



000011

*Comisión de Legislación y
Puntos Constitucionales*

*Congreso de la República
Guatemala, C.A.*

08 de diciembre de 2010

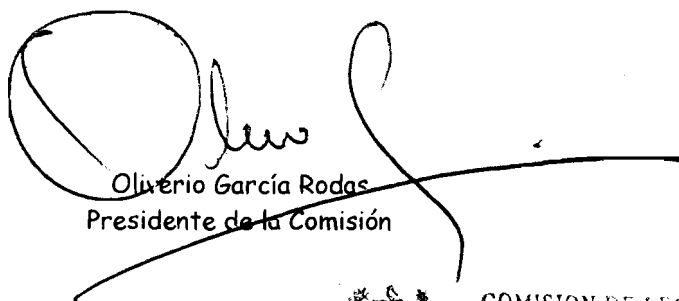
Licenciada
Ana Isabel Antillón
Dirección Legislativa
Congreso de la República
Su Despacho

10 7011
FELMA JAF

Apreciable Señora Directora:

De manera atenta me dirijo a usted y de conformidad con lo regulado en los artículos 39, 40 y 41 de la Ley Orgánica del Organismo Legislativo, adjunto el **DICTAMEN FAVORABLE**, emitido en la Comisión de Legislación y Puntos Constitucionales, el día seis de diciembre del año dos mil diez, a la **Iniciativa de Ley número 4055**, que dispone aprobar **LEY DE DELITOS INFORMATICOS**.

Sin otro particular, aprovecho la oportunidad para reiterar a la Señora Directora las muestras de mi alta estima.


Oliverio García Rodas
Presidente de la Comisión

COMISION DE LEGISLACION
Y PUNTOS CONSTITUCIONALES
Congreso de la República de Guatemala, C.A.

cc. arch.



*Comisión de Legislación y
Puntos Constitucionales*

*Congreso de la República
Guatemala, C.A.*

000012

DICTAMEN NÚMERO 17-2009

INICIATIVA NÚMERO 4055

LEY DE DELITOS INFORMATICOS

HONORABLE PLENO:

Con fechas 18 de agosto del año 2009, el Honorable Pleno del Congreso de la República conoció la iniciativa número 4055, denominada "**Ley de Delitos Informáticos**", misma que fue remitida para su estudio y dictamen a la Comisión de Legislación y Puntos constitucionales. Esta iniciativa pretende crear una normativa de prevención y sanción de los delitos informáticos para brindar protección e inviolabilidad a los derechos de toda persona en cuanto a la confidencialidad, integridad y disponibilidad de datos y tecnologías de la información que posea y utilice; asimismo, dicha iniciativa tiene por finalidad crear un marco jurídico que sea uniforme con los convenios internacionales sobre ciberdelincuencia a efecto de crear mecanismos eficaces de prevención y sanción de los delitos informáticos que comúnmente son de naturaleza transnacional.

ANTECEDENTES

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

En nuestro país ya existe regulación sobre Comercio Electrónico, según el contenido de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto número 47-2008 del Congreso de la República de Guatemala, lo que también obliga a crear una ley especial para prevenir, sancionar y erradicar los delitos de naturaleza informática que pudieran afectar el objeto o materia de la normativa de comercio electrónico, y todos aquellos actos ilícitos de naturaleza informática, cumpliendo a cabalidad con todas las pautas y reglas a nivel internacional tomando como base el Convenio sobre la Ciberdelincuencia suscrito en Budapest con fecha veintitrés de noviembre del año dos mil uno, que ha sido la ley modelo para la regulación de cibercrimen.



000013

*Comisión de Legislación y
Puntos Constitucionales*

*Congreso de la República
Guatemala, C.A.*

CONTENIDO DE LA INICIATIVA

La iniciativa en mención pretende establecer normas especiales que sean suficientes para prevenir y sancionar las conductas de cibercrimen que no tienen fronteras, ni poseen lenguaje específico, y que se realizan en un espacio virtual o ciberespacio. Con el contenido de dicha iniciativa se pretende brindar protección integral de la información de las personas que se almacena, opera o transmite por medio de sistemas que utilizan tecnologías de la información, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas físicas o jurídicas.

Dicha normativa será de aplicación general y regirá en todo el territorio nacional y en cualesquiera de los lugares establecidos en el contenido de la misma.

**CONSIDERACIONES CON RELACION AL AVANCE DE REGULACION DE
LOS DELITOS INFORMATICOS DE GUATEMALA Y
LOS PAISES DE LATINO AMERICA**

Para establecer el avance de la regulación se ha tomado en cuenta el informe "Estado situacional y perspectivas del derecho informático en América Latina y el Caribe", que analiza la situación de la regulación en materia de Delitos Informáticos y Delitos por medio de las tecnologías de la información.

Durante varios años el desarrollo normativo ha estado focalizado en la penalización del uso de las Tecnologías de la Información (TIC), sobre todo en tema de pornografía infantil, aunque hay que indicar que se sigue el lineamiento doctrinario de que no era necesario una regulación sino una adecuada formación de los jueces y actores jurídicos relacionados en interpretar las normativas existentes.

Sin embargo hay que indicar que esta serie de legislaciones se encuentran con problemas de persecución por parte de las fuerzas de la ley que no tienen formación en la materia o se encuentran en sus fases iniciales del establecimiento de las normas que regulen este tipo de delitos en contra de la ciberdelincuencia.

A la fecha diversos países han iniciado trabajos para firmar y ratificar el acuerdo de Budapest sobre "CIBERCRIMEN", sin embargo en la región de América Latina no hay ningún país que haya firmado dicho convenio, ello significa que mientras los países firmantes del tratado se encuentran armonizando sus legislaciones y además utilizando los instrumentos de



000014

Comisión de Legislación y Puntos Constitucionales

*Congreso de la República
Guatemala, C.A.*

cooperación, América Latina esta trabajando aisladamente y aún peor sin uniformidad, lo que hace necesario que se inicie por parte del Estado de Guatemala a través de los Organismos correspondientes y con ello adecuar las normativas correspondientes.

Debemos tomar en cuenta el aumento de la penetración de Internet, ya que es un factor que sirve como detonante para analizar y plantear adecuadamente la regulación legal en la materia, sin embargo no será hasta que se logre la adopción de leyes y reglamentos para que realmente avance adecuadamente, y lo mismo pasa por la diversidad de definiciones que se tienen hacia lo que es un delito informático. La presente iniciativa es precisamente un conjunto de factores que buscan combatir los crímenes informáticos.

Es preciso hacer mención que hemos tomado en cuenta diversos criterios que sirven de base para la presente Iniciativa de ley a nivel de Latino América tal el caso de los conceptos de la declaración de cibercrimen y lo dispuesto en la Asamblea General de la Organización de Estados Americanos (OEA) de fecha ocho de junio del dos mil cuatro, lo cual deseamos que se refleje en el contenido de la Iniciativa de ley, una legislación avanzada que ha considerado los mejores procesos normativos de la Región para ser aplicados dentro de nuestra normativa interna y regular drásticamente las penas y sanciones en contra de los delitos relacionados con el tema.

Debe tomarse en cuenta las necesidades que deben satisfacerse y las soluciones que conlleva el contenido de la presente iniciativa de ley:

La presente iniciativa busca la uniformidad sustancial y procesal de las normas penales ya determinadas en nuestro país y analizar a su vez las necesidades que sobre el avanzado tema de cibercrimen existe hoy en día y que la misma ha tomado en cuenta los asuntos presentes y futuros que van día con día creándose de una manera impredecible, razón por la cual se consideraron los siguientes puntos:

- a) Que es necesario proteger a la sociedad frente a la amenaza de los delitos cometidos por vía informática.
- b) Se deben crear leyes homogéneas no solo para nuestra Región, sino además para el resto de los países del mundo.
- c) La naturaleza volátil de estos delitos crea la necesidad de buscar mecanismos de cooperación nacional e internacional claros y funcionales.



000015

Comisión de Legislación y Puntos Constitucionales

*Congreso de la República
Guatemala, C.A.*

- d) Es necesario garantizar a la sociedad la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y de los sistemas que utilicen tecnologías de la información y comunicación.
- e) Se hace necesario crear, capacitar y dotar de tecnología a Organismos del Estado que manejen la seguridad especializada en sistemas informáticos y de los sistemas que utilicen tecnologías de la información y comunicación.
- f) Es necesaria la participación activa de nuestro país en actividades relacionados con la ciberdelincuencia, de manera que tengamos la capacidad de detectar vulnerabilidades, genera soluciones, generar las propias herramientas técnicas y estrategias de investigación.

