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

LOS HACKER EN LA INTERNET Y LAS CONSECUENCIAS PENALES DE LA FALTA DE REGULACIÓN

GEORGINA DONIS DE LA CRUZ

GUATEMALA, NOVIEMBRE DE 2011

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

LOS HACKER EN LA INTERNET Y LAS CONSECUENCIAS PENALES DE LA FALTA DE REGULACIÒN

TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y sociales

de la

Universidad de San Carlos de Guatemala

Por

GEORGINA DONIS DE LA CRUZ

Previo a conferirle el Grado Académico de

LICENCIADA EN CIENCIAS JURDICAS Y SOCIALES

Guatemala, noviembre de 2011

HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	Lic. Bonerge Amilcar Mejía Orellana
VOCAL I:	Lic. Avidán Ortiz Orellana
VOCAL II:	Lic. Mario Ismael Aguilar Elizardi
VOCAL III:	Llc. Luis Fernando López Díaz
VOCAL IV:	Br. Modesto José Eduardo Salazar Diéguez
VOCAL V:	Br. Pablo Josè Calderon Gàlvez
SECRETARIO	Lic. Marco Antonio Villatoro López

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

Carlos Antulio Salazar Urízar
Abogado y notario

Guatemala, 16 de Abril de 2009

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
29 ABR. 2009
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Licenciado
Carlos Manuel Castro Monroy
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales

Respetable Licenciado:

En el cumplimiento del nombramiento como asesor de Tesis de la Bachiller **GEORGINA DONIS DE LA CRUZ**, me dirijo a usted con el objeto de informar sobre mi labor y expongo lo siguiente:

El trabajo de Tesis se denomina "**LOS HACKER EN LA INTERNET Y LAS CONSECUENCIAS PENALES DE LA FALTA DE REGULACIÓN**"

Al respecto he de manifestar que el contenido del trabajo cumplió con los aspectos legales, doctrinarios, jurisprudenciales y de derecho comparado respecto al tema en mención, también se ajusto a los requerimientos científicos y técnicos que se deben cumplir de conformidad con la normativa respectiva, la metodología y técnica de investigación utilizada, la redacción, las conclusiones y recomendaciones a que arriba la autora y bibliografía utilizada son congruente con los temas desarrollados dentro de la investigación. Asimismo para el mejor desarrollo del trabajo se hicieron algunas correcciones a los temas y subtemas tratados en el trabajo.

En ese orden de ideas, considero que el trabajo de tesis correspondientes llena los requisitos establecidos en el artículo 32 del normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Publico, por lo que resulta procedente emitir **DICTAMEN FAVORABLE** al mismo.

Lic. Carlos Antulio Salazar Urízar
Abogado y Notario
Asesor
Colegiado 6,279

LIC CARLOS ANTULIO SALAZAR URIZAR
ABOGADO Y NOTARIO

8ª. Avenida 20-22 zona 1 Edificio Castañeda, 1º. Nivel Of. 4 Guatemala Ciudad
Teléfono 57096727

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Edificio S-7, Ciudad Universitaria
Guatemala, C. A.

UNIDAD ASESORÍA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, treinta de abril de dos mil nueve.

Atentamente, pase al (a la) LICENCIADO (A) EDDY AUGUSTO AGUILAR MUÑOZ, para que proceda a revisar el trabajo de tesis del (de la) estudiante GEORGINA DONIS DE LA CRUZ, Intitulado: "LOS HACKER EN LA INTERNET Y LAS CONSECUENCIAS PENALES DE LA FALTA DE REGULACIÓN".

Me permito hacer de su conocimiento que está facultado (a) para realizar las modificaciones de forma y fondo que tengan por objeto mejorar la investigación, asimismo, del título de trabajo de tesis. En el dictamen correspondiente debe hacer constar el contenido del Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, el cual dice: "Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes, su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que estimen pertinentes".

LIC. CARLOS MANUEL CASTRO MONROY
JEFE DE LA UNIDAD ASESORÍA DE TESIS

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

cc.Unidad de Tesis
CMCM/sllh

BUFETE CORPORATIVO
11 CALLE 4 -52 ZONA 1
Edificio Asturias Oficina 4

Guatemala, 27 Mayo de 2009

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
18 JUN. 2009
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

Licenciado
Calos Manuel Castro Monroy
Jefe de la Unidad de Asesoría de Tesis
FACULTAD DE Ciencias Jurídicas y Sociales

Respetable Licenciado:

En intención a la designación de esta unidad, según providencia de fecha treinta de Abril de dos mil nueve, procedí a revisar el trabajo de Tesis denominado **"LOS HACKER EN LA INTERNET Y LAS CONSECUENCIAS PENALES DE LA FALTA DE REGULACIÓN",** elaborado por la Bachiller **GEORGINA DONIS DE LA CRUZ.**

Al respecto he de manifestar que el contenido del trabajo contemplo los aspectos legales, doctrinarios, jurisprudenciales y derecho comparado respecto al tema en mención, también se ajusto a los requerimientos científicos y técnicas que se deben cumplir de conformidad con la normativa respectiva, la metodología y técnicas de investigación utilizada, la redacción, las conclusiones y recomendaciones a que arriba la autora y bibliografía utilizada son congruentes con el tema desarrollados dentro de la investigación. Asimismo para el mejor desarrollo del trabajo se hicieron algunas correcciones a los temas y subtemas tratados.

