el robo o hurto de software. 4. El Robo de Servicios. 5. El Acceso no autorizado a Servicios Informáticos."[10]

Hechas las definiciones anteriores, conceptos, clasificaciones y comentarios debemos analizar el punto central de nuestra investigación, como lo son los principales beneficios jurídicos y sociales que se derivan de la creación de un marco jurídico tendiente a regular las conductas ilícitas en las tecnologías informáticas, tomando en consideración que la informática está presente en la gran mayoría de ámbitos de la vida moderna.

La relación que se establece entre la informática y el fenómeno delictivo resulta una cuestión de impacto de las nuevas tecnologías en el ámbito social. Por lo que la implementación y avances tecnológicos han dado lugar al análisis si es suficiente o eficaz el sistema jurídico actual para regular nuevas conductas o escenarios, en los cuales se manifiestan conflictos en cuanto al uso y abuso de la actividad informática y la repercusión en la situación actual de la sociedad.

En cuanto a los beneficios jurídicos nos encaminamos al campo de seguridad normativa, la cual deriva de los principios de legalidad y seguridad jurídica, que en su

[10] Acurio del Pino, Santiago. Ibid., Págs.23-29

conjunto se manifiesta en las diversas normas jurídicas necesarias para lograr una eficaz prevención y sanción de las conductas contrarias a la seguridad e integridad de los sistemas informáticos, por lo que al crearse una ley que regule específicamente los delitos informáticos, su principal efecto benéfico es la protección de los derechos de las personas en cuanto a integridad, confidencialidad, incluso patrimonial ante la nueva generación de delincuentes cibernéticos. Como resultante de la creación y aplicación de una normativa eficaz encontramos los beneficios sociales que le son otorgados a la colectividad, es decir, usuarios, todas aquellas personas que hacen uso de los avances tecnológicos en la vida moderna cotidianamente y que pueden resultar afectados al cometerse un ilícito en esta materia en su contra, de allí devine la importancia de la creación de la normativa, puesto que al no existir una norma vigente no es capaz el sistema de justicia de juzgar las infracciones cometidas en contra de los ciudadanos, impedir violaciones y restituirles sus derechos.

En efecto por medio de los análisis realizados le damos una panorámica a la presente investigación de cómo se ha de desarrollar; tomando en consideración su forma de recopilación de información, sus diferentes ámbitos de estudio, hacia quien va dirigida la investigación, el diseño utilizado, entre otros aspectos que permitan establecer el rumbo de la investigación.

PLANTEAMIENTO DEL PROBLEMA:

Nuestra sociedad se encuentra en constante evolución y la tecnología informática que nos rodea no es la excepción, ya que ésta ejerce una influencia en gran parte de las áreas de la vida social, podemos observan que con el paso del tiempo han surgido nuevos comportamientos prohibidos que antes eran impensables y como consecuencia quedaron fuera de la tipificación de las normas penales tradicionales, estos comportamientos son denominados delitos informáticos, delincuencia informática o criminalidad informática y por lo tanto a quienes adecuan su conducta a los mismos se les denomina cibercriminales.

Se debe tener presente que en nuestro país nos encontramos con un gran obstáculo, que en cuanto al ordenamiento jurídico en materia penal no se cuenta con una ley

específica capaz de regular los delitos informáticos. Si bien es cierto los organismos encargados de crear las leyes y hacer cumplirlas suelen adaptarse con lentitud a las nuevas tendencias, mientras que los grupos delictivos se adaptan con mayor rapidez y aprovechan los avances tecnológicos para desarrollar sus actividades ilícitas, allí nace la imperiosa necesidad de regular tales actividades a través de un marco jurídico penal vigente que contemple nuevos tipos penales, en virtud del principio de legalidad.

A través de estas acciones se logra la protección de los sujetos afectados con tales conductas prohibidas, como lo son los usuarios de ordenadores que inician almacenando información en archivos computarizados, crean programas y bases de datos, los comparten y la resultante es la posible afectación que puedan sufrir en su patrimonio, derechos e intimidad; el fin primordial es el alcance del respeto y la tutela efectiva a través del ordenamiento jurídico que logra el bienestar de la población.

Entonces, ante tal problemática, surge la interrogante ¿Cuáles son los Principales Beneficios Jurídicos y Sociales de la creación de la ley que regule los Delitos Informáticos?

OBJETIVO GENERAL:

Determinar los principales beneficios jurídicos y sociales al crear la ley que regule los delitos informáticos.

OBJETIVOS ESPECÍFICOS:

1. Identificar que conductas desarrolladas a través de los sistemas informáticos son constitutivas de delitos informáticos.
2. Demostrar la necesidad de fortalecer las normas jurídico penales existentes actualmente en materia de delitos informáticos.
3. Analizar las iniciativas de ley existente en materia de delitos informáticos.
4. Indicar los beneficios jurídicos y sociales.
5. Precisar el efecto de los beneficios de la creación de la ley que regule los delitos informáticos.

METODOLOGÍA:

Para el desarrollo del presente trabajo de tesis se aplicarán los métodos inductivo y deductivo. La metodología que se utiliza en el presente estudio se rige por las técnicas de investigación tomando como base la unidad de análisis como lo es la encuesta, teniendo en consideración que para esta técnica se empleará el método deductivo, el cual permitirá partir de un principio general hasta descender a premisas particulares y la entrevista a informantes claves, cuya finalidad es la obtención de información, empleando para la misma el método inductivo con el cual se obtendrán conclusiones generales a partir de premisas particulares; las preguntas que están en la boleta provienen de la operacionalización de la hipótesis, se pretende encuestar a cincuenta profesionales especializados en las ciencias de la informática del municipio de Quetzaltenango, quienes conforma una muestra representativa del 16% del universo de los profesionales que se encuentran en Quetzaltenango, siendo estos un total de 300; dicha información será recopilada y tabulada para determinar el análisis, consecuentemente se conocerá el resultado de la investigación. Las encuestas y entrevistas como instrumentos nos servirán para recolectar información de la realidad como parte del diagnóstico. En este caso la encuesta de percepción, es el método probado y más efectivo que consiste en llevar a cabo encuestas directas a ingenieros en sistemas para que respondan sobre los efectos de la ausencia de un marco jurídico penal vigente que regule ilícitos penales en materia informática, con el fin de establecer a fondo los principales beneficios jurídicos y sociales que se deriven de la creación de la misma. Así mismo las entrevistas realizadas a informantes claves nos indicaran los efectos de la ausencia de un marco jurídico penal vigente que regule los delitos informáticos y los beneficios resultantes de la implementación de dicha normativa que se manifiestan al brindar una protección eficaz de bienes jurídicos específicos, seguridad de la información personal, protección de datos informáticos contenidos en sistemas tecnológicos, la represión de las conductas delictivas a través de una sanción eficaz y la actualización del sistema de justicia.

El ciclo de ejecución de la encuesta y la entrevista se llevara a cabo de la siguiente manera:

1. Definición del objeto, este nos guía que queremos saber y para qué.

2. Diseño maestral

3. Diseño del instrumento. También se le conoce como cuestionario.

4. Ejecución de la encuesta y la entrevista.

5 Procesamiento de la recolección de datos

6. Análisis de los resultados de la encuesta y la entrevista.

7. Difusión del resultado.

TÉCNICAS DE INVESTIGACIÓN A UTILIZAR:

a) Investigación Bibliográfica
b) Investigación de Campo
    - Encuesta
    - Entrevista

HIPÓTESIS:

Los principales beneficios jurídicos y sociales al crear la ley que regule los delitos informáticos son: la protección de bienes jurídicos específicos, la seguridad de la información personal e institucional, la prevención y sanción de los delitos informáticos y la actualización del Sistema de Justicia de Guatemala.

OPERACIONALIZACIÓN DE LA HIPÓTESIS

- VARIABLE DEPENDIENTE: Esta variable se basa en: “la creación de la ley que regule los delitos informáticos.”

INDICADORES VARIABLE DEPENDIENTE:

a) Es de conocimiento común que no existe una ley que regule los delitos informáticos

b) Los delitos informáticos son cada vez más recurrentes

c) La globalización y avance tecnológico requiere una protección jurídica especializada

d) Los tipos penales se deben de adecuar a la realidad nacional e internacional

- VARIABLES INDEPENDIENTES

a) **La protección de bienes jurídicos específicos**

b) **La seguridad de la información personal e institucional**

c) **La prevención y sanción de los delitos informáticos**

d) **La actualización del Sistema de Justicia de Guatemala**

INDICADORES DE LA PRIMERA VARIABLE INDEPENDIENTE**:**

a) La protección de bienes jurídicos específicos

- ✓ La falta de regulación específica de delitos informáticos
- ✓ Tutela de bienes jurídicos lesionados con el cibercrimen
- ✓ La necesidad de una protección jurídica especializada de la información y el patrimonio
- ✓ El avance tecnológico ha creado nuevas formas de delinquir

INDICADORES DE LA SEGUNDA VARIABLE INDEPENDIENTE:

b) La seguridad de la información personal e institucional

- ✓ La necesidad de garantizar la inviolabilidad de la información pública y privada
- ✓ La Manipulación indebida de la información personal e institucional
- ✓ La Confidencialidad en el almacenamiento de datos, programas y correos

INDICADORES DE LA TERCERA VARIABLE INDEPENDIENTE:

c) La prevención y sanción de los delitos informáticos

- ✓ Cada día son más las amenazas y ataques a los medios informáticos

- ✓ El cibercrimen es una forma de delinquir que se intensifica en el país
- ✓ La falta de regulación de conductas que atentan a los medios informáticos
- ✓ El desconocimiento de la población de los delitos informáticos

INDICADORES DE LA CUARTA VARIABLE INDEPENDIENTE:

d) La actualización del Sistema de Justicia de Guatemala

- ✓ La lucha contra el cibercrimen debe de adecuarse a los avances tecnológicos de investigación criminal
- ✓ Falta de personal especializado en delitos informáticos
- ✓ La falta de Fiscalías y Juzgados especializados en la materia
- ✓ La formación de equipos multidisciplinarios de lucha contra el cibercrimen

CAPITULO I

LA INFORMÁTICA

1.1 DEFINICIÓN

La informática en la actualidad tiene una marcada injerencia en la mayoría de campos de la vida moderna, como manifestación de los avances tecnológicos y resulta necesario tomar en consideración que nuestro tema principal es determinar los "Principales Beneficios Jurídicos y Sociales de la creación de la Ley que Regule los Delitos Informáticos", se inicia definiendo la Informática como "un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información con miras a una adecuada toma de decisiones".[11]

Según el diccionario de la Real Academia de la Lengua Española, es el "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamientoauto mático de la información por medio de computadoras". [12]

Partiendo de estas definiciones se determina el objetivo principal de la Informática, el cual es el establecimiento de procedimientos o técnicas encaminadas a la recopilación, procesamiento y utilización de datos, administrándolos de tal manera que permitan la toma de decisiones, es decir el procesamiento de la información a través de la administración de datos.

En esta perspectiva, es importante destacar que tanto la información como los datos son conceptos que van de la mano, ya que para que exista información es necesario proveerla de datos y una vez procesados esos datos se almacena en archivos informáticos que son espacios de memoria permanente de un dispositivo que almacena información digital.

Anteriormente se contaba con la certeza que la información personal era inaccesible, concebida como solo una forma de llevar los registros, sin embargo con el gran avance

[11] Tellez Váldez, Julio. Derecho Informático, Cuarta Edición, McGRAW-HILL/INTERAMERICANA, EDITORES, S.A. de C.V. 2008 Pag. 6
[12] Http:www.rae.es

de las industrias de la computación, nacen sistemas que se especializan en el almacenamiento de la información personal, institucional o de cualquier tipo, allí es donde la Informática se ha convertido en un integrante activo de la sociedad, existiendo una gran diversidad de campos que la utilizan y la aplican, ya que el hombre actual vive y se desarrolla en un medio donde los datos y la información son parte importante de la vida daría, de esta manera nos encontramos en la era de la informática.

1.2 DERECHO INFOMÁTICO

Se concibe como una nueva rama del conocimiento jurídico en la cual se manifiesta la interrelación entre la Informática y el Derecho, la que antes era impensable amalgamar. Las primeras manifestaciones de esta fusión se conciben a partir del año de 1949.

"De acuerdo con esa tónica, cabe enunciar el siguiente concepto de derecho informático: es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática"[13]

"Es el conjunto de doctrinas, principios y normas, que regulan los bienes jurídicos que la Informática crea, las acciones y las responsabilidades de las personas derivadas del uso de la tecnología"[14]

Al hablar del Derecho Informático como un conjunto de leyes, se hace referencia a los ordenamientos jurídicos nacionales e internacionales, que si bien son escasos, hacen alusión a lo que es el fenómeno informático. En cuanto a los principios se refiere a los postulados que expresan jueces, magistrados, tratadistas y doctos en la materia. De acuerdo con los actos, estos son resultante de un fenómeno relacionado con la informática y provocado por el hombre.

Por el nivel de evolución que ha tenido la tecnología y su impacto en todas las actividades humanas, nace el Derecho Informático, que si bien, no cuenta con una histórica trayectoria en la legislación nacional, pero la exigencia de implementar un control y aplicación lícita de los instrumentos informáticos, determina su importancia,

[13] Tellez Valdez, Julio Ibid., Pág. 13
[14] Barrios Osorio, Omar Ricardo. Introducción de las Nuevas Tecnologías en el Derecho. Instituto de la Defensa Pública Penal 2da Edición Guatemala 2010.

con el objetivo fundamental de regular todas aquellas controversias jurídicas que no son susceptibles de ser resueltas con una respuesta clásica, puesto que surge la necesidad de implementar nuevas normas jurídicas específicas y la reinterpretación de las ya constituidas que tiendan a regular nuevas situaciones jurídico-informáticas.

Desde la aparición de la informática como la ciencia de la computación y su aplicación a diversos ámbitos de la vida, se han logrado grandes avances y beneficios para el hombre, pero debe tenerse presente que ante los cambios, nos enfrentamos al surgimiento de nuevas conductas o comportamientos, allí es donde se originan los actos delictivos cometidos a través de la Informática, lo que ha devenido en la génesis de esta rama del derecho.

Una de las principales dificultades que enfrenta el derecho informático estriba en que el sistema jurídico no logra asimilar la realidad tecnológica que estamos enfrentando, y este inconveniente se manifiesta en la incapacidad de adecuar la realidad social a los cambios introducidos por las nuevas tecnologías informáticas.

1.2.1 Contenido del derecho informático

No existe una fórmula específica para describir el contenido del Derecho Informático, ya que este es amplio y se encuentra en un constante desarrollo. Sin embargo entre los principales se encuentran los siguientes:

1. “El valor probatorio de los soportes modernos de información, provocado por la dificultad en la aceptación y apreciación de elementos de prueba derivados de estos soportes entre los órganos jurisdicciones.
2. La protección de datos personales, ante el manejo inapropiado de informaciones nominativas que atenta contra derechos fundamentales de las personas.
3. Los delitos informáticos, es decir, la comisión de verdaderos actos ilícitos en los que se tenga a los computadores como instrumentos o fines.
4. El flujo de datos transfronterizos, con el favorecimiento o restricción en la circulación de datos a través de las fronteras nacionales.

5. La protección de los programas computacionales como respuesta a los problemas provocados por la piratería de software que atenta contra la propiedad intelectual.
6. Los contratos informáticos, en función de esta categoría contractual sui generis con evidentes repercusiones fundamentalmente económicas.
7. La regulación de los bienes informacionales, en función del innegable carácter económico de la información como producto informático.
8. La ergonomía informática, como aquellos problemas laborales suscitados por la informatización de actividades."[15]

En cuanto a los aspectos anteriormente mencionados, se debe tener presente que la regulación jurídica de la informática materializada en el Derecho Informático, debe ser capaz de lograr una perfecta gobernanza de las tecnologías, enfocada en regular aspectos relacionados al internet, redes sociales, protección de datos personales, delitos informáticos; todo encaminado a lograr el buen uso de las tecnologías y de esta manera evitar que se engendren menoscabos a los derechos de las personas, transgresiones patrimoniales, violaciones a la intimidad o confidencialidad de los datos, robo de información, acceso ilícito a sistemas informáticos, incluso aquellas relativas al honor.

Otro aspecto importante en cuanto al contenido del Derecho Informático y que vale la pena enfatizar de manera especial, es en cuanto a los documentos electrónicos presentados como elementos probatorios, ya que en el sector justicia se presentan de manera errónea, por ejemplo un perfil de red social impreso, es totalmente contradictorio a lo que es la esencia de la tecnología, pero este conflicto es consecuencia de una carencia a la que se enfrentan jueces y magistrados ante poca modernización del sistema de justicia, en este sentido no cuentan con los medios idóneos para llevar a cabo una eficaz valoración de este tipo de elementos probatorios.

Por último, el Derecho ante la posibilidad de ser dinámico, cambiante y jamás permanecer estático, debe ofrecer soluciones justas a los problemas de la realidad

[15] Barrios Osorio, Omar Ricardo, Ibid., Págs. 51 y 52.

social que se enfrenta actualmente, por lo que debe regular de manera eficaz las temáticas derivadas de la tecnología.

2.3 INFORMATICA JURÍDICA

La informática como ciencia ha logrado incorporarse en el Derecho dando lugar a uno de sus instrumentos más significativos, como lo es la Informática Jurídica, concebida como la disciplina que busca el tratamiento lógico y automático de la información legal.

Surge por primera vez en Estados Unidos, en la época de 1959, al desarrollarse las primeras investigaciones destinadas a la recuperación de documentos jurídicos en forma automatizada. Iniciando el uso de las computadoras u ordenadores no solo como instrumentos destinados a trabajos matemáticos, sino también para los lingüísticos. De esta manera John Horty concibe la idea de crear un mecanismo por medio del cual se pudiera tener acceso a la información legal automatizada, colocando los ordenamientos jurídicos de Pennsylvania en cintas magnéticas, y es en este lugar donde nace la recopilación legal informática.

Ha sufrido variaciones a lo largo de su evolución, hasta ser considerada un instrumento indispensable para la expansión del Derecho, descubriendo técnicas o conocimientos enfocados a la recuperación y tratamiento de la información jurídica.

Es considerada “la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como a la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación”.[16]

Su objetivo primordial se concentra en el estudio del tratamiento automatizado de las fuentes del conocimiento jurídico, dichos conocimientos se pueden obtener de sistemas de documentación legislativa, mecanismos informáticos que coadyuven en el proceso legislativo y la decisión judicial, así también en cuanto a la organización de los instrumentos con los que se gestiona el Derecho.

[16] Tellez Valdez, Julio Ibid., Pág. 10

La relación existente entre la informática y el Derecho a través de esta disciplina ha dado lugar a que sea denominada de diversas maneras, entre las que destacan:

- Jurimetrics (jurimetría)
- Giuscibernética (juscibernética)
- Computers and Law (en los países anglosajones)
- Rechtsinformatique (en Alemania)
- Jurismática (en México)

2.3.1 Clasificación de la informática jurídica

Es conveniente clasificar esta disciplina de la siguiente manera:

Informática Jurídica Documentaria: Es una de las primeras manifestaciones de la Informática Jurídica, se basa en el análisis de la información contenida en documentos jurídicos con el objetivo de formar bancos de datos documentales. Todo esto a través de la aplicación de técnicas informáticas de análisis, archivo y recuperación de la información contenida en la legislación, jurisprudencia, doctrina o cualquier otro documento de tipo jurídico.

El efecto es un análisis documental, destinado a la representación del contenido, con el fin de facilitar la consulta o la búsqueda posterior de la información almacenada, de modo que permita una recuperación y localización de la información de relevancia jurídica.

En los últimos años el volumen de documentos jurídicos, inclusive al hablar de los ordenamientos jurídicos que han crecido al generarse nuevos hechos sociales, por lo que contar con un acceso constante a esa información no puede quedar limitada, en nuestro medio hablamos del Diario Oficial en formato papel, es allí donde la Informática Jurídica Documentaria encuentra su razón de ser, al establecerse mecanismo que permitan una consulta rápida, como la que se puede obtener por medio del sitio de internet del Congreso de la República, que ha logrado un desarrollo al incorporar digitalmente las publicaciones del Diario Oficial en formato PDF.

Así también otros órganos que colocan su normativa en línea, como la Superintendencia de Administración Tributaria, el Banco de Guatemala, incluso entidades de carácter privado que manejan información pública, empresas que cuentan con bases de datos relevantes para juristas e investigadores.

Informática Jurídica de Gestión: Se concentra en la automatización de las actividades y gestiones de carácter jurídico que se desarrollan en la oficina jurídica, tribunales de justicia y administración pública.

La Informática Jurídica de Gestión a su vez se subclasifica en dos formas:

- **Registral:** Encargada de la información contenida en los registros, para facilitar a los usuarios el acceso a los datos contenidos en los mismos, de manera eficiente y rápida, en Guatemala se encuentra un claro ejemplo en el Registro General de la Propiedad y el Registro Mercantil.
- **Operacional:** Se ocupa de la facilitación de las actuaciones y funcionamiento del campo jurídico procesal, tanto en la vía administrativa como la judicial. En Guatemala se manifiesta a través del Centro Administrativo de Gestión Penal y en el Centro de Servicios Auxiliares de la Administración de Justicia, al monitorearse el control electrónico del trámite de los procesos y consulta de expedientes.

Informática Jurídica Decisional: Es también denominada Metadocumental, se caracteriza por la utilización de ordenadores, los cuales ayudan a la toma de decisiones de carácter jurídico; va más allá de la simple recuperación de información, con el objetivo de resolver problemas jurídicos. No pretende que el ordenador resuelva la decisión que le corresponde al juzgador.

2.4 LEGISLACIÓN INFORMÁTICA

Hoy en día, se desarrollan infinidad de ordenamientos jurídicos que se encargan de regular diferentes actos o hechos y la informática no es la excepción, con la aparición de nuevas tecnologías, también hay nuevas conductas que se aprovechan de esos avances de modernización. Por medio de la informática se pueden realizar actos que

perjudiquen a terceros o que por la naturaleza de los mismos deben ser regulados a través de una normativa específica.

En función de lo anterior, la legislación informática se define como la colección de reglas jurídicas que con un carácter preventivo y correctivo, pretenden regular el uso inadecuado de la informática, es decir el empleo incorrecto de la información personal o bien institucional que se encuentre en internet, dispositivos electrónicos y cualquier otro medio digital por el cual se pueda cometer un delito.

La reglamentación debe abarcar puntos específicos tendientes a cuestionarse si las normas existentes son suficientes para ser aplicadas a los problemas que surjan. O bien si es necesaria la creación de un nuevo cuerpo de normas jurídicas que den lugar a una ley de carácter específico, diferentes a las ya existentes. Y una vez creadas estas normas pretender la evolución de la jurisprudencia en relación a la dimensión de casos que se presenten ante los órganos jurisdiccionales correspondientes, los cuales deben tener como finalidad pautas resolutorias o conciliatorias.

La legislación informática comprende aspectos como la regulación de la información, protección de datos personales, regulación jurídica de internet, propiedad intelectual y delitos informáticos. Si bien es cierto, existen normas nacionales que tienden a regula ciertos aspectos informáticos, pero la carencia de una norma específica, refleja las deficiencias a las que se enfrenta el sistema de justicia al momento de pretender proteger la utilización abusiva de la información.

Los marcos legales y las regulaciones de carácter internacional que se relacionan con las tecnologías de la información, tratan de adecuarse a los grandes cambios a la velocidad que estos surgen, allí surge la relevancia de marco regulatorio eficaz.

CAPITULO II

EL DELITO

2.1 DEFINICIÓN

Tratar de definir el delito es una tarea complicada, en virtud de que existen diversidad de opiniones al respecto y corrientes que le brindas características propias, además la legislación guatemalteca no contempla una definición expresa de lo que este significa, por lo que al momento de establecer una definición acertada se deben tomar en cuenta los elementos puestos de manifiesto en la teoría jurídica de la siguiente manera: Es una acción típica, antijurídica, culpable señalada en la legislación, merecedora de una sanción.

El delito ha estado sujeto a una diversidad de variaciones consecuencia de la evolución de la sociedad, de esta manera formándose un criterio que establece un castigo al delito cometido el cual se relaciona directamente con el daño ocasionado.

A lo largo de la historia ha recibido varias denominaciones entre las cuales se encuentran: Noxa o Noxia que significa daño; Flagitum, Scelus, Facinus Fraus, Crimen para identificar a delitos de gravedad y Delictum para señalar una infracción leve.

2.2 ELEMENTOS DEL DELITO

En base a la teoría del delito, al momento de establecer los elementos, estos se dividen en 2 principales grupos:

Elementos positivos:

- Acción
- Tipicidad
- Antijuricidad
- Culpabilidad

Elementos Negativos:

- Ausencia de Acción

- Atipicidad
- Causas de Justificación
- Causas de inculpabilidad

Acción:

"Se llama acción a todo comportamiento dependiente de la voluntad humana. Solo el acto voluntario puede ser penalmente relevante. La voluntad implica siempre una finalidad".[17]

Es por lo anterior, que se considera un comportamiento dependiente de la voluntad humana implica una finalidad, es decir el ejercicio de una voluntad final. Y esta dirección final establece dos fases:

a) **Fase Interna**: que es el querer o desear, tiene lugar en el pensamiento del autor, es decir en la cual se planifica la realización del fin.

b) **Fase externa**: es la materialización de lo planeado, es decir la realización en el mundo exterior, poner en marcha lo planeado.

La acción abarca tanto comportamientos activos como omisivos, de esto deviene las formas de operar de la acción o conducta delictiva, que origina la clasificación de los delitos atendiendo a las formas de acción entre los cuales se establecen:

a) Delitos de acción o comisión: consiste en hacer algo que infringe una ley prohibitiva.

b) Delitos de pura omisión: consiste en no hacer algo, infringiendo la ley preceptiva, que ordena hacer algo.

c) Delitos de comisión por Omisión: la conducta humana infringe la ley prohibitiva, mediante la infracción de una ley preceptiva.

d) Delitos de pura actividad: son aquellos que no requieren de un cambio efectivo al mundo exterior, es suficiente la simple conducta humana.

[17] Muñoz Conde, Francisco y García Arian, Mercedes. Manual de Derecho Penal Parte General. 2ª edición. Tirant to Blanch, editora. Valencia España 1998. Página 228

Tipicidad:

"Es la característica o cualidad que tiene una conducta (acción u omisión) de encuadrar, subsumir o adecuarse a un tipo penal"[18].

La tipicidad abarca dos conceptos específicos en primer lugar Tipificar: que es la encuadrabilidad de la conducta humana en el tipo penal, dicha acción es realizada por el fiscal, defensa, policía o el mismo estudiante de abogacía. En segundo lugar la Tipificación es la encuadrabilidad de la conducta en un tipo penal, sin embargo la diferencia sustancial con la anterior es que esta acción la realiza únicamente el juez.

Antijuricidad:

Es también denominada antijuridicidad, es toda conducta o acción contraría a lo que establece el Derecho o el orden jurídico.

Culpabilidad:

Es el elemento por medio del cual se establece el juicio de reproche a quien ha cometido un hecho delictivo, es decir comportarse en contra de lo que establece el ordenamiento jurídico. El fundamento del reproche se basa en la facultad que tiene el sujeto de decidir el abstenerse de realizar un comportamiento delictivo.

Para que la culpabilidad sea considerada como tal son necesarios los siguientes requisitos:

a) Imputabilidad o capacidad de culpabilidad: la cual se refiere a contar con la madurez psíquica y física para poder sujetarse a lo que establece la ley penal, y cuentan con ésta los mayores de edad y los mentalmente sanos.
b) Conocimiento de la antijuricidad: Se refiere al conocimiento que tiene el individuo de que lo la conducta realizada es contraria a la ley.
c) Exigibilidad de obediencia al Derecho: refiere que el comportamiento antijurídico se ha realizado en condiciones normales, es decir que no han existido situaciones excepcionales en la comisión del hecho delictivo.

Elementos Negativos:

[18] Girón Palles, José Gustavo. Teoría del delito. Instituto de la Defensa Pública Penal. Guatemala 2013. Pág. 29.

Ausencia de Acción

Para que exista el delito como tal no basta con la fase interna de la acción debe exteriorizarse lo planificado, es decir, que en la ausencia de la acción no hay materialización de la voluntad, por lo tanto no hay delito.

Atipicidad

Como elemento del delito establece que para que sea determinado como tal debe estar contemplado o regulado en la ley penal, de esta forma si no se encuentra descrito en un cuerpo normativo ya no es típico, por lo tanto tampoco delito.