El Convenio del Consejo de Europa ha definido cuatro categorías de delitos informáticos, entiéndase cualquier acto cometido dentro del uso de las tecnologías de la información y comunicación, siendo estas las siguientes:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos.
2. Delitos estrictamente informáticos.
3. Delitos relativos al contenido.
4. Delitos relativos a la violación de los derechos de autor y derechos afines.

Cabe manifestar, que la Unión Europea ha dado prioridad, en cuanto se refiere a estos aspectos sustanciales, a la pornografía infantil, entre otros.

En cuanto al aspecto procesal, la presente iniciativa contiene regulaciones que evitan la dificultad creada en los delitos que por sí solos son transnacionales, junto con las velocidades de la comisión y la flexibilidad de la comisión de dichos delitos. Entre estos aspectos, se ha tomado en cuenta las interceptaciones de comunicaciones, la retención de datos sobre tráfico, el anonimato, la cooperación internacional, la jurisdicción y el valor probatorio de la evidencia de la prueba recabada en toda investigación.

Los constantes avances tecnológicos y los altos niveles de conocimientos técnicos involucrados en los nuevos desarrollos de sistemas que utilizan tecnologías de la información y comunicación, forman un reto para presentar una definición general de lo que puede denominarse un delito por computadora. En ese sentido, existen múltiples interpretaciones y sugerencias que buscan modelar esta naciente y conflictiva área para el derecho y las tecnologías de información. El no contar con una definición concreta sobre el tema desestima los esfuerzos para una adecuada detección, investigación y



000016

Comisión de Legislación y Puntos Constitucionales

*Congreso de la República
Guatemala, C.A.*

juzgamiento de este tipo de conductas cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas físicas o jurídicas.

La delincuencia informática es una realidad que requiere de iniciativas de leyes como la que hoy se presenta, en las que contienen estrategias de prevención y combate de la misma. Insinuar que la criminalidad informática es un problema jurídico, o tecnológico, o social o mercantil, sería negarnos o cerrarnos las puertas a la posibilidad de haber presentado la iniciativa de ley que lo que busca es el profundizar en las problemáticas de las vulnerabilidades, de la inseguridad de los individuos a nivel de la informática.

PROPUESTA DE REGULACION LEGAL, CONTENIDO EN EL CONVENIO DE BUDAPEST

El Convenio sobre la Ciberdelincuencia es un tratado internacional suscrito en Budapest el 23 de noviembre del 2001, por los miembros del Consejo de Europa COE, para incrementar la cooperación entre los funcionarios de las instituciones policiales de diferentes países. El Convenio de Budapest fue oficialmente redactado por los 43 países miembros del Consejo de Europa, junto con los EE.UU., Canadá, Japón y otros que participaron como observadores.

El Convenio está vigente ya que hasta la fecha lo han suscrito 43 Estados y ratificado 20 Estados.

Mediante el Convenio de Budapest se propone fundamentalmente:

1. Incluir una relación de delitos que cada Estado miembro debe considerar como tales. El tratado tipifica como delitos a las infracciones de piratería, la producción, venta o distribución de herramientas de piraterías, la pornografía infantil y una lista amplia de infracciones de la propiedad intelectual (Artículos 2-11).
2. Requiere que todos los Estados signatarios concedan nuevos poderes de búsqueda e intervención a las autoridades policiales, incluida la facultad de exigir a los servidores de Internet que preserven los registros de uso de Internet de cada ciudadano u otros datos y la facultad de controlar en tiempo real las actividades en línea de los ciudadanos (Artículos 16-22)
3. Requiere también el cumplimiento de la ley en todos los países participantes de manera que estos cooperen con los cuerpos de policía de otros países participantes ante una "solicitud de asistencia mutua" de



000017

Comisión de Legislación y Puntos Constitucionales

Congreso de la República
Guatemala, C.A.

la policía de otro país "en la mayor medida de lo posible" (Artículos 23-35).

De acuerdo con lo previsto en el artículo 37 del Convenio, relativo a la Adhesión al mismo, aquellos países que no participaron en la elaboración del Convenio, podrán ser invitados por el Comité de Ministros del Consejo de Europa, previa consulta y consentimiento unánime de los Estados contratantes del Convenio, para adherirse al mismo.

Por otro lado, el Capítulo IV prevé la posibilidad de que el país o países adherentes determinen el territorio donde se aplicará la convención y hagan declaraciones, reservas o enmiendas.

Una posibilidad clara para que los Países de América Latina adapten su normativa y establezcan lazos estrechos de cooperación que les permita enfrentar la ciberdelincuencia, lo constituye la adhesión al Convenio sobre la Ciberdelincuencia suscrito en Budapest en noviembre de 2001.

Dicho Convenio está abierto a la adhesión de terceros países, distintos a los que son miembros u observadores del Consejo de Europa, para ello debe mediar la invitación por parte del Comité de Ministros del Consejo de Europa, previa consulta y consentimiento unánime de los Estados Contratantes del Convenio.

Para ello, es preciso que los países manifiesten de manera inequívoca su voluntad política de ser parte del convenio y lleven a cabo una gestión diplomática al más alto nivel para que se obtenga la invitación de Ministros referida.

La base para esta propuesta se encuentra en la *Tarea Pendiente 1 de Delitos Informáticos*, del documento **"Estado situacional y perspectivas del derecho informático en América Latina y el Caribe"**, que propone el: "(...) *diseño de una propuesta normativa mínima, basada entre otros en las propuestas del tratado de Cybercrimen, ya existentes*". Siendo así que la Convención de Cybercrimen y su Protocolo Adicional, son la base de esta propuesta de iniciativa de ley.

Puesto que la Convención de Cybercrimen no solo analiza delitos informáticos en su forma "pura", y también actúa sobre los relacionados a los "contenidos", que pudieran estar ya cubiertos en los delitos mediante el uso de las TIC, consideramos que la adhesión y ratificación del tratado solo requerirían de



000018

Comisión de Legislación y Puntos Constitucionales

Congreso de la República
Guatemala, C.A.

ajustes menores regulatorios, además de permitir un acceso a una regulación especializada con caracteres internacionales sobre la materia.

Debemos indicar que hay una consecuencia entre al propuesta de firmar la Convención sobre Ciberdelito y lo que los Ministros de Justicia de la Organización de Estados Americanos presentaron a los miembros en abril de 2004, donde invitaban "a evaluar las posibilidades de implementar los principios de la Convención del Consejo de Europa sobre Ciberdelito de 2001 y a considerar la posibilidad de ser Parte de esa convención", que concuerda con lo expresado por los Ministros de Justicia de las Américas en abril del 2006 donde mencionaron: "Que, teniendo en cuenta las recomendaciones adoptadas por el Grupo de Expertos Gubernamentales y por la REMJA-V y los avances alcanzados entre esa y la presente reunión se continúe fortaleciendo la cooperación con el Consejo de Europa con el fin de facilitar que los Estados Miembros de la OEA consideren la aplicación de los principios de la Convención del Consejo de Europa sobre la delincuencia Cibernética y la adhesión a la misma, así como la adopción de las medidas legales y de otra naturaleza, que sean necesarias para su implementación".

Presupuestos del Ciberdelito en la Red.

El ciberdelito representa el estado más sofisticado de la conducta antijurídica.

Esencialmente no existe mucha diferencia entre las conductas antijurídicas y punibles tradicionales con aquellas que se cometen a través de medios informáticos. Es justamente la adjetivación del delito, "informático", la que convierte al delincuente en algo apartado de la tradición y envuelve el hecho de unas connotaciones que lo dotan de cierta autonomía conceptual. El ordenador se convierte en un instrumento del delito, no por sí solo, sino por su conexión a una red interna (intranet) o a una red externa (internet), por donde circulan usuarios, estudiantes, empresarios, profesionales, pederastas, grandes sumas de dinero encriptadas, estafadores, sabotadores, niños y terroristas.

Predominantemente existen dos formas de comunicación a través de Internet:

El correo electrónico y la World Wide Web. Simplificaremos nuestra exposición ignorando otros modos de comunicación en red que han perdido protagonismo o que poseen una importancia delictiva muy limitada, como el Bulletin Board System BBS, Internet Relay Chats (IRC), usenet, website "guest books", weblogs, File Transfer Protocol, P2P, particulares aplicaciones como Napster, Gnutella, sin perjuicio de que gran parte de lo dicho en estas páginas sea aplicable a dichos sistemas de comunicación. Por otro lado existe otra



000019

Comisión de Legislación y Puntos Constitucionales

*Congreso de la República
Guatemala, C.A.*

modalidad como la WWW, el Webcasting, que define como "grupo de servicios emergentes que utilizan Internet para la entrega de contenidos a los usuarios, de una forma muy similar a los servicios de comunicación".