En este orden de ideas, considero que el trabajo de Tesis correspondiente llena los requisitos establecidos en el Artículo 32 del Normativo para la elaboración de tesis de Licenciatura de Ciencias Jurídicas y Sociales y del Examen General Publico, estimado que el mismo debe ser aprobado, para los efectos consiguientes emito el presente **DICTAMENT FAVORABLE** aprobando el trabajo de tesis revisado.

En argumento de lo anterior, procedí a revisar los diferentes métodos y técnicas aplicadas en la investigación, opinando que fueron aplicados adecuadamente, en virtud de que con ellos, se obtuvieron la información necesaria y objetiva para la elaboración, redacción y cuadros estadísticos para la presentación final del trabajo de tesis.

Atentamente

Lic. Eddy Augusto Aguilar Muñoz
Abogado y notario
Revisor
Colegiado 6,410

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Edificio S-7, Ciudad Universitaria
Guatemala, C. A.

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, uno de febrero del año dos mil once.

Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante GEORGINA DONIS DE LA CRUZ, Titulado LOS HACKER EN LA INTERNET Y LAS CONSECUENCIAS PENALES DE LA FALTA DE REGULACIÓN. Artículos 31, 33 y 34 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.-

CMCM/sllh.

DEDICATORIA

A Dios	Le doy gracias porque siempre estuvo conmigo cuando ya no quería continuar con este sueño que hoy se hace realidad, y por la intercesión de la Virgen María.
A mis padres	Manuela de la Cruz Pérez y José Augusto Donis López, por sus sabios consejos.
A mi esposo	René Aroldo Mollinedo Enríquez.
A mis hijos	Claudia Eugenia, Karla Georgina, Mónica Gabriela y René Aroldo por el sacrificio para mi preparación académica
A mis hermanos	Eloísa, Luis Humberto, Daniel, Juan José y María Dolores.
A mis amigos	Por haber estado conmigo en la realización de este sueño.
A:	La Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, por haberme dado la oportunidad de forjar mi preparación académica, por medio de sus maestros de calidad y por los consejos que recibí de ellos en el momento en que los necesité.

ÍNDICE

Pág.

CAPÍTULO IV

INTRODUCCIÓN

El presente trabajo de investigación, se realizo debido a que diversas empresas se dedican a proporcionar información de personas individuales o jurídicas, ya sea por medio de referencias comerciales, legales, laborales y por compartimiento ya sea de depósitos o pagos; esta información es extraída por cualquier persona a través del uso de la Internet, violando códigos privados.

Se puede señalar que con el presente trabajo se comprobó la hipótesis basada en la falta de regulación acerca de la actividad ilícita que realizan los hacker en el derecho virtual, lo cual perjudica a la sociedad guatemalteca por lo que es necesario que se regule en el Código Penal.

Este trabajo tuvo como objetivo establecer la necesidad que tiene la sociedad de experimentar una serie de cambios en el ámbito tecnológico, que de alguna manera debe trascender a las esferas de los marcos jurídicos, precisamente para que esos avances, esos cambios no transgredan bienes jurídicos ya establecidos en las leyes vigentes que perjudiquen sus derechos, y en este caso la necesidad de que se prohíban los abusos y las prácticas desleales que puedan producir perjuicio a la sociedad.

Con el aparecimiento de los denominados hacker en el Internet que claramente se evidencia o se refleja el atraso de la ley penal guatemalteca en relación al avance de la Internet (Internacional Network) y a las diversas herramientas virtuales que son creadas para vestir y actualizar cada año a dicha invención, que se ponen a disposición y servicio gratuito u oneroso de millones de usuarios a nivel mundial y por consecuencia, desafortunadamente se constata dicho atraso, si se le compara inevitablemente, con las leyes penales que se están implementando a nivel internacional para describir y combatir los llamados Cyber delitos o delitos informáticos, como sucede con el caso de la intervención de criminales denominados hacker.

Por ello, luego del desarrollo del trabajo bibliográfico, documental y de campo, se ha establecido la necesidad de que se regule la prohibición de la intromisión de los denominados hacker en la Internet, porque atentan contra los sistemas de computo y precisamente motivados provocan perjuicio a persona ajena que puede ser también, una persona individual o jurídica. Para una mayor comprensión, el trabajo ha sido dividido en capítulos.