Causas de Justificación

Son condiciones que evidencian que el actuar del sujeto en una conducta es justificada en virtud de la concurrencia de determinadas situaciones que justifican ese actuar ilícito. Estas se encuentran descritas en el Código Penal Decreto 17-73 en artículo 24 de la siguiente forma:

a) Legítima defensa: Justifica el obrar siempre se actué en defensa de la persona, bienes o derechos. Siempre exista una agresión ilegítima, la necesidad racional del medio empleado para impedirla o repelerla y la falta de provocación suficiente por parte del defensor.

b) Estado de necesidad: Justifica la acción cundo esta se realiza obligado por la necesidad de salvarse o salvar a otros de un peligro, no causado por él, ni evitable de otra forma.

c) Legítimo ejercicio de un derecho: justifica la actuación de un acto ordenado o permitido por la ley en ejercicio legítimo de un cargo público, de la profesión a que se dedica, de la autoridad que ejerce o ayuda que presta a la justicia.

Causas de Inculpabilidad

Son ciertas circunstancias de extinción de la responsabilidad ya que no existe la voluntad del sujeto, es decir que en la comisión del delito no existe dolo, culpa o preterintencionalidad. Es se encuentras descritas en el Código Penal Decreto 17-73 en el artículo 25 de la siguiente forma:

a) Miedo invencible: es ejecutar el hecho motivado por el miedo de un daño igual o mayor al que se sufre.

b) Fuerza exterior: Es la ejecución del hecho violentado por una fuerza material exterior aplicada directamente sobre el sujeto de forma irresistible.

c) Error: Es la ejecución de hecho en la creencia racional que existe una agresión ilegítima contra el sujeto.

d) Obediencia debida: Es la ejecución del hecho en virtud de obediencia debida, siempre que haya subordinación jerárquica entre quien ordena y quien ejecuta el acto, la orden sea dictada dentro del ámbito de las atribuciones de quien la emite y la ilegalidad del mandato no sea manifiesta.

e) Omisión justificada: Sucede al incurrir en omisión hallándose impedido de actuar por causa legítima e insuperable.

2.3 ELEMENTOS BÁSICOS DEL TIPO PENAL

El tipo penal existe cuando se configuran todos los elementos propios de la descripción de una conducta prohibida que lleva a la imposición de una pena, por lo que al establecer su estructura se encuentran los elementos básicos y los elementos esenciales, en cuanto a los primeros estos son de tres tipos:

- Los sujetos
- El bien jurídico
- La acción

Los sujetos del tipo penal: entre estos encontramos 3 tipos:

a) Sujeto Activo: Es el ofensor o el autor que realiza, comete y participa en la acción o comportamiento que la ley indica. Y sobre este recae la consecuencia jurídica del delito, es este a quien se le impone la pena o medida de seguridad, dependiendo de la gravedad del delito.

b) Sujeto Pasivo: Es el titular del bien jurídico vulnerado, quien sufre las consecuencias por la acción u omisión típica y es a quien protege la ley penal.

c) El Estado: Es el ente encargado de perseguir ejerciendo la acción penal, también es quien se encarga de juzgar las conductas delictivas contempladas en la ley penal.

El Bien jurídico:

Es el objeto de ataque del delito, en este sentido el Estado es el ente al cual le corresponde exclusivamente brindar la protección adecuada a los bienes jurídicos que sean atacados frente a la comisión de un hecho delictivo.

La Acción:

Se refiere a la conducta realizada por la persona y se desenvuelve a través de dos aspectos:

"A. TIPO OBJETIVO

Constituye tipo objetivo, el sujeto, la acción (como la aparición externa del hecho producido por la conducta desarrollada por medio de verbos rectores como, sustraer, entrar en morada ajena, simular etc.), el bien jurídico. Lo pueden integrar la relación de causalidad y la imputación objetiva.

B. TIPO SUBJETIVO

Se refiere a la función de relación psicológica entre el autor y la acción o resultado, de donde se deriva el término DESVALOR DE ACCIÓN y se refiere a la finalidad, el ánimo, la tendencia que impulsó actuar al sujeto activo a realizar la acción y omisión, a título de dolo o de culpa. De este elemento se deriva el tipo doloso y el tipo culposo, y la doctrina dominante los incluye dentro de la tipicidad"[19].

2.4 ELEMENTOS ESENCIALES DEL TIPO

Estos se encuentras establecidos en los supuestos de hecho de la norma penal, están conformados por los elementos:

- **Elemento descriptivo**:

  Se refiere a aquel que se puede apreciar a través de los sentidos, y establece las características en la que se produce el hecho ilícito, como por ejemplo una lesión la cual puede ser percibida por medio de la revisión que efectúa un médico forense, quien determina la forma en la cual esta fue producida, el tiempo de tratamiento o curación, con lo cual se establece el tipo de acción ilícita que se cometió y la pena correspondiente.

- **Elemento Normativo:**

[19] Girón Palles. Teoría del delito, Ibid., Pág. 32.

Este elemento a diferencia del anterior tiene una denotación más profunda ya que se aprecia a través del intelecto, para por establecerlo se debe llevar a cabo una valoración jurídica del mismo, al momento de realizar esta valoración se debe contar con el auxilio de otras ramas del derecho para conocerlo e interpretarlo. Como por ejemplo lograr justipreciar la propiedad, posesión o la asociación ilícita.

2.5 OBJETO DEL DELITO

Se refiere a la persona, bien o interés que cuenta con la protección y resguardo de la ley penal, es decir, los bienes jurídicos tutelados que se constituyen como los valores defendidos por el Estado, para mantener el orden social. Para su estudio se divide en dos aspectos:

a) Objeto Material:

Es la persona o cosa que es afectada de forma directa por la conducta delictiva y sobre la cual se produce un resultado dañoso, es decir que sobre este objeto recae físicamente la acción típica. Por ejemplo en un robo la cosa mueble ajena es el objeto material afectado.

b) Objeto Jurídico:

Es el derecho que el legislador al momento de crear la norma jurídica penal, ha seleccionado para ser protegido por medio de ésta, es denominado bien jurídico tutelado. También puede ser llamado el interés jurídicamente tutelado por la ley, y el derecho penal lo protege en cada conducta considerada como delito, con el objetivo de mantener una armonía social. Por ejemplo en el delito de homicidio se resguarda la vida humana como bien jurídico tutelado.

La diferencia sustancial entre ambos objetos radica en que el objeto material del delito se refiere al objeto corporal externo, sobre el cual se realiza la acción, y cuando se habla del objeto jurídico se define al bien jurídico el cual se identifica como el objeto que intenta proteger la ley.

2.6 EJECUCIÓN DEL DELITO

Se refiere a la realización del delito o también denominado el Iter Críminis, que consiste en la serie de etapas que van desde la ideación, planificación selección de medios hasta la ejecución de un hecho ilícito. Este se divide en dos fases:

- Fase interna:

  Únicamente sucede en la mente del agente del delito, a través de esta fase se lleva a cabo la decisión, planificación y selección de los medios o instrumentos adecuados para posteriormente llevar a cabo la comisión del delito. No es penada por la ley, ya que no se puede castigar el pensamiento sino únicamente las acciones establecidas como delito.

- Fase externa:

  Es la materialización del hecho previamente planificado, es decir que el pensamiento sale de lo abstracto a lo concreto, origina la realización o ejecución de acciones que tienen como fin la comisión del delito.

Se esta manera la perfecta forma de ejecutar el delito es la consumación, mientras que la forma imperfecta es la tentativa.

Al hablar de consumación es referirse al Delito Consumado, el cual es definido por el artículo 13 del Código Penal, Decreto 17-73 como tal cuando concurren todos los elementos de su tipificación.

La tentativa por el contrario significa tratar de realizar un delito y por diversas razones no se logra su ejecución. El Código Penal Decreto 17-73 en su artículo 14 establece la tentativa cuando con el fin de cometer un delito, se comienza su ejecución por actos exteriores e idóneos, sin embargo no se llega a consumar por causas independientes a la voluntad del agente.

2.7 CLASIFICACIÓN DE LOS DELITOS

Doctrinariamente los delitos se calcifican de la siguiente forma:

Por su gravedad:

a) Delitos: Se constituyen como graves infracciones a la ley penal.

b) Faltas: Son contravenciones leves a la ley penal.

Por la conducta del agente:

a) Acción: Requieren el movimiento del agente del delito para ser cometidos.

b) Omisión: Se deja de hacer lo que está obligado, requieren la inactividad del agente del delito.

Por el resultado:

a) Formales: Para perfeccionarse no requieren de ningún resultado.

b) Materiales: Para perfeccionarse requieren de un resultado.

Por el daño que causan:

a) De lesión: Provocan una disminución del bien jurídicamente tutelado

b) De peligro: Provocan un riesgo en el bien jurídicamente tutelado.

Por su duración:

a) Instantáneos: Su consumación y perfección tiene lugar en un solo movimiento.

b) Permanentes: El efecto negativo se prolonga a través del tiempo.

c) Continuados: A través de la ejecución de varios actos se produce una sola lesión.

Por su elemento interno

a) Culposos: El agente no tiene la intención de causar el daño, y se produce por imprudencia, negligencia, descuido o torpeza.

b) Dolosos: El agente del delito tiene la absoluta intención de cometer el hecho.

c) Preterintencionales: El resultado va más allá de la intención del agente del delito.

Por su estructura:

a) Simples: lesionan un solo bien jurídico.

b) Complejos: Lesiona dos o más bienes jurídicos.

CAPITULO III

DELITOS INFORMÁTICOS

3.1 ANTECEDENTES HISTÓRICOS

El avance de la tecnología a través de las computadoras, redes informáticas e internet nos enfrenta a la era de la informática, por lo que se crean instrumentos de almacenamiento y transferencia de información gubernamental, corporativa, personal, información de sumo interés, lo que ha dado lugar al surgimiento de comportamientos encaminados al uso indebido o abuso de los sistemas computacionales dando origen a los llamados delitos informáticos.

La historia y evolución de los delitos informáticos deviene de la misma que el internet, motivando los primeros delitos a través de simples hackeos con la finalidad de sustraer información de redes locales, sin embargo a medida que el internet a tenido un mayor alcance y modernización, también lo han hecho los ataques. Si bien la creación de nuevos métodos digitalizados le da mayor desarrollo a la humanidad, hace lo mismo con los criminales.

Paralelamente a los grandes avances tecnológicos y su influencia en la vida social, han surgido interrogantes si el sistema de justicia es lo suficientemente capaz de regular estas nuevas acciones delictuosas. El Derecho es una ciencia que se encuentra en constante evolución y el Derecho Penal no debe ser la excepción, debe transformase para cubrir las necesidades de la sociedad.

En esta perspectiva, cronológicamente se ubica en el siglo XX el origen de los delitos de carácter informático; entre las primeras manifestaciones de estos encontramos en el

año de 1959 la creación de programas que paulatinamente disminuían la memoria de las computadoras, 1972 la aparición de los primeros virus que afectaron los sistemas informáticos, en 1980 ataques de virus dirigidos a sistemas gubernamentales.

Fue hasta el año de 1938 que la Organización de Cooperación y Desarrollo Económico (OCDE) realiza los primeros estudios para la creación y aplicación en el plano internacional de leyes penales, e iniciar la lucha contra el uso indebido de los programas de computadoras. Posteriormente elaboró un conjunto de normas destinadas a regulación de la seguridad de los sistemas de información, estableciendo las bases para que los demás Estados fueran capaces de erigir un marco de seguridad de los sistemas informáticos.

A pesar de los avances que se lograban, a finales de los años 80 se desató la primera gran ola en delitos informáticos, utilizando la plataforma del correo electrónico, dando lugar a que se produjeran fraudes por medio del envío de un malware a los usuarios, la estrategia consistía en que ingresaba a la bandeja de entrada un correo solicitando ayuda para causas benéficas, por lo que muchas de las personas que utilizaban estos medios de comunicación caían en la trampa.

Ese despertar en el ámbito internacional se siguió generalizando, por lo que fue en 1992 que la Asociación Internacional de Derecho Penal, adoptó diversas recomendaciones respecto a los delitos informáticos, entre las principales la insuficiencia del Derecho Penal actual para modificar la definición de los delitos existentes o bien la creación de nuevas figuras.

Con el paso de los años los delitos informáticos fueron evolucionando, con la implementación de los navegadores web en la época de los años 90, los cuales fueron vulnerables a los virus, que eran enviados a través de conexiones a internet siempre que se ingresaba a determinados sitios web; las variedades de virus afectaban a las computadoras ocasionando un funcionamiento lento de los equipos, o bien la aparición de publicidad molesta que invadía las pantallas, otros redirigían los enlaces a páginas de pornografía.

El verdadero despertar de los delitos informáticos se da a principios del año 2,000 al cobrar vida las redes sociales, por medio de éstas gran cantidad de personas coloca información personal en los perfiles, lo que da acceso prácticamente ilimitado a los delincuentes, para hacer mal uso de esa información, provocando el robo de identidad, fraudes y un sin fin de conductas contrarias a la ley.

En cuanto a la evolución de los delitos informáticos en Guatemala, si existían conductas cuya finalidad era el ataque a los equipos tecnológicos o a la información contenida en estos, no se podía considerar delito, en base al principio de legalidad; con el afán de proteger los bienes vulnerados por estas conductas en la legislación nacional a partir del año de 1996, en el Código Penal el decreto 17-73 se regulan por primera vez este tipo de delitos, siendo en la actualidad bastante escuetos atendiendo a la realidad nacional que se vive, puesto que las conductas se han diversificado y el grado de ataques es mayor. A pesar de contar con esta regulación, el ordenamiento jurídico en materia penal, no ha tenido avance alguno en estos últimos tiempos a diferencia de otras legislaciones, por lo que es necesario para enfrentar este tipo de criminalidad informática que los tipos penales tradicionales, sean actualizados y lograr una efectiva seguridad jurídica, evitando que las conductas que no están reguladas por una legislación eficiente queden impunes.

3.2 DEFINICIÓN

Los delitos informáticos son también denominados por la doctrina como Ciberdelitos, delincuencia informática o criminalidad informática. Para poder entender que es delito informático, se debe partir del Convenio Sobre la Ciberdelincuencia del Consejo de Europa, suscrito en Budapest el 23 de Noviembre de 2001, dicho convenio lo define como todo acto dirigido contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, estableciendo conductas propias de este tipo de delitos, que traen consecuencias de tipo penal para quien incurra en ellas.

“En este sentido puede definir el delito informático como toda aquella acción típica y antijurídica, que se sirve o utiliza una computadora para su realización, o ben va dirigida

a obtener el acceso no autorizado a registros, programas o de un sistema informático, o a producir un resultado de daño en ésta o de los sistemas que la misma hace operar."[20]

"Delincuencia Informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera."[21]

Más que una forma específica de delitos, se basa en una pluralidad de comportamientos delictivos vinculados con la tecnología, es decir, computadoras, información, sistemas, todo aquello que involucra abuso informático perpetrado por quien posea los conocimientos necesarios en tecnología.

La interconexión entre la tecnología, la información, las redes y sistemas es cada vez más convergente, lo que proporciona ventajas inimaginables a la población en general, pero también significa un riesgo creciente ante las conductas mal intencionadas que se transforman en delitos, las que pueden adoptar diferentes formas de materializarse como el acceso ilegal, la difusión de programas perjudiciales y ataques por denegación de servicios. Dichas conductas no solo afectan al patrimonio, sino también perjudican otros bienes jurídicos como la intimidad personal, incluso la seguridad nacional.

La informática está conformada por características que la convierten en el medio perfecto para cometer varios tipos delictivos que en gran parte del mundo ni siquiera han podido ser catalogados como tales, situación en la que se encuentra la legislación guatemalteca. Y no necesariamente se enfrentan nuevos delitos, si no que se trata de una novedosa forma de llevar a cabo delitos tradicionales. Tomando en consideración que los delincuentes son especialistas capaces de efectuar el crimen, con los conocimientos necesarios para incluso borrar toda huella de los hechos.

El ámbito en el que se llevan a cabo este tipo de conductas, se caracteriza por el empleo de ataques a sistemas operativos, intromisión o acceso ilegal a las bases de

[20] Noriega Salazar, Hans Aarón, Delitos Informáticos, Instituto de la Defensa Pública Penal Guatemala 1ª Edición 2011. Pág. 23

[21] Acurio Del Pino, Santiago, Derecho Penal Informático, 2015 Ecuador. Pág. 14

datos o archivos, así también el empleo de los aparatos tecnológicos como instrumentos para ejecutar los delitos.

Con respecto a los Delitos Informáticos estos reúnen las siguientes características que los catalogan como tales:

“1. Son conductas criminales de cuello blanco, en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas.

2. Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando.

3. Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.

4. Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.

5. Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física.

6. Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica específica.

7. Son muy sofisticados y relativamente frecuentes.

8. Presentan grandes dificultades para su comprobación, por su carácter técnico.

9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.

10. Ofrecen a los menores de edad facilidades para su comisión.

11. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional."[22]

En el estudio de este tipo de delitos se pueden establecer otros aspectos característicos de estas conductas como por ejemplo el estatus socioeconómico con el que debe contar el sujeto activo del delito, ya que se requieren determinados conocimientos que se obtienen a través de un nivel específico de educación y de los instrumentos para cometer los actos criminales, por lo que no se pueden atribuir a pobreza, mala habitación, baja educación, poca inteligencia o inestabilidad emocional.

En concordancia con todo lo anterior es importante hacer referencia a la creciente aparición de conductas que encuadran en los delitos informáticos, observando casos de relevancia como la obstrucción a los servicios de páginas web de entidades gubernamentales, fugas de información, violación de datos personales e interceptación de datos informáticos accediendo a comunicaciones privadas sin contar con una orden judicial, sin embargo la falta de una normativa eficaz para sancionar estas conductas ocasiona perjuicio a las personas víctimas de este tipo de conductas maliciosas.

3.3 SUJETOS EN EL DELITO INFORMÁTICO

Al determinar quiénes son los sujetos que intervienen en los delitos informáticos el Derecho Penal establece una específica división de sujeto activo y sujeto pasivo, quienes a su vez pueden ser personas naturales o jurídicas. De esta manera el titular del bien jurídico lesionado o perjudicado es el sujeto pasivo, por otro lado quien lesiona el bien tutelado a través de la realización de la conducta delictiva es el sujeto activo.

Sujeto Activo:

"Las personas que cometen los Delitos Informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas

[22] Tellez Valdez, Julio Ibid., Pág. 188

informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos."[23]

De acuerdo con la anterior definición el actuar de los sujetos activos en los delitos informáticos puede realizarse desde dos perspectivas. La primera cuando los delitos se comenten desde dentro del sistema, es decir por aquellas personas que lo operan, que están familiarizadas con el mismo y tienen libertad de acceso, denominado Insiders. La segunda tiene lugar cuando se comete la conducta delictiva a través del mal uso del ciberespacio, es decir el cometido a distancia, denominado Outsiders.

Si bien los delitos informáticos se encuentran categorizados como "delitos de cuello blanco", algunas de sus características los determinan como tales, en virtud de que los sujetos responsables de cometerlos cuentan con un alto grado de conocimientos y recursos en el área de informática, es decir que no pueden ser cometidos por cualquier persona, ya que esta debe poseer los conocimientos necesarios, sin embargo el internet en la bastedad de posibilidades que le proporciona a los usuarios permite que cualquiera tenga acceso a sistemas, redes, información o los conocimientos que se requieren para incurrir en estos delitos.

Es por lo anterior que existe una controversia en cuanto al nivel de aptitudes con las que debe contar el sujeto activo para ser considerado como tal, es por esa razón que muchas veces es difícil descubrirlos y sancionarlos ya que la sociedad incluso llega a considerarlos como respetables, al no segregarlos, despreciarlos o desvalorizarlos. Puede que tenga injerencia la falta de conocimiento hacia esas conductas o bien que no sean vistos como los delincuentes típicos que incurren en actos de violencia para lograr sus objetivos.

Los sujetos activos en el delito informático también llamados delincuentes informáticos o ciberdelincuentes, pueden clasificarse de la siguiente forma:

- **Piratas informáticos:** Se refiere a las personas que hacen uso del software creado por un tercero, a través de copias ilegales, sin contar con los permisos o licencias correspondientes.

[23] Acurio Del Pino, Santiago, Ibid. Pág. 15

- **Hacker**: tiene su origen de la palabra en inglés Hack, que significa cortar o derribar, es considerado un experto o especialista en el ámbito informático capaz de ingresar sin autorización a cualquier sistema informático, con el objetivo de dañar, apropiarse, interferir, difundir o destruir información que se encuentre almacenada, llevando a cabo sus actividades tanto en entidades públicas como privadas. Se caracteriza por la búsqueda de dejar en evidencia las vulnerabilidades de los sistemas informáticos.

- **Cracker**: se origina del vocablo ingles Craker que significa romper, este sujeto utiliza sus conocimientos para irrumpir la seguridad de los sistemas informáticos con el objetivo de robar, destruir información, realizar transacciones ilícitas, o bien impedir el buen funcionamiento de las redes informáticas o de las computadoras.

- **Lammers**: Intentan vulnerar la seguridad de los sitios web aprovechando el conocimiento adquirido y publicado por expertos, sin embargo no cuentan con los conocimientos suficientes para lograr su cometido, se encuentran en una menor categoría que los Hackers.

- **Phreakers**: Son crackers realizan ataques a compañías telefónicas con la finalidad de obtener llamadas gratis.

- **Bucaneros**: Se dedican a la comercialización de los productos craqueados, no cuentan con los conocimientos para vulnerar la seguridad de los sistemas informáticos, su objetivo principal es revender los productos.

La diversidad de autores en los delitos informáticos es amplia, pero la diferencia entre los mismo se ve marcada en la naturaleza del delito que estos cometen.

Sujeto Pasivo:

“Es la víctima del delito, es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Las víctimas pueden ser individuos, instituciones crediticias,

instituciones militares, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros."[24]

Cualquier persona puede ser víctima de un delito informático, ya sea una física o jurídica, siempre que esta haya establecido una conexión a internet que es la principal ventana por la que se cometen los ataques, o bien que maneje información valiosa que se encuentre almacenada en un equipo informático.

Los sujetos pasivos juegan un papel importante en este tipo de delitos, ya que a través de la denuncia que estos realicen, es la única forma de descubrir a los autores, sin embargo la falta de cultura de denuncia hace imposible la efectiva persecución de los criminales y aunada a esto la ausencia de leyes que protejan a las víctimas, la poca preparación de las autoridades para investigar, juzgar y sancionar; estas conductas se mantienen impunes.

Considerando la dificultad para reprimir los delitos informáticos, los acuerdos de cooperación internacional y tratados internacionales buscar remediar algunas de las dificultades que enfrentan los Estados como el de Guatemala, en el que no existe legislación eficiente sobre esta clase de conductas ilícita, perjudicando la situación de las víctimas.

3.4 ANONIMATO DE LOS SUJETOS EN EL DELITO INFORMÁTICO

El anonimato en internet es una acción destinada a garantizar que el acceso a una Red se realiza de tal forma que no se pueda conocer quien está llevando a cabo esa conexión, por lo que el sujeto activo en los delitos informáticos es el más beneficiado, permitiéndole evadir sus responsabilidades en cuanto a las infracciones que cometa. Las formas de beneficiarse del anonimato pueden ser variadas, desde no usar su propio sistema informático empleando el de un tercero, como en el caso de los correos no deseados o SPAM, hasta la implementación de programas de enmascaramiento o que no permitan ver la verdadera dirección del correo electrónico o número IP.

[24] http://www.delitosinformaticos.info/definición.html. 30 de septiembre de 2018

El incremento de los delitos informáticos es producto de la facilidad con la que los cibercriminales pasan inadvertidos o anónimos en el mundo cibernético, por lo que el rastreo eficaz de las direcciones de Red IP son acciones que le corresponden a las autoridades, logrando mantener visible en internet a los usuarios y evitando la comisión de este tipo de delitos.

Los niveles del anonimato pueden darse de dos maneras:

- A nivel del dispositivo:

Se caracteriza por no dejar rastro en el equipo que se esté utilizando, en cuanto al uso, operaciones o transacciones realizadas en internet. Valiéndose de las funciones que ofrecen los diversos navegadores se puede lograr este tipo de anonimato, sin embargo está limitada al ordenador o navegador que se esté utilizando. Permitiendo que no se guarde información sobre los accesos a internet que su hubieren utilizado.

- A nivel del internet.

Evita que la página o el servicio con el que se realiza la conexión sepa quien está realizándola, por medio de un software determinado se pueden lograr estas medidas.

Otra de las manifestaciones más relevantes del anonimato de los sujetos en los delitos informáticos la encontramos en la llamada Deep web o internet profunda u oculta, es una parte de la Red de internet en la cual el ingreso a los contendido únicamente se realiza a través de un determinado software o protocolo específico.

Al hablar de anonimato también se debe hacer alusión a la privacidad la cual consiste en acciones que garanticen que la información privada es protegida en accesos o bien publicaciones en internet. Esta es eficaz para los sujetos pasivos, que ven vulnerada su información ante los sujetos activos que emplean en mayor medida el anonimato.

3.5 BIENES JURÍDICOS TUTELADOS EN EL DELITO INFORMÁTICO

“En el entendido que 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.”[25]

Los bienes jurídicos juegan un papel fundamentan en las ciencias penales, ya que la afectación de estos permite la fundamentación del correspondiente castigo punitivo a las conductas que los lesionan o bien los ponen en peligro. En consideración al grado de afectación que sufran los bienes jurídicos se establece la pena, lo que permite la determinación del injusto específico de cada delito. En el caso de los delitos informáticos existe una tendencia hacia la protección de bienes jurídicos desde la perspectiva de los delitos tradicionales, a través de la reinterpretación de los tipos penales ya existentes. Así también, existen posiciones, las cuales suponen que en los delitos informáticos existe una pluralidad de benes jurídicos que son afectados, totalmente diferentes a los ya existentes en los delitos tradicionales.

Las teorías que explican que tipo de bienes jurídicos deben ser tutelados en los delitos informáticos son diversas. Por una parte, está la tesis que asume que los delitos informáticos tutelan un bien jurídico específico, propiamente informático, el cual es **la información**, que constituye un elemento totalmente diferente a los bienes jurídicos que protegen los delitos tradicionales. Sin embargo se debe tomar en consideración que la información incorpora también valores inmateriales, es decir que esta no puede ser tratada de la misma manera que la legislación actual toma a los bienes corporales.

La información debe ser considerada en diferentes formas, ya sea como valor económico, como valor intrínseco de la persona, por su fluidez y tráfico jurídico, así como los sistemas que la procesan o automatizan, los cuales se asemejan a los bienes jurídicos tutelados tradicionales.

Por otro lado, está la tesis en la cual se defiende la idea que en los delitos informáticos no se tutela un bien jurídico específico propiamente informático, sino una pluralidad de bienes entre los cuales encontramos:

[25] Noriega Salas, Hans Aarón. Ibid. Pág. 24

- **El Patrimonio**: en cuanto a las acciones dirigidas a sabotaje, fraudes informáticos, manipulaciones de datos, daño, destrucción o pérdida de equipos de computación.
- **La reserva, intimidad y confidencialidad de los datos**: en cuanto a las agresiones informáticas que vulneran la intimidad en general y específicamente bancos de datos.
- **La seguridad o fiabilidad del tráfico jurídico y probatorio**: en cuanto a las falsificaciones de datos o documentos probatorios obtenidos por medios informáticos.
- **El derecho de propiedad**: en cuanto a la información o el uso de ordenadores para la reproducción no autorizada de documentos.

Es importante mencionar que ha tomado relevancia como bien jurídico tutelado en los delitos informáticos **la calidad, pureza e idoneidad de la información contenida en un sistema informático**, el cual tiene un sentido, que es totalmente diferente a los bienes tutelados por los delitos tradicionales. Sin embargo presenta dificultades al tratar de determinase de una manera específica en cuanto a la información la llamada calidad, pureza e idoneidad, ya que son connotaciones sumamente amplias, la problemática se vería reflejada en cuanto a los instrumentos, valores o criterios necesarios para afirmar que una conducta afectó estos atributos.

Por último, algunos criterios presentan el **Internet** como bien jurídico tutelado en los delitos informáticos, tomando en consideración que es el medio por el cual se ejecutan las conductas delictivas. Si bien es cierto actualmente el número de delitos informáticos cometidos a través del internet va en ascenso, pero se debería tener en consideración diferentes instrumentos que involucran la criminalidad como las redes computacionales y no solo el internet, lo que resulta en conflicto al tomarlo como un bien jurídico tutelado.