La World Wide Web (WWW), es un sistema de hipertexto que funciona sobre Internet, a través del cual, y con la ayuda de una aplicación informática destinada al efecto, el navegador web, se extrae información (llamada "documentos" o "páginas web") y se muestra en la pantalla del usuario. Siguiendo los hiperenlaces, el usuario puede acceder a múltiples páginas, lo que se denomina "navegación". Dicha páginas se encuentran hospedadas en servidores donde se almacena la información en discos duros.

Es frecuente que los responsables de las páginas y portales Web utilicen vías distintas de acceso para transferir los contenidos. El más utilizado es el protocolo FTP. Del mismo modo que el conductor ebrio, para cometer un delito contra la seguridad del tráfico, necesita un vehículo a motor, drogas tóxicas o bebidas alcohólicas y, generalmente, una vía pública asfaltada como escenario, el ciberdelincuente requiere disponer de un terminal de ordenador (el vehículo a motor), una conexión a Internet (la vía pública) y las distintas estaciones que posibilitan la circulación: proveedores de servicios, de contenido, mirrors, proxys, etc. (el asfalto.)

Principalmente son tres o cuatro sujetos, como mínimo, los que participan en el fenómeno del cibercrimen. El sujeto activo del delito, que inicia la conducta punible (sea enviando contenidos a un servidor, sea descargando archivos prohibidos, sea remitiendo e-mails difamatorios); los sujetos coadyuvantes sin cuya intervención el ciberdelincuente carecería de los medios técnicos necesarios para desarrollar su conducta criminal (el servidor de acceso, que posibilita la conexión a la red y el servidor de contenidos, en cuyos discos duros se alberga la información delictiva, que más tarde ofenderá o causará perjuicios); y, por último, el sujeto pasivo del delito, caracterizado en Internet por ser plural, a veces masivo, internacional y, casi siempre, indeterminado y desconocido para el delincuente. Generalmente, serán estos sujetos los protagonistas del cibercrimen, pero, en ocasiones, si el delito consiste en el envío directo de e-mails, no intervendría el servidor de contenidos, cifrándose en tres los participantes.

Naturalmente los sujetos, humanos o cibernéticos, se pueden multiplicar por medio de mirrors¹³ y proxys¹⁴, por lo que las combinaciones del itinerario criminal aumentan considerablemente.



Comisión de Legislación y Puntos Constitucionales

*Congreso de la República
Guatemala, C.A.*

003020

JUSTIFICACIÓN

Características de Internet

Internet, medio donde se desenvuelve el delincuente, y que engloba el ámbito objeto de esta iniciativa de ley (el WWW), contiene unos elementos especialmente favorables para la comisión de delitos.

Estas características representan un reto para el jurista y desafía la soberanía de los Estados, tal como se muestra a continuación.

I. Entorno sin fronteras.

La red de redes supone la absoluta libertad de movimientos, la posibilidad de atravesar fronteras sin limitaciones, visados, impedimentos aduaneros. El usuario puede viajar, virtualmente, de un país a otro, adentrándose en otras jurisdicciones, incluso con absoluta ignorancia de que lo hace.

II. Independencia geográfica.

Desde cualquier lugar del mundo se puede teclear en el navegador del ordenador la dirección URL deseada. En una fracción de segundo, el usuario visita páginas web localizadas en distintos lugares del planeta. Si la navegación transcurre con normalidad, el internauta comprobará como, independientemente de que la página visitada se encuentre en su propio país o en las antípodas, la velocidad de conexión es prácticamente la misma (instantánea), no siendo un elemento determinante la medición tradicional de las distancias.

III. Independencia de lenguaje.

Al contrario que los sistemas de comunicación precedentes (teléfonos, radiofonía, telégrafo, etc.), la World Wide Web, por medio de una sofisticada tecnología, posibilita el acceso multilingüe a las páginas visitadas. Ello permite, a través de aplicaciones ofrecidas por diferentes operadores, que cualquier persona se incorpore a Internet sin mayores impedimentos. Se desarrolla asimismo un sistema peculiar de comunicación, una jerga propia de internautas.

IV. Permite la comunicación de uno a muchos.

Esta característica es trascendental para el jurista. El ciberdelincuente suele conocer este rasgo de la World Wide Web y utiliza la tela de araña para que los efectos de su acción se multipliquen y perjudiquen a multitud de personas. Este elemento, aleja el ciberdelito del delito tradicional, por cuanto los efectos de aquél pueden producirse, incluso simultáneamente, en una pluralidad de



000021

Comisión de Legislación y Puntos Constitucionales

*Congreso de la República
Guatemala, C.A.*

jurisdicciones, aunque la acción inicial partiera de un lugar muy concreto y lejano.

V. Sistema incomparable de distribución de información.

Ni la televisión ni la radio ni, por supuesto, los sistemas de comunicación predecesores poseen la fuerza distributiva de la WWW. Cualquier persona, con escasos medios técnicos y financieros, puede entrar al circuito y utilizar la red para difundir sus opiniones, investigaciones, filosofías y doctrinas. Las posibilidades de delinquir aumentan expotencialmente.

VI. Ampliamente utilizado, cada día más.

En pocos años la difusión de Internet ha llegado a casi todos los hogares de los países desarrollados. En países subdesarrollados el uso se incrementa, sin que la precariedad de la economía sea un obstáculo insalvable. Países en vías de desarrollo, como India y Filipinas, se sitúan a la cabeza mundial en los avances informáticos relacionados con Internet. El acceso a tal tecnología y, por consiguiente al ciberdelito, es abierta y popular. Precisamente, esta facilidad unida a la precariedad normativa en materia de persecución del cibercrimen en países subdesarrollados, hacen de éstos paraísos cibernéticos, donde los propios estados fomentan el vacío legal para atraer explotaciones que en otros estados serían ilícitas.

OPINIONES MERECIDAS

La iniciativa se socializó a través de diversos foros y presentaciones y logró agruparse con distintos sectores y sus representantes a través de mesas de dialogo, conferencias, entrevistas durante estos últimos 12 meses, cuyas personas, representantes, entidades y grupos o sectores participantes, fueron los siguientes:

- Consejo Nacional de Ciencia y Tecnología
- Universidad de San Carlos de Guatemala
- Universidad Rafael Landívar
- Universidad del Valle de Guatemala
- Universidad Francisco Marroquín
- Asociación Guatemalteca de Exportadores -AGEXPORT-
- Cámara de Industria de Guatemala
- Ministerio de Relaciones Exteriores
- Ministerio de la Defensa Nacional
- Ministerio Público



000022

Comisión de Legislación y Puntos Constitucionales

Congreso de la República

Guatemala, C.A.

- Entidades privadas
- Ciudadanos, estudiantes, catedráticos

ASPECTOS DE FONDO Y CONTENIDO DE LA LEY

En general la redacción y la estructura de esta iniciativa se adapta a los aspectos técnico-jurídicos y los mismos se enmarcan a nivel internacional tal como lo es el tratado de Ciberdelincuencia contenido en el Convenio de Budapest, el cual es la base legal para poder elaborar un proyecto de iniciativa de Ley como la presente.

Es necesaria esta comparación ya que la legislación en materia de Ciberdelincuencia debe ser homogénea y uniforme con las normas internacionales que han servido de base para las legislaciones de ciertos países en América Latina.

Asimismo, sigue una estructura y estilo de redacción conocidos que tiende a facilitar su comprensión y entendimiento por parte de los interesados que serán los usuarios y también facilita el análisis y entendimiento para su aprobación por parte del Honorable Congreso de la República.

La iniciativa de ley contiene IV TITULOS, VI capítulos de la siguiente forma:

TITULO I

Disposiciones Generales y Conceptuales

Sección I

Objeto, Ámbito y Principios

Sección II

Definiciones

TITULO II

Normativa efectiva a nivel nacional

Sección I

Derecho Penal Sustantivo

Capítulo I



000023

Comisión de Legislación y Puntos Constitucionales

Congreso de la República

Guatemala, C.A.

Delitos contra la Confidencialidad, Integridad y Disponibilidad de datos y tecnologías de la información

Capítulo II

Delitos contra la persona.

Capítulo III

Delitos contra la Nación y Actos de Terrorismo

TITULO III

Organismos Competentes y Reglas de Derecho Procesal

Capítulo I

Organismos Competentes

Capítulo II

Medidas Cautelares y Procesales

TITULO IV

Disposiciones Finales

CONCLUSIONES

- a) La presente iniciativa de ley, cubre en buena medida las necesidades legales existentes con respecto a la tipificación de los delitos relacionados con el cibercrimen.
- b) Considera aspectos novedosos que otros países en Latino América no han tomado en cuenta.
- c) Presenta una combinación adecuada de respeto a la garantía que merece la sociedad en la confidencialidad, la integridad y la disponibilidad de los sistemas que utilicen tecnologías de la información y comunicación y su contenido.
- d) Actualmente el país, requiere de una importante necesidad de la creación de una normativa de índole procesal y en la coordinación internacional e inter-institucional.