En el capitulo primero se establece un breve análisis de los delitos informáticos; en el capítulo segundo, se demuestra los hackers en la doctrina y la legislación comparada; en el capítulo tercero, se hace una descripción de los delitos informáticos que regula el Código Penal guatemalteco, las actividades ilícitas que se realizan en la Internet por medio de los hackers, y la necesidad de su inclusión en el Código Penal; en el capítulo cuarto, se presentan los resultados del trabajo de campo, y las bases para el establecimiento de una reforma legal, en el Código Penal de Guatemala.

Los métodos contenidos en la presente investigación son los siguientes: Analítico, Deductivo, Sintético, e inductivo. Se utilizaron las técnicas de la observación y entrevista.

CAPÍTULO I

1-. Antecedente de los delitos informáticos

A lo largo de la historia el hombre ha necesitado transmitir y tratar la información de forma continua. La humanidad no ha cesado en la creación de métodos para procesar información. Con ese fin nace la informática, con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo o de gestión.

"Luego nace la Internet como una tecnología que pondría la cultura, la ciencia y la información al alcance de millones de personas de todo el mundo. Mucho se habla de los beneficios que los medios de comunicación y el uso que la informática han aportado a la sociedad actual, el objeto de este trabajo es analizar la otra cara de la moneda, las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática".[1]

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo; Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

1.1 Aspectos históricos sobre la informática y delitos que comenten los llamados hackers.

Se dice que el término de hacker surgió de los programadores del instituto tecnológico de Massachussets (MIT), que en los 60, por usar hacks, se llamaron a sí mismo

[1] Alcalá Zamora Luis **Derecho Procesal Penal.** Pág. 62

hackers, para indicar que podían hacer programas mejores y aun mas eficaces, o que hacían cosas que nadie había podido hacer.

Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica, relacionada con la informática programación redes de computadoras, sistemas operativos, hardware de red/vos etc. Se suele llamar hackeo y hackear a las obras propias de un hacker. También se dice que la palabra deriva "Hack". "hachar" en ingles, termino que se utilizaba para describir la forma en que los técnicos telefónicos arreglaban cajas defectuosas, un golpe seco. Y la persona que hacia eso era llamada hacker.

"El término "hacker" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que esta en la cúspide de la excelencia en su profesión, ya que en la descripción mas pura, un hacker es aquella persona que le apasiónale conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de estas."[2]

Hacker usando la palabra inglesa, quiere decir divertirse con el ingenio Cléber Ness, usar la inteligencia para hacer algo difícil. No implica trabajar solo ni con otros necesariamente es posible en cualquier proyecto. No implica tampoco hacerlo con computadoras. Es posible ser un hacker de las bicicletas. Por ejemplo, una fiesta sorpresa tiene el espíritu del Hack, usa el ingenio para sorprender al homenajeado, no para molestarle.

También se asocia el termino hacker a aquellas personas que poseen elevados conocimientos de sistemas y seguridad informática, los cuales pueden emplear en beneficio propio y de la comunidad con que comparten intereses. En tales casos suele distinguirse entre aquellos cuyas acciones son de carácter constructivos, informativo o

[2] Goldstein, Raúl. **Diccionario de Derecho Penal y Criminología**. 2ª. Edición, Editorial Astro Buenos Aires, 1983.

solo intrusivo, o que además lo son de tipo destructivo, catalogados respectivamente de hackers y crackers, o en círculos anglosajones, a veces, por las expresiones inglesas "White hat" y "Black hat". Recientemente ha aparecido el termino, mas neutro, "grey hat" ("sombreo gris") para referirse a aquellos hackers que ocasionalmente traspasan los limites entre ambas categorías, o los que realizan acciones que sin ser éticamente reprobables son tachadas por la legislación vigente o ideología dominante como acciones delictivas, ilícitas o ilegales, o incluso a la inversa.

Tipos de Hackers

a) Daek hats o blackers Negro

"Hackers negro también busca de los sistemas informáticos, pero de una manera maliciosa, buscando una satisfacción personal y/o económica. El hacker negro muestra sus habilidades en informática rompiendo computadoras, colapsando servidores. Entrando a zonas restringidas, infiriendo redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos hacking. Disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa."[3]

b) White hats o hackers Blanco.

Por lo general el hacker Blanco es una persona que busca los Bugs de los sistemas informáticos, por decir así de una manera genérica, dando a conocer a las compañías desarrolladoras de software o empresas sus vulnerabilidades, claras sin ánimo de perjudicar. Sin embargo hay algunos de ellos que si buscan el interés personal, queriendo entrar a sitios restringidos, estafando.

---

[3] De Silva Sánchez Luis **El Delito Informático** Pág. 65

c) Samurai

Son los más parecidos a una amenaza pura. Sabe lo que busca, donde encontrarlo y como lograrlo. Hace su trabajo por encargo y a cambio de dinero, no tiene conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers

d) Newbie

La palabra es una probable corrupción de newboy, arquetipo del "niño nuevo", que debido a la falta de intenciones socioculturales, queda vulnerable a varios tipos de abusos por parte de los otros. Son los hacker novatos, se introduce en sistemas de fácil acceso y fracasan en muchos intentos, solo con el objeto de aprender las técnicas que puedan hacer de él, un hacker reconocido, se dedica a leer, escuchar ver y probar las distintas técnicas que va aprendiendo. Solo pregunta a otros hackers, después de días de prueba sin resultados, de manera que mas que pregunta, expone su experiencia y pide opiniones o deja en el aire preguntas muy concretas.