Por lo tanto las nuevas tecnologías, proporcionan importantes elementos que atentan contra los bienes jurídicos ya sean los existentes o aquellos que surgen, por lo que debe tenerse presente que las conductas derivadas de los delitos informáticos tienen un

carácter pluriofensivo, que no solo afectan un bien jurídico determinado, sino una diversidad de ellos, los cuales ponen en relieve un interés colectivo, tomando en consideración que el tema respecto al bien jurídico protegido en los delitos informáticos, es un tanto impreciso, lleno de opiniones tan variadas. Por lo que la protección no puede estar limitada a un bien en específico, sino por el contrario debe se amplia, en virtud de los constantes cambios que enfrentan los avances tecnológicos y la realidad social.

3.6 CLASIFICACIÓN DE DELITOS INFORMÁTICOS

Desde que se observaron las primeras manifestaciones de los delitos informáticos han sido objeto de análisis, diversas legislaciones han tipificado estas conductas delictivas. No existe una clasificación única de este tipo de delitos, por lo que cada legislación establece las circunstancias en la cual es cometido, la forma de investigación y la sanción que considere.

Por lo que una de las clasificaciones más completas es la que realiza el Doctor Santiago Acurio del Pino, estableciéndola de la siguiente forma:

"Los Fraudes

- Los Datos Falsos o Engañosos (Data didding):

Conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como *manipulación de datos de entrada*, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismo.

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

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos

programas o nuevas rutinas. Un método común utilizado es insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

- La Técnica del Salami:

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

- Falsificaciones Informáticas:

Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada. Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

- Manipulación de los Datos de Salida:

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

- Pishing:

Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor.

En estos momentos también existe una nueva modalidad de Pishing que es llamado *Spear Pishing o Pishing segmentado*, el cual ataca a grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior.

El Sabotaje Informático

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

- Bombas Lógicas (Logic Bombs):

Es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimiento especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Son difíciles de detectar antes de que exploten; poseen el máximo potencial de daño. Puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

- Gusanos:

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

- Virus Informático y Malware:

Son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian y de un eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.

El malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y las debilidades de los sistemas desactiva los controles informáticos de la máquina afectada y causa que se propaguen los códigos maliciosos.

- Ciberterrorismo:

Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro de los tipos de delitos informáticos, especialmente los de tipo de Sabotaje.

- Ataques de Denegación de Servicio:

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a muchos usuarios.

El Espionaje informático y el robo o hurto de software

- Fuga de Datos (Data Leakage):

También conocida como la divulgación no autorizada de datos reservados, es una variedad de espionaje industrial que sustrae información confidencial de una empresa.

- Reproducción no autorizada de Programas Informáticos de Protección Legal:

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

El Robo de Servicios

- Hurto del Tiempo del Computador:

Consiste en el hurto del tiempo de uso de las computadoras, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de internet, para que con esa clave, pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está

autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

- Apropiación de Informaciones Residuales (Scavenging):

Es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. Tomando la información residual que ha quedado en memoria o soportes magnéticos.

- Parasitismo Informático (Piggibacking) y Suplantación de Personalidad:

En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización o empresa determinada.

El Acceso no autorizada a Servicios Informáticos

- Las Puertas Falsas (Trap Doors):

Consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

- La Llave Maestra 8sUPERZAPPING):

Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.

- Pinchado de Líneas (Wiretapping):

Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un modem y una impresora.

- Piratas Informáticos o Hackers

El acceso se efectúa a menudo desde un lugar exterior, el delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. Se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes."[26]

Es importante incluir en la clasificación de los Delitos Informáticos aquellos que atentan contra la privacidad, la intimidad, la libertad o indemnidad sexual, y entre estos encontramos:

- Violación a la privacidad de la información personal o a las comunicaciones
- Revelación indebida de información personal
- Pornografía infantil a través de internet.

3.7 EL CIBERCRIMEN

El campo de aplicación del cibercrimen son los delitos cibernéticos que en otras palabras son los denominado delitos informáticos de los cuales ya se ha hablado con anterioridad, sin embargo por la falta de conocimiento suelen tomarse como figuras totalmente diferentes, pero tienen el mismo significado.

Hablar de cibercrimen es referirse a las conductas, típicas, antijurídicas, culpables, señaladas en la ley que traen consigo una sanción, pero se debe tener en consideración el medio empleado para materializar esas conductas, en el caso de los delitos cibernético o delitos informáticos puede realizarse a través de la vulneración de información contenida en in sistema informático o bien que el medio de comisión del delito sea un medio digital.

El máximo objetivo de los cibercriminales es acceder sin el consentimiento debido a bases de información o datos, los cuales son propiedad de personas, empresas o incluso entidades gubernamentales.

[26] Acurio del Pino Santiago. Ibid. Págs. 23 a la 29.

La principal característica de los ataques que se realizan en el cibercrimen es que estos nunca serán físicos, es decir que todo se lleva a cabo de forma virtual. Así también la facilidad con que vulneran los sistemas de seguridad, empleando medios remotos y en un periodo muy corto de tiempo, lo que produce grandes dificultades al intentar rastrear a los delincuentes cibernéticos.

Existen diversas maneras de combatir el cibercrimen, como por ejemplo el empleo de contraseñas que sean complejas, que incluyan combinaciones de números, letras, mayúsculas y minúsculas, que no involucren aspectos de la vida privada y cambiarlas con frecuencia.

Así también tener el cuidado correspondiente a lo que se publica en internet, especialmente en las redes sociales, en cuanto a datos personales o toda aquella información de carácter personal, incluso financiera que puede ser objeto de un ataque a través del cibercrimen.

CAPITULO IV

DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL GUATEMALTECA

4.1 DELITOS INFORMÁTICOS EN LA LEGISLACIÓN PENAL GUATEMALTECA

En la década de los años noventa frente a la utilización de nuevas tecnologías en diferentes ámbitos del país, nace la preocupación por regular nuevas formas de comisión de hechos delictivos, lo que provoca la reforma del Código Penal Decreto 17-73, por el Congreso de la República a través del Decreto 33-96 publicado en fecha 21 de Junio de 1996, con el objetivo de regular delitos informáticos en beneficio de la población. Quedando tipificados en el Libro II, Título VI de los delitos contra el patrimonio, Capítulo VII De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos. Estableciéndose la tipificación de 7 delitos informáticos siendo estos:

a) Artículo 274 “A” Destrucción de registros informáticos

b) Artículo 274 “B” Alteración de programas
c) Artículo 274 “C” Reproducción de instrucciones o programas de Computación.
d) Artículo 274 “D” Registros prohibidos
e) Artículo 274 “E” Manipulación de información
f) Artículo 274 “F” Uso de información
g) Artículo 274 “G” Programas destructivos.

4.1.1 Análisis

a) Destrucción de Registros Informáticos:

En esta figura delictiva realiza la acción quien destruya, borre, inutilice, altere o dañe registros informáticos tanto del ámbito público como privado. Al referirse a registros informáticos establece una protección sobre archivos, bases de datos o todos aquellos medios de almacenamiento informático, este tipo delictivo es denominado por otras legislaciones como Sabotaje informático, describiendo una conducta que tienda a destrucción tanto de la información como del medio en el cual se almacena es decir la computadora. La tipificación de este delito se hace de una manera muy generalizada sin especificar modos, formas, medios de lo que constituye un registro informático, determinando tanto una pena de prisión como de multa.

b) Alteración de programas:

En este delito la acción se realiza al alterar, borrar o inutilizar las instrucciones o programas que utilizan las computadoras. Es una figura delictiva que establece una tipificación muy general, ya que únicamente define como elemento material del tipo penal tres especificas acciones, tomando en consideración que actualmente con los avances tecnológicos existen formas más novedosas con las cuales se puede tener un acceso ilícito no solo a programas de computadoras, sino que también aplicaciones, redes informáticas que permiten realizar tareas diversas en esto medios. Establece tanto una pena de prisión como de multa.

c) Reproducción de instrucciones o programas de computación:

La acción se realiza por medio de la copia o cualquier modo de reproducción sin autorización del autor de instrucciones o programas de computación. Este tipo penal establece una estrecha relación con el delito de violación a los derechos de autor, sin embargo dirigido a un medio informático. Es una conducta que no ha desaparecido con el paso del tiempo, todo lo contrario puesto que se encuentra muy marcada en la sociedad actual, ya que como lo señalan los expertos en su mayoría se desarrolla en los hogares, al emplear un software sin las respectivas licencias, lo que comúnmente se denomina piratería de software. Este tipo penal es sancionado con una pena de prisión y multa.

d) Registros prohibidos:

El elemento material en este tipo penal establece la creación de un banco de datos o registro informático con datos que puedan afectar la intimidad de las personas. La acción se creta a crear un registro ilícito con información íntima o personal de los usuarios. Figura que en legislaciones internacionales es denominada suplantación de sitios web para capturar datos personales, la cual ha tenido variaciones significativas en los medios para crear estos bancos o registros de datos, ya que actualmente la tecnología brinda mayores posibilidades para su comisión. Este delito es sancionado con una pena de prisión y multa.

e) Manipulación de información:

Se produce la acción cuando se utilizan registros informáticos o programas de computación para alterar o distorsionar información requerida para una actividad comercial, en el cumplimiento de una obligación Estatal, o para alterar estas contables o la situación patrimonial de una persona física o jurídica.

Este delito puede ser cometido por un empleado, el propietario de una empresa o el particular que distorsiona o falsifica la información, con el objetivó de eludir una obligación para con el Estado, o modificar la situación patrimonial de una persona, conductas que actualmente no se han erradicado, sino todo lo contrario cada vez, la tecnología brinda nuevas herramientas para incurrir en ellas, por lo que actualizarlas

sería beneficioso tanto para el Estado como para la sociedad.

f) Uso de información:

En este delito la acción se efectúa al utilizar u obtener datos contenidos en registros informáticos, bancos de datos o archivos electrónicos sin autorización. Sin embargo este no especifica si se trata de información personal o institucional, ni la forma en la cual puede ser utilizada, situación que puede comprometer el tipo penal a interpretarlo de maneras diversas y lo trae consigo muchas veces aplicaciones erróneas en casos concretos.

g) Programas destructivos:

En este tipo penal la acción se efectúa al distribuir o colocar en circulación programas o instrucciones destructivas para causar perjuicio a registros, programas o equipos de computación. Conducta que no se acopla con la realidad social, ya que actualmente las modalidades para realizarla son múltiples y no solo se puede hablar de distribuir o colocar, mucho menos de programas o instrucciones destructivas, lo que ahora se conoce como malware y está compuesto por una infinidad de variantes para atacar sistemas informáticos.

Los tipos penales en materia de delitos informáticos establecidos en 1996 constituían un gran avance para la época, sin embargo actualmente son muy escuetos al tratar de regular conductas delictivas en este ámbito, tomando en consideración que la tecnología avanza a pasos agigantados, de la misma manera lo hacen los delincuentes informáticos, por lo que se necesita reformar drásticamente las figuras delictivas contenidas en ese capítulo a través de la creación de una ley penal específica.

4.1.2 Bienes jurídicos tutelados

En los tipos penales en materia de delitos informáticos regulados en el actual Código Penal, delimitan ciertos bienes jurídicos tutelados como el patrimonio, la información y los derechos de autor. Sin embargo estos deben ir más allá no limitarse a esos específicos, recordando que este tipo de delitos se caracterizan por vulnerar una diversidad de bienes jurídicos.

Es importante terminar con la estrecha relación que se maneja en este cuerpo normativo entre los delitos informáticos y los derechos de autor, que si bien a través de los sistemas tecnológicos se realizan actividades que atentan contra los derechos de autor, estos no son los únicos que son agredidos, actualmente existen otros bienes como la información, la propiedad, la intimidad, incluso el honor de las personas que den ser objeto de tutela.

Una correcta tipificación de delitos informáticos que atienda a la realidad tecnológica que actualmente se vive en el país, abre la puerta a la prevención y control de conductas que realmente se producen con los medios informáticos, así como la efectiva tutela de los bienes y la protección de derechos de la población en general

El derecho penal se constituye como una ciencia que se encuentra en constante evolución no puede detenerse y únicamente proteger cierto tipo de derechos o sancionar determinadas conductas, la implementación de una ley específica en esta materia es la perfecta solución a la impunidad que se vive con este tipo de conductas delictivas.

4.2 LEYES QUE REGULAN ASPECTOS TECNOLÓGICOS EN GUATEMALA

a) **Ley de Reconocimiento de Comunicaciones y Firmas Electrónicas. Decreto Número 47-2008**:

Este cuerpo normativo se encarga de regular todo lo relacionado con las actividades electrónicas en el campo del comercio electrónico, suministro o intercambio de bienes o servicios, distribución, representación o mandato comercial, documentos electrónicos o mensajes de datos, operaciones financieras, la contratación electrónica y firmas electrónicas.

b) Ley de Acceso a la Información Pública. Decreto Número 57-2008:

Marco jurídico por el cual se establece la importancia de la protección de datos personales, así como los delitos o infracciones que se puedan cometer en cuanto violentar el derecho a la intimidad de las personas con relación a los datos personales, tomando en cuenta que gran parte de la información puede ser almacenada en medios tecnológicos, ya que las principales bases de datos son

electrónicas, esta ley se encuentra ligada en cuanto a la vulneración de los equipos que almacena la información.

c) **Código Procesal Penal. Decreto Número 51-92**

Con las últimas reformas efectuadas se incorpora el uso de videoconferencias para lo cual se emplea la plataforma de internet.

d) **Ley de Telecomunicaciones. Decreto Número 94-96**

Este cuerpo normativo establece el marco legal de las telecomunicaciones, regulando el uso del espectro radioeléctrico, los derechos de los usuarios, la actividad de los proveedores de servicio de telecomunicaciones y se crea la Superintendencia de Telecomunicaciones.

e) **Ley de Derechos de Autor y Derechos Conexos. Decreto 33-98**

Establece el marco legal que determina regulaciones relacionadas con los programas de ordenados y bases de datos. Además de ser el único cuerpo normativo en el cual se encuentran definidos que es un ordenador.

f) **Ley de Protección al consumidor. Decreto Número 6-2003:**

La cual se encuentra íntimamente ligada con la Ley de reconocimiento de comunicaciones y firmas electrónicas, en cuanto a la vigilancia que se debe efectuar para beneficio de comerciantes, empresas mercantiles y todas aquellas que realicen comercio electrónico.

g) **Ley del Registro Nacional de las Personas. Decreto 90-2005:**

Marco jurídico en el cual se regulan varios aspectos relacionados con datos personales, designando la responsabilidad a la Dirección de Informática y Estadística de proteger y custodiar la base de datos, así como la elaboración de respaldos electrónicos.

h) **Ley de Contrataciones del Estado. Decreto Número 57-92:**

Cuerpo normativo a través se regula es sistema de GUATECOMPRAS, medio electrónico por el cual se llevan a cabo los procesos de compra, venta y contratación de bienes, suministros, obras y servicios, desde la convocatoria hasta la adjudicación por parte del Estado.

i) **Ley de Promoción del Desarrollo Científico y Tecnológico Nacional. Decreto Número 63-91:**

Crear el marco general para el fomento, organización y orientación de las actividades científicas y tecnológicas, a efecto de estimular su generación, difusión, transferencia y utilización. Así como la regulación de oferta de servicios científicos y tecnológicos a nivel nacional.

La estimulación y promoción de gestiones e innovaciones tecnológicas como instrumentos de búsqueda de la productividad y competitividad.

A través de esta ley se crea el Consejo Nacional de Ciencia y Tecnología.

4.3 CIBERDELITOS EN GUATEMALA

El fenómeno de la globalización ha traído consigo la difusión de la tecnología a los rincones más inimaginables y Guatemala no es la excepción en cuanto a la apertura a las nuevas tendencias tecnológicas, los adelantos traen consigo beneficios, pero también oportunidades para la proliferación y masificación de los ciberdelitos, que cubren diversos estratos sociales, desde niños, estudiantes, personas comunes, empresarios, incluso hasta las instituciones de gobierno.

Estas conductas ilícitas son muy diversas y no son ajenas a la sociedad guatemalteca, es cierto que a nivel internación se tiene mayor conocimiento de la recurrencia de los delitos informáticos, cuentan los legislaciones específicas para contrarrestas sus efectos, pero en el caso de Guatemala, existen estas conductas por muy extrañas que parezcan, dentro de las infracciones más comunes se encuentran difamaciones, amenazas o ataques a la intimidad, robo de identidad, tráfico y robo de datos de información y el espionaje electrónico.

Si bien existe la Sección contra Delitos Informáticos de la Policía Nacional Civil, la mayoría de la población no tiene conocimiento de la misma, situación que es desfavorable para todas aquellas personas que son víctimas de este tipo de conductas, puesto que pueden acudir a promover sus denuncias.

Una de las principales debilidades que enfrenta el país es la falta de una ley contra los delitos informáticos, si bien existe un órgano en cual se puede denunciar, muchas de las conductas no encajan con la precaria normativa vigente, de que sirve esta organización, si no se puede aplicar una justicia eficaz ante la falta de tipos penales adecuados, ya que las conductas delictivas van más allá de un simple virus informático.

4.4 CONVENIOS INTERNACIONALES EN MATERIA DE DELITOS INFORMÁICOS

El creciente avance tecnológico ha traído consigo desarrollo en diversos ámbitos sociales, tanto a nivel nacional como internacional, siendo el internet el principal instrumento de evolución tecnológica e informática, ha generado una multiplicidad de beneficios personales, sociales, comerciales e incluso estatales. Sin embargo aunado a esto se han originado nuevas amenazas como consecuencia del uso irresponsable de la información que transita por internet, la cual puede ser malversada o manipulada para invadir la privacidad de los usuarios, destruir datos contenidos en computadoras hasta obstaculizar funciones gubernamentales.

Es por todo lo anterior que la particular naturaleza de los delitos informáticos trasciende fronteras, estás acciones ilícitas no pueden ser abordadas por un solo gobierno, lo que origina la necesaria unificación de criterios y esfuerzos en la persecución penal de este tipo de conductas; de esa cuenta la cooperación internacional juega un papel de suma importancia, para lo cual se han creado diversos convenios internacionales en materia de delitos informáticos, entre los de mayor trascendencia se encuentran:

g) Convenio de Cibercriminalidad de la Unión Europea

Suscrito el 21 de noviembre del año 2001 en Budapest Hungría por los Estados miembros del Consejo de Europa. Los puntos principales que abarca el convenio se basan en:

a) Definiciones de términos en los cual se incluyen conceptos de sistema, datos de tráfico o proveedor de servicios, disposiciones sobre uniformidad de la terminología en el ámbito de la informática.

b) Medidas que deben ser adoptadas por los Estados como leyes sustantivas penales, describiendo elementos tipo a ser tomados en cuanta por las legislaciones de los Estados suscriptores, aspectos de procedimiento, condiciones, garantías, medios de prueba o bien reglas jurisdiccionales.

c) Aspectos de cooperación internacional que incluyan figuras como las reglas para definir las cuestiones de extradición, asistencia mutua, reglas aplicables cuando no existan acuerdos internacionales y redes de comunicaciones.

El objetivo fundamental del convenio el coordinar esfuerzos que permitan hacer efectiva la persecución penal en el ámbito de los delitos informáticos a nivel internacional, para cual sienta las bases que permiten la armonización de las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático. Así también, provee directrices de procedimiento penal que brindan a las autoridades de cada Estado las facultades necesarias para llevar a cabo la investigación y persecución de los delitos informáticos.

Este convenio constituye un instrumento de suma trascendencia, que refleja el esfuerzo internacional más importante en contra de las actividades criminales cometidas a través de medios informáticos, el cual beneficia en gran medida a los países europeos, sin embargo, corresponde a los países latinoamericanos hacer propios los lineamentos establecidos en el convenio, logrando implementar sanciones y mecanismos de investigación adecuados, avanzados y dinámicos que permitan hacer frente a los delitos informáticos, ya que el mismo se encuentra abierto a la adhesión, a lo cual únicamente lo han suscrito Costa Rica, República Dominicana, México, Argentina y Chile.

h) Convenio No. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

Elaborado por el Consejo de Europa en Estrasburgo el 28 de enero de 1981, es uno de los documentos más importantes en el escenario internacional, para la creación de un marco legal en materia de protección de datos personales. Se constituye como el primer

instrumento internacional jurídicamente vinculante en el área de la protección de datos y el primero abierto a países no miembros de la Unión Europea.

El objetivo fundamental de este instrumento es garantizar a cualquier persona sin importar su nacionalidad la protección de la información personal con respecto al tratamiento automatizado de los mismos, a través del respeto a sus derechos y libertades fundamentales, concretamente su derecho a la vida privada. Al mismo tiempo mantener el libre flujo de datos personales entre los países.

Los puntos principales abordados por el convenio establecen que los datos obtenidos por los países firmantes deben ser adquiridos de manera legal y legítima; deben ser tratados para finalidades determinadas; así también ser conservados de tal forma que se permita identificar al titular de los datos durante el tiempo de conservación que no puede ser mayor aquel necesario para las finalidades para las cuales se han obtenido. Por lo que los Estados tienen el compromiso de establecer medidas de prevención y sanciones para los que accedan de forma ilícita a los datos personas contenidos en las respectivas bases.

Teniendo en consideración que varios de los delitos informáticos vulneran la intimidad de las personas, a través del acceso no autorizado a los ordenadores personales o a los datos que ellos guardan, este convenio es de vital importancia frente a la preocupación existente de estas nuevas formas de delinquir capaces de traspasar fronteras, a pesar que fue elaborado en la década de los ochenta, cuando los avances tecnológicos no tenían los alcances que hoy en día logran, las disposiciones que en él se contienen lo constituyen un instrumento de importancia para la prevención y sanción de las conductas ilícitas cometidas por medios informáticos.

i) Decisión marco 2005/222/JAI del Consejo de Europa relativa a los ataques contra los sistemas de información

Suscrita el 24 de Febrero de 2005 en Bruselas Bélgica.

El objetivo principal de este instrumento es propiciar, mantener y reforzar la cooperación entre las autoridades judiciales o aquellas encargadas de perseguir penalmente los

delitos que propicien ataques contra los sistemas de información. De esta manera la unificación de los esfuerzos internacionales a través de la aproximación de las normas penales de sus Estados miembros logra combatir eficazmente este tipo de conductas ilícitas.

Entre los puntos principales en los que se basa la decisión marco del Consejo de Europa se encuentran:

a) Regular pautas comunes de coordinación que precisen elementos como sistemas de información y datos informáticos.

b) Unificación de criterios en cuanto a delitos como acceso ilegal a los sistemas de información, intromisión ilegal en los sistemas de información, intromisión ilegal en los datos, inducción, complicidad y tentativa.

c) La obligación de señalar penas efectivas, disuasorias y proporcionadas atendiendo a la gravedad de los delitos, por parte de los Estados miembros.

d) Al tratarse de delincuencia organizada establecer penas que impongan sanciones que se encuentren entre 2 y 5 años de prisión, independientemente de la sanción común.

e) Establecer sanciones contra las personas jurídicas cuando éstas se beneficien de la comisión de delitos informáticos, entre las que se incluyan la exclusión del disfrute de ventajas o ayudas públicas, la prohibición temporal o permanente del desempeño de actividades comerciales, vigilancia judicial, así como la liquidación de la persona jurídica.

j) Undécimo congreso de Naciones Unidas para la prevención del delito y la justicia penal

Realizado en el año 2005 en Bangkok, Tailandia, al celebrarse el congreso se desarrollaron medidas para prevenir los delitos informáticos en el ámbito internacional, para lo cual fueron citadas dos resoluciones emitidas por la asamblea general, siendo estas:

a) Resolución de la Asamblea General de la Organización de las Naciones Unidas número 56/121: en la que se atribuye a la Comisión de Prevención del Delito y Justicia penal, a través de su labor logros importantes en la investigación de estrategias, que permitan a los Estados elaborar leyes, políticas nacionales y prácticas que intensifiquen la lucha contra la utilización de la tecnología de la información con fines delictivos.
b) Resolución de la Asamblea General de la Organización de las Naciones Unidas 56/261: A través de la cual se hace referencia a los planes de acción tendientes a la aplicación de la Declaración de Viena, que motiva la penalización del uso indebido de las tecnologías de la información, así como la formulación y aplicación de normas o de procedimientos que permitan la investigación eficaz de delitos relacionados con la informática.

Los principales aportes del Congreso celebrado incluyen la recomendación del empleo de expertos dedicados al estudio de la delincuencia informática disponibles 24 horas al día, en continua capacitación y la implementación de equipo actualizado, para responder eficazmente a los casos relacionados con delitos informáticos en cada Estado.

k) Declaración de VIENA sobre la delincuencia y la justicia frente a los retos del siglo XXI 55/59

Celebrada el 4 de diciembre del año 2000 por la Organización de las Naciones Unidas, a través de este instrumento se formulan recomendaciones de políticas que impulsen acciones de prevención, control y sanción de los delitos informáticos.

Dicho instrumento tiene como punto de partida la preocupación a nivel internacional del crecimiento desmedido de los delitos cibernéticos y la necesaria labor que debe realizarse por los Estados para lograr la unificación de criterios que propicien la persecución penal, estrategias de política criminal, estandarización de conductas tipo, y la asistencia jurídica internacional que logre la prevención y sanción de este tipo de conductas ilícitas.

l) Resolución 57/239 sobre los elementos para la creación de una cultura mundial de seguridad cibernética

Aprobada el 31 de Enero del año 2003 por la Asamblea General de la Organización de las Naciones Unidas, establece la importancia de fomentar la seguridad cibernética como medida ante el desmedido aumento de conductas ilícitas en ámbitos informáticos. Haciendo énfasis en los siguientes aspectos:

a) La conciencia que deben tener individuos, instituciones y Estados acerca de la necesidad de implementar medidas de seguridad en sistemas y redes de información.

b) Responsabilidad de examinar constantemente las políticas de los Estados participantes.

c) Respuestas prontas y oportunas frente a los ataques contra la seguridad de los sistemas y redes de información, así como la implementación de procedimientos ágiles de cooperación estatal.

d) Evaluación de los riesgo, amenazas y vulnerabilidades periódicamente.

e) La creación e implementación de mecanismos de seguridad informática.

f) Examen de los sistemas de seguridad que determine la eficacia de los mismos, así como la incorporación de las modificaciones necesarias para frenar las amenaza en la medida que estas se presentan.

m) Manual de las Naciones Unidas para la prevención y control de delitos informáticos

Este instrumento examina la multidimensionalidad de las nuevas y emergentes formas de delincuencia informática a partir de sus posibles elementos impulsores, así como la forma en la que estas son operadas, con el objetivo de prevenir, afrontar y erradicar estas crecientes manifestaciones de crímenes transnacionales a través de la cooperación internacional.

Señalando como los principales factores que se deben afrontar por parte de los Estados:

a) La falta de acuerdos globales que determinen las conductas tipo que deben ser consideradas como delitos informáticos

b) La carencia de leyes especializadas en materia procesal o sustantiva capaces de normar los delitos informáticos, así como la casi inexistencia de técnicas de investigación que permitan evidenciar las actividades delictivas cometidas a través de medios informáticos.

c) La ausencia de tratados de extradición, acuerdos o mecanismos que permitan la plena eficacia de la cooperación internacional, evidencian la dificultad de persecución de los delitos informáticos en virtud del carácter transnacional de los mismos.

n) **Estrategia Interamericana para combatir las amenazas a la seguridad informática. Resolución AG/RES.1939 XXXIII-O/03**.

Aprobada el 10 de Junio de 2003 en la Asamblea General de la Organización de Estados Americanos, este instrumento desarrolla una estrategia integral para la protección de las infraestructuras de informática, es decir la seguridad cibernética, a través de un enfoque internacional.

Evidencia la gravedad que representan las amenazas hacia la seguridad cibernética, vulnerando la seguridad de los sistemas de información esenciales, infraestructuras, incluso economías en el mundo, para lo cual dicho problema deber abordado a través de la cooperación internacional, contando con la coordinación de entidades gubernamentales y no gubernamentales.