DICTAMEN

En base a las consideraciones Constitucionales, legales y políticas vertidas anteriormente, esta Comisión emite **DICTAMEN FAVORABLE** al proyecto de decreto contenido en la iniciativa 4055 por ser viable, oportuno, conveniente y Constitucional.



003324

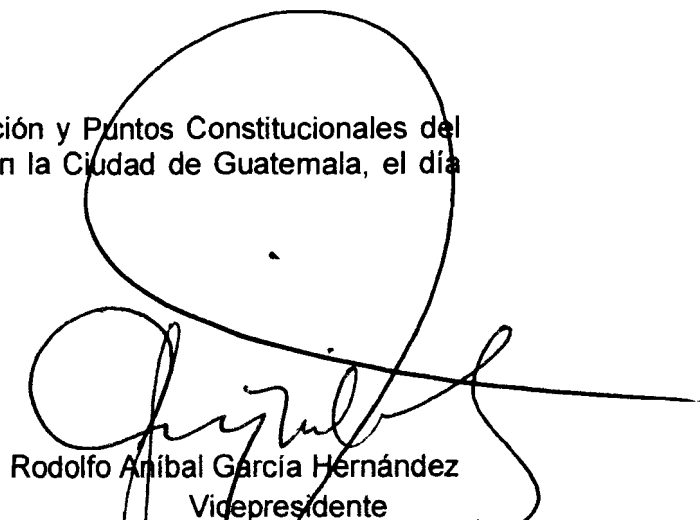
Comisión de Legislación y Puntos Constitucionales

Congreso de la República
Guatemala, C.A.

Dado en la sala de la Comisión de Legislación y Puntos Constitucionales del
Congreso de la República de Guatemala, en la Ciudad de Guatemala, el día
seis de diciembre del año dos mil diez.



Oliverio García Rodas
Presidente



Rodolfo Anibal García Hernández
Vicepresidente



José Alberto Gándara Torrebiarte
Secretario



Rosa María Ángel Madrid de Frade



Jorge Mario Barrios Falla

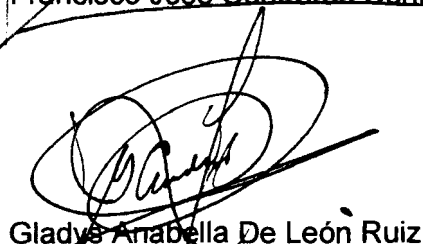


Alicia Dolores Beltrán López



Francisco José Contreras Contreras

César Augusto Del Águila López



Gladys Anabella De León Ruiz



Ronnie Danilo Escobar



000025

*Comisión de Legislación y
Puntos Constitucionales*

*Congreso de la República
Guatemala, C.A.*

Carlos Valentín Gramajo Maldonado

Oscar Valentín Leal

Carlos Enrique López Girón

Otilia Lux de Cotí

Héctor Alfredo Nuila Ericastilla

Roderico Martínez Escobedo

Mariano Rayo Muñoz

Humberto Leonel Sosa Mendoza



DECRETO NÚMERO _____

000026

LEY DE DELITOS INFORMÁTICOS

EL CONGRESO DE LA REPÚBLICA DE GUATEMALA

CONSIDERANDO:

Que es indispensable la aprobación de una ley especial que contenga disposiciones que tiendan a proteger los derechos de toda persona en cuanto a la integridad, disponibilidad y confidencialidad de los sistemas que utilicen tecnologías de la información y sus componentes, a fin de garantizar certeza jurídica en las transacciones propias del comercio electrónico y así, armonizar y contribuir con las disposiciones internacionales con relación a la prevención y sanción de los delitos informáticos.

CONSIDERANDO:

Que debido a que en nuestro país ya existe regulación sobre comercio electrónico, según el contenido de la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto número 47-2008 del Congreso de la República de Guatemala, se hace necesario emitir una ley especial para prevenir y sancionar los delitos de naturaleza informática que pudieran afectar el objeto o materia de la normativa de comercio electrónico y todos aquellos actos ilícitos de naturaleza informática.

CONSIDERANDO:

Que para poder contrarrestar los ataques cibernéticos el Estado de Guatemala debe crear normas para prevenir y sancionar esas acciones, las cuales deben ser congruentes con la normativa internacional.

CONSIDERANDO:

Que es necesaria la efectiva creación y aplicación de normas especiales en materia de delitos informáticos, toda vez que, por la naturaleza de los actos de cibercrimen y que son delitos transfronterizos, se complica la aplicación de las actuales normas del Código Penal, lo que se traduce en lagunas legales que permiten al delincuente realizar actos ilícitos por medio de las nuevas tecnologías de la información.



POR TANTO:

000027

En ejercicio de la atribuciones que le confiere la literal a) del artículo 171 de la Constitución Política de la República de Guatemala.

DECRETA:

La siguiente:

LEY DE DELITOS INFORMÁTICOS

TÍTULO I

DISPOSICIONES GENERALES Y CONCEPTUALES

SECCIÓN I

OBJETO, ÁMBITO Y PRINCIPIOS

Artículo 1. Objeto de la ley. La presente ley tiene por objeto la protección integral de las personas, sus bienes y derechos, mediante el establecimiento de un marco jurídico relativo a los sistemas que utilicen tecnologías de la información, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas físicas o jurídicas, en los términos previstos en esta ley.

La integridad y disponibilidad de la información contenida en sistemas que utilizan tecnologías de la información y sus componentes, la información o los datos que se almacenan o transmiten a través de éstos, las transacciones y acuerdos comerciales o de cualquiera otra índole que se llevan a cabo por su medio y la confidencialidad de éstos, son todos bienes jurídicos protegidos.

Artículo 2. Ámbito de aplicación. Esta ley es de aplicación general y rige en todo el territorio de la República de Guatemala, a toda persona física o jurídica, nacional o extranjera, que cometa un hecho sancionado por sus disposiciones, en cualquiera de las circunstancias siguientes:

- a) Cuando el sujeto activo origina u ordena la acción delictiva dentro del territorio nacional;
- b) Cuando el sujeto activo origina u ordena la acción delictiva desde el extranjero, produciendo efectos en el territorio nacional;



000028

- c) Cuando el origen o los efectos de la acción se produzcan en el extranjero, utilizando medios que se encuentran en el territorio nacional; y,
- d) Cuando se caracterice cualquier tipo de complicidad desde el territorio guatemalteco.

Artículo 3. Acción pública. Los delitos regulados en la presente Ley se consideran de acción pública, conforme a lo previsto en el Código Procesal Penal.

SECCIÓN II

DEFINICIONES

Artículo 4. Definiciones. Además de las definiciones contenidas en la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Decreto 47-2008 del Congreso de la República, y para los efectos de la presente ley, se entenderá por:

- a) **Confidencialidad**
Constituye un atributo de la información para prevenir su divulgación a personas o usuarios no autorizados.
- b) **Correo electrónico**
Es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos.
- c) **Datos informáticos**
Toda representación de hechos, instrucciones, caracteres, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.
- d) **Datos de tráfico**
Designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.
- e) **Disponibilidad**
Constituye una característica de la información para garantizar que ésta se encuentre disponible para quien tiene la autorización de acceder a ella, sean personas, procesos o aplicaciones en cualquier momento.



000029

- f) **Documento electrónico**
Registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contengan información acerca de hechos o actos capaces de causar efectos jurídicos.
- g) **Hash**
Se refiere a una función o método para generar claves o llaves que representen de manera unívoca a un documento, registro y/o archivo.
- h) **Hipertexto**
Texto que contiene elementos a partir de los cuales se puede acceder a otra información.
- i) **Infoestructura**
Son infraestructuras reconocidas como el medio generador por el cual una nación convierte los activos, ya sea materiales en bruto, tecnologías o ideas, en productos de valor y servicios.
- j) **Integridad**
Constituye un atributo de la información para asegurar que ésta, al almacenarse o al ser trasladada, no sea modificada de ninguna forma no autorizada.
- k) **Internet**
Conjunto descentralizado de redes de comunicación interconectadas que utilizan el protocolo de control de transporte y el protocolo de Internet, según sus siglas en inglés: TCP/IP; garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.
- l) **Página Web**
Documento situado en una red informática, al que se accede mediante enlaces de hipertexto.
- m) **Proveedor de servicio**
Toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático.

Cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios.
- n) **Salario mínimo legal vigente**
Es el salario mínimo que establece la ley como retribución mensual para un trabajador que realice actividades no agrícolas. Con relación a las penas



000030

establecidas en la presente ley, debe aplicarse el salario mínimo legal vigente al momento de la comisión del delito.

o) **Sistema informático:**

Dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos.

p) **Sistema operativo**

Programa especial que se carga en un computador luego de ser encendido y cuya función es gestionar los demás programas o aplicaciones, que se ejecutarán en dicho computador como, por ejemplo, un procesador de texto, una hoja de cálculo, la impresión de un texto en una impresora o una conexión a internet.

q) **Software**

Se refiere al equipamiento lógico o soporte lógico de un computador digital, y comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica.

r) **Correo electrónico masivo**

Constituye todos aquellos mensajes no solicitados o no deseados por el destinatario y de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.

s) **Tarjeta inteligente**

Es una tarjeta con circuitos integrados que permite la ejecución de una lógica programada para proveer servicios de seguridad de la información.

t) **Tecnologías de la información**

Rama de la tecnología que se dedica al estudio, aplicación y procesamiento de información, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, protección, procesamiento, transmisión y recuperación de información, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso de equipos y programas, cualesquiera de sus componentes y todos los procedimientos vinculados con el procesamiento de información.

TÍTULO II

000031

DE LOS DELITOS

CAPÍTULO I

DELITOS CONTRA LA CONFIDENCIALIDAD, INTEGRIDAD Y

DISPONIBILIDAD DE DATOS Y TECNOLOGÍAS DE LA INFORMACIÓN

Artículo 5. Acceso ilícito. Quien acceda a sistema que haga uso de tecnologías de la información, sin autorización o excediéndola, será sancionado con prisión de dos a cuatro años y multa de cien a quinientas veces el salario mínimo legal vigente.

La pena será de tres a seis años de prisión y multa de doscientas a setecientas veces el salario mínimo legal vigente en los siguientes casos:

- a) Cuando, para acceder al sistema se suplante la identidad del destinatario o del remitente;
- b) El hecho de utilizar programa, equipo, material o dispositivo para obtener acceso a sistema que utilice tecnologías de la información o cualquiera de sus componentes, para ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de dichos servicios;
- c) Cuando el acceso se realice al generar, copiar, grabar, capturar, utilizar, alterar, divulgar, traficar, desenscriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares o falsificando cualquier tipo de dispositivo de acceso al mismo;
- d) El hecho de utilizar programa, equipo, material o dispositivo para obtener acceso a equipos o sistemas que utilicen tecnologías de la información o cualquiera de sus componentes, haciendo uso no autorizado del mismo, para procesar o realizar cualquier tipo de acción no autorizada por el propietario o legítimo usuario.

Artículo 6. Daño informático. Comete el delito de daño informático quien, sin estar autorizado, alterare, destruyere, inutilizare, suprimiere, modificare, o de cualquier modo o por cualquier medio, dañare un sistema que utilice tecnologías de la información o un componente de éste será sancionado con prisión de cuatro a ocho años y multa de cien a quinientas veces el salario mínimo legal vigente.

Artículo 7. Reproducción de dispositivos de acceso. Quien de manera deliberada, cree, utilice, altere, capture, grabe, copie o transfiera de un dispositivo

de acceso a otro similar, o cualquier instrumento destinado a los mismos fines, los códigos de identificación y/o acceso al servicio o sistema que haga uso de tecnologías de la información, que permita la operación paralela, simultánea o independiente de un servicio legítimamente obtenido, será sancionado con prisión de cuatro a ocho años y multa de cien a quinientas veces el salario mínimo legal vigente.

Artículo 8. Dispositivos fraudulentos. Quien produzca, utilice, comercialice u ofrezca sin autorización o causa legítima, uno o varios programas informáticos, equipo, material o dispositivo cuyo uso principal sea el de emplearse como herramienta o medio para cometer los delitos regulados en la presente ley, se sancionará de la manera siguiente:

- a) Con pena de tres a siete años de prisión para el solicitante;
- b) Con pena de cuatro a ocho años de prisión para el productor;
- c) Con pena de cuatro a ocho años de prisión para el que comercializa u ofrece;
- d) Con pena de tres a siete años de prisión para el que lo utiliza;

Cuando exista concurrencia de las agravantes específicas mencionadas, se aplicará la de mayor penalidad. Además de la pena de prisión que corresponda, el delito será sancionado con multa de cien a setecientas veces el salario mínimo legal vigente.

Artículo 9. Espionaje informático. Comete el delito de espionaje informático quien, sin estar facultado para ello, se apodere, obtenga, revele, transmita o difunda el contenido, parcial o total, de sistema que utilice tecnologías de la información o dato informático, de carácter público o privado, será sancionado con prisión de seis a diez años y multa desde doscientas a setecientas veces el salario mínimo legal vigente.

La pena será aumentada en una tercera parte, cuando para la realización del hecho, se creare o desarrollare sistema que utilice tecnologías de la información, dispositivo o dato informático que afecte la intimidad o privacidad de las personas.

Artículo 10. Violación a la disponibilidad. Quien por cualquier medio, provoque la denegación de acceso a redes, información y sistemas que utilicen tecnologías de información, a las personas que están legitimadas para hacerlo, se sancionará con pena de seis a diez años de prisión y multa desde cien a quinientas veces el salario mínimo legal vigente.

Cuando se deniegue la confirmación de identidad del destinatario o del remitente, ocasionando repudiación de los sistemas a las personas que están autorizadas o legitimadas para hacerlo, la pena se elevará de doce a quince años de prisión y multa desde doscientas hasta ochocientas veces el salario mínimo legal vigente.

000033

Igual pena se aplicará cuando la denegación de acceso, sea provocada por el envío masivo de mensajes electrónicos, publicitarios o de cualquier otra índole.

Artículo 11. Fraude informático. Quien, para obtener algún beneficio para sí mismo o para un tercero, mediante cualquier artificio tecnológico o manipulación de sistema que haga uso de tecnologías de la información, o, a sus componentes, procure la transferencia no autorizada de cualquier activo patrimonial en perjuicio de otro, será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente.

Artículo 12. Interceptación ilícita. Quien intercepte de forma deliberada e ilegítima por cualquier medio, datos informáticos en transmisiones restringidas, dirigidas u originadas en un sistema que utilice tecnologías de la información, incluidas las emisiones electromagnéticas provenientes o efectuadas dentro del mismo, que transporte dichos datos informáticos, será penado con prisión de seis a diez años y multa desde cien hasta mil veces el salario mínimo legal vigente.

La pena se aumentará en una tercera parte, cuando la interceptación se cometa desde un sistema que utilice tecnologías de la información conectado a otro sistema de la misma naturaleza.

Artículo 13. Falsificación informática. Quien a través de cualquier medio, copie, altere, sustituya deliberada e ilegítimamente datos informáticos de un sistema que haga uso de tecnologías de la información o uno de sus componentes, generando un resultado no auténtico o para inducir a usuarios a la provisión de datos personales y/o financieros, será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente.

La pena se aumentará en una tercera parte, si la intención es que el resultado sea utilizado a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.

Artículo 14. Agravantes generales. En las acciones delictivas descritas en los artículos del 5 al 13, 16, 17, 18, 19 y 20 en cuanto sea aplicable, la pena se aumentará en una tercera parte, en los casos siguientes:

- a) Cuando el hecho sea realizado por cualquier persona que preste o haya prestado sus servicios, directa o indirectamente a la persona física o jurídica afectada. En caso de que el delito hubiera sido realizado por empleado o funcionario público, además de la pena aplicable, será inhabilitado para ejercer funciones públicas por un período no menor de siete años;



00.0034

- b) Cuando de la acción realizada resulte la denegación de acceso, supresión o la modificación de datos confidenciales, reservados o de seguridad nacional, contenidos en el sistema que utilice tecnologías de la información;
- c) Cuando el acto se realice para recibir ilícitamente beneficio pecuniario o de cualquier otra índole, ya sea propio o para terceros, o para gozar de los servicios ofrecidos a través de cualquiera de estos sistemas;
- d) Quien a sabiendas de la comisión de un hecho ilícito cometido por un tercero, obtuviere beneficio pecuniario o de cualquier otra índole, ya sea propio o para terceros, o para gozar de los servicios ofrecidos a través de cualquiera de estos sistemas;
- e) Cuando el hecho cometido forma parte de una acción más amplia, que constituya un acto hostil;
- f) Cuando el hecho cometido sea realizado para deteriorar la infoestructura del Estado de Guatemala.

CAPÍTULO II

DELITOS CONTRA LA PERSONA

Artículo 15. Delitos de pornografía infantil. Cuando las infracciones establecidas en el Código Penal Decreto Número 17-73, y el Decreto Número 09-2009 sobre Ley Contra la Violencia Sexual, Explotación y Trata de Personas, se cometan a través del empleo de sistemas que utilicen tecnologías de la información, o de cualquiera de sus componentes, se sancionará con las penas establecidas en las respectivas leyes para estos ilícitos, exceptuando lo contenido en el artículo 16 de la presente ley.