1. 2 Definición de los delitos informáticos.

Antes de definir en que consisten los delitos informáticos y como surgieron en la realidad guatemalteca, es importante señalar en que consiste el delito como tal El delito para Bering citado por Raúl Gold Stein en el Diccionario de Derecho Penal y criminología, establece que "es una acción" típica, antijurídica, culpable, cubierta con una sanción penal adecuada a la culpabilidad y que llena las condiciones legales de punibilidad. Garland, citado por Zaffaroni, en su obra Tratado de Derecho Penal,

establece que delito es una conducta humana culpable, que viola las normas del Estado y que las leyes penales colocan bajo pena.

"Cuando se habla del delito informático se ha dicho que no hay definición de carácter universal propia para este, sin embargo, se ha evidenciado que se pretende efectuar una definición clara y adecuada para esta clase de delitos tan complejos que ofrece dificultades para los expertos que se han ocupado del tema, por eso se dice que no existe una definición con carácter universal, y esto ha tenido como consecuencia que se hayan formulado conceptos funcionales atendiendo a realidades nacionales concretas en los distintos países.

"El departamento de investigación de la Universidad de México"[4] entiende que delitos informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

"Otros autores entienden que para efectuar una definición de delito informático podrían adoptarse las posturas: estrígida: Es aquel hecho en el que, independientemente del perjuicio que pueda causarse a otros bienes jurídicamente tutelados y que eventualmente pueden concurrir en forma real o ideal, se atacan elementos puramente informáticos. Por ejemplo el uso indebido del software, apropiación indebida de datos, etc.

b) Amplia: Toda acción típicamente antijurídica y culpable para cuya consumación se utiliza o se afecta a una computadora o sus accesorios.

[4] El Delito Informático en México. **www.goesjurídica.com.htlm** Consulta internet: 14-2-2009.

c) El delito: del informático implica actividades criminales que en primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

"Se entiende por delitos informáticos a aquellas acciones típicas, antijurídicas y culpables que recaen sobre la infamación, atentando contra su integridad confidencialidad o disponibilidad, en cualquiera de las fases que tienen vinculación con su flujo o tratamiento, contenida en los sistemas informáticos de cualquier índole sobre los que operan las maniobras dolosas".[5]

1.3 Los bienes jurídicos tutelados de los delitos informáticos.

Los bienes jurídicos tutelados son la materia prima de la función o la razón de ser del Derecho Penal. A través de los mismos, se crea un conjunto de normas jurídicas y una serie de instituciones que pretenden, precisamente protegerlos. Dentro de los bienes jurídicos tutelados que están legitimados por la naturaleza de los mismos, esta la vida, el patrimonio, la libertad .

El Derecho Penal lo primero que ha de hacer es fijar los bienes jurídicos que han de ser protegidos penalmente y sobre esos principios variables en el tiempo y en el espacio, configurar específicamente los delitos y establecer la pena que a cada uno de ellos corresponde.

[5] **Dentro de ellos**, Luis De Silva Sánchez. **Ob. Cit**. Pág. 66

El bien que se resguardaría mediante la tipificación de delitos informáticos sería la pureza de la técnica que supone la informática, o sea el resguardo de los medios que supone la computación. Pero es evidente de que esto trasciende hacia otros bienes jurídicos tutelados tradicionales, como el patrimonio, la seguridad, la seguridad pública, etc.

"Todo atentado que signifique desviar el correcto desempeño de la máquina con la finalidad de obtener un perjuicio que redunde en beneficio material o moral para sí o para otro, constituirá el elemento caracterizante del delito en su manifestación más común".[6]

1.4 Los elementos intervinientes en los delitos informáticos.

a) elemento objetivo

El elemento objetivo del delito está dado por la acción que la ley tipifica como delito. Así, en el homicidio, "el que matare a otro" (Art. 123, del Código Penal); en la estafa, "el que defraudare a otro mediante cualquier ardid o engaño" (Art. 252, del Código Penal); (Art. 274 del código penal) etc.

[6] **Ibíd.** Pág. 345

En los delitos informáticos la acción no resulta tan clara, dada la diversidad de bienes jurídicos tutelados como de formas de perpetrar el delito. Así en algunos casos la acción tiende a afectar elementos componentes de la computadora; mientras que en otros casos el computador solo es utilizado como medio o instrumento para cometer el delito. Por último puede consistir en el uso o utilización indebida de una computadora sin la correspondiente autorización.