Dicha estrategia encuentra sus bases en los estudios e investigaciones realizadas por el Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Expertos Gubernamentales de la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). Su principal objetivo es establecer un marco capaz de proteger las redes y sistemas de información que integran el internet, que demuestre eficacia al momento de

responder a los incidentes que se puedan suscitar. Para lo cual establece las siguientes directrices:

o) “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;
p) 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;
q) 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
r) Se promueva la adopción de políticas y legislación sobre el delito cibernético que protejan a los usuarios de internet y prevenga y disuadan el uso indebido e ilícito de computadoras y redes.”[27]

Los Convenios Internacionales en materia de delitos informáticos constituyen instrumentos indispensables para la prevención, investigación, regulación y sanción de estas conductas ilícitas cometidas contra la seguridad cibernética. A lo largo de historia diferentes organizaciones se han preocupado por evidenciar las posibles dificultades que los Estados pueden enfrentar ante el creciente desarrollo de la tecnología y en especial las tecnologías de la información, puesto que no es un problema que tienda afecta un territorio determinado, sino todo lo contrario, el avance es tan significativo que es capaz de trascender fronteras, es allí donde radica la importancia de la cooperación internacional en busca de soluciones eficaces. En el caso de Guatemala, se enfrenta un severa crisis por la falta de regulaciones jurídicas específicas en este ámbito, y aún más preocupante la falta de interés de las entidades gubernamentales para adherirse a los tratados internacionales, ya que de los anteriormente expuestos, ninguno ha suscrito Guatemala.

[27] Acurio Del Pino, Santiago, Ibid. Pag. 44

4.5 FENÓMENO DE LA DELINCUENCIA INFORMÁTICA EN GUATEMALA

Abordar el estudio del impacto de las nuevas tecnologías en el fenómeno de la delincuencia es una necesidad, ya que Guatemala en los últimos años ha experimentado un incremento en los delitos no convencionales, es decir en aquellos delitos que emplean la tecnología para materializar conductas ilícitas.

Con el gran auge que ha tenido la tecnología a nivel mundial, Guatemala no queda relegada de esa situación, ya que se considera una nación que tiene un alto consumo en tecnología, lo que también puede ser perjudicial puesto que deja un panorama más abierto al crimen organizado y a las pandillas que incursionan en estos avances con fácil acceso, dejando vulnerables a los usuarios finales que pueden ser cualquier persona o instituciones públicas y privadas en temas de delitos informáticos.

El principal problema radica en la inapropiada tipificación del delito informático o ciberdelito en el Código Penal, ya que dentro de estas actividades ilícitas podemos encontrar una gran variedad no solamente las allí incluidas, como por ejemplo pornografía infantil, ataques a la intimidad, robo de identidad, tráfico y robo de datos o información, espionaje electrónico, estafas online, phising, los ataques a las páginas web privadas o gubernamentales y el ciberterrorismo, conductas ilegales y lesivas que proliferan día con día, las cuales en su gran mayoría se realizan a través de las redes sociales o bien por medio de plataformas abiertas a miles de usuarios que son vulneradas.

La excesiva, rápida e imparable modernización de la sociedad exige una regulación apropiada que sea capaz de normar eficientemente los delitos informáticos, establecer los parámetros necesarios para su persecución, rastreo y proceso judicial, permitiendo al sistema de justicia una pronta respuesta. Ahora bien, la realidad nacional presenta grandes desventajas, frente a la carencia de leyes relacionadas con este fenómeno, únicamente se han presentado 2 iniciativas de ley que quedaron fallidas y una tercera que espera ser tomada en consideración. Estas acciones advierten un problema para las instituciones llamadas a perseguir los ciberdelitos, que se traducen a la falta de infraestructura necesaria, como centros de vigilancia computarizada, modernas

herramientas tecnológicas necesarias para la investigación, la formación especial que requieren los principales cuerpos responsables de perseguir esta clase de criminalidad.

Un importante avance realizado en este ámbito es la Sección contra los Delitos Informáticos de la Policía Nacional Civil, cual se creó en el año 2016 como una de las primeras instituciones que busca fortalecer las acciones de prevención, investigación y atención a las víctimas de delitos informáticos. Cualquier persona que se considere afectada por este tipo de conductas ilícitas, puede presentar su denuncia a través de la línea Cuéntaselo a Waldemar que tiene por objeto recibir denuncias de forma anónima por medio del call center 1561 o bien al número 110 dicha institución.

Sin embargo uno de los sectores que aún no da el paso a la modernización, y sigue sin adaptarse a las nuevas tecnologías es el sector Judicial. La falta de preparación suficiente por parte de Jueces y Magistrados en estos temas, constituye uno de los principales obstáculos para impartir justicia por los órganos adecuados, la principal solución radica en la constante capacitación del sector justicia.

Por otro lado la falta de conocimiento acerca de los delitos informáticos por parte de la población, la convierte en el punto más vulnerable frente a estas acciones delictivas, esto se manifiesta a través del uso irresponsable de las redes sociales o todos aquellos medios tecnológicos por los cuales puedan compartir información que pueda ser objeto de ataque. Así también las instituciones gubernamentales corren con la misma suerte, al manejar información de importancia, incluso confidencial, son un blanco fácil para los cibercriminales, que buscan vulnerar la seguridad de los sistemas y apropiarse de ese tipo de datos.

Es por estas razones que contar con leyes e instrumentos eficaces, la infraestructura adecuada, recursos humanos calificados, es de suma importancia para continuar la lucha contra la delincuencia informática y hacerle frente a este tipo de delitos, ya que muchas de estas actividades ilícitas no son constitutivas de delito por no estar expresamente prohibidas en virtud del principio de legalidad.

4.6 ANÁLISIS DE LA INICIATIVA 4054

La iniciativa de Ley contra el Cibercrimen, Número 4054, fue recibida en la dirección legislativa del Congreso de la República el 12 de mayo del año 2009 y presentada al Pleno del Congreso de la República de Guatemala el 18 de agosto del año 2009. En su exposición de motivos establece puntos relevantes que motivaron su nacimiento, entre estos el crecimiento exponencial de usuarios en internet, desencadena conductas contrarias a la ley, los llamados ciberdelitos, que remarcan la importancia de poseer medidas especiales de prevención, detección e inicio de acciones judiciales contra dichas conductas ilícitas. Presenta a los ciberdelitos como tipos novedosos, potencialmente lesivos, de dimensión transnacional y en constante evolución, todas estas características los hacen difíciles de perseguir.

Los ciberdelitos que se pretendían regular por medio de esta iniciativa de Ley, no encontraban tipificados en el actual Código Penal guatemalteco, entre los cuales se pueden mencionar: Códigos de acceso, clonación de dispositivos de acceso, acceso ilícito, acceso ilícito para servicios a terceros, dispositivos fraudulentos, interceptación e intervención de datos o señales, daño o alteración de datos, sabotaje, atentado contra la vida de la persona, robo mediante la utilización de alta tecnología, obtención ilícita de fondos, estafa especial, chantaje especial, robo de identidad, falsedad de documentos y firmas, uso de equipos par invasión de privacidad, comercio ilícito de bienes y servicios, difamación especial, injuria pública, atentado sexual y delitos de telecomunicaciones.

Un aspecto relevante de esta iniciativa de Ley es la propuesta para crear una Comisión contra Crímenes y Delitos de Alta Tecnología (CDAT), la que tendría entre sus funciones la coordinación y cooperación con gobiernos e instituciones tanto nacionales como internacionales, para prevenir y reducir la comisión de los ciberdelitos.

Esta iniciativa constituye el primer esfuerzo para contar en nuestro país con una normativa legal capaz de tipificar y regular los ciberdelitos, así como el establecimiento de instituciones especializadas en la materia, sin embargo no prospero en el Congreso de la República a tal punto que ni siquiera llego a conocerla una comisión específica en el proceso legislativo.

4.7 ANÁLISIS DE LA IICIATIVA 4055

Iniciativa de ley denominada Ley de los Delitos Informáticos, Número 4055 fue conocida por el pleno del Congreso de la República de Guatemala el 18 de agosto del año 2009. En su exposición de motivos establece como punto principal de su creación el establecimiento de un marco regulatorio sobre los posibles usos indebidos o los actos ilícitos de naturaleza informática que sean cometidos en Guatemala o que surtan efectos jurídicos en su territorio, así como la imposición de sanciones drásticas a los responsables de los ilícitos tipificados por la misma.

Establece como bien jurídico tutelado a la información en cuanto a sus atribuciones de integridad, disponibilidad y confidencialidad. Así también busca resguardar los derechos de las personas en cuanto a la integridad, disponibilidad y confidencialidad de los sistemas que utilicen tecnologías de la información.

El objeto de esta iniciativa de ley se concentra en establecimiento de medidas de prevención y sanción en contra de los actos ilícitos de naturaleza informática, los cuales pueden ser cometidos por aparatos tecnológicos, mensajes de datos, sistemas o datos informáticos. Así también hace énfasis en la protección contra la explotación, pornografía o cualquier otra forma de abuso sexual en menores de edad, siempre se realicen por medio de sistemas informáticos.

Su ámbito de aplicación se traduce hacia los responsables de los hechos delictivos cometidos en el territorio de Guatemala, así también hace mención que cuando el delito sea cometido fuera del territorio de la República, pero produce efectos dentro del territorio y no hubiere sido juzgado por un tribunal extranjero, quedará sujeto a las disposiciones del proyecto de ley.

Esta iniciativa establece como definiciones las siguientes: Datos informáticos, documento, pornografía infantil, sistema informático, tarjeta inteligente y tecnología de información.

La presente iniciativa tipifica los siguientes delitos informáticos:

a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso son autorización
- Daño informático
- Posesión de equipos o prestación de servicios para daño informático
- Espionaje informático

b) Delitos Informáticos relacionados con la propiedad y autenticidad:

- Fraude informático
- Uso fraudulento de tarjetas inteligentes o instrumentos análogos
- Provisión de equipo para falsificaciones
- Posesión de equipo para falsificaciones
- Falsificación informática
- Invitación de acceso

c) Delitos relacionados con el contenido:

- Pornografía infantil
- Alteración de imágenes.

Por último propone la creación y organización de una Unidad de Investigación especializada de delitos Informáticos, por parte del Ministerio Público.

Esta iniciativa fue presentada hace 9 años, sin embargo fue un avance trascendental para lograr la creación de disposiciones normativas que regulen los delitos informáticos, regulando diversos módulos que contemplan definiciones y la tipificación de conductas delictivas más acordes a la realidad, sin embargo desde su presentación hasta la fecha han surgido cambios sustanciales en el campo de la tecnología y en la realidad nacional. No contó con el apoyo suficiente por lo que no tuvo mayores avances para ser aprobada por el Congreso de la República y quedo relegada como una iniciativa más fallida en el campo de los ciberdelitos.

4.8 ANÁLISIS DE LA INICIATIVA 5254

Constituye la tercera iniciativa con la que se pretenden normar las conductas delictivas en materia informática, denominada Ley contra la ciberdelincuencia Número 5254; es recibida en la Dirección Legislativa el 8 de marzo del año 2017 y presentada el 9 de marzo del mismo año al Pleno del Congreso de la República de Guatemala.

La exposición de motivos de esta iniciativa hace referencia a la constate evolución en la que se encuentra la tecnología y derivado a los alcances de la misma se ha incurrido en la configuración de nuevas formas de criminalidad, desencadenadas por el abuso desmedido del internet, sistemas o redes informáticas. Por lo que se hace necesario contar con un instrumento jurídico penal que contenga las figuras penales necesarias para encuadrar todos aquellos actos ilícitos, en el ámbito tecnológico. En virtud que la tipificación actual de los delitos informáticos en el Código penal, no responde a las modalidades de los delitos que se comente por medio de redes o sistemas informáticos, incapaz de brindar la protección necesaria a intereses individuales o colectivos, reflejados en la información, datos o seguridad de sistemas.

El objeto de la iniciativa de Ley es tipificar figuras delictivas, así como adecuar las normas penales ya existentes y enfrentar las nuevas formas de ciberdelincuencia. Hace referencia la implementación de reglas procesales capaces de incorporar medios de prueba digitales o bien electrónicas en el proceso penal.

En cuanto a los bienes jurídicos tutelados a través de esta iniciativa se encuentran bienes de personas tanto individuales como jurídicas, entre ellos los datos personales, intimidad informática, indemnidad sexual de menores, la confidencialidad, la integridad y disponibilidad de la información o datos contenidos en sistemas informáticos, las comunicaciones transmitidas por estos medios, así como bienes, activos o pasivos patrimoniales representados en las transacciones u operaciones comerciales o financieras que se realicen por esos medios.

El ámbito de aplicación se extiende al territorio de la República de Guatemala y demás ámbitos extraterritoriales establecidos de conformidad con los casos regulados en el

Código Penal, así como el medio para la comisión de este tipo de acciones delictivas lo define como el ciberespacio.

Por otro se hace referencia a varias definiciones para efecto del respectivo proyecto de ley, entre las cuales están: Ciberdelincuencia, ciberdelitos, ciberentorno, ciberespacio, ciberseguridad, CSIRT-GT, confidencialidad de la información y de los datos, datos informáticos, datos relativos al tráfico, disponibilidad de la información y de los datos, habeas data, infraestructura critica, ingeniería social, integridad de la información y de los datos, intimidad informática, medios cibernéticos, protección de datos personales, proveedor de servicios, sistema informático, tecnologías de la información y las comunicaciones y relacionadas.

Tipifica los delitos informáticos de la manera siguiente:

a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos o sistemas que utilicen tecnologías de la información y las comunicaciones:

- Acceso ilícito
- Interceptación ilícita
- Ataque a la integridad de los datos
- Ataque a la integridad del sistema

b) Delitos informáticos:

- Falsificación informática
- Apropiación de identidad ajena
- Abuso de dispositivos
- Fraude informático
- Agravantes generales

c) Ciberdelitos contra las personas:

- Pornografía infantil
- Acoso por medios cibernético

- Delito contra la integridad sexual de una menor o contacto a menor con fines sexuales a través de las Tics.
- Propiedad intelectual

Entre las propuestas de la iniciativa se encuentra la creación del Centro de Seguridad Interinstitucional de Respuesta Técnico-jurídica ante incidentes informáticos-Guatemala (CSIRT-GT), como la institución especializada en la detección, atención y control de los casos de delitos informáticos, el cual estará bajo la dirección del Ministerio de Gobernación.

Es por todo lo anterior que esta iniciativa de ley contra la ciberdelincuencia es la más completa a comparación de las dos anteriores, sin embargo el proceso de aprobación ha sido tardío, a pesar que regular este tipo de conductas delictivas debería ser una prioridad, ya que la tecnología es una herramienta indispensable para la gran mayoría de personas, instituciones o sectores de la sociedad que desarrollan sus actividades o almacenan información o datos confidenciales a través de estos medios o instrumentos tecnológicos y la carencia de una norma capaz de regular este tipo de conductas ilícitas dañosas, que irrumpen la seguridad informática, personal e institucional, representa un problema difícil de prevenir. Por lo que el desarrollo de un cuerpo normativo adecuado evita la impunidad en este tipo de delincuencia, además de constituir el primer paso para investigación, persecución y sanción de los delitos informáticos.

CAPITULO V

PROCESO LEGISLATIVO EN GUATEMALA

5.1 DEFINICIÓN

“El proceso legislativo es el conjunto de etapas y pasos que la Constitución Política de la República y la Ley Orgánica del Organismo Legislativo señalan para la formación de la ley. Los pasos indicados deben seguirse en un orden cronológico con el objeto de no

violar los preceptos señalados en los cuerpos legales citados y por consiguiente no incurrir en la violación del debido procedimiento legislativo."[28]

En Guatemala el proceso legislativo se encuentra fundamentado en dos cuerpos legales específicos, en primer lugar en la Constitución Política de la República de Guatemala en los artículos 174 al 181 y en segundo lugar en la Ley Orgánica del Organismo Legislativo Decreto 63-94, en los artículos 109 al 133. Dicho procedimiento comprende desde la presentación de la iniciativa de ley hasta la entrada en vigencia, las etapas que lo componen son las siguientes:

- Iniciativa de ley
- Presentación
- Discusión
- Consulta
- Aprobación
- Redacción
- Sanción
- Veto
- Promulgación
- Publicación
- Vigencia

5.2 INICIATIVA DE LEY

“Documento formal que los órganos o actores facultados legalmente presentan ante el Congreso de la República para su estudio, discusión y, en su caso, aprobación. Tiene como propósito crear, reformar, adicionar, derogar o abrogar disposiciones constitucionales o legales. Representa el acto jurídico con el que da inicio el proceso legislativo.”[29]

[28] http://www.academia.edu/12203020/El_proceso_de_creacion_y_sancion_de_la_ley_en_Guatemala. 8 de octubre de 2018.
[29] http:// www.bordepolitico.com/que-es-una-iniciativa-deley. 8 de octubre de 2018

Tienen iniciativa de ley como lo establece la Constitución Política de la República de Guatemala en su artículo 174 los siguientes:

- Diputados al Congreso de la República de Guatemala
- Organismo Ejecutivo
- Corte Suprema de Justicia
- Universidad de San Carlos de Guatemala
- Tribunal Supremo Electoral.

La iniciativa de ley también denominada proyecto de ley debe definir con claridad lo que cualquiera de los sujetos con capacidad para proponerla desean plasmar en la disposición jurídica. Para la presentación de este se deben tener definidos, identificados y analizados los objetivos que se pretenden alcanzar con el mismo, así también haber agotado todas aquellas actividades, estudios o investigaciones sobre el tema que se pretende regular con el proyecto de ley. Además de contar con el auxilio técnico-jurídico de personas conocedoras de la materia.

La elaboración de un proyecto debe contener los siguientes aspectos:

a) **Exposición de motivos**: Se refiere a la causa, necesidad o razón por la cual se crea, es decir todos aquellos argumentos que especifican el motivo por el cual se promueve el proyecto de ley.

b) **Preámbulo de la ley**: Son los considerandos, nombre de la Ley y su fundamento Constitucional o legal para crear la ley. Establece los argumentos concretos y precisos de la ley que se presenta.

c) **Por tanto**: Lo constituye el fundamento constitucional que tiene el Congreso de la República para emitir leyes, es decir la facultad para decretar, reformar y derogar leyes.

d) **Parte dispositiva**: Formada por el articulado o el conjunto de artículos que integran la ley, está puede estar dividida por títulos, capítulos y secciones.

e) **Disposiciones finales y derogatorias**: Se refiere a los artículos transitorios, es decir las medidas cuya aplicación es temporal o de rápida aplicación.

f) **Derogatoria**: es la parte en la cual se especifica que ley concluye su vigencia al entrar en vigor la nueva ley.

g) **Vigencia**: La cual establece si la ley se aprueba de forma ordinaria o por urgencia nacional, así como la indicación del día en que entrará en vigor.

5.3 PRESENTANCIÓN

La presentación de una iniciativa de ley comienza ante la Dirección Legislativa del Congreso de la República de Guatemala, redactada en forma de decreto, separando la parte considerativa de la dispositiva, se deben agregar a la misma la exposición de motivos, estudios técnicos y documentados que la justifiquen. Al momento de su recepción se le asignara un número que en su orden le corresponda según el registro, anotando la fecha y hora del mismo, este número le servirá para ser identificada.

Existen dos formas por las cuales se debe llevar a cabo la presentación de un proyecto de Ley, en primer lugar por escrito, debiendo ir cada hora numerada y rubricada por él o los proponentes. La segunda forma consiste en un formato digital, con la finalidad de ponerlo a disposición de los diputados al Congreso de la República, por diferentes medios electrónicos, para que cualquiera de ellos pueda realizar las consultas que considere pertinentes. Este formato digital será introducido por la Dirección Legislativa al sistema electrónico, con las firmas del o los proponentes.

Presentación al pleno:

La presentación de la iniciativa de Ley ante el Pleno del Congreso de la República se lleva a cobo a través de la lectura de la exposición de motivos, la cual es realizada por el diputado o diputados proponentes y sin más trámite pasa a la comisión correspondiente para su conocimiento.

Por otro lado si la iniciativa fue presentada por el Organismo Ejecutivo, se presentará el Ministro de Estado respectivo para justificar o explicar la misma. O bien si hubiese sido presentada por cualquier otro organismo o personas facultadas para ello, la justificación la realizará un funcionario con suficiente jerarquía, el cual es invitado por el Presidente del Congreso.

Posterior a la presentación en el Pleno del Congreso, se envía la Iniciativa a una Comisión de acuerdo a la materia que se pretenda normar con la iniciativa de Ley, la cual se integra por diputados quienes al recibir el proyecto, realizan un estudio para establecer la finalidad que se persigue, incluso pueden proponer enmiendas al contenido ya sea parcial o totalmente. Si se presentaren enmiendas la comisión debe conceder audiencia al ponente de la iniciativa, para discutirlas.

La comisión en su actuar se enfrenta a tres circunstancias:

a) Emitir un dictamen favorable a la iniciativa, aprobándolo con el voto favorable de la mayoría de sus integrantes y considerando beneficioso que el proyecto continúe el proceso legislativo.

b) Emitir un dictamen desfavorable, si no considera pertinente legislar sobre esa materia. Si el pleno aprueba el dictamen negativo la iniciativa de ley será desechada y se mandará a archivar. Caso contrario, se indica a la comisión que vuelva a estudiar la iniciativa.

c) Archivar el expediente y no pronunciarse sobre el mismo.

Finalizado el trámite en la comisión el proyecto se entregará a la Dirección Legislativa para su registro y difusión por medios electrónicos a los diputados; posteriormente se procederá a la discusión.

5.4 DISCUSIÓN

El proyecto de ley se pondrá a discusión conjuntamente con el dictamen emitido por la comisión en 3 sesiones, las cuales se celebran en distintos días y será aprobado hasta tenerse por suficientemente discutido en el tercer debate. Con excepción de los casos en los cuales el proyecto es declarado de urgencia nacional por el Congreso de la República, se requiere el voto favorable de las dos terceras partes del total de diputados. Para lo cual no es necesario el dictamen de la comisión en estos casos.

Los debates se desarrollan de la siguiente forma:

a) Primer debate: se lee en su totalidad tanto el proyecto de ley como el dictamen, se somete a discusión en términos generales, tomando mayor relevancia sobre la constitucionalidad, importancia, conveniencia y oportunidad del proyecto, sin embargo en esta sesión no se efectúa ningún tipo de votación.

b) Segundo debate: Sigue el mismo procedimiento que el primer debate en cuanto a la lectura, sin embargo una diferencia sustancia es la posibilidad de solicitar que se omita la lectura material del proyecto, a través de una moción privilegiada; en esta cualquier diputado solicita la palabra, expone la moción, la cual puede tener como efecto la declaratoria de urgencia nacional o solicitar el retorno a la comisión para realizar un nuevo estudio o emitir un nuevo dictamen. Resulta la moción posteriormente se somete a discusión el proyecto de ley y tampoco es sujeto a votación.

c) Tercer debate: En esta etapa el proyecto de ley se discute en su totalidad, se procede a efectuar la votación sobre la conveniencia o no de la aprobación del mismo, Si la votación es favorable se continuará con la discusión por artículos y se procede a la redacción final. Por el contrario si el voto es negativo el proyecto se desecha y se ordena su archivo.

No obstante lo anterior, la excepción a este procedimiento tiene lugar en los casos de declaración de urgencia nacional, al realizarse una solo lectura, lo cual consta al final de la ley.

5.5 CONSULTA

Al discutirse un proyecto de ley se puede consultar a la Corte de Constitucionalidad en los siguientes casos:

Consulta obligatoria: Tiene lugar al concluirse la discusión de un proyecto de ley en el tercer debate y se trate de reformar leyes constitucionales, para la cual la Corte de constitucionalidad emite un dictamen, con el cual se busca recabar su opinión favorable.

Consulta facultativa: Se puede llevar a cabo durante cualquiera de los debates, es propuesta al Pleno del Congreso por 5 diputados, solicitando la opinión de la Corte de

Constitucionalidad sobre la constitucionalidad del proyecto de ley en discusión, así también sobre tratados o convenios. Para lo cual el debate se suspenderá hasta recibir la opinión solicitada. Si en el plazo de 60 días no se hubiere recibido la opinión, el Pleno debe resolver si continúa el proyecto el proceso legislativo.

5.6 APROBACIÓN

Consiste en la votación que realiza el pleno del Congreso de la República posterior a la discusión del proyecto de ley, por lo que la Constitución Política de la República de Guatemala en su artículo 159 establece que las resoluciones deben tomarse con voto favorable de la mayoría absoluta de diputados que integran el pleno, se debe tener en consideración que en el proceso legislativo la mayoría puede ser absoluta o calificada.

Tomando en consideración que actualmente el Congreso de la República se encuentra integrado por 158 diputados, se entiende que la mayoría absoluta está conformada por la mitad más uno, representada esta por ochenta diputados, por ejemplo, al tratarse de una ley de carácter ordinario. Por otro lado la mayoría calificada se integra por las dos terceras partes del total de diputados del Congreso de la República, la cual se representa con 105 o 106 diputados, por ejemplo al referirse a una ley declarada de urgencia nacional.

5.7 REDACCIÓN

"Una vez aprobado el proyecto de ley por artículos se leerá en la misma sesión o a más tardar durante las tres próximas sesiones. Los Diputados podrán haber objeciones y observaciones a la redacción, pero no será procedente presentar enmiendas que modifiquen el sentido de lo aprobado por el pleno del Congreso. Agotada la discusión se entrará a votar sobre la redacción final y en esta forma quedará aprobado el texto. Los decretos declarados de urgencia nacional serán leídos en redacción final en la misma sesión. "[30]

En este sentido, el proyecto se leerá completamente, es decir desde el preámbulo hasta el último de los artículos, incluidas las enmiendas aprobadas. Aprobado pasará a

[30] Artículo 125, Ley Organica del Organismo Legislativo Decreto 63-94 del Congreso de la República.

constituir un decreto, al cual se le asigna un número correlativo seguido de un guion y los números del año en el cual se aprueba. Esta numeración correlativa es anual, iniciando con el número 1.

Agotada completamente la discusión en cuanto a la redacción final del texto del proyecto, 15 o más diputados pueden solicitar como moción privilegiada la revisión del texto aprobado con el objetivo de volver a discutirlo. Presentada la moción se entrará a discutir de una vez, para lo cual el pleno señalará día y hora para la nueva discusión de lo aprobado. Cumplido este requisito, la secretaría procederá con la lectura del fondo el cual se pondrá a discusión. Aprobado, se votará en su redacción final y pasará a formar parte de la ley.

Posteriormente la Junta Directiva del Congreso envía la ley aprobada a una comisión, la cual tiene como función corregir o redactar en forma apropiada el texto, dándole la construcción gramatical más adecuada, antes de enviarla al Ejecutivo para su sanción y promulgación. Los cambios que se realicen serán puramente de estilo y forma, pero nunca de fondo.

Por último antes de ser enviado el decreto aprobado al Organismo Ejecutivo para su sanción, promulgación y publicación, el presidente del Congreso entregará copia a todos los diputados, quienes tienen el plazo de 5 días para presentar sus observaciones, si no se manifiestan en dicho plazo, se enviará al Ejecutivo para que continúe su trámite.

5.8 SANCIÓN

El Organismo Ejecutivo recibe el decreto por medio de la Secretaría General de la Presidencia, para lo cual se procede a su estudio y análisis por el Presidente de la República, además de uno o varios Ministros de Estado, para luego sancionarlo, vetarlo o asumir una actitud pasiva al respecto.

A través de la sanción el Presidente de la república confirma la ley, es decir que acepta el decreto aprobado por el Congreso de la República, el cual se adapta a las necesidades de la realidad nacional.

5.9 VETO

Es la facultad que le asiste al Organismo Ejecutivo a través del Presidente de la República de no aprobar una ley. Recibido el decreto por el Presidente de la República dentro de los 15 días siguientes podrá devolverlo con las observaciones que estime pertinentes. Si el Congreso está de acuerdo con los argumentos del Presidente, mandara a archivar la ley vedada, por el contrario si no está de acuerdo puede ordenar que se publique aún en contra de la voluntad del Presidente.

Conforme lo establece la Ley Orgánica del Organismo Legislativo en su artículo 129 al tener conocimiento el Congreso de un decreto vetado por el Presidente de la República, la Junta Directiva es la encargada de ponerlo en conocimiento del Pleno, para lo cual se dará lectura de las razones del veto y se suscitan tres circunstancias, en primer lugar se pueden aceptar las razones del veto; en segundo lugar rechazar el veto mediante acuerdo; y por último remitir el expediente a la comisión para que estudie y dictamine sobre el veto.

En el caso que se hubiere rechazado el veto por el Congreso, para tal situación se necesita el voto favorable de las dos terceras partes del total de diputados, en consecuencia el Organismo Ejecutivo está obligado a sancionar y promulgar el decreto dentro de los 8 días siguientes. Si no cumpliere con esta función, la Junta Directiva del Congreso ordenará su publicación en un plazo de 3 días.

5.10 PROMULGACIÓN

Consiste en la declaración que estable que una ley debe considerarse de observancia obligatoria en el territorio de la República de Guatemala.