Artículo 16. Control de acceso a pornografía infantil. Los proveedores de servicio de internet, deberán establecer normas mínimas de seguridad para bloquear el acceso a portales o páginas web que contengan material pornográfico infantil, y, en caso de incumplimiento, se les considerará coautores juntamente con las personas responsables de los delitos relativos a la pornografía infantil en lo que fuera aplicable.

Estas normas mínimas de seguridad se emitirán y actualizarán anualmente por el Comité de Respuesta a Incidentes de Seguridad Informática para Guatemala.

Artículo 17. Difusión y alteración de imágenes personales. Quien sin la autorización explícita y por escrito del titular, modifique, altere, envíe, difunda, transmita o almacene imágenes de otra persona por medio de sistemas que utilicen tecnologías de la información, para fines fraudulentos o con intención de perjudicar el honor de una persona, será sancionado con prisión de cuatro a seis años y multa de cien a trescientas veces el salario mínimo legal vigente.

No constituyen delito o falta las publicaciones que contengan denuncias, críticas o imputaciones contra funcionarios o empleados públicos por actos efectuados en el ejercicio de sus cargos.

Artículo 18. Uso de identidad ajena. Quien haga uso de una identidad ajena, a través de medios que utilicen tecnologías de la información, será sancionado con pena de prisión de tres a siete años y multa de trescientas a setecientas veces el salario mínimo legal vigente.

CAPÍTULO III

DELITOS CONTRA LA NACIÓN Y ACTOS DE TERRORISMO

Artículo 19. Delitos contra la Nación. Los actos que se realicen a través de un sistema que utilice tecnologías de la información, que atenten contra los intereses fundamentales y seguridad de la Nación, tales como el sabotaje, el espionaje o proveer información no autorizada, serán castigados con penas de diez a veinte años de prisión y multa de mil a diez mil veces el salario mínimo legal vigente.

Artículo 20. Actos de terrorismo informático. Todo aquel que con el uso de sistemas que utilicen tecnologías de la información, ejerza actos de terrorismo contra la infoestructura del Estado, será castigado con pena de diez a veinte años de prisión y multa de mil a diez mil veces el salario mínimo legal vigente.

TÍTULO III

ORGANISMOS COMPETENTES Y REGLAS DE DERECHO PROCESAL

CAPÍTULO I

ORGANISMOS COMPETENTES

Artículo 21. Comité de Respuesta a Incidentes de Seguridad Informática para Guatemala. Se crea el Comité de Respuesta a Incidentes de Seguridad Informática para Guatemala, que, por sus siglas en inglés, podrá denominarse "CSIRT-gt", como un ente adscrito al Ministerio de la Defensa Nacional.

El CSIRT-gt tendrá a su cargo la promoción de la seguridad informática a nivel nacional, lo que incluye las funciones siguientes:

- a) **Proactivas:** Consistentes en educación, asesoramiento técnico, alertas y promoción de estándares de seguridad;
- b) **Reactivas:** Consistentes en la asistencia a incidentes de seguridad informática, tanto a instituciones públicas como privadas y la realización de todos aquellos actos de mitigación de daño en materia informática. Asimismo, el CSIRT-gt deberá formular las recomendaciones necesarias para el cumplimiento de la presente ley, su reglamento y las normas relativas a la prevención de incidentes de seguridad informática contenidas en manuales, reglamentos o circulares emitidos por dicho Comité;
- c) **Investigación y desarrollo:** Consistentes en actividades que generen proyectos de investigación y desarrollo de tecnologías convergentes a la iniciativa de seguridad informática.

Artículo 22. Organización del Comité de Respuesta a Incidentes de Seguridad Informática (CSIRT-gt). El CSIRT-gt, estará integrado de la manera siguiente: (a) Un Comité Director; (b) Un Comité Operativo; y, (c) Por todas aquellas personas jurídicas, públicas o privadas, que deseen adherirse al CSIRT-gt, de conformidad con las normas establecidas en el Reglamento respectivo.

A. Comité Director:

Este Comité estará integrado por un representante de cada una de las instituciones siguientes:

- a) Ministerio de la Defensa;
- b) Ministerio de Relaciones Exteriores;
- c) Ministerio Público;
- d) Ministerio de Gobernación;
- e) Superintendencia de Bancos;
- f) Superintendencia de Telecomunicaciones; y,
- g) Secretaría Técnica del Consejo Nacional de Seguridad.

Los miembros del Comité Director elegirán, entre sus miembros, con el voto de la mayoría, al Coordinador Nacional del CSIRT-gt, el que durará en sus funciones dos años y no podrá ser reelecto.

B. Comité Operativo:

Este Comité estará integrado por dos o más delegados de las instituciones siguientes:

- a) Ministerio de la Defensa;
- b) Ministerio Público; y,

c) Ministerio de Gobernación

000037

Cada uno de los miembros del Comité Operativo deberá contar con acreditación de seguridad informática extendida por un ente certificador debidamente autorizado y cumplir con el perfil establecido en el reglamento correspondiente.

C. Personas adheridas:

Cada uno de los organismos del Estado, sus instituciones y dependencias, deberán formar parte del CSIRT-gt, a efecto de participar activamente en la generación y cumplimiento de las políticas de seguridad informática a nivel nacional.

Artículo 23. Funciones del Comité Director. El Comité Director tendrá como funciones principales:

- a) La coordinación y cooperación entre las diferentes entidades e instituciones públicas y privadas, sobre la forma de afrontar las diferentes amenazas informáticas;
- b) Establecer y definir la infoestructura estratégica del Estado de Guatemala;
- c) Identificar los riesgos y amenazas de la infoestructura del Estado de Guatemala; y,
- d) Representar al Estado de Guatemala ante cualquier organismo internacional o nacional y otros organismos internacionales con funciones similares al CSIRT-gt, como el ente responsable de la respuesta ante incidentes de seguridad informática

Artículo 24. Reglamento y funciones del CSIRT-gt. En un plazo no mayor de noventa días a partir del inicio de vigencia de la presente Ley, el CSIRT-gt desarrollará su reglamento y funciones.

Artículo 25. Fiscalía Especial del Ministerio Público. El Ministerio Público deberá contar con una Fiscalía Especial en la investigación y persecución de los delitos contenidos en la presente ley. La que debe ser creada y organizada en el plazo de tres meses a partir de la entrada en vigencia de la presente ley. Para la operatividad de esta fiscalía, se conformará una fuerza de tarea conjunta.

Artículo 26. Garantía de funcionamiento de la persecución penal. Para la garantía del funcionamiento armónico y adecuado de la persecución penal, las dependencias centralizadas, descentralizadas, autónomas y semiautónomas que hasta la entrada en vigencia de la presente ley realizan actividades concernientes a la investigación de delitos informáticos, deberán poner a disposición directa del Ministerio Público las unidades o dependencias que estén creadas y en funcionamiento, a efecto de que esta coordine la actividad de investigación

relacionada a los delitos contenidos en la presente ley y otros que por su naturaleza se necesite de la aplicación de conocimientos técnicos especializados. Dichas dependencias conformarán una fuerza de tarea conjunta.

El CSIRT-gt deberá proporcionar la asesoría técnica que sea necesaria para la investigación de delitos informáticos.

Artículo 27. Personal de la fuerza de tarea conjunta. El personal que conforme la fuerza de tarea conjunta deberá contar con certificaciones de seguridad informática o documentación correspondiente, que avalen su pericia en el área de la informática, así como de la investigación y áreas afines.

Artículo 28. Organización de la fuerza de tarea conjunta. El Ministerio Público coordinará con las instituciones dedicadas a la investigación criminal relativa a delitos informáticos, la conformación de las unidades que sean necesarias, las cuales estarán integradas por personal especializado de las dependencias puestas a su disposición, y actuarán de conformidad con las facultades que la ley otorgue a cada una de las dependencias a las cuales pertenecen, lo cual se entenderá como una fuerza de tarea común, que coadyuve en el proceso investigativo y de persecución de este tipo de delitos.

Artículo 29. Reglamentación administrativa y operativa. El Ministerio Público y demás superiores jerárquicos de las dependencias que actualmente cuentan con unidades de combate a delitos informáticos, nombrarán sus representantes correspondientes para crear los reglamentos administrativos y operativos que contengan como mínimo la estructura organizacional, formas de enlace y coordinación con las instituciones que sean puestas a su disposición, unidades de inteligencia, investigaciones, operaciones, recuperación de evidencia, personal operativo y administrativo, planificación, capacitación, régimen disciplinario y otras acciones necesarias que garanticen su funcionamiento. El tiempo para la creación de los reglamentos será de seis meses a partir de la entrada en vigencia de la presente ley.