Dentro de estos tres grandes grupos estaría encuadrado el elemento objetivo del delito informático (la acción) debiendo el legislador tipificar a través de figuras lo más exactas posibles tales acciones.

b) El elemento subjetivo

Como en todos los delitos, el elemento subjetivo está constituido por el dolo o la culpa con que actúe el delincuente.

"Parte de la doctrina sostiene que, aparte del dolo o culpa genéricos, podría exigirse para este tipo de delitos un dolo específico, tal como el contenido para ciertas figuras delictivas en las que el legislador introduce algún elemento subjetivo. Otros autores, por su parte, creen que bastará que el legislador defina la acción punible. El dolo estará dado no solo por la voluntad de producir el resultado tipificado por la ley sino también cuando se tenga conciencia de la criminalidad de la acción, y, a pesar de ello, se obre." [7]

[7] Guibour. Ricardo. A **Manual de Informática Jurídica**. Pág. 273

1.5 Los sujetos en el delito informático

a). Sujeto activo

El sujeto activo es la persona que realiza la conducta a describir por el tipo Las personas que cometen delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes. Estos sujetos 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.

Teniendo en cuenta estas características, estudiosos del tema han catalogado a los delitos informáticos como "delitos de cuello blanco" (White collar crimes). Estos delitos se definen como el acto o la serie de actos ilegales cometidos por medios no violentos y mediante ocultamiento o engaño para obtener dinero o bienes, para evitar el pago o la pérdida de dinero o bienes o, para obtener ventajas comerciales o personales. Generalmente el sujeto activo de este tipo de delitos es una persona de cierto status socioeconómico.

Es decir, que las personas que cometen este tipo de delitos no son los tradicionales delincuentes de delitos comunes y que de ellos esta saturada las cárceles del país, sino que el Estado que dentro de su cúpula también, se infiltran este tipo de criminales, podría estar reacio a proceder cuando no le sea conveniente, circunstancia esta que pone de manifiesto que la sociedad guatemalteca se encuentra ante un problema muy complejo.

b) Características personales

Empiezan muy pequeños a explicar la computadora son fans desde temprana edad (8 ,10) se vuelcan activamente al estudio tanto de comunicaciones (Internet) como de leguajes y sistemas operativos, especialmente linux. Para su operatoria precisan saber como funciona la Web; para realizar los "asaltos" y lo hacen desde el sistema operativo linux y el cual les provee el acceder o trabajo sobre el sistema operativo, maquina o sitio a hacker desde la barra de comando o símbolos del sistema de computo.

"Los ya expertos generalmente, son personas jóvenes (entre 18 y 40 años). La mayoría de las veces los perpetradores fundamentales han sido hombres ya que las mujeres que han intervenido lo han hecho casi siempre en carácter de cómplices. Otra de las características es que habitualmente el individuo no posee antecedentes criminales aunque en la actualidad se han registrado casos en los que ha estado involucrada la mafia. Ejemplo de ello fue lo ocurrido en un Banco de Datos de EE.UU., el que brindaba información de créditos a las grandes tiendas. El fraude consistió en que se fraguaron a través del computador legajos cuyos datos permitieron, una vez consultados por los usuarios del sistema, la concesión de créditos a personas insolventes, por lo que los mismos se tornaban incobrables".[8]

A aquel joven de menos de 30 años, carente de antecedentes penales, casi siempre varón, inteligente, instruido y con afán de notoriedad debemos agregar a la delincuencia profesional en forma de crimen organizado los casos del empleado medio y a menudo frustrado.

[8] Alcalá Ruidosa Luis. **Los Hacker en la Internet** Pág. 65

c) Relaciones entre el sujeto activo y su empleo o función Maniobras que pueden emplearse desde los diversos puestos de trabajo y áreas relacionadas:

1) Programadores: Pueden violar o inutilizar controles protectores del programa o sistema; dar información a terceros ajenos a la empresa; atacar el sistema operativo; sabotear programas; modificar archivos; acceder a información confidencial.

2) Analistas de sistemas: es comúnmente el que conoce la operación de un sistema completo; puede estar en colusión con el usuario u operador.

d) De comunicaciones: es la persona que diseña la seguridad del sistema de comunicaciones por lo que conoce los métodos para violar la seguridad con fines de fraude.

e) Supervisores: Tienen conocimiento global de las operaciones y debilidades del sistema de seguridad; pueden manipular los archivos de datos y los ingresos y salidas del sistema.

f) Personal técnico y de servicio: Generalmente tienen libre acceso al Centro de Cómputos; poseen mayores conocimientos de los sistemas operativos y de base de datos.

g) Funcionarios superiores: Tienen conocimiento general de los proyectos por lo que implican una amenaza potencial.

h) Auditores: Conocen las debilidades del sistema toda vez que implementan las medidas de seguridad instalando controles preventivos u otros que a posteriori permitan detectar el fraude antes de que la persona involucrada pueda escaparse.

i) Bibliotecarios: Como responsable del mantenimiento de la documentación de sistemas, puede vender la documentación a competidores u otros compradores.