“Acción y efecto de promulgar, de publicar formalmente una ley u otra disposición de la autoridad, a fin de que sea cumplida y hecha cumplir como obligatoria. Pero, corrientemente, en el léxico jurídico esa expresión está reservada al decreto que el jefe del Estado, cuando no hace uso de su facultad de veto, suscribe con el ministro

refrendatario, ordenando la publicación y ejecución de una ley sancionada por el poder legislativo".[31]

La promulgación tiene por finalidad autentificar la existencia de una ley y ordenar su ejecución, es decir, ordenar cumplirla y hacerla cumplir, dándole a la misma fuerza ejecutiva y carácter imperativo.

5.11 PUBLICACIÓN

"Publicación de las leyes: Acto de llevar a conocimiento general de los ciudadanos o súbditos de un país el texto legal o el de decretos, reglamentos y demás disposiciones generales y obligatorias, mediante la inserción en el periódico oficial o, con carácter urgente, por otros medios de difusión, como la radio o la televisión."[32]

En el proceso de formación y sanción de las leyes, para que estas obtengan validez formal y carácter de obligatoriedad, deben ser publicadas, como lo establece la Constitución Política de la República de Guatemala, el medio oficial para llevar a cabo estas publicaciones es el Diario de Centroamérica o también conocido como Diario Oficial.

La publicación de la ley es el medio por el cual una vez ha sido discutida, aprobada y sancionada una ley esta se dé a conocer a los habitantes, a través del órgano de difusión oficial, con cual esta adquiere fuerza obligatoria, inicia su vigencia y despliega todos sus efectos.

5.12 VIGENCIA

En cuanto a la vigencia el mismo decreto puede contener el plazo para esta o de lo contrario empezara después de los 8 días de su publicación en el Diario Oficial a menos que la misma restrinja o amplíe el mismo, este precepto se encuentra regulado en el artículo 180 de la Constitución Política de la República de Guatemala y en la Ley del Organismo Judicial Decreto 2-89, en su artículo 6, en este cuerpo normativo también se hace mención que para dicho pazo todos los días y horas son hábiles.

[31] Ossorio Manuel, Ibid, Página 783.
[32] Ossorio Manuel, Ibid, Página 794.

Es importante hacer mención que la Ley Orgánica del Organismo Legislativo en su artículo 133 establece una excepción en cuanto al plazo establecido en los anteriores cuerpos normativos, para lo cual la publicación de un decreto por el Congreso de la República en el caso que el Ejecutivo no lo hubiere sancionado, promulgado, ni vetado, se debe realizar en un plazo que no exceda de 3 días.

Es por todo lo anterior que al hablar de la vigencia de una ley se hace referencia al periodo de vida que esta tendrá dentro del ordenamiento jurídico, y por lo tanto se entiende que se extenderá hasta que esta sea derogada por una ley posterior, por declaración expresa de una nueva ley o bien por declaración de inconstitucionalidad, dictada en sentencia firme por la Corte de Constitucionalidad.

5.13 PROPUESTA DE TIPOS PENALES

La creación de una Ley que regule los delitos informáticos es de vital importancia, atendiendo a la realidad social actual, por lo que esta debe contener tipos penales capaces de regular todas aquellas conductas ilícitas que repercuten en los avances tecnológicos, el mal uso de los medios o instrumentos empleados por las personas en el desenvolvimiento de sus actividades tanto laborales, educativas como sociales, así como acciones destinadas al resguardo de la información personal e institucional. Por lo que a mi criterio el ordenamiento jurídico que regule los delitos informáticos debería contener los siguientes tipos penales:

DELITOS CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS NFORMÁTICOS

Artículo 1. Interceptación de datos informáticos. Quien sin orden de juez competente intercepte datos informáticos en su origen, destino o interior de un sistema informático, será sancionado con prisión de dos (2) a cuatro (4) años.

Artículo 2. Acceso ilícito. Quien sin la debida autorización accede a todo o parte de un sistema informático, vulnerando de manera ilícita medidas de seguridad, o acceda al sistema informático excediendo la autorización que le hubiere sido concedida, será sancionado con prisión de uno (1) a tres (3) años.

Artículo 3. Daño informático. Comete el delito él que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, será sancionado con prisión de cuatro (4) a seis (6) años.

Artículo 4. Uso de software malicioso. Quien sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, será sancionad con de prisión de cuatro (4) a seis (6) años

Artículo 5. Fraude informático. Quien a través de las tecnologías de la información procure para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, así como cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será sancionado con prisión de cinco 5 a ocho 8 años. Se impondrá el doble de la pena que le corresponda, cuando se afecte el patrimonio del Estado.

Artículo 6. Abuso de mecanismos y dispositivos informáticos Quien fabrique, diseñe, desarrolle, venda, facilite, distribuya, importe u obtenga para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicios que contribuyan a ese propósito, será sancionado con prisión de uno 1 a tres 3.

DELITOS INFOMÁTICOS RELACIONADOS CON LA CONFIDENCIALIDAD DE DATOS PERSONALES

Artículo 7. Violación de datos personales. Comete el delito el que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique, emplee códigos personales, datos personales contenidos en archivos, bases de datos o medios semejantes, será sancionado con prisión de dos (2) a cuatro (4) años.

Artículo 8. Suplantación de sitios web para capturar datos personales. Quien con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute,

programe o envíe páginas electrónicas, enlaces o ventanas emergentes, con el objetivo de capturar datos personales será sancionado con prisión de tres (3) a cinco (5) años.

Si la acción contemplada en el párrafo anterior estuviere destina a modificar el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, Se impondrá el doble de la pena que le corresponda.

Artículo 9. Suplantación de identidad. Quien mediante las tecnologías informáticas suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será sancionado con prisión de tres (3) a cinco (5) años.

Artículo 10. Espionaje informático. Comete el delito la persona que indebidamente obtenga, revele o difunda los datos o información contenida en archivos, bases de datos o programas de computación con el fin de obtener algún tipo de beneficio para sí o para otro, será sancionado con prisión de tres (3) a seis (6) años. Se impondrá el doble de la pena que le corresponda si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 11. Violación de privacidad de las comunicaciones. Quien mediante el uso de tecnologías informáticas acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de uno (1) a tres (3) años.

Artículo 12. Revelación indebida de datos o información de carácter personal. Quien sin la debida autorización revele, difunda o ceda, en todo o en parte, hechos descubiertos, imágenes, audio, así como cualquier dato o información obtenidos de manera ilícita por instrumentos de tecnología informática será sancionado con prisión de dos (2) a seis (6) años.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de una tercera parte.

Artículo 13. Acoso por medios cibernéticos. Comete el delito quien en forma deliberada, sin autoridad o excediendo la que posea, sin el debido permiso, de forma recurrente acosare a una persona, a través de ataques personales o la divulgación de información confidencial o falsa, por medio de sistemas informáticos o cualquier medio de comunicación electrónico, será sancionado con prisión de uno (1) a tres (3) años.

CAPITULO VI

BENEFICOS JURÍDICOS Y SOCIALES

6.1 BENEFICIOS

6.1.1 Definición

“La palabra Beneficio es un término genérico que define todo aquello que es bueno o resulta positivo para quien lo da o para quien lo recibe, entiéndase como un beneficio todo aquello representativo del bien, la cuestión enmarca una utilidad la cual trae consecuencias positivas que mejoran la situación en la que se plantean las vicisitudes o problemas a superar. Un beneficio es obtenido de cualquier manera y para poder identificarlos es necesario aplicar el concepto a cualquier campo en específico. Los más comunes son los económicos y sociales, los cuales producen elementos que son beneficiosos en ambos sentidos (para quien lo da o para quien lo recibe). Proveniente del latín “benefician” se deriva de Benedicto, bendición, bien, por lo que es claro que lo que representa son acciones positivas y realmente buenas. Un beneficio aporta a quien los recibe, felicidad, tranquilidad, paz y alegría, puesto que están dispuestos a satisfacer las necesidades de los que lo desean.”[33]

En este sentido, en cuanto al tema objeto de estudio los beneficios se ven configurados en dos formas específicas, en primer lugar se pueden establecer beneficios jurídicos

[33] https://conceptodefinicion.de/beneficio/

que traen consigo, la estructuración de un cuerpo legal capaz de regular y tipificar los delitos informáticos, por otra parte los beneficios sociales que se enfocan en el bien que se confiere a la sociedad en general, es decir, a través de un ordenamiento vigente se logra la tutela de bienes jurídicos y en consecuencia la protección de derechos, tanto a personas individuales como jurídicas, quienes son los sujetos que se encontrarían bajo la esfera de protección al momento de aprobarse la ley que regule los delitos informáticos o ciberdelitos.

Los beneficios ya sean jurídicos o sociales únicamente se verán materializados en el momento que los organismos estatales correspondientes conviertan en realidad, lo que hasta la fecha únicamente han sido propuestas, para lograr un cambio sustancial en la actual situación política, institucional y legislativa de la Nación.

6.2 BENEFICOS JURÍDICOS

6.2.1 Prevención de la delincuencia informática

Actualmente la lucha contra la ciberdelincuencia se ve marcada por una gran cantidad de dificultades, como la sofisticación de las actividades ilícitas, por lo que el Estado debe implementar herramientas legales necesarias para perseguir a los delincuentes. Enfocarse en la actualización del derecho penal de forma que sea capaz de dar una respuesta inmediata a las amenazas que plantean los delincuentes informáticos.

Al momento de crearse y aprobarse la ley que regule los delitos informáticos, se estarían llenando los vacíos jurídicos en cuanto a estas actividades ilícitas, lo que le daría la capacidad al sistema de justicia para aplicar estrategias de prevención eficaces contra los ataques presentes o futuros.

Por lo que la prevención se dirige a la implementación de medidas o la realización de acciones tendientes a evitar una conducta o comportamiento que puede dañar y convertir a las personas en víctimas de un ilícito.

La prevención de los delitos informáticos se da desde diversos ámbitos, en primer lugar como forma de control por parte del sistema de justicia, es decir, un medio de control que evite la comisión de actividades ilícitas relacionadas con la informática, la

prevención se materializa a través de campañas de difusión de información u orientación a la ciudadanía sobre que conductas son consideradas como ciberdelitos, formas de protección, a que órganos acudir al momento de ser víctimas de un ilícito, así también por medio del fortalecimiento de las entidades responsables de llevar a cabo la persecución de los delitos, brindándoles la capacidad para la investigación cibernética.

Otro de los entornos que en los cuales cobra relevancia la prevención de los delitos informáticos es el sector empresarial o institucional, ya que las empresas son las primeras en buscar estrategias de prevención, entre las cuales se pueden mencionar la inclusión de cláusulas especiales en los contratos de trabajo con el personal informático, establecer un código ético de carácter interno en la empresa, la adopción de rigurosas medidas en el acceso y control de las áreas de informática, capacitación adecuada al personal informático y el control de las claves de acceso a los sistemas.

Por último el sector más importante al hablar de prevención es la sociedad en general, es decir los usuarios comunes, que en su gran mayoría hacen uso de los medios tecnológicos para desarrollar sus actividades y quienes se encuentran más vulnerables frente a estos ilícitos penales, las principales formas por las cuales se logra una prevención eficaz son:

- La utilización de contraseñas seguras;
- El empleo de doble factor de autenticación para servicios en línea, como el correo electrónico o la banca en línea;
- La elaboración de respaldos de forma periódica y el almacenamiento de estos en discos externos;
- La verificación de correos de origen desconocido;
- Constatar operaciones de comercio electrónico;
- Comprobación del nivel de confidencialidad de los sitios web y la seguridad de la conexión.
- Especial Cuidado en el tipo de información personal se comparte en las redes sociales.

6.2.2 Sanción de los Delios Informáticos

La sanción en términos generales es la prohibición determinada en la legislación, aplicable a quienes la incumple. También conocida como la consecuencia del delito o pena.

Al hablar de los delitos informáticos la sanción es la medida impuesta por el Estado, ante la lesión de un bien jurídico (la información ya sea personal o institucional, el patrimonio o la intimidad), el cual es previamente protegido por una ley específica en esta materia. Se trata de un castigo impuesto a los ciberdelincuentes, como consecuencia de la comisión de una conducta jurídicamente reprochable (acceso ilícito, daño informático y violación de datos personales). Esa sanción tiene como finalidad el cumplimiento de las normas, incluso resarcir el daño causado y una pena al haberse lesionado el bien jurídico.

La creación, aprobación y aplicación de la ley que regule los delitos informáticos crea las condiciones necesarias para establecer la lucha contra este tipo de ilícitos, ya que los autores de estos delitos podrán ser identificados, investigados, llevados a juicio y un tribunal competente imponer la sanción más adecuada.

Por lo anterior se contemplan gran diversidad de beneficios bastante positivos para la sociedad, que son los objetivos en los que se fundamenta la aplicación coercitiva de la pena. La cual puede ser prisión, arresto o multa, tomando en consideración las iniciativas de ley en materia de delitos informáticos o ciberdelitos que se han presentado al Congreso de la República, estas coinciden en las penas a imponer, siendo la pena de prisión que va desde 1 a 12 años y la pena de multa que va de Q. 10,000.00 a Q. 300,000.00.

Una adecuada legislación logra efectos no solo coercitivos con la imposición de penas, si no como resultado a estas eventualmente efectos preventivos de dos maneras:

- Prevención general: Dirigida la sociedad en su conjunto, logrando a través de la imposición de una pena, una coacción psicológica con la cual se amenaza a los potenciales delincuentes se abstengan a delinquir.

- Prevención especial: Se limita al delincuente que es condenado y consecuencia cumple una condena en un centro preventivo, con lo cual se busca impedir que vuelva a cometer un delito.

Dado lo anterior, con la prevención y sanción de los delitos informáticos se envía un claro mensaje disuasivo a los autores potenciales de ataques contra los sistemas de información, de esta manera se reducirían en gran medida este tipo de acciones que provocan un sinfín de daños a intereses individuales, sociales, incluso gubernamentales. Los beneficios se ven reflejados en la creación de un espacio de libertad, seguridad y justicia, el cual se logra con la eficiente lucha contra la delincuencia informática, no solo a nivel nacional sino también internacional, a través de la cooperación política y judicial, en virtud del carácter transnacional de este tipo de delitos.

6.2.3 Actualización del Sistema de Justicia

El sistema de Justicia en Guatemala se encuentra integrado por organizamos, entidades descentralizadas, autónomas y semiautónomas. La cabeza del sistema se ubica en la Corte Suprema de Justicia quien tiene a su cargo la administración del mismo, dentro de los demás organismos se encuentran Salas de la Corte de Apelaciones, Tribunales de Sentencia, Juzgados de Primera Instancia, Juzgados de Paz .

La actualización se refiere a la modernización de las técnicas, procedimientos o instrumentos empleados en la investigación y persecución en específico de los delitos informáticos. Ya que estas conductas ilícitas no conocen límites a medida que los medios tecnológicos empleados para cometerlos, se encuentran en constante evolución, por lo que se hace necesario contar con las herramientas científicas más modernas para hacer una persecución penal efectiva.

Al hablar de herramientas científicas, estas pueden consistir en equipo tecnológico, softwares, aplicaciones móviles, sistemas web, desktop, registro de huellas en cuestiones de seguridad para los equipos empleados por las entidades encargadas de la persecución penal y actualización constante de los equipos de cómputo.

Otro aspecto importante en la modernización del Sistema de Justicia es el elemento humano, es decir todas aquellas personas que laboran en las entidades encargadas de la investigación, persecución y juzgamiento de los sujetos que incurren en la comisión de delitos informáticos. A través del establecimiento de lineamientos, programas, actividades y contenidos tendientes a la profesionalización del personal de las instituciones de seguridad pública (Unidad de Cibercrimen de la Policía Nacional Civil), instituciones destinadas a la persecución penal (Ministerio Público) y el órgano encargado del juzgamiento (Organismo Legislativo). La profesionalización de las instituciones mencionadas se alcanzaría con la integración de programas de formación inicial y continua, que contemplen la actualización, especialización y alta dirección en ámbitos de delincuencia informática, logrando desarrollar en las personas involucradas capacidades, conocimientos, también habilidades para prevenir, detectar y sancionar los este tipo de delitos.

Por último la divulgación de las posibles conductas ilícitas derivadas del uso de la tecnología, la alerta hacia las potenciales víctimas para que tomen las precauciones necesarias a fin de prevenir este tipo de delitos y la creación de una adecuada legislación que proteja los intereses de la sociedad, más modernización y la preparación del personal encargado de la procuración, administración e impartición de justicia para atender e investigar los ciberdelitos, se lograría un avance inimaginable en el camino de la lucha contra la delincuencia informática, que cada día se expande.

6.2.4 Formas de Control de los Delitos Informáticos

El flujo nacional e internacional de datos aumenta progresivamente, lo que conlleva a la posibilidad creciente de hechos ilícitos en estas actividades, ya sea por el uso de las computadoras, a través de redes informáticas o por la interconexión de equipos de cómputo, es por ello que los delitos informáticos tienen la característica de ser de cuello blanco, es decir que son difíciles de detectar y de descubrir a los autores.

Ante esas dificultades las formas de control de los delitos informáticos son los principales medios por los que se intenta frenar los ataques contra los sistemas informáticos. El principal control es la legislación nacional e internacional, en primer

lugar la legislación nacional juega un papel trascendental, ya que al implementarse las adecuadas disposiciones jurídicas en el derecho penal sustantivo, se logra el establecimiento de la adecuada tipificación, prevención y sanción de este tipo de conductas ilícitas. Es forma de control que permite establecer que conductas específicamente constituyen delitos en este ámbito, la imposición de medias que motiven a los sujetos a no cometer este tipo de conductas contrarias a la ley, y la protección a intereses personales y sociales.

En segundo lugar la legislación internacional, constituida por todos aquellos convenios o acuerdos en materia de delitos informáticos creados como mecanismos de cooperación internacional para contrarrestar la incidencia de la criminalidad informática. Dado el carácter transnacional de estos delitos, la legislación internacional constituye acuerdos de ayuda mutua que buscan la unificación de las legislaciones en materia informática, así como la implementación de medidas adecuadas para su persecución.

Entre otras formas de control se pueden mencionar:

- La especialización de policías, fiscales, funcionarios judiciales en el campo de los delitos informáticos.
- La armonización entre leyes penales nacionales acerca de la investigación de delitos informáticos.
- La creación de estrategias para regular el acceso a los sistemas de información institucional o gubernamental.

6.3 BENEFICIOS SOCIALES

6.3.1 Bienes jurídicos tutelados

En cuanto a los beneficios sociales resultantes de la creación de la ley que regule los delitos informáticos los bienes jurídicos tienen gran relevancia, ya que constituyen los derechos, valores o atributos propios de las personas que deben ser protegidos por el Estado a través del Derecho Penal, esto quiere decir que ante la evidente ausencia de un cuerpo normativo específico en delitos informáticos, los bienes jurídicos vulnerados por este tipo de conductas ilícitas se encuentran en un total estado de indefensión.

Tomando en consideración que entre estos bienes jurídicos se pueden mencionar la integridad y disponibilidad de la información, el patrimonio, la reserva, confidencialidad e intimidad de datos contenidos en sistemas informáticos.

Es por lo anterior que se debe tener en consideración que al momento de crearse una ley específica en esta materia, se logran importantes beneficios sociales, los cuales se ven reflejados en distintos ámbitos. Entre estos la protección y seguridad que el Estado debe brindar a las personas, los cuales constituyen fines y deberes establecidos constitucionalmente, que deben ser cumplidos para lograr el bienestar de la sociedad en su conjunto o el bien común.

Así también, a través de la delimitación de los bienes jurídicos que son vulnerados por este tipo de conductas ilícitas, se logra el establecimiento de la fundamentación de las penas a imponer a quienes los lesionen, de acuerdo al grado de afectación que estos sufran. Lo que trae consigo la imposición de sanciones acordes para los sujetos responsables de las conductas ilícitas en materia informática, y por último la certeza a los ciudadanos que si fueren víctimas de un hecho ilícito de este tipo, dicha acción no quedaría impune, obteniendo la justicia que en muchos casos es reclamada por la sociedad en general.

6.3.2 Seguridad de la Información Personal e Institucional

En primer término la seguridad de la información está integrada por un conjunto de medidas encaminadas a la prevención y pronta respuesta frente a los ataques a la información, por medio de sistemas tecnológicos que permiten resguardar y proteger esta información.

En cuanto a la seguridad de la información personal, es importante hacer énfasis que para el hombre como individuo, la seguridad de su información tiene un gran efecto significativo en cuanto a su privacidad. Tomando en consideración la gran trascendencia que ha adquirido la información, la cual puede ser medida en función de su utilidad, importancia económica y que se constituye como un bien susceptible de apoderamiento, como tal requiere de tutela jurídica específica en razón de los diferentes derechos y obligaciones que derivan de la misma.

Al ser los medios tecnológicos como las computadoras, los instrumentos que permiten un manejo rápido y eficiente de grandes volúmenes de información, facilitan la concentración de datos, por lo que al tener un gran valor o constituirse como un poder, es susceptible de ser mal utilizada, divulgada, robada, borrada o saboteada, lo que trae consigo afecciones en cuanto a su disponibilidad.

La seguridad se ve manifestada a través de aspectos específicos como:

- Confidencialidad que se refiere al poder de impedir la divulgación de la información a individuos, entidades o procesos no autorizados, es decir que asegura el acceso a esta, solamente a quienes tengan la debida autorización.
- Integridad que permite el manteniendo de la información o datos libres de modificaciones no autorizadas.
- Disponibilidad de la información únicamente a quienes deben accede a ella, ya sean personas, procesos o aplicaciones.

Cada persona es responsable de la información personal que quiere divulgar a través de las redes sociales, o aquella que tiene almacenada en sistemas informáticos o medios tecnológicos, por lo que el conocimiento de los efectos lesivos hacia esta, es de vital importancia para no verla vulnerada a través de una actividad ilícita, así también contar con herramientas tecnológicas que le permitan protegerla de ataques, constituye la principal forma de resguardarla.

Al hablar de seguridad de la información institucional, se debe determinar que está constituida por todos aquellos datos confidenciales que pueden pertenecer a una empresa (clientes), sistemas financieros (la banca) o incluso gubernamentales (decisiones de Estado, proyectos y programas).

El objetivo de la protección no son los datos en sí mismo, sino el contenido de la información, que es principal motor para la implementación de medidas de seguridad por parte de las instituciones. Estas medidas deben ser encaminada a la protección de la privacidad digital, para evitar el acceso no autorizado a los datos o información que se pueda encontrar en ordenadores, bases de datos o sitios web.

La tecnología constituye una poderosa herramienta para el cumplimiento de la gestión institucional e interinstitucional de la Administración Pública, por lo que el gobierno debe otorgar mayor atención a la protección de la información, a través de la implementación de estándares de seguridad que garanticen la protección y en esta medida generar confianza en la ciudadanía, en las propias instituciones y minimizar riesgos derivados de vulnerabilidades informáticas.

Sin embargo a la fecha Guatemala no cuenta con un ordenamiento jurídico eficaz para penalizar las acciones que provoquen perjuicios tanto a la información personal como institucional contenida en medios informáticos, por lo que no puede garantizar la debida protección a la ciudadanía, mucho menos confianza. Únicamente en el presente año 2018 se ha creado la Estrategia Nacional de Seguridad Cibernética, que se articula como un instrumento de seguridad de la Nación para mitigar los riesgos y amenazas provenientes del ciberespacio, por medio de estrategias de protección y la creación de un Comité Técnico de Seguridad Cibernética.

6.3.3 Protección de Equipos Tecnológicos

Con el aumento de la implementación de la tecnología informática en los diferentes ámbitos de la vida cotidiana, se debe tener un control sobre los posibles elementos de daño contra los datos que se procesen, redes, internet y softwares, con el objetivo de mantener la integridad, disponibilidad y confidencialidad de los datos y de los equipos en donde se desarrollen y almacenen estos datos.

En este sentido hablar de protección de equipos tecnológicos es referirse a la Ciberseguridad, la cual se enfoca en la protección de la infraestructura de una computadora, todo lo relacionado con esta y en especial la información contenida en ella o aquella que circula a través de las redes de computadoras.

Debido a la dependencia de los sistemas informáticos, estos se hacen cada vez más vulnerables a ciberataques, por lo que los problemas de seguridad no pueden ser resueltos únicamente con un programa por más sofisticado y completo que parezca, sin embargo existen medios de protección para los equipos como antivirus, firewall, el control de contenidos web, antiespias, entre otros.

El factor humano juega un papel importante ante la evidente carencia en nuestro medio de un ordenamiento jurídico específico en materia penal, que regule conductas en cuanto al acceso ilícito a la seguridad de los equipos tecnológicos, por lo que se deben implementar estrategias de seguridad por medio de los programas adecuados como claves de identidad, firma digital y antivirus.

Si bien el asunto de seguridad no es algo que depende únicamente de los programas que vigilan los equipos computacionales y las personas, un fuerte marco jurídico logra prevenir los posibles ataques, esta prevención se da a través del condicionamiento de las personas que al momento de cometer una actividad ilícita contra la seguridad un equipo tecnológico, estos se enfrentarían a una sanción específica que puede llegar hasta el encarcelamiento en un centro preventivo. Sin embargo en ese ordenamiento jurídico deben existir tipificadas las conductas propias o adecuadas para definirlas como ataques a la seguridad de los equipos tecnológicos, tarea que le corresponde al Sistema Legislativo, la cual debe llevar a cabo con eficacia.

Por lo que al implementarse la Ley que regule los delitos informáticos, se obtienen beneficios en este sentido, logrando una protección adecuada y seguridad a las personas que ante cualquier posible ataque cuentan con un instrumento jurídico que les brinde la confianza de esas conductas serán sancionadas y los ataques por parte de los ciberdelincuentes verse reducidos.

CAPÍTULO VIII

PRESENTACIÓN DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN

7.1 ENCUESTAS

Modelo de la boleta de Encuesta

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE OCCIDENTE
DIVISION DE CIENCIAS JURIDICAS Y SOCIALES
CARRERA ABOGADO Y NOTARIO

BOLETA DE ENCUESTA

La presente boleta de encuesta tiene como objeto recabar datos de campo relativos a la tesis denominada: PRINCIPALES BENEFICIOS JURÍDICOS Y SOCIALES DE LA CREACIÓN DE LA LEY QUE REGULE LOS DELITOS INFORMÁTICOS, que se presenta como requisito previo a la obtención de los Títulos Profesionales de Abogado y Notario y del Grado Académico de Licenciado en Ciencias Jurídicas y Sociales. Se hace de su conocimiento que la información que usted brinde será tratada en forma confidencial y utilizada única y exclusivamente para fines académicos. Al agradecer el favor de su atención se le ruega marcar con una "X" la opción que considere correcta y ampliar cuando el caso así lo amerite.

Ciudad de Quetzaltenango, octubre de 2018.

Profesión: _____

Sector Laboral: Publico_____ Privado_____

1 ¿Sabe que es un delito?

SI_____ NO_____

2 ¿Tiene conocimiento de que es un delito informático?

SI_____ NO_____

3. ¿Considera que en Quetzaltenango se Comenten Delitos Informáticos?

SI_____NO_____

4. ¿Conoce si existe alguna ley que regule los delitos informáticos en Guatemala?

SI_____ NO_____

5. ¿Cómo profesional le perjudica la no existencia de una ley especial que regule delitos informáticos?

SI_____NO_____ POR QUE_____

_____

6. ¿Qué tipo de conductas considera que pueden provocar cometer un delito informático?

a) Robo de Información ☐
b) Manejo inadecuado de software ☐
c) Introducción de datos falsos en un software ☐
d) Alteración de documentos almacenados en forma computarizada ☐
e) Ingreso fraudulento a un sistema de cómputo o una red ☐

7. ¿Conoce algún órgano que sancione esas conductas actualmente en Quetzaltenango?

SI_____ NO_____ CUAL_____

8. ¿Qué tipo de información puede ser vulnerada ante un delito informático?

a) Información Pública ☐
b) Información Privada ☐
c) Información Personal ☐
d) Información Institucional ☐

9. ¿Ha sido víctima de alguna conducta que encuadre en un delito informático?

SI_____ NO_____ CUAL_____

10. ¿Cree necesario crear una ley que regule los delitos informáticos?

SI_____ NO_____

11. ¿Se consideraría protegido al crearse la ley que regule los delitos informáticos?

SI_____ NO_____

12. ¿A quiénes considera beneficiados con la creación de la ley que regule los delitos informáticos?