CAPÍTULO II

MEDIDAS CAUTELARES Y PROCESALES

Artículo 30. Aplicación del Código Procesal Penal. Los medios de investigación regulados dentro del Código Procesal Penal y otras leyes vigentes, se aplicarán en lo que fueren procedentes, para la obtención y preservación de los datos contenidos en un sistema que utilice tecnologías de la información o sus componentes, datos de tráfico, conexión, acceso o cualquier otra información de utilidad, en la investigación de los delitos penalizados en la presente ley y para todos los procedimientos establecidos en este Capítulo.

Todas las medidas cautelares a que se refiere la presente ley, deberán ser decretadas por juez competente, en un plazo no mayor de veinticuatro horas, pudiéndose solicitar y decretar por medios electrónicos.

El Ministerio Público podrá disponer de medidas cautelares sin previa autorización judicial, en caso de urgencia determinada por los medios investigativos, y que sean indispensables para evitar un daño irreparable o cuando los hechos sean irreproducibles en otro momento. Estas medidas deberán ser convalidadas por el juez contralor dentro de un plazo de cuarenta y ocho horas a partir del momento de su ejecución.

Artículo 31. Conservación de datos informáticos almacenados. Toda persona individual o jurídica que provea servicio de conexión a internet, deberá, a requerimiento de autoridad judicial competente, conservar datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema que utilice tecnologías de la información, debiendo proteger su integridad el tiempo que se le indique en la orden judicial correspondiente.

La conservación será por un plazo mínimo de noventa días a partir de la notificación de la autoridad judicial correspondiente, con el fin de que las autoridades competentes puedan obtener su revelación. Dicho plazo podrá ser prorrogado a solicitud de dicha autoridad, con diez días de antelación a la fecha de vencimiento.

La persona o institución que custodia los datos o los conserva, deberá mantener bajo confidencialidad la ejecución de dichos procedimientos.

Artículo 32. Orden de presentación. Toda persona individual o jurídica, a requerimiento de la autoridad judicial competente, deberá presentar datos informáticos que obren en su poder o bajo su control, almacenados en un sistema que utilice tecnologías de la información o en un dispositivo de almacenamiento informático independientemente a que estos se encuentren dentro del territorio nacional o fuera de éste.

Para efectos del presente artículo se entenderá por "datos relativos a los abonados" cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

- a) El tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
- b) La identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a

la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio; y,

- c) Cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

Artículo 33. Facultades del Ministerio Público. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, peritos, instituciones públicas o privadas, u otra autoridad competente. Asimismo el Ministerio Público tendrá la facultad de:

- a) Ordenar a una persona física o jurídica la entrega de la información que se encuentre en un sistema de información o en cualquiera de sus componentes;
- b) Ordenar a una persona física o jurídica preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un periodo de hasta noventa (90) días, pudiendo esta orden ser renovada por periodos sucesivos;
- c) Acceder u ordenar el acceso a dicho sistema de información o a cualquiera de sus componentes;
- d) Ordenar a un proveedor de servicios, incluyendo los proveedores de servicios de internet, a suministrar información de los datos relativos de un usuario que pueda tener en su posesión o control;
- e) Tomar en secuestro o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte;
- f) Recolectar o grabar los datos de un sistema que utilice tecnologías de la información o de cualquiera de sus componentes, a través de la aplicación de medidas tecnológicas;
- g) Ordenar el mantenimiento de la integridad del contenido de un sistema de información o de cualquiera de sus componentes;
- h) Hacer inaccesible o remover el contenido de un sistema de información o de cualquiera de sus componentes, que haya sido accesado para la investigación;
- i) Ordenar a la persona que tenga conocimiento acerca del funcionamiento de un sistema que utilice tecnologías de la información o de cualquiera de sus componentes o de las medidas de protección de los datos en dicho sistema, a proveer la información necesaria para realizar las investigaciones;

- j) Solicitar al proveedor de servicios recolectar, extraer o grabar los datos relativos a un usuario, así como el tráfico de datos en tiempo real, a través de la aplicación de medidas tecnológicas;
- k) Realizar la intervención o interceptación de las telecomunicaciones en tiempo real, según el procedimiento establecido en la Ley contra la Delincuencia Organizada, Decreto Número 21-2006 del Congreso de la República, para la investigación de todos los hechos punibles en la presente ley;
- l) Ordenar cualquier otra medida aplicable a un sistema que utilice tecnologías de la información o sus componentes para obtener los datos necesarios y asegurar la preservación de los mismos; y,
- m) Ordenar la confiscación y/o destrucción del sistema que utilice tecnologías de la información o sus componentes, propiedad del sujeto activo utilizado para cometer el delito.

Artículo 34. Registro y confiscación de datos informáticos almacenados.

Las partes vinculadas a la investigación con autorización de juez competente, podrán registrar o tener acceso a todo sistema que utilice tecnologías de la información o parte del mismo, así como a los datos informáticos en él almacenados cuando dichos datos sean accesibles a partir del sistema inicial, situado en el territorio nacional, pudiendo extenderse el registro a otro sistema, independientemente de su ubicación geográfica.

Esta disposición faculta y obliga al Ministerio Público a confiscar y/u obtener de un modo similar los datos informáticos a los que se hubiera accedido en aplicación del párrafo anterior.

Estas medidas incluirán las siguientes:

- a) Confiscar u obtener de sistema que utilice tecnologías de la información o una parte del mismo, todos aquellos datos informáticos que puedan ser útiles para la investigación;
- b) Realizar y conservar una copia protegida de esos datos informáticos, preservando su llave hash;
- c) Preservar la identidad e integridad de los datos informáticos almacenados;
- d) Hacer accesibles dichos datos informáticos;
- e) Suprimir dichos datos informáticos del sistema consultado, cuando su contenido sea objeto o materia de los delitos de pornografía infantil y alteración

000042

y difusión de imágenes, previo a cumplir lo establecido en el inciso "b" de este artículo.

El Ministerio Público tendrá las facultades necesarias para ordenar a quien ejerza control, administre, use sistema que utilice tecnologías de la información, las medidas aplicables para proteger los datos informáticos, proporcionando la información necesaria, que permita la aplicación de las medidas previstas en los párrafos anteriores.

Artículo 35. Obtención en tiempo real de datos relativos al tráfico. Se faculta al Ministerio Público, con autorización de juez competente, a lo siguiente:

- a) Por sus propios medios, podrá obtener o grabar los datos relativos al tráfico generado por sistema que utilice tecnologías de la información, necesarios para la investigación;
- b) Obligar a cualquier proveedor de servicio, en la medida de sus capacidades técnicas a obtener o grabar en tiempo real, los datos relativos al tráfico generado por sistema que utilice tecnologías de la información, necesarios para la investigación; y,
- c) Cuando el requerido no pueda adoptar las medidas enunciadas en el inciso anterior, deberá colaborar técnicamente en la obtención y/o grabación en tiempo real de los datos relativos al contenido.

Todo proveedor de servicio deberá mantener bajo confidencialidad el hecho de que se haya ejercido cualquiera de las facultades previstas en el presente artículo, así como la información relacionada.

Artículo 36. Interceptación de datos relativos al contenido. Se faculta al Ministerio Público, con autorización de juez competente, a lo siguiente:

- a) Por sus propios medios, podrá interceptar, obtener y/o grabar los datos generados por sistema que utilice tecnologías de la información, necesarios para la investigación;
- b) Por sus propios medios o con colaboración del CSIRT-gt, podrá alterar, suspender o borrar cualquier actividad, que haga uso de sistema que utilice tecnologías de la información, en la comisión de los delitos establecidos en la presente ley; y,
- c) Obligar a cualquier proveedor de servicios:
 - 1. A facilitar la obtención, grabación o, a interceptar los datos relativos a comunicaciones específicas transmitidas dentro del territorio nacional, por medio de un sistema que utilice tecnologías de la información.

2. Por sus propios medios, obtenga o grabe los datos relativos al tráfico generado por sistemas que utilicen tecnologías de la información, necesarios para la investigación.

Artículo 37. Mejores prácticas de recopilación de evidencia. El Ministerio Público y demás instituciones auxiliares, implementarán las normas reglamentarias que incluyan el uso de buenas y mejores prácticas y métodos eficientes, dentro de los estándares internacionales, en los procesos de investigación para la ubicación, documentación, recuperación y conservación de evidencia.

Artículo 38. Proveedores de servicios de Internet. El Ministerio Público, la Superintendencia de Telecomunicaciones, CSIRT-gt y dependencias que forman la fuerza de tarea conjunta, crearán el reglamento para el procedimiento de obtención y preservación de datos e información por parte de los proveedores de servicios de internet, en un plazo de seis meses a partir de la entrada en vigencia de la presente ley. Dicha normativa deberá regular lo referente a la importancia de preservación de la prueba, no obstante la cantidad de proveedores involucrados en la transmisión o comunicación.