j) Personal de limpieza, mantenimiento, custodia: Pueden vender el contenido de los cestos de papeles a competidores u otros compradores; fotografiar documentos dejados sobre los escritorios; sustraer información o listados del Centro de Cómputos; sabotear el sistema con explosivos.

k) Usuarios: Tienen la posibilidad de hacerse pasar por otros usuarios, modificar, omitir o agregar información con propósitos fraudulentos; vender información a competidores y efectuar un uso no autorizado de tiempo del sistema.

l) La ubicación jerárquica de los autores implica mayor conocimiento de las operaciones y de sus controles. Ello hace menos necesaria la colusión y coincidentemente es superior el monto defraudado.

e) Móviles:

Las razones que impulsan al autor de estos ilícitos para proceder en tal sentido, son:

1. La obtención de una ganancia personal.

2. La comisión del delito conlleva la idea que tal actitud significa robar a los ricos (síndrome de Robin Hood) aunque las ganancias no son repartidas entre los pobres sino que son celosamente guardadas por quien comete el fraude.

3. Sus autores sienten el desafío y satisfacen su ego venciendo los controles que les puedan haber puesto.

4. El odio a la empresa y los deseos de venganza.

5. Los altibajos financieros.

6. El no tener antecedentes criminales induce al individuo a cometer el fraude pensando que lo que está haciendo no reviste el carácter de tal;

7. La despersonalización de la computadora la convierte en la víctima ideal ya que carece de sentimientos, pertenece a la empresa y no tiene capacidad de respuesta frente a la agresión.

8. La perturbación mental.

f) Sujeto pasivo:

"El sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Generalmente los diferentes ilícitos que se cometen son descubiertos casuísticamente debido al desconocimiento del modus operandi. Ha sido prácticamente imposible conocer la magnitud de estos delitos puesto que la mayoría no son descubiertos o no son denunciados a las autoridades responsables por el temor de las empresas al desprestigio con la consecuente pérdida económica que esto pudiera ocasionar."[9]

[9] Alcalá Ruidosa. Luis. **Ob. Cit.** Pág. 66

Los blancos codiciados por estos delincuentes son entre otros: Bancos, Financieras, Compañías de Seguros. Entes estatales de servicios públicos, Dirección General Impositiva o de Rentas, Municipalidades, Universidades y Colegios, etc.

Los Bancos figuran entre las víctimas de los delitos con computadoras por el uso creciente de los sistemas de transferencia de fondos en forma electrónica.

Las Compañías de Seguros también son campo propicio para los fraudes, a través de reclamos o demandas ficticias, préstamos fraudulentos contra pólizas de algunos clientes, cancelación de las pólizas para ganar reembolsos.

CAPÍTULO II

2. Los Hacker en la doctrina y la legislación comparada.

Se ha dicho que los hackers es un término que se ha utilizado para designar a alguien con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionada con las operaciones de computadora, redes, seguridad, etc.

Es la persona que disfruta aprendiendo detalles de los sistemas de programación y cómo extender sus capacidades, tan intensamente como, al contrario, muchos usuarios prefieren aprender sólo el mínimo necesario. "El término hacker", se utiliza para identificar a los que únicamente acceden a un sistema protegido como si se tratara de un reto personal sin intentar causar daños.

En las definiciones anteriores, pareciera que este personaje no puede ser que actué como un criminal, de manera tal que amerite su regulación. Sin embargo, muchos Hackers constituyen individuos que usan sus habilidades y recursos para invadir sistemas informáticos ajenos, provocando con ello una serie de perjuicios morales y patrimoniales.

Hackers una palabra de origen inglés que significa cortador (Hack: cortar) pero que en actividad informática tiene dos significados que, si bien pueden coincidir en cuando al medio de acceso a la información, los objetivos son distintos.

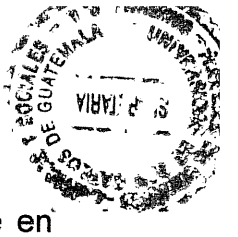
La actividad del Hacker consiste en interceptar en forma dolosa un sistema informático para apoderarse, interferir, dañar, destruir, conocer, difundir o hacer uso de la información que se encuentra almacenada en los ordenadores pertenecientes a instituciones públicas y privadas, de seguridad, "entidades financieras y usuarios particulares". Son auténticos genios de la informática, entran sin permiso en ordenadores y redes, husmean, rastrean y a veces, dejan tarjetas de visita. Los Hacker, posmodernos corsarios de la red, son la última avanzada de la "delincuencia informática de este final de siglo.

"La palabra hacker aplicada en la computación se refiere a la persona que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites. Los hackers tienen un saludable sentido de curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas. No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos."[10]

Existen otras denominaciones que tienen mucha relación con los hackers en el mundo de las computadoras, estos son:

a) Cracker:

Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obsceno propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas Web, tales como rutinas



desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutada automáticamente pueden lograr vulnerar claves de "accesos de los sistemas"

Obviamente que antes que llegar a ser un cracker se debe ser un buen hacker. Asimismo se debe mencionar que no todos los hackers se convierten en crackers.