_____

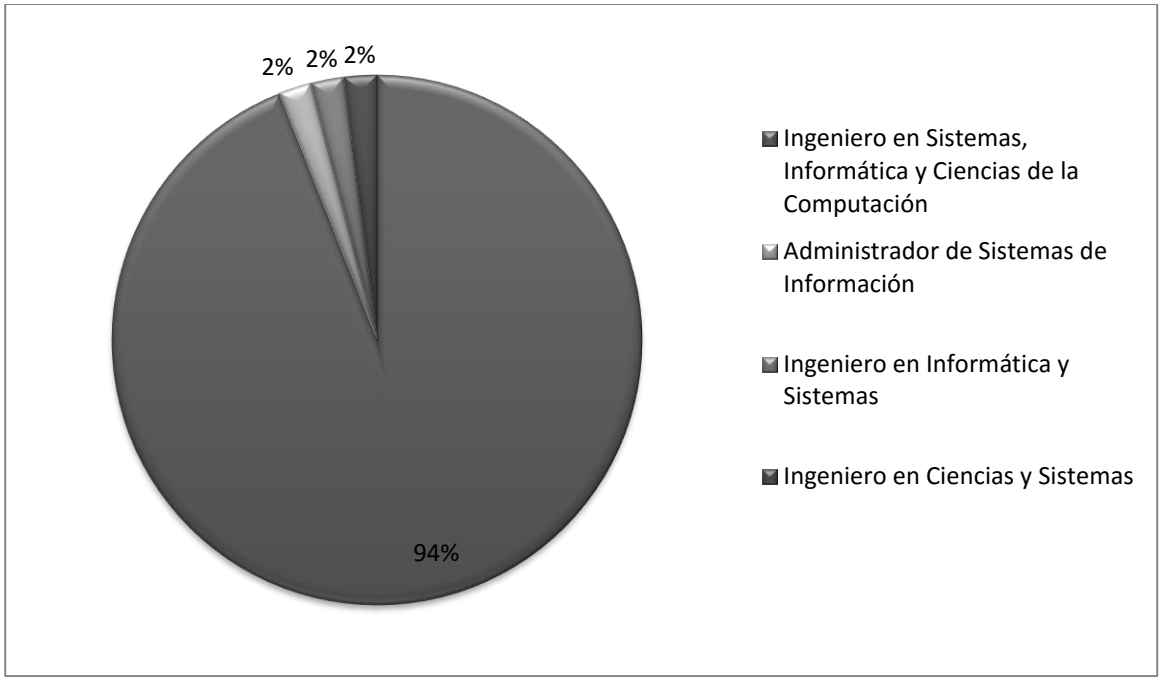
13. ¿Considera que al crearse la Ley que regula los delitos informáticos se contribuya a la prevención y combate del cibercrimen?

SI_____NO_____

"ID Y ENSEÑAD A TODOS "

7.2 GRÁFICAS Y ANÁLISIS DE RESULTADOS

PROFESIÓN

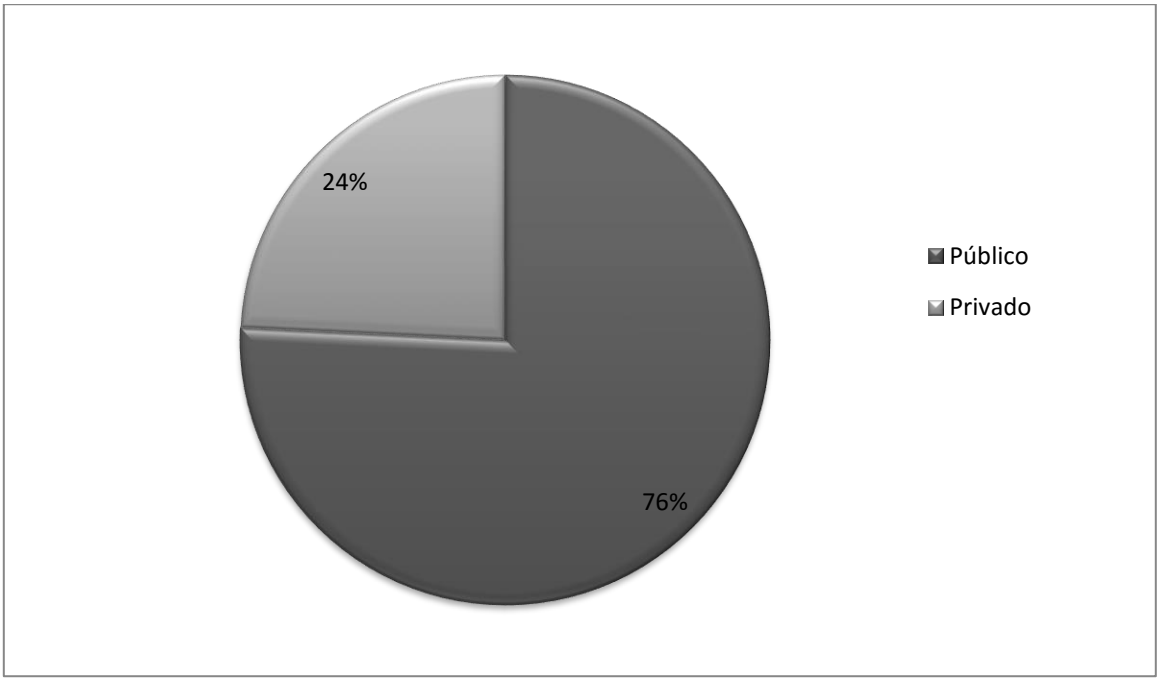


INTERPRETACIÓN

Para realizar la encuesta se tomaron en consideración únicamente Ingenieros en sistemas, sin embargo como lo manifestaron los mismo, dependiendo la Universidad de la cual estos egresaron así cambia la denominación a la carrera, por lo que del total de personas encuestada (50) el 94% que representa a 47, son Ingenieros en Sistemas, Informática y Ciencias de la Computación, el 2% que representa 1 es Administrador de Sistemas de Información, el 2% que representa 1 es Ingeniero en Informática y Sistemas, el 2% que representa 1 es Ingeniero en Ciencias y Sistemas.

SECTOR LABORAL:

Publico_____ Privado_____

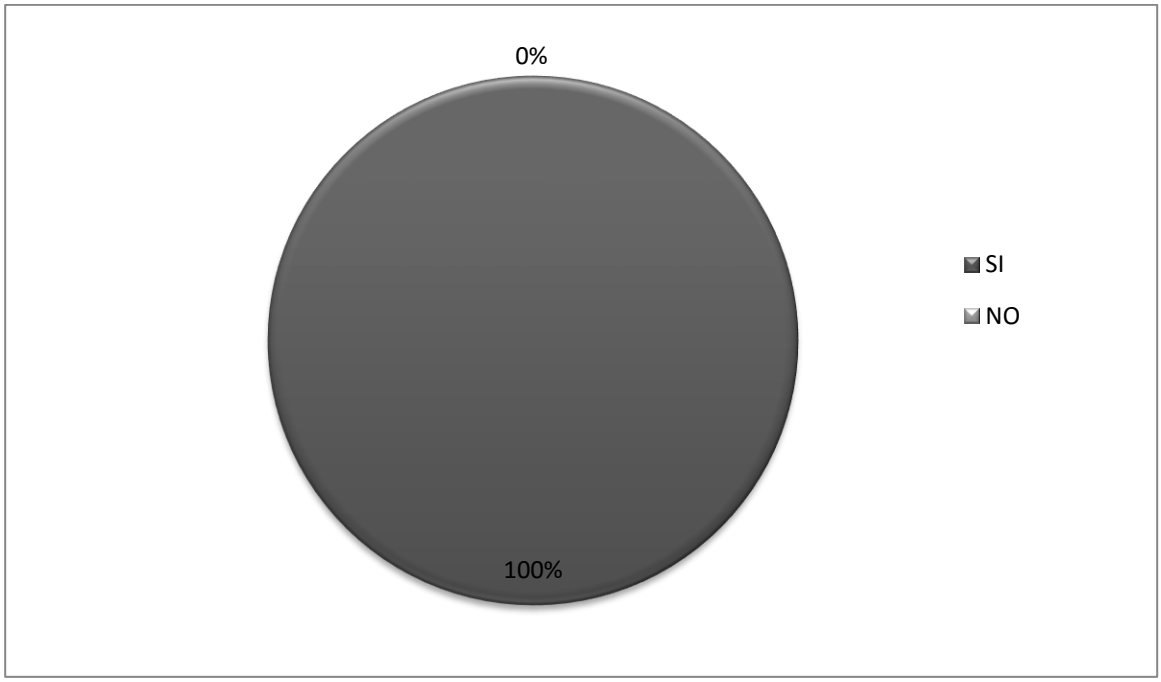


INTERPRETACIÓN

Del total de personas encuestadas el 76 % que representa 41 Ingenieros en Sistemas laboran en el sector privado, quienes constituyen la mayoría; mientras que el 21% que representan 9 Ingenieros en Sistemas laboran el sector público, dado lo anterior el campo privado es más accesible para que estos desempeñen sus labores.

1. ¿Sabe qué es un delito?

SI_____ NO_____

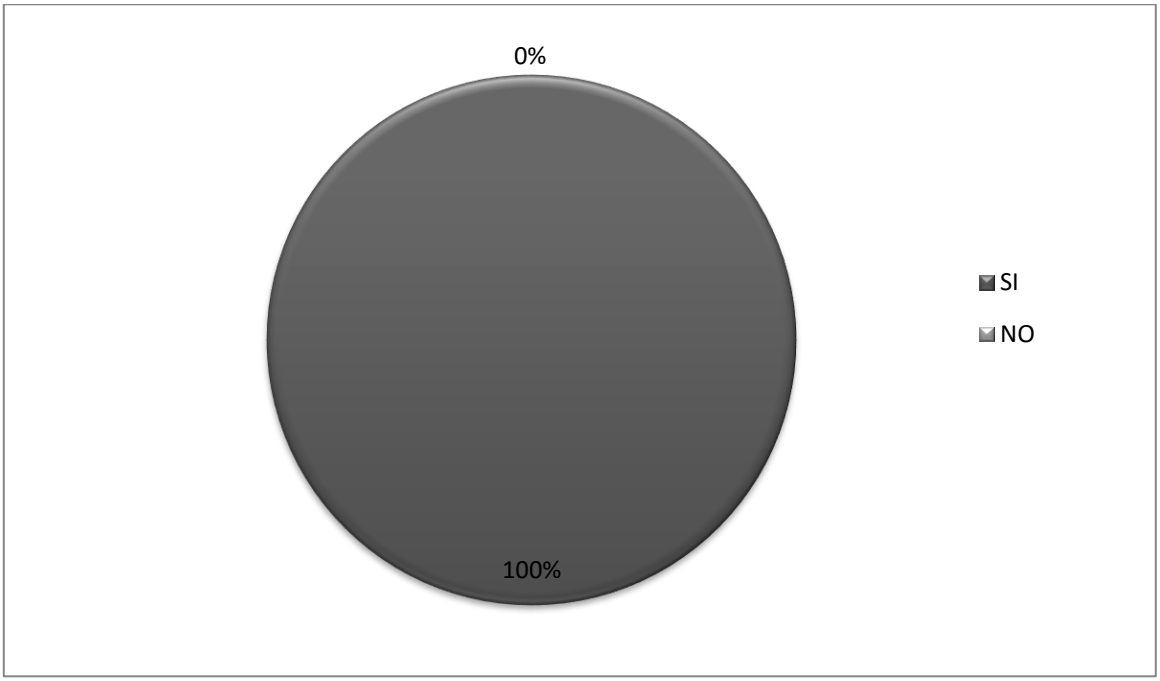


INTERPRETACIÓN

La grafica anterior nos demuestra que el 100% del total de personas encuestadas tiene conocimiento de lo que es un delito, es decir que manejan perfectamente el concepto de comisión de una conducta ilícita o contraria a la ley y la sanción correspondiente a la misma.

2. ¿Tiene conocimiento de que es un delito informático?

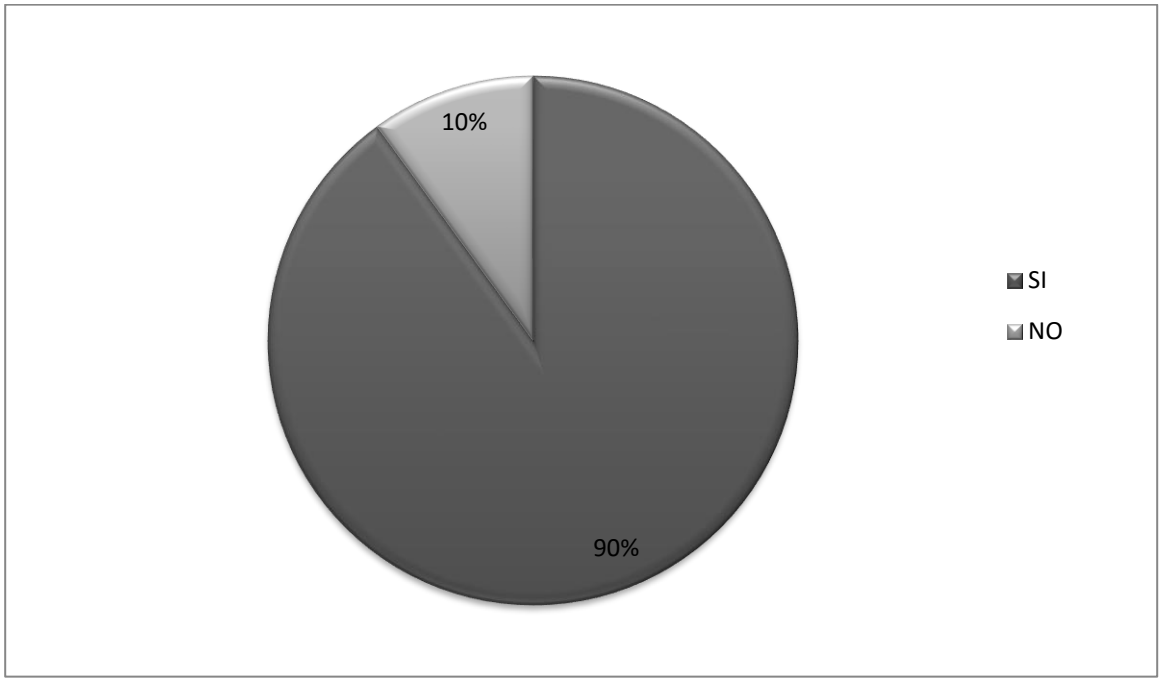
SI_____ NO_____



INTERPRETACIÓN

Con respecto a la pregunta realizada el 100% del total de Ingenieros encuestados, conocen lo que es un delito informático, es decir, que tomando en consideración la profesión que ejercen, estos manejan perfectamente los temas informáticos y las conductas contrarias al buen actuar de las personas en este tipo de campo.

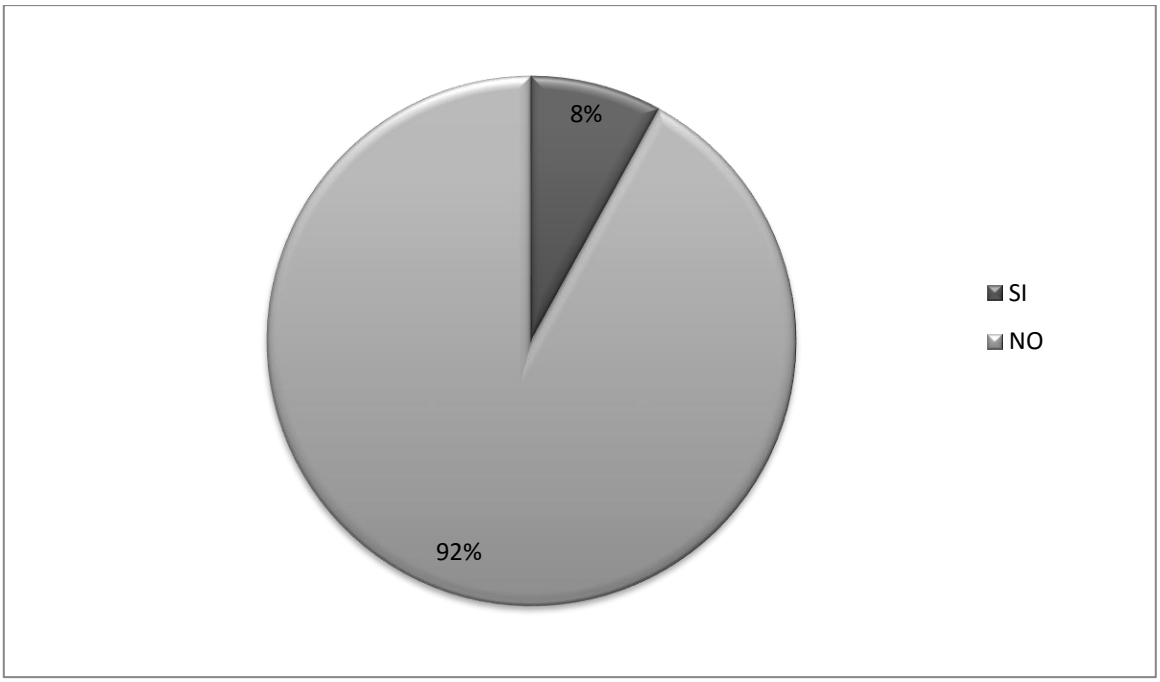
3. ¿Considera que en Quetzaltenango se comenten Delitos Informáticos?
SI_____NO_____



INTERPRETACIÓN

Como lo reflejan los resultados anteriores y lo indica la gráfica el 90% de los encuestados que representa 45 Ingenieros en Sistemas, considera que en el municipio de Quetzaltenango, si se comenten conductas que pueden considerarse delitos informáticos, mientras que el 10% que representa a 5, mantiene la creencia que no se dan ese tipo de conductas ilícitas. El criterio de la comisión de estos ilícitos, se observa en la mayoría de la población, tomando como base que en el municipio se tiene fácil y rápido acceso a los medios informáticos.

4. ¿Conoce si existe alguna ley que regule los delitos informáticos en Guatemala?
SI_____ NO_____



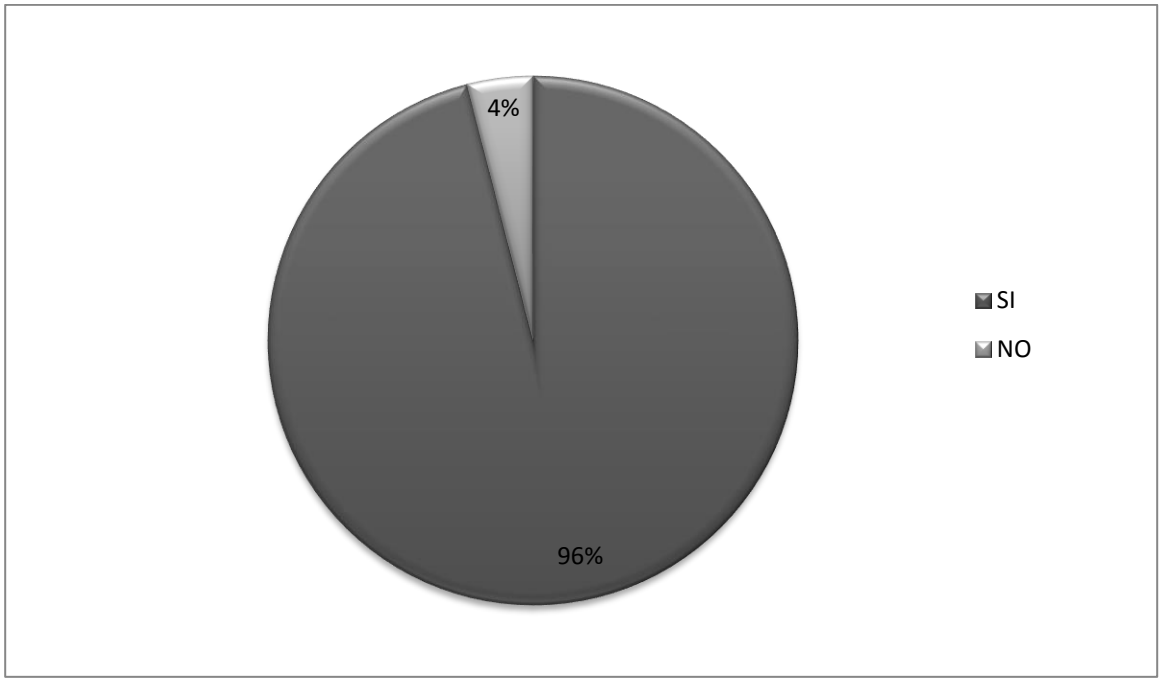
INTERPRETACIÓN

En esta interrogante el 92% que representa a 46 de los ingenieros encuestados establecen el desconocimiento de un cuerpo normativo que regule los delitos informáticos, es decir que para ellos no existe tal ley, por otro lado en 8% que representa a 4, expresa que si conocen una ley que regula los delitos informáticos, sin embargo es importante aclarar que los encuestados se refirieron a las iniciativas presentadas al Congreso de la República y a los delitos establecidos en el Código Penal vigente.

5. ¿Cómo profesional le perjudica la no existencia de una ley especial que regule delitos informáticos?

SI_____NO_____

PORQUE_____

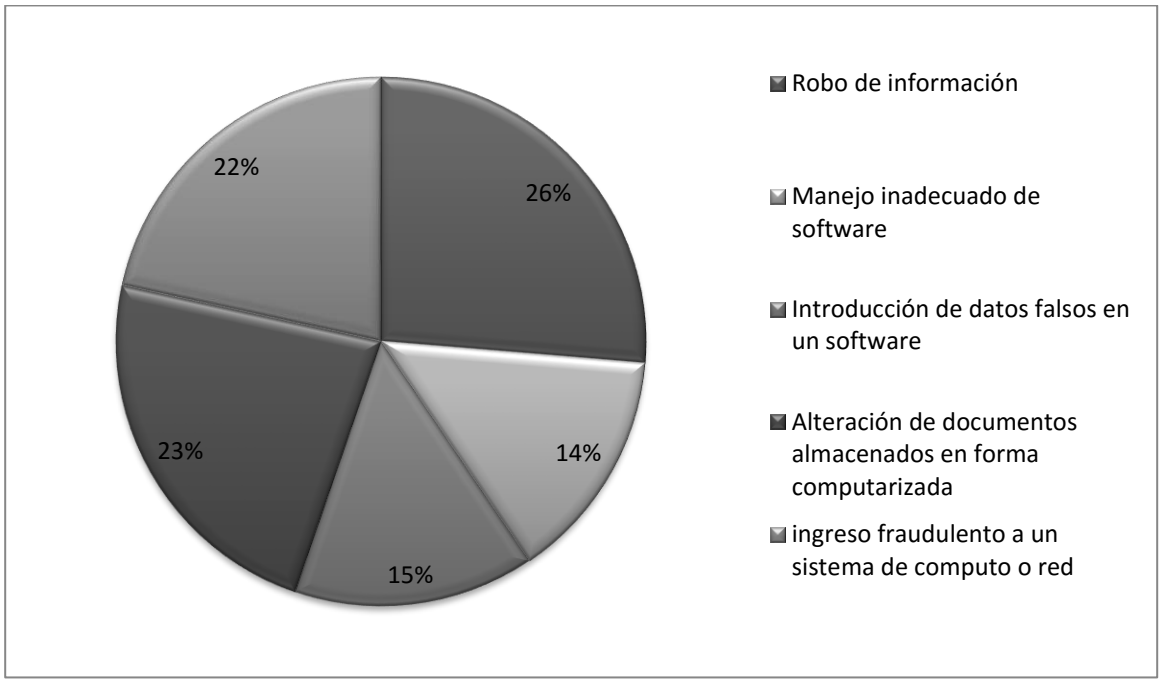


INTERPRETACIÓN

Los encuestados en un 96% que representa a 48 Ingenieros en Sistemas, consideran que al no existir una ley especial que regule los delitos informáticos se ven perjudicados en mayor medida en el desenvolvimiento de sus labores profesionales, ya que es un campo que no cuenta con normas adecuadas que brinden protección tanto a los datos, información contenida en ordenadores, sistemas, así como todas aquellas conductas que vulneren el trabajo que ellos realizan. El 4% que representa a 2, considera que como profesional no se ve afectado frente a la ausencia de un marco legal en delitos informáticos.

6. ¿Qué tipo de conductas considera que pueden provocar cometer un delito informático?

f) Robo de Información
g) Manejo inadecuado de software
h) Introducción de datos falsos en un software
i) Alteración de documentos almacenados en forma computarizada
j) Ingreso fraudulento a un sistema de cómputo o una red



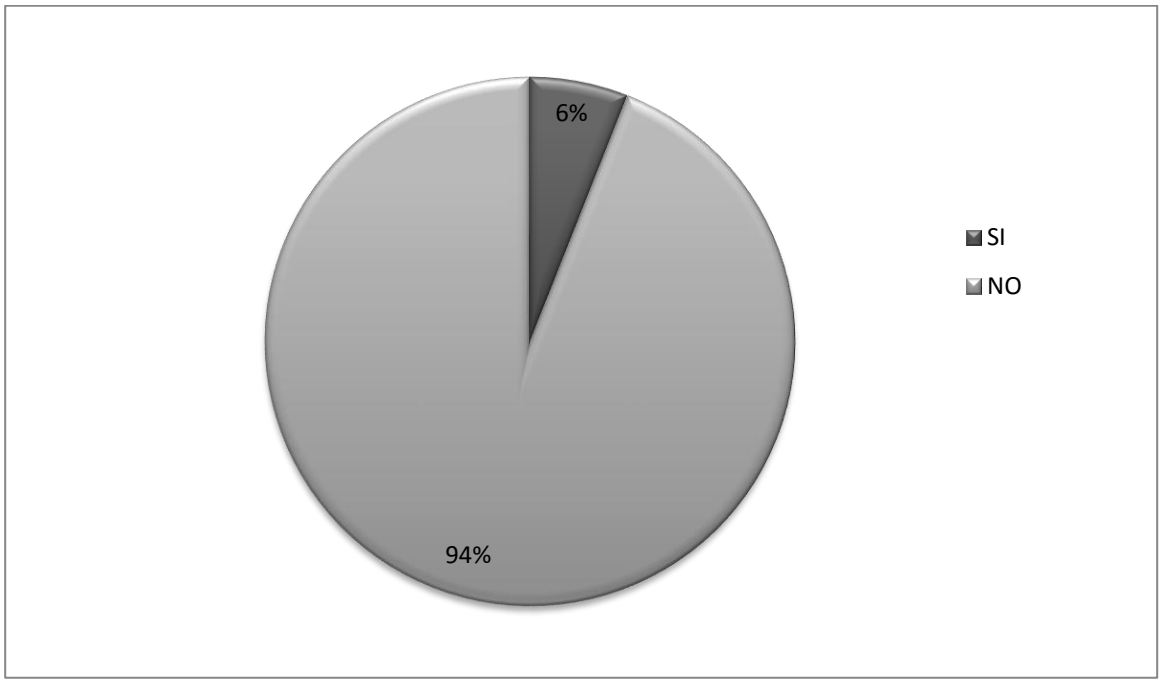
INTERPRETACIÓN

Según la gráfica todas las conductas mencionadas en la encuesta pueden ser consideradas delitos informáticas, sin embargo unas tienen mayor incidencia que otras, estableciendo los porcentajes de la siguiente forma:

Robo informático	26%
Alteración de documentos almacenados en forma computarizada	23%
Ingreso fraudulento a un sistema de cómputo o red	22%
Introducción de datos falsos en un software	15%
Manejo inadecuado de software	14%

7. ¿Conoce algún órgano que sancione esas conductas actualmente en Quetzaltenango?