Artículo 39. De las responsabilidades de los proveedores de servicio de internet. El proveedor de servicio que incumpla cualquiera de las obligaciones aquí establecidas, quedará sujeto a responsabilidad por daños y perjuicios, independientemente de cualquier otra sanción, falta o delito que sea aplicable.

Artículo 40. Desnaturalización del proceso investigativo. La desnaturalización de los hechos de investigación por parte de las autoridades competentes será sancionada con la destitución inmediata del cargo del responsable, prisión de tres a cinco años y multa de cien a mil veces el salario mínimo legal vigente.

Dentro de los actos de desnaturalización, se considerarán, entre otros:

- a) La realización de actos que no tengan relación con el proceso;
- b) El tráfico y comercialización de los datos obtenidos durante la investigación;
- c) La divulgación de datos personales y/o comerciales de la persona sindicada, distintos a la naturaleza de la investigación.

Artículo 41. Responsabilidad del custodio. La persona encargada de la preservación o custodia de sistema que utilice tecnologías de la información o de cualquiera de sus componentes, así como de su contenido, deberá conservar la confidencialidad, disponibilidad e integridad de los mismos, impidiendo que terceros no autorizados y/o ajenos a la diligencia, tengan acceso y conocimiento de ellos.

Asimismo, dicha persona encargada, no podrá hacer uso del objeto custodiado para fines distintos a los concernientes al proceso.

Artículo 42. Confidencialidad de la investigación. Quien colabore o participe en el proceso de investigación, en cuanto a la recolección, conservación, interceptación e intervención de datos de un sistema que utilice tecnologías de la información o de sus componentes, o cualquiera otra acción, incluyendo a los proveedores de servicios, mantendrá bajo confidencialidad lo realizado por parte de la autoridad competente.

Artículo 43. Violación de confidencialidad. La persona que viole la obligación de confidencialidad contenida en los artículos de la presente ley, será sancionada con prisión de seis meses a dos años y multa de cien a trescientas veces el salario mínimo legal vigente. Si la persona fuere empleado público se aplicarán las medidas establecidas en el artículo 16 en cuanto fuere posible.

TÍTULO IV

COOPERACIÓN INTERNACIONAL Y ASISTENCIA JURÍDICA MUTUA

Artículo 44. Cooperación internacional. El Estado de Guatemala deberá propiciar la cooperación técnica y económica internacional a través de sus órganos competentes, con el fin de fortalecer los programas de prevención, investigación y represión de todas las actividades relacionadas con los delitos informáticos.

Artículo 45. Capacitación. El Estado de Guatemala promoverá la capacitación regular y técnica de los funcionarios responsables de los controles de seguridad interna y externa, relacionados con delitos informáticos. Con tal finalidad, se promoverá una estrecha cooperación con los países de la región, o de cualquier otro continente, para proveer apoyo técnico y entrenamiento para aquellos que lo requieran, de manera que se alcance un objetivo común de armonización gradual del entrenamiento y calificación del personal responsable de la seguridad informática.

Artículo 46. Reuniones interinstitucionales. El Estado de Guatemala fomentará reuniones interinstitucionales de seguridad informática con carácter nacional e internacional.

Artículo 47. Convenios. El Estado de Guatemala procurará concertar acuerdos bilaterales y/o multilaterales para llevar a cabo y facilitar la persecución penal de los delitos informáticos, la realización de sus componentes procesales y acciones

administrativas coordinadas o no, que fomenten la armonía en temas de cooperación internacional y asistencia jurídica mutua.

Artículo 48. Asistencia Jurídica Mutua. El Estado de Guatemala podrá formalizar con otros Estados de conformidad con la práctica internacional, la prestación de asistencia judicial recíproca en las investigaciones, procesos y actuaciones judiciales referentes a delitos tipificados en la presente ley, con apego al derecho interno y los instrumentos internacionales de los cuales Guatemala es parte.

Artículo 49. Doble incriminación. Para la prestación de asistencia jurídica mutua no será exigible el requisito de la doble incriminación, salvo que se tratare de medidas de carácter coercitivo.

Artículo 50. Inmovilización de activos. El Ministerio Público cuando sea procedente instruirá a las instituciones financieras, para que impidan la realización de operaciones que involucren a personas, respecto de las cuales existan indicios de estar vinculadas a organizaciones criminales relacionadas con los delitos contenidos en la presente ley. La decisión deberá comunicarse inmediatamente al tribunal competente, el cual, consideradas las circunstancias del caso, determinará si correspondiere, sin previa notificación, la inmovilización de los activos de las personas involucradas en los hechos delictivos, considerados en la presente ley.

TÍTULO V

DISPOSICIONES FINALES

Artículo 51. Responsabilidad civil y penal de las personas jurídicas. Además de las sanciones que se indican más adelante, las personas jurídicas son responsables civilmente de las infracciones cometidas por sus órganos, representantes, empleados o cualquier persona que preste sus servicios para dicha entidad.

La responsabilidad penal por los delitos contenidos en esta ley, se extiende a quienes ordenen o dispongan de su realización y a los representantes legales de las personas jurídicas que conociendo de la ilicitud del hecho y teniendo la potestad para no permitirlo, lo permitan, tomen parte en él, lo faciliten o lo encubran. La responsabilidad penal de las personas jurídicas no excluye la de cualquier persona física, autor o cómplice de los mismos hechos. Cuando las personas jurídicas sean utilizadas como medios o cubierta para la comisión de un delito, o se incurra a través de ella en una omisión punible, las mismas se sancionarán con una, varias o todas de las penas siguientes:

- a) Una multa igual o hasta el doble de la contemplada para la persona física para el hecho ilícito contemplado en la presente ley;

000046

- b) La disolución, cuando se trate de un delito sancionado en cuanto a las personas individuales o físicas se refieren con una pena privativa de libertad superior a cinco años;
- c) La prohibición, a título definitivo o por un período no mayor de cinco años, de ejercer directa o indirectamente una o varias actividades profesionales o sociales;
- d) La sujeción a la vigilancia por un período no mayor de cinco años;
- e) La clausura definitiva o por un período de hasta cinco años, de uno o varios de los establecimientos de la empresa, que hubieran servido para cometer los hechos imputables;
- f) La exclusión de participar en los procesos de cotización y licitación, a título definitivo o por un período no menor de cinco años;
- g) La prohibición definitiva o por un período no menor de cinco años, de participar en actividades destinadas a la captación de títulos valores;
- h) La confiscación del bien o bienes que han servido o estaban destinados a cometer la infracción, o de la cosa que es su producto; y,
- i) La publicación de la sentencia pronunciada o la difusión de ésta, sea por la prensa escrita o por otro medio de comunicación.

Asimismo, se considerará responsable civilmente a una persona jurídica cuando la falta de vigilancia o de control de su representante legal o empleado haya hecho posible la comisión de un acto ilícito previsto en la presente ley.

Artículo 52. Acciones administrativas. Lo establecido en la presente ley no impide recurrir a las acciones administrativas que puedan resultar de leyes y reglamentos especiales aplicables.

Artículo 53. Pago de indemnizaciones. Sin perjuicio de las sanciones penales y/o administrativas que puedan resultar de leyes y reglamentos especiales, las personas físicas o jurídicas podrán ser condenadas al pago de indemnizaciones civiles a favor del sujeto pasivo.

Artículo 54. Tribunal competente. Los procesos judiciales correspondientes a los delitos que se comentan haciendo uso de sistemas que utilicen tecnologías de la información, serán conocidos por los tribunales ordinarios correspondientes o por los Juzgados de la Niñez y la Adolescencia, dependiendo del caso. Los jueces podrán valerse de la presentación de un peritaje para el conocimiento del fondo del caso.

Artículo 55. Derogatoria. Con la promulgación de la presente Ley, se deroga el contenido del artículo 274 "A", 274 "B", 274 "C", 274 "D", y 274 "F" del Código Penal, así como cualquier norma o disposición que le sea contraria a la misma en esta materia.

Artículo 56. Resoluciones electrónicas. Debido a que los actos regulados en la presente ley, son de naturaleza informática y se producen en tiempo real, se hace necesario que los tribunales competentes y la fiscalía especial del Ministerio Público cuenten con firma electrónica como un medio seguro de comunicación. Para el efecto, la Corte Suprema de Justicia y el Ministerio Público deberán generar firma electrónica para los jueces y fiscales competentes que garanticen la celeridad del proceso.

Artículo 57. Reglamentos. Las instituciones encargadas de la elaboración de los reglamentos establecidos en la presente ley, deberán ser emitidos en los plazos ya determinados.

Artículo 58. Entrada en vigencia. Esta ley iniciará su vigencia ocho días después de su publicación en el Diario de Centro América.