Un cracker también puede ser el que se dedica a realizar esos pequeños programas que destruyen los datos de las PC, sí los "Virus Informáticos".

"Los mismos crackers, pueden usar herramientas (programas) hechas por ellos mismos o por otros crackers, que les sirven para des-encriptar información, "romper" los passwords de las PC, e incluso de los programas y compresores de archivos; aunque si estos programas no son manejados por malas manos, pueden ser muy útiles para los técnicos o para uno mismo... claro con los archivos y ordenadores de cada quien."[11]

Los crackers, pueden ser empleados rencorosos o frustrados de alguna compañía, que tengan fines maliciosos o de venganza en contra de alguna empresa o persona, o pueden ser estudiantes que quieran demostrar sus habilidades pero de la manera equivocada o simplemente personas que lo hagan solo por diversión.

---

[10] Blossiers Mazini, Juan José **Descubriéndolos Delitos Informáticos**. Pág. 280

b) Los Phreacker

"El Phreacker es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos".[12]

c) El Lamer:

Un Lamer es "simple y sencillamente un tonto de la informática, una persona que se siente Hacker por haber bajado de Internet el Netbus, alguien a quien le guste bajar virus de la red e instalarlos en la PC de sus amigos, aunque mas bien podría decírsele como un Cracker de pésima calidad; en general alguien que cree que tiene muchos, conocimientos de informática y programación, "pero no tiene ni la más mínima idea de ello.

d) Relación entre ellos:

Un Cracker es parecido al Hacker en cuanto a que el cracker, también puede tener la habilidad de entrar en sistemas ajenos, solo que el cracker destruye la información que encuentra e inclusive la vende. Un Lamer, pretende ser Hacker, haciendo cosas que los Crackers ya pasaron. Un Phreacker solo tiene similitud entre

[11] **Ob. Cit.** Pág. 68
[12] **Ob. Cit.** Pág. 281

estos en que ocupan programas para generar tarjetas de crédito, en lo demás son totalmente diferentes.

Por último, cuando se escuche o lea la palabra Hacker, solo hay que pensar en que es una persona que solo busca información para su uso personal, y no es como el cracker que se dedica a destruir, aunque esto no quiere decir que los hackers no puedan destruir la información, solo que no lo hacen, por ética.

2.1 Antecedentes del surgimiento de los denominados hackers.

"Existen una serie de antecedentes históricos que refieren cómo surgieron los denominados hackers, a continuación se señalan algunas. El apelativo de hacker se crea a fines del siglo pasado cuando los Estados Unidos de América empieza a recibir un masivo movimiento migratorio de personas de todos los países del mundo que esperaban encontrar en el "país de las oportunidades" un bienestar económico y progreso."[13]

"Los hackers eran estibadores informales" [14] que se pasaban todos el día bajando las maletas y bultos de las personas y familias completas que llegaban en los barcos a los puertos de New York, Boston, San Francisco, etc. Estos trabajadores eran infatigables, pues trabajaban muchas veces sin descansar y hasta dormían y comían entre los bultos de los muelles con el objeto de no perderse una oportunidad de ganar dinero. La palabra "Hack" en inglés significa hacha en español, como si fuesen

[13] **Ob. Cit.** Pág. 19

taladores de árboles que usan su hacha, en forma infatigable hasta llegar a tumbarlos, su tesonero propósito les mereció este apelativo.

La revolución de la computación ha sido lograda gracias a los hackers. Un Hacker es una persona dedicada a su arte, alguien que sigue el conocimiento hacia donde este se dirija, alguien que se apega a la tecnología para explorarla, observarla, analizarla y modificar su funcionamiento, es alguien que es capaz de hacer algo raro con cualquier aparato electrónico y lo hace actuar distinto, alguien que no tiene límites para la imaginación y busca información para después compartirla, es alguien al que no le interesa el dinero con lo que hace, solo le importa las bellezas que pueda crear con su cerebro, devorando todo lo que le produzca satisfacción y estimulación mental... Un hacker es aquel que piensa distinto y hace de ese pensamiento una realidad con diversos "métodos". Es aquel que le interesa lo nuevo y que quiere aprender a fondo lo que le interesa.

"El Hacker, era originalmente, un aficionado a los ordenadores o computadoras, un usuario totalmente cautivado por la programación y la tecnología informáticas. En la década de 1980, con la llegada de las computadoras personales y las redes de acceso remoto, este término adquirió una connotación peyorativa y comenzó a usarse para denominar a quien se conecta a una red para invadir en secreto computadoras, y consultar o alterar los programas o los datos almacenados en las mismas. También se utiliza para referirse a alguien que, además de programar, disfruta desmenuzando sistemas operativos y programas para ver cómo funcionan. "[15]

El Hacking se considera una ofensa o ataque al Derecho de gentes, y no tanto un delito contra un Estado concreto, sino más bien contra la humanidad. El delito puede

[14] Consulta Internet. **Los Hackers más Famosos. www.goesjurídica.com.htlm.** "Día de consulta: 16-2-2009"
[15] Azpicueta, Hermilio **Derecho Informático**. Pág. 18

ser castigado por los tribunales de cualquier país en el que el agresor se halle. La esencia del Hacking consiste en que el pirata no tiene permiso de ningún Estado soberano o de un Gobierno en hostilidades con otro. Los Hackers "son considerados delincuentes comunes en toda la humanidad, dado que todas las naciones tienen igual interés en su captura y castigo".[16]

Desde los inicios de la computación electromecánica a base de relés, bobinas y tubos de vidrio al vacío, las tareas de programación eran muy tediosas y "el lenguaje de esos años era el críptico lenguaje de máquina y posteriormente se empleó el Assembler Pnemónico. En la fase inicial de las computadoras, "no como se concibe ahora, hubieron hombres, mujeres, jóvenes y adultos entregados por entero a diversificadas tareas de investigación y experimentación, considerándose su trabajo, rutinario, sumamente perseverante y cuyos resultados sólo se han podido reconocer a través de los años". [17]

"Una mujer, la "almirante de la armada norteamericana Grace Hooper" es considerada el primer hacker de la era de la computación. Mientras ella trabajaba e investigaba en la computadora Mark I, durante la Segunda Guerra Mundial, fue la primera persona que aseguró que las computadoras no solamente servían para fines bélicos, sino que además podrían ser muy útiles para diversos usos a favor de la humanidad. Ella creó un lenguaje de "programación denominado FlowMatic y años después inventó "nada menos que el famoso lenguaje COBOL". [18]

[16] Rob Rosenberg y Ross Greenberg. **Consulta Internet. www.goesjurídica.com.htlm**. "Día de consulta: 16-2-2009"..
[17] Los Hackers en el mundo. **www.goesjurídica.com.thlm**. Consulta: 20-2-2009
[18] **Los Hackers más Famosos**. Díaz Oliverri Luis. Pág. 98

"En el sitio THE HACKER FAQ. Citado por la misma publicación, "se dice que los hackers no son aquellos que violan la seguridad de los sistemas. Estos son los crackers. Los hackers disfrutan jugando con las computadoras. Pasan mucho tiempo observando un sistema para saber todo sobre él, sobre sus medidas de seguridad. Pero no lo hacen con malicia, sino por simple seguridad. Según esta última definición el accionar de un hacker no es robar, sino obtener información sobre un sistema. El problema surge cuando esa información o acceso a la misma, es restringida. En este caso, el hacker no admite limitaciones y procurará traspasar todas las barreras por medio de técnicas denominadas por ellos mismos como "ingeniería social" que consiste en utilizar cualquier medio informático para acceder a las claves de acceso de cualquier fuente de información".[19]

Sin embargo, como se dijo anteriormente, también, se tiene como antecedente histórico del surgimiento de estas personalidades del Internet, y de los sistemas computarizados, que en los últimos 2 años, la intrusión en las computadorasse ha más que triplicado, los usuarios se han preguntado, quienes están interesados en robar la información para un fin lucrativo, entonces, en respuesta lógica, surgen los denominados hackers.

La Internet está llena de sitios y consejos que sirven a los hackers neófitos en sus fechorías, tanto jóvenes, como criminales y terroristas tienen acceso a ella, lo que significa que un mayor número de intrusos está tocando las puertas.

A pesar de una mayor seguridad en la Web y de penalidades más estrictas por irrumpir en los sistemas, los ataques de los hackers están por encima del triple en los últimos 2 años.

La mayoría de las compañías rehúsan informar sobre los ataques con el fin de evitar un impacto negativo en la publicidad. Las estadísticas cubren desde las

[19] Davara Rodríguez Miguel Ángel. Luis **Derecho Informatico**. Pág. 12

irrupciones en las redes locales (que le dan acceso al hacker a los archivos con la información), hasta el vandalismo en los sitios Web, (los ataques de negación de servicios y el robo de la información).

Los riesgos que se corren aquí son personales y profesionales. Los hackers se pueden robar las contraseñas y los números de cuentas bancarias de su PC ó pueden apoderarse de los secretos comerciales desde la red local de su compañía.

"Este fenómeno también representa un riesgo contra la seguridad nacional, porque los terroristas más conocedores ó los gobiernos más hostiles, pudieran interrumpir los sistemas satelitales"[20] llevar a cabo una guerra económica interfiriendo en las transferencias financieras ó incluso crear problemas en el control de tráfico aéreo.

Pero no todos los hackers tienen malas intenciones, algunos se encargan de la seguridad de los sistemas de las compañías y otros contribuyen a la seguridad avisándoles a los fabricantes de software, si encuentran algo vulnerable; sin embargo por cada hacker que cambia su sombrero negro por uno blanco, existen docenas que mantienen en vilo a las compañías y al gobierno.

Antes la