SI_____ NO_____
CUAL_____

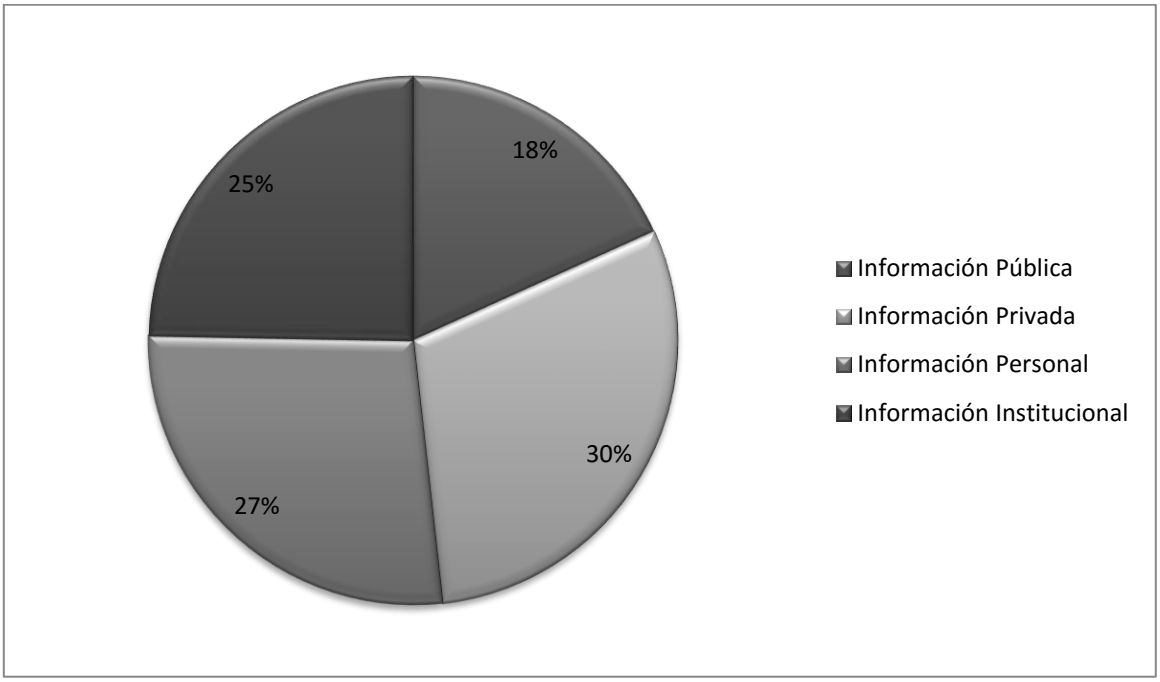


INTERPRETACIÓN

La gran mayoría de Ingenieros encuestados desconoce la existencia de algún órgano judicial capaz de sancionar en el municipio de Quetzaltenango los delitos informáticos, constituyendo tal cifra el 94% que representa 47 del total, mientras que el 6% que representa a 3, si conoce de un órgano, dentro de estos órganos fueron mencionados el Ministerio Público y la Unidad de Delitos Informáticos de la Policía Nacional Civil, la única que actualmente funciona.

8. ¿Qué tipo de información puede ser vulnerada ante un delito informático?

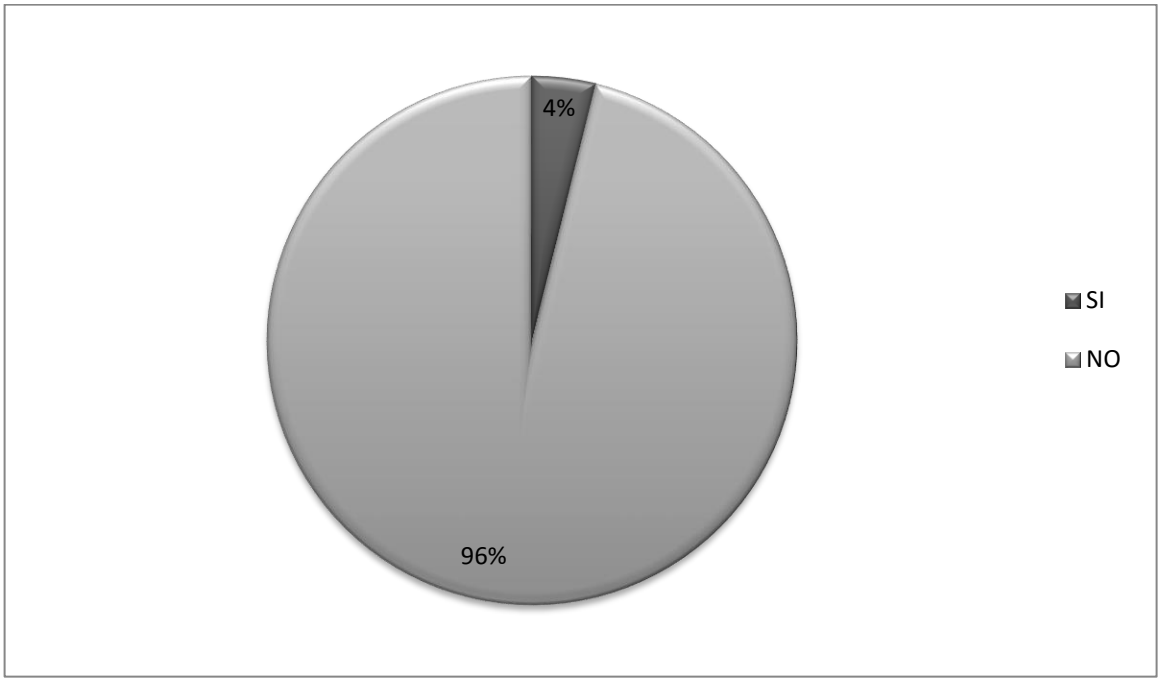
e) Información Pública
f) Información Privada
g) Información Personal
h) Información Institucional



INTERPRETACIÓN

En relación a los resultados que muestra la gráfica se puede apreciar que la información más vulnerada es la privada en un 30%, en segundo lugar la información personal en un 27%, en tercer lugar la información institucional en un 25% y por último la información pública en un 18%.

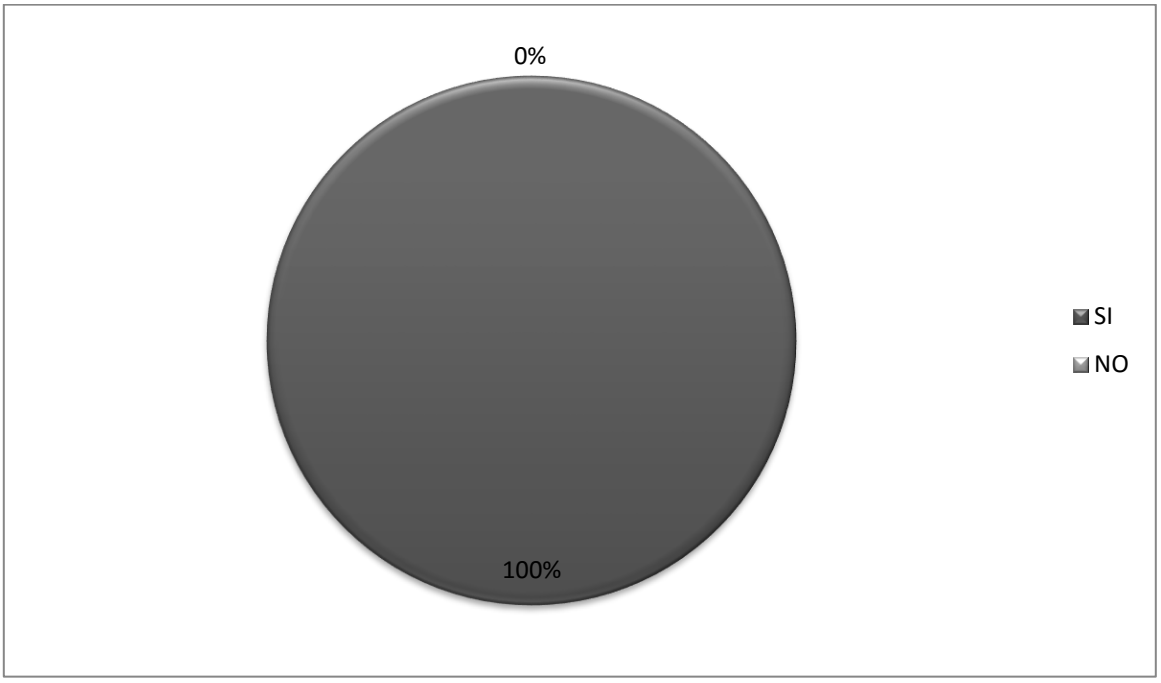
9. ¿Ha sido víctima de alguna conducta que encuadre en un delito informático?
SI_____NO_____ CUAL_____



INTERPRETACIÓN

La gran mayoría de los Ingenieros encuestados expresaron no haber sido víctima de delitos informáticos, constituyendo el 96% de estos que representa a 48, sin embargo únicamente el 4% que representa a 2, manifestó que si han sido víctimas de conductas ilícitas en materia informática, siendo estas el ciberacoso y Phishing o fraude informático.

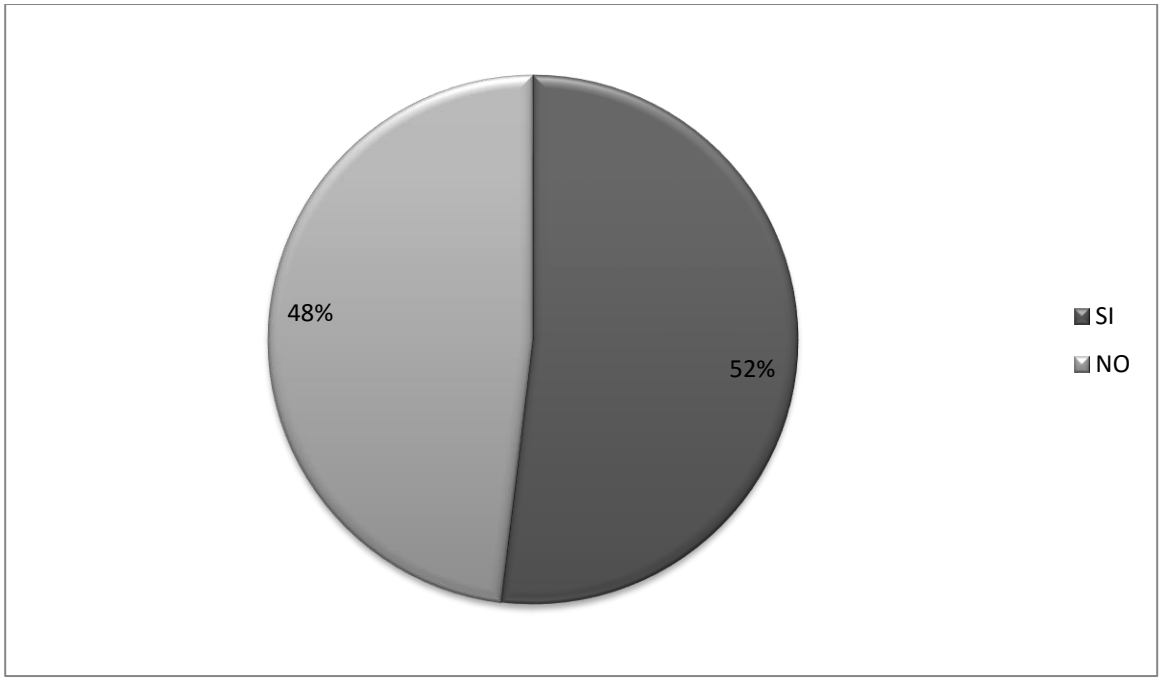
10. ¿Cree necesario crear una ley que regule los delitos informáticos?
SI_____ NO_____



INTERPRETACIÓN

Como lo muestra la gráfica el 100% del total de ingenieros encuestados, manifiestan la necesidad de crear una ley que regule los delitos informáticos, ya que en este campo la ausencia de normas específicas, traen consigo grandes perjuicios a los profesionales y usuarios.

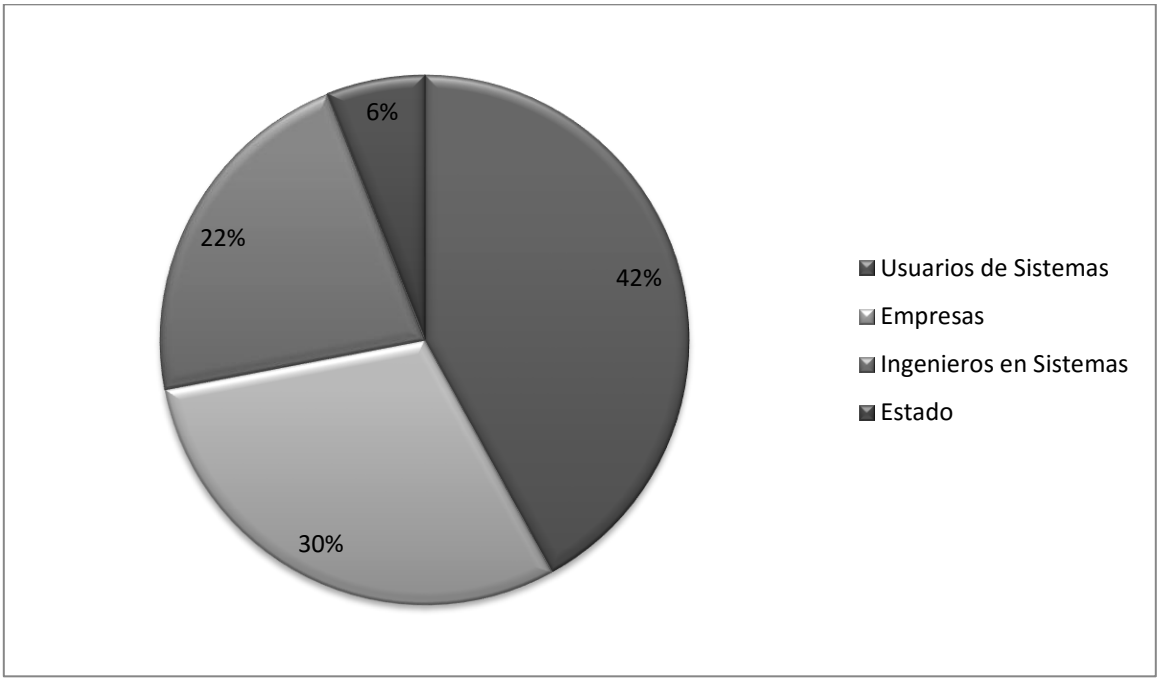
11. ¿Se consideraría protegido al crearse la ley que regule los delitos informáticos?
SI_____ NO_____



INTERPRETACIÓN

Con respecto a esta pregunta en los porcentajes de respuesta se pueden observar mínimas diferencias, ya que el 52% que representa a 26 Ingenieros en Sistemas considera que sí, mientas que el 48 % que representa a 24 considera que no. Lo que demuestra las deficiencias del Sistema de Justicia para investigar y sancionar los delitos a pesar de existir las normas.

12. ¿A quiénes considera beneficiados con la creación de la ley que regule los delitos informáticos?



INTERPRETACIÓN

Los principales beneficiados mencionados conforme a las respuestas obtenidas en la encuesta son:

Usuarios de Sistemas 42%

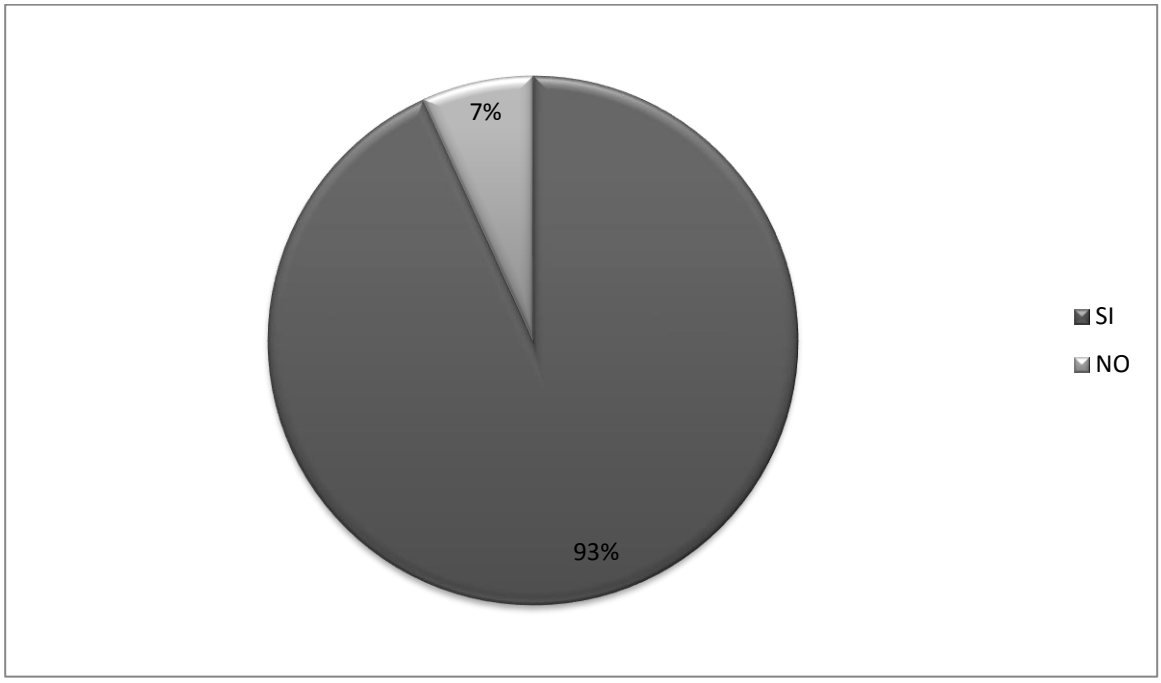
Empresas 30%

Ingenieros en Sistemas 22%

El Estado 6%

13. ¿Considera que al crearse la Ley que regula los delitos informáticos se contribuya a la prevención y combate del cibercrimen?

SI_____NO_____



INTERPRETACIÓN

Del total de Ingenieros en Sistemas encuestados 43 que representan el 93% confían que al crearse la ley que regule los delitos informáticos se propicia la prevención y combate del cibercrimen, mientras que 7 que representan el 7% no creen en estos efectos beneficiosos de la ley.

7.3 ENTREVISTAS REALIZADAS

Modelo de Entrevista

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE OCCIDENTE
DIVISIÓN DE CIENCIAS JURÍDICAS Y SOCIALES
CARRERA DE ABOGADO Y NOTARIO

GUIA DE ENTREVISTA

OBJETO DE ESTUDIO: “Principales Beneficios Jurídicos y Sociales de la Creación de la Ley que Regule los delitos informáticos.”

ENTREVISTADO: _____

CARGO: _____

FECHA DE LA ENTREVISTA:_____

1. ¿Considera que la actual legislación penal regula eficientemente los delitos informáticos?

2. ¿En su criterio que conductas se pueden considerar como delitos informáticos?

3. ¿En base a su conocimiento, considera que afecta el desconocimiento de la población hacia los delitos informáticos?

4. ¿Cuáles son los bienes jurídicos vulnerados al cometerse un delito informático?

5. ¿En su experiencia considera que es necesario crear una ley especial que regule los delitos informáticos?

6. ¿Cree necesaria una protección jurídica especializada para la lucha contra los delitos informáticos?

7. ¿Considera importante la protección de la información pública y privada y de esta manera motivar su inviolabilidad?

8. ¿Considera necesaria la actualización del sistema de justicia de Guatemala, al crearse la ley que regule los delitos informáticos?

9. ¿Cuáles serían los órganos que deben crearse para investigar y sancionar los delitos informáticos?

10. ¿De acuerdo a su experiencia ha recibido alguna denuncia o conocido al caso de una conducta que encuadre en un delito informático?

11. ¿En su criterio cuáles serían los principales beneficios Jurídicos de la creación de la ley que regule los delitos informáticos?

12. ¿En su criterio cuáles serían los principales beneficios Sociales de la creación de la ley que regule los delitos informáticos?

RESUMEN DE ENTREVISTAS REALIZADAS

Ingeniero IVAN GALINDO
Jede del departamento de Informática-INTECAP
Fecha de la Entrevista: 2 de octubre de 2018

1. ¿Considera que la actual legislación penal regula eficientemente los delitos informáticos?
   No, la legislación actual es insuficiente ya que solo existen propuestas pero no prosperan.

2. ¿En su criterio que conductas se pueden considerar como delitos informáticos?
   Todo lo que vaya en contra de la ética, en contra del bien, en contra de la verdad, en contra de la naturaleza del ser humano.

3. ¿En base a su conocimiento, considera que afecta el desconocimiento de la población hacia los delitos informáticos?
   No, porque nadie se percata de lo que sucede a su alrededor, solo les afecta cuando hayan sido agredidos.

4. ¿Cuáles son los bienes jurídicos vulnerados al cometerse un delito informático?
   La propiedad privada, datos o información personal, información financiera, producir contenido y que alguien más lucre con este sin autorización.

5. ¿En su experiencia considera que es necesario crear una ley especial que regule los delitos informáticos?
   Si, sobre todo para garantizar bienes informáticos y para proteger al sector productivo.

6. ¿Cree necesaria una protección jurídica especializada para la lucha contra los delitos informáticos?

   Tiene que ser así, es una realidad y muchas cosas que suceden nos afectan, como por ejemplo el robo de información o alteración de la información. Ya que se cometen delitos informáticos, y no existen estadísticas sobre esto, por lo que nada que nos defiende, porque no hay un fundamento legal.

7. ¿Considera importante la protección de la información pública y privada y de esta manera motivar su inviolabilidad?

   Esta información es importante debe estar resguardada, motivar que sea inviolable es difícil, pero debe existir algún reglamento que la proteja y que ayude a tomar decisiones con respecto a los responsables si llegara a pasar.

8. ¿Considera necesaria la actualización del sistema de justicia de Guatemala, al crearse la ley que regule los delitos informáticos?

   Si, por su puesto, actualmente no hay nada en este rubro, ni que evite delitos informáticos, tampoco legislación que promueva el desarrollo en este sector productivo.

9. ¿Cuáles serían los órganos que deben crearse para investigar y sancionar los delitos informáticos?

   Creación de un fiscal de informática, entidades en los distintos poderes del Estado, capacitaciones al Organismo Judicial.

10. ¿De acuerdo a su experiencia ha recibido alguna denuncia o conocido al caso de una conducta que encuadre en un delito informático?

    Si, una empresa privada con programadores coreanos, fueron acusados de hackeo, acudió el Ministerio de Gobernación y medios de comunicación, no sabían cómo actuar porque no existen normas, ningún abogado quería acudir porque desconocían el tema, el único que atendió el llamado únicamente participo como mediador, este expreso que el Ministerio de Gobernación no

podía investigar como si fuera escena del crimen, en ese momento los del Ministerio se fueron, el argumento era que solo el Ministerio Público puede hacer eso, los periodistas únicamente tomaron fotos a los monitores pero no sabían a qué le tomaban fotos, se complicó el tema al apagar los servidores por lo que el dueño de la empresa considero que se vulneraron sus derechos y él fue el que empezó a pedir justicia. Solo intentaron ponerse de acuerdo para resolver el problema, pero base legal nunca hubo

11. ¿En su criterio cuáles serían los principales beneficios Jurídicos de la creación de la ley que regule los delitos informáticos?
    Si hay una ley en el tema informático se pueden evidenciar y reducir estos hechos delictivos.

12. ¿En su criterio cuáles serían los principales beneficios Sociales de la creación de la ley que regule los delitos informáticos?
    Ante los cambios generacionales, como toda herramienta tienen sus beneficios y consecuencias, con una ley que atienda los delitos informáticos se esperaría q hubiera un menor deterioro en las personas que pertenecen a la sociedad guatemalteca

Licenciada Aurora Beatriz Gutierrez Andrade

Juez de Paz

Fecha de la entrevista: 9 de octubre de 2018.

1. ¿Considera que la actual legislación penal regula eficientemente los delitos informáticos?
   No, realmente la legislación guatemalteca tiene muy deficiente este tipo penal, no existe una normativa positiva.

2. ¿En su criterio que conductas se pueden considerar como delitos informáticos?
   Delitos tradicionales como robo, fraude, chantaje, falsificación, malversación, difamación, injuria, etc., de lo información pública de personas particulares, ya que surgen de la implementación y desarrollo de la programación y el internet.

3. ¿En base a su conocimiento, considera que afecta el desconocimiento de la población hacia los delitos informáticos?
   De gran manera la población desconoce de conductas no adecuadas y que violentan derechos como la privacidad, intimidad, libertad de pensamiento, y propiedad, porque consideran que el internet es una herramienta de protección y aliado a delinquir sin establecer la identidad.

4. ¿Cuáles son los bienes jurídicos vulnerados al cometerse un delito informático?
   La seguridad jurídica, bienes informáticos, patrimonio, intimidad personal,

5. ¿En su experiencia considera que es necesario crear una ley especial que regule los delitos informáticos?
   Crear una ley considero que no es necesario sino reformar adecuadamente el código penal, para fortalecer el tipo penal. Ya que la reforma 33-96 del Congreso de la Republica dejo en el aire muchas circunstancias que contiene los delitos informáticos que no se regularon

6. ¿Cree necesaria una protección jurídica especializada para la lucha contra los delitos informáticos?
   Considero que una fiscaliza especial con conocimientos y equipo adecuado para realizar la investigación.

7. ¿Considera importante la protección de la información pública y privada y de esta manera motivar su inviolabilidad?
   Si es importante, pero más que todo informar a la población el limite a la violación a la intimidad, y los riesgos que pueden existir del abuso a estos alcances informativos.

8. ¿Considera necesaria la actualización del sistema de justicia de Guatemala, al crearse la ley que regule los delitos informáticos?
   No considero necesario, pues la actualización del sistema de justicia de Guatemala no tiene relación con la creación de la Ley que regule lo delitos informáticos, pues la creación de leyes le corresponde al Organismo legislativo y el Organismo Judicial le corresponde Juzgar, es decir el sistema de justicia es distinto al sistema legislativo.

9. ¿Cuáles serían los órganos que deben crearse para investigar y sancionar los delitos informáticos?
   Realmente por parte del ente investigador, Ministerio Publico, sería una Fiscalía especializada en Delitos -Informáticos. Y de la misma manera la creación de un Juzgado Especializado para conocer este tipo de delitos que cuente con las instalaciones adecuadas para desarrollar el proceso penal.

10. ¿De acuerdo a su experiencia ha recibido alguna denuncia o conocido al caso de una conducta que encuadre en un delito informático?

Si he recibido denuncias, como chantajes, estafas, injurias, difamaciones.

11. ¿En su criterio cuáles serían los principales beneficios Jurídicos de la creación de la ley que regule los delitos informáticos?
    Que existiera un procedimiento y una claridad en el tipo penal de delito informático.

12. ¿En su criterio cuáles serían los principales beneficios Sociales de la creación de la ley que regule los delitos informáticos?
    El beneficio sería un mejor manejo de la programación y el uso adecuado del internet como de las redes sociales. Buscando la paz y la armonía de la sociedad.

Licenciada Karen Julissa Ramírez Samayoa

Abogada Litigante

Fecha de la entrevista: 10 de octubre de 2018.

1. ¿Considera que la actual legislación penal regula eficientemente los delitos informáticos?
   No, El decreto 17-73 regula muy pocos delitos informáticos y requiere de una actualización.

2. ¿En su criterio que conductas se pueden considerar como delitos informáticos?
   Todas las conductas que puedan atentar contra la privacidad y la integridad de las personas y los sistemas informáticos.

3. ¿En base a su conocimiento, considera que afecta el desconocimiento de la población hacia los delitos informáticos?
   Si, por el mismo desconocimiento realizan actitudes antijurídicas, sin saber que constituye un delito.

4. ¿Cuáles son los bienes jurídicos vulnerados al cometerse un delito informático?
   La intimidad, la privacidad, la seguridad, el patrimonio, la confidencialidad, la integridad, tanto de las personas como de los sistemas informáticos.

5. ¿En su experiencia considera que es necesario crear una ley especial que regule los delitos informáticos?
   Sí, es de carácter urgente aprobar una ley que regule estos delitos, el avance tecnológico es inminente y la necesidad de una ley especial es necesaria.

6. ¿Cree necesaria una protección jurídica especializada para la lucha contra los delitos informáticos?
   Si, definitivamente el conocimiento de esta rama es fundamental para luchar contra los delitos informáticos.

7. ¿Considera importante la protección de la información pública y privada y de esta manera motivar su inviolabilidad?
   Si, sobre todo tener conciencia de la cantidad de información que se maneja en redes sociales y cualquier sistema informático.

8. ¿Considera necesaria la actualización del sistema de justicia de Guatemala, al crearse la ley que regule los delitos informáticos?
   Si, la tecnología y los sistemas informáticos avanzan y así el sistema de justicia tiene que actualizarse y avanzar.

9. ¿Cuáles serían los órganos que deben crearse para investigar y sancionar los delitos informáticos?
   Unidades especializadas del Ministerio Publico que controlen Fraudes en el uso de las comunicaciones, Fraudes en Internet, Fraude Informáticos, fraudes de comercio electrónico, pornografía infantil y todas las conductas que surjan de este tipo de delitos.

10. ¿De acuerdo a su experiencia ha recibido alguna denuncia o conocido al caso de una conducta que encuadre en un delito informático?
    Si, una de publicidad indebida.

11. ¿En su criterio cuáles serían los principales beneficios Jurídicos de la creación de la ley que regule los delitos informáticos?
    El desarrollo de políticas de seguridad informática, la prevención de delitos informáticos, aumento de profesionales en la rama de la informática y un mejor manejo de información.

12. ¿En su criterio cuáles serían los principales beneficios Sociales de la creación de la ley que regule los delitos informáticos?

    La prevención de los daños que causan estos delitos a la integridad de las personas.

Ingeniero Enrique López

Ingeniero en Sistemas, desarrollador y docente de la Universidad Mesoamericana

Fecha de la Entrevista: 10 de octubre de 2018.

1. ¿Considera que la actual legislación penal regula eficientemente los delitos informáticos?
   Solo una parte, hace mención a ciertos actos, no contempla otras conductas como el hacking de información, suplantación de identidad, aspectos que en otros países si están regulados.

2. ¿En su criterio que conductas se pueden considerar como delitos informáticos?
   Suplantación de identidad, hackeo, robo informático de datos sensibles.

3. ¿En base a su conocimiento, considera que afecta el desconocimiento de la población hacia los delitos informáticos?
   Sí, no se le ha dato énfasis a esta área y por ejemplo en los hogares se da la piratería de softwares.

4. ¿Cuáles son los bienes jurídicos vulnerados al cometerse un delito informático?
   Lo referente a lo intelectual y la información.

5. ¿En su experiencia considera que es necesario crear una ley especial que regule los delitos informáticos?
   Sí, es importante dar ese paso.

6. ¿Cree necesaria una protección jurídica especializada para la lucha contra los delitos informáticos?
   Si la legislación creada lo necesitare.
7. ¿Considera importante la protección de la información pública y privada y de esta manera motivar su inviolabilidad?
   Sí, debe ser protegida, tener conocimiento de los riesgos.

8. ¿Considera necesaria la actualización del sistema de justicia de Guatemala, al crearse la ley que regule los delitos informáticos?
   Sí, es necesario.

9. ¿Cuáles serían los órganos que deben crearse para investigar y sancionar los delitos informáticos?
   Aquellos suficientemente capacitados en temas tecnológicos, con el personal adecuado.

10. ¿De acuerdo a su experiencia ha recibido alguna denuncia o conocido al caso de una conducta que encuadre en un delito informático?
    Solo he conocido casos en empresas privadas que los encargados de equipos informáticos al ser despedidos borran la información. Son conductas bastante recurrentes.

11. ¿En su criterio cuáles serían los principales beneficios Jurídicos de la creación de la ley que regule los delitos informáticos?
    Ponerle énfasis a la información que se resguarda.

12. ¿En su criterio cuáles serían los principales beneficios Sociales de la creación de la ley que regule los delitos informáticos?
    Regular el comportamiento a nivel empresarial, social, más educación y sensibilizar a los ciudadanos en cuanto a los riesgos.

Ingeniero Richard Mazariegos

Decano de la Facultad de Ingeniería de la Universidad Mesoamericana.

Fecha de la entrevista: 12 de octubre de 2018.

1. ¿Considera que la actual legislación penal regula eficientemente los delitos informáticos?
   No totalmente, hay varios elementos que no acoplan a la realidad actual de la tecnología y del país, tiene como consecuencia que lo que existe en la normativa penal no es suficiente para regular delitos informáticos.

2. ¿En su criterio que conductas se pueden considerar como delitos informáticos?
   El uso de datos sin el consentimiento del propietario, sin importar si se trata de una persona individual o jurídica.
   El uso de herramientas de sistemas de información para fines que tengan como objetivo dañar la integridad física de la persona, tanto en el entorno real como virtual.

3. ¿En base a su conocimiento, considera que afecta el desconocimiento de la población hacia los delitos informáticos?
   Si, la población debe estar informada para conocer que es un delito informático y que no lo es, que se puede hacer y que dentro de las tecnologías de la información.

4. ¿Cuáles son los bienes jurídicos vulnerados al cometerse un delito informático?
   Los datos que se encuentran en cualquier dispositivo tecnológico.
   El honor de las personas al generar contenidos virtuales que puedan perjudicar la imagen de las personas.

5. ¿En su experiencia considera que es necesario crear una ley especial que regule los delitos informáticos?

Si, se debe encajar correctamente que constituye un delito informático y posteriormente regularlo, tomando en cuenta que la tecnología es cambiante, deben ser normas acordes.

6. ¿Cree necesaria una protección jurídica especializada para la lucha contra los delitos informáticos?
   Si, deben ser normas adecuadas a los cambios tecnológicos.

7. ¿Considera importante la protección de la información pública y privada y de esta manera motivar su inviolabilidad?
   Sí, pero también depende de las personas darle la protección adecuada a través de las plataformas virtuales. También las empresas han creado sus propios medios de protección.

8. ¿Considera necesaria la actualización del sistema de justicia de Guatemala, al crearse la ley que regule los delitos informáticos?
   Si, deben brindar protección y regular adecuadamente los daños por medios tecnológicos.

9. ¿Cuáles serían los órganos que deben crearse para investigar y sancionar los delitos informáticos?
   Los órganos la existen, en virtud de la estructura de nuestro país, sin embargo requieren una fuerte formación en temas de sistemas de información y delitos informáticos y generar capacidades en las instituciones para darle seguimiento a este tipo de situaciones, no habría que crear otros.

10. ¿De acuerdo a su experiencia ha recibido alguna denuncia o conocido al caso de una conducta que encuadre en un delito informático?
    Personalmente, no, sin embargo he participado en actividades a nivel internacional en los cuales se han mencionado ejemplos de casos reales a nivel de Latinoamérica.

11. ¿En su criterio cuáles serían los principales beneficios Jurídicos de la creación de la ley que regule los delitos informáticos?

    El principal debe ser tener claro que delimitar, ósea que se va a proteger y que no en cuanto a delitos informáticos.

12. ¿En su criterio cuáles serían los principales beneficios Sociales de la creación de la ley que regule los delitos informáticos?

    Pues la mayor certeza que se protegen los datos a nivel de sistemas de información y recupera la confianza de la sociedad hacia el sistema de justicia del país.

Ingeniero Armando Monzón Escobar

CISO

Fecha de la entrevista: 13 de octubre de 2018.

1. ¿Considera que la actual legislación penal regula eficientemente los delitos informáticos?

   No. Ninguna ley tipifica los delitos informáticos como tal, es decir, mientras no hayan pruebas digitales de dicho delito es complicado poder pensar en penas. Actualmente la falta de visibilidad en las empresas sobre su ecosistema no permiten darse cuenta de ataques hasta por 1 año de efectuado.

2. ¿En su criterio que conductas se pueden considerar como delitos informáticos?

   Es complejo, primero debemos de saber a qué se le llama delito informático y cuáles son sus alcances, hay todos los días tantos intentos de ataques para robo o comprometimiento de información, que con eso ya debería de tipificarse como un delito, es como decir, voy a intentar robar el banco hoy, pero como no se puede intentare mañana, la otra semana, el otro mes, etc.

3. ¿En base a su conocimiento, considera que afecta el desconocimiento de la población hacia los delitos informáticos?

   Más que desconocimiento, es la falta de conciencia tecnológica y sus riesgos inherentes, vivimos en un mundo tecnificado que el uso de cualquier dispositivo podría ser utilizado para cometer delitos, robo de credenciales, fotos, videos, etc.

4. ¿Cuáles son los bienes jurídicos vulnerados al cometerse un delito informático?

   Definido el delito se definen los bienes.

5. ¿En su experiencia considera que es necesario crear una ley especial que regule los delitos informáticos?

Definitivamente, Guatemala ha hecho esfuerzos anteriormente para aplicar una pero es complicado, el desconocimiento hace que aunque se tenga la gana hay que cambiar muchas leyes para tipificar los delitos informáticos.

6. ¿Cree necesaria una protección jurídica especializada para la lucha contra los delitos informáticos?

   El MP, la PNC, los Organismos del estado tienen unidades que realizan estas actividades.

   En mi libro se especifican estas unidades

del cibercrimen. Todas las areas de la entidad trabajan en conjunto para generar los procedimientos y documentos que surgen a partir del análisis de riesgos, con el objetivo de que todas las entidades bancarias y financieras sigan los mismo

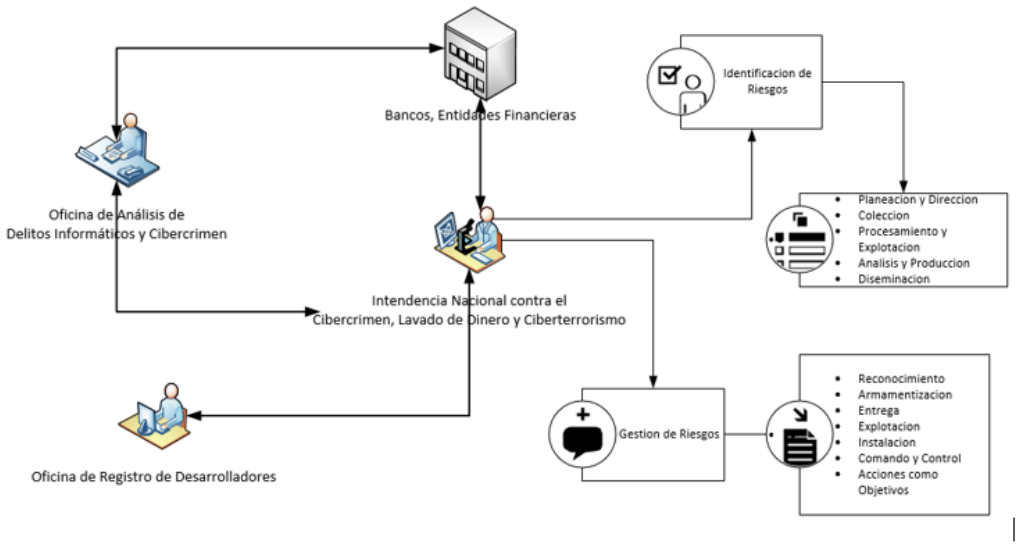


Ilustración 15 Intendencia Nacional Contra El Cibercrimen, LD y CT
Fuente: Mon.zone 2018 – Elaboración propia

negocio y organizacional.

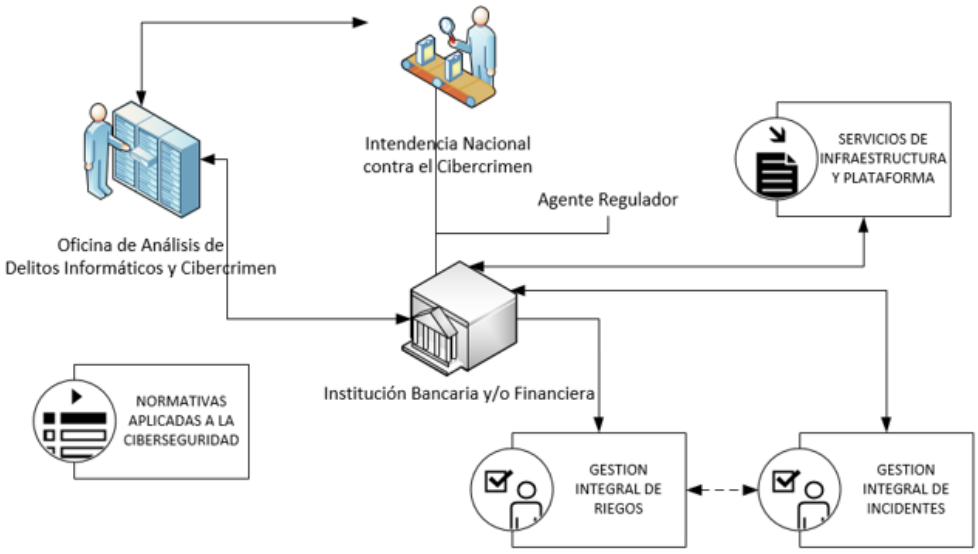


Ilustración 16 Instituciones Bancarios y/o Financieras
Fuente: Mon.zone 2018 – Elaboración propia

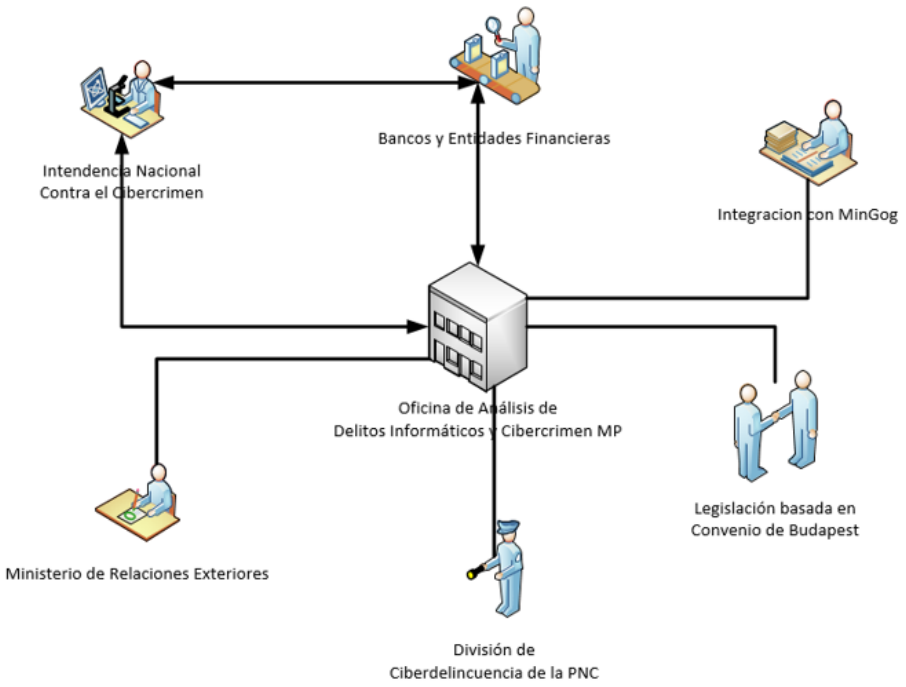


Ilustración 17Oficina de Análisis de Delitos Informáticos
Fuente: Mon.zone 2018 – Elaboración propia

a. Legislación basada en el convenio de Budapest, para perseguir el crimen

7. ¿Considera importante la protección de la información pública y privada y de esta manera motivar su inviolabilidad?

   Toda información deberá de cumplir con Integridad, Disponibilidad y Confiabilidad, utilización de tecnología deberá de aplicarse a ella para su enforzamiento de seguridad.

8. ¿Considera necesaria la actualización del sistema de justicia de Guatemala, al crearse la ley que regule los delitos informáticos?

   Definitivamente.

9. ¿Cuáles serían los órganos que deben crearse para investigar y sancionar los delitos informáticos

   MP, PNC y Organismos del Estado como lo ilustre en la pregunta 6.

10. ¿De acuerdo a su experiencia ha recibido alguna denuncia o conocido al caso de una conducta que encuadre en un delito informático?

    Claro, como consultor del MP, PNC, MINGOB se tiene conocimiento de denuncias, pero cuantas se han penalizado, sabe? Ninguna, porque no se tiene ley que tipifique exactamente el delito.

11. ¿En su criterio cuáles serían los principales beneficios Jurídicos de la creación de la ley que regule los delitos informáticos?

    Protección de la información y su tratamiento público.

12. ¿En su criterio cuáles serían los principales beneficios Sociales de la creación de la ley que regule los delitos informáticos?

    Proteger a la población, que a la larga no tiene conocimiento de ello. Evitar el robo de información de sitios web transaccionales, muchos más…

7.5 COMPROBACIÓN DE HIPÓTESIS

De conformidad con la investigación realizada y los resultados obtenidos por medio de las encuestas practicadas, se puede establecer que la hipótesis fue comprobada, en virtud de los siguientes aspectos:

La protección de bienes jurídicos específicos es uno de los principales beneficios jurídicos al crearse la ley que regule los delitos informáticos, bienes que son afectados por la comisión de estos hechos ilícitos, entre los cuales están la información, el patrimonio, la reserva, intimidad y confidencialidad de datos.

La seguridad de la información personal e institucional es un beneficio para la sociedad en general, dicha protección se logra únicamente con el establecimiento de un cuerpo normativo eficaz, información cuya vulneración es preocupante tanto para los usuarios comunes, empresas y Estado.

La prevención y sanción de los delitos informáticos únicamente se logra con una ley específica que los regule, y que permita el establecimiento de medidas coercitivas que prevengan la comisión de los delitos.

En cuanto a la actualización del Sistema de Justicia de Guatemala, a través de la especialización y capacitación constante de las entidades encargadas, se obtienen mayores resultados en cuanto a la investigación y juzgamiento de estos ilícitos.

7.6 DISCUSIÓN DE RESULTADOS

A través de las encuestas realizadas a Ingenieros en Sistemas, así como por medio de las entrevistas efectuadas a informantes clave, se revelaron importantes datos acerca de la investigación realizada.

En primer lugar las encuestas fueron realizadas a 50 profesionales especializados en las ciencias de la informática, de los cuales la gran mayoría labora en el sector privado, al momento de contabilizar las respuestas obtenidas, en su totalidad los profesionales

tienen conocimiento de lo que es un delito y las conductas que pueden ser consideradas delitos informáticos.

Así también, un importante porcentaje establece que en el municipio de Quetzaltenango tiene lugar la comisión de delitos informáticos, tomando en cuenta que los avances tecnológicos han prosperado en la ciudad y cada vez son más las personas que tiene acceso a medios o instrumentos tecnológicos, lo que conlleva a el uso desmedido por algunos.

Los resultados demuestras que la inexistencia de un marco jurídico en materia de delitos informáticos es de conocimiento por la mayoría de los profesionales encuestados, quienes expresan su preocupación y ven como una necesidad imperiosa la creación de esta ley, ya que muchos se consideran desprotegidos, y es muy poco el porcentaje que conoce con exactitud las conductas que se encuentran reguladas en el Código Penal vigente, así como las iniciativas presentadas al Órgano Legislativo.

Es por lo anterior que al ser consultados si se considerarían protegidos al crearse la ley que regule los delitos informáticos, se encontraron opiniones muy divididas, ante la evidente falta de confianza hacia es sistema jurídico y judicial de Guatemala, al momento de impartir justicia y crear normas acordes a la realidad nacional.

En cuanto a las entrevistar realizadas a los informantes claves, estas opiniones demuestran que existe una deficiencia en el sistema legislativo de la Nación, ya que la informática es un campo emergente en nuestra sociedad, que se encuentra en constante evolución por lo que necesita normas acordes a los usos inadecuados en las tecnologías informáticas.

Así como la especialización que necesitan los entes encargados de impartir justicia al momento de regular este tipo de conductas ilícitas. Ya que los sujetos entrevistados manifestaron en su mayoría tener conocimiento de conductas que encuadran perfectamente en delitos informáticos, es decir que son conductas que si se están produciendo en nuestro entorno pero que quedan impunes ante la falta de una normativa eficaz en esa materia.

Por último los resultados revelan que al momento de crearse la ley que regule los delitos informáticos, los beneficios tanto jurídicos como sociales, son muchos, los cuales van desde la delimitación, tipificación y sanción de conductas ilícitas en materia informática, hasta la protección a los derechos de los ciudadanos que traerían consigo armonía y beneficio común.

CONLUSIONES

1. Los delitos informáticos son todas aquellas acciones o comportamientos típicos, antijurídicos, culpables encaminados al uso indebido o abuso de sistemas computacionales o tecnológicos, dirigidos a alterar, destruir o manipular cualquier sistema informático por quien tiene los conocimientos necesarios en este campo.

2. Que la investigación de campo demostró que en la actualidad en el Municipio de Quetzaltenango si se producen conductas que encuadran en la concepción de los delitos informáticos, encontrando entre los afectados, usuarios comunes, empresas y profesionales en las ciencias de la informática.

3. Que al no existir un marco jurídico especifico que regule los delitos informáticos, quienes cuentan con las capacidades necesarias en este ámbito, se valen de estos conocimientos para con mala intención producir ataques a sistemas operativos, acceso ilegal a bases de datos o empleo de aparatos tecnológicos para ejecutar delitos.

4. La falta de información por parte de las autoridades encargadas y el desconocimiento por parte de la sociedad en general en materia de delitos informáticos, ha propiciado que estos sean cada vez más recurrentes, y que queden impunes, puesto que piensan que al no existir una ley no hay ningún órgano al cual puedan ser denunciados.

5. Los principales beneficios jurídicos al crearse la Ley que regule los delitos informáticos son:

a) La tipificación de las conductas que encuadran como delitos informáticos.
b) La prevención y sanción de los delitos informáticos
c) Resguardo de bienes jurídicos
d) La certeza de protección ante estas conductas ilícitas
e) La regulación de comportamientos ilícitos tanto de personas como empresas.
f) Desarrollo de políticas de seguridad informática.

6. Los principales beneficios sociales al crearse la Ley que regule los delitos informáticos son:

a) Confianza de la sociedad hacia el sistema de justicia del país.
b) Sensibilización de la ciudadanía en cuanto a los riesgos de la comisión de delitos informáticos.
c) Una cultura de educación basada en el manejo eficiente de los medios informáticos, internet y redes sociales.

RECOMENDACIONES

1. La creación de una Ley penal especial de Delitos Informáticos, a través de la cual se establece el marco regulatorio en cuanto a los posibles actos ilícitos de naturaleza informática que se comentan en el territorio nacional, así como la determinación de las sanciones correspondientes a los mismos.

2. La correcta tipificación de conductas ilícitas susceptibles de ser cometidas en el ámbito informático, que atiendan a la realidad nacional, de acuerdo a los avances y limitaciones que enfrenta nuestra sociedad.

3. La creación y promoción de una Política de Seguridad Cibernética, en base a la ley de delitos informáticos, que establezca estrategias de prevención y protección que tiendan a mitigar los riesgos y amenazas derivadas de la comisión de delitos informáticos.

4. La modernización del Sistema de Justicia, a través de la educación y capacitación del personal que integre los órganos encargados de investigar, juzgar y sancionar los delitos en materia informática.

5. Sensibilizar a la sociedad acerca del manejo, seguridad, confidencialidad de la información personal, el buen uso de los perfiles en redes sociales y los riesgos derivados del indebido manejo de los medios tecnológicos.

6. Que el Estado de Guatemala lleve a cabo la adhesión y suscripción de Convenios Internacionales en materia de delitos informáticos, que permitan la unificación de criterios en cuanto a la prevención y persecución de este tipo de conductas ilícitas, con los demás Estados a nivel mundial.

BIBLIOGRAFÌA

DOCTRINA

1. Acurio Del Pino, Santiago. DELITOS INFORMÁTICOS GENERALIDADES. Pontifica Universidad Católica del Ecuador. Quito Ecuador 2008.
2. Acurio Del Pino, Santiago, DERECHO PENAL INFORMÁTICO. Corporación de Estudios y Publicaciones. ISBN 978-9942-10-262-1,Año 2015, Quito, Ecuador.
3. Barrios Osorio, Omar Ricardo. INTRODUCCION DE LAS NUEVAS TECNOLOGIAS EN EL DERECHO. Instituto de la Defensa Pública Penal 2da. Edición 2010 Guatemala.
4. De León Velasco, Héctor Aníbal, y varios autores, coordinados por Diéz Ripollés, José Luis y Giménez Sallinas i Colomer, Esther. MANUAL DE DERECHO PENAL GUATEMALTECO, PARTE GENERAL, Impresos Industriales S.A. Guatemala, 2001Págs. 143 a 146.
5. De Mata Vela, José Francisco, De león Velasco, Héctor Aníbal. DERECHO PENAL GUATEMALTECO, Parte General y Parte Especial. Vigésima segunda edición. Magna Terra editores S.A. Guatemala 2012.
6. Escobar Cárdenas, Fredy Enrique. COMPILACIONES DE DERECHO PENAL, Parte General, Novena Edición. Guatemala 2018.
7. Giron Pallez, José Gustavo. TEORÍA DEL DELITO. Instituto de la Defensa Pública Penal 2da Edición 2013 Guatemala.
8. Noriega Salazar, Hans Aarón. DELITOS INFORMÁTICOS. Instituto de la Defensa Pública Penal,. 1ª Edición 2011 Guatemala.
9. Muñoz Conde, Francisco y García Arian Mercedes. MANUAL DE DERECHO PENAL PARTE GENERAL. 2ª. Edición. Titant lo Blanch editora. Valencia España 1998
10. Rolando Alvarado, Ronald Morales. CIBERCRIMEN. Ius Ediciones S.A. Guatemala 2012.
11. Téllez Valdés, Julio. DERECHO INFORMÁTICO. Cuarta Edición, McGraw-Hill/INTERAMERICANA Editores, S.A. de C.V. México 2008.

12. INFORME SOBRE LOS CIBERDELITOS 2017. Observatorio Guatemalteco de Delitos Informáticos.
13. ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNETICA. Edición Digital. Guatemala marzo de 2018.
14. Iniciativa de Ley de Delitos Informáticos número 4055, Congreso de la República de Guatemala 2009.
15. Iniciativa de Ley Contra la Ciberdelincuencia número 5254, Congreso de la República de Guatemala 2017

DICCIONARIOS

1. Caballenas de Torres, Guillermo. DICCIONARIO JURIDICO ELEMENTAL. Editorial Heliasta S. R.L., Argentina. Duodécima Edición, 1997.
2. Ossorio, Manuel. DICCIONARIO DE CIENCIAS JURÍDICAS, POLÍTICAS Y SOCIALES. 1era Edición Electrónica. Dastacan S.A. Guatemala 1999.
3. Océano Uno. Diccionario Enciclopédico, Barcelona, España, Océano Grupo Editorial, S.A., 1995.

PAGINAS WEB

1. www.academia.edu.com
2. www. biblioteca.usac.edu.gt
3. www.estuderecho.com
4. www.estrategiaynegocios.net
5. www.mzaghi.com
6. www.profesorlegal.com
7. www.revistaitnow.com
8. www.informáticalegal.com
9. www.palermo.edu
10. www.ecured.cu
11. www.derechoinformático.wordpress.com
12. www.delitosinformaticos.info
13. www.rae.es

LEGISLACIÓN:

1. CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE GUATEMALA.
2. CÓDIGO PENAL. Decreto 17-73.
3. LEY DEL ORGANISMO LEGISLATIVO. Decreto 2-89.
4. LEY ORGANICA DEL ORGANISMO LEGISLATIVO. Decreto 63-94.
5. LEY DE RECONOCIMIENTO DE COMUNICACIONES Y FIRMAS ELECTRÓNICAS. Decreto 47-2008
6. LEY DE ACCESO A LA INFORMACIÓN PÚBLICA. Decreto Número 57-2008.
7. LEY DE TELECOMUNICACIONES. Decreto Número 94-96
8. LEY DE CONTRATACIONES DEL ESTADO. Decreto Número 57-92
9. LEY DE PROMOCIÓN DEL DESARROLLO CIENTÍFICO Y TECNOLÓGICO NACIONAL. Decreto Número 63-91
10. LEY 1273 DE 2009 Congreso de Colombia.
11. Ley 9048 Congreso de Costa Rica.
12. LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS. La asamblea nacional de la República Bolivariana de Venezuela.
13. CONVENIO SOBRE CIBERCRIMINALIDAD 2001.
14. CONVENIO Nº 108 DEL CONSEJO DE EUROPA, DE 28 de enero de 1981, PARA LA PROTECCION DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARACTER PERSONAL.
15. DECISIÓN MARCO 2005/222/JAI DEL CONSEJO DE EUROPA. Febrero de 2005.
16. UNDÉCIMO CONGRESO DE NACIONES UNIDAS PARA LA PREVENCIÓN DEL DELITO Y LA JUSTICIA PENAL.
17. CONVENCION DE PALERMO 15 de noviembre de 2000.
18. DECLARACION DE VIENA SOBRE LA DELINCUENCIA Y LA JUSTICIA FRENTE A LOS RETOS DEL SIGLO XXI. 55/59.
19. RESOLUCIÓN 57/239 SOBRE LOS ELEMENTOS PARA LA CREACIÓN DE UNA CULTURA MUNDIAL DE SEGURIDAD CIBERNÉTICA.
20. EL MANUAL DE LAS NACIONES UNIDAS PARA LA PREVENCIÓN Y CONTROL DE DELITOS INFORMÁTICOS.

21. TRATADO DE LA ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL SOBRE EL DERECHO DE AUTOR.
22. 12º CONGRESO DE LAS NACIONES UNIDAS SOBRE PREVENCIÓN DEL DELITO Y JUSTICIA PENAL.
23. ESTRATEGIA DE LA OEA SOBRE SEGURIDAD INFORMÁTICA resolución AG/RES.1939 (XXXIII-0/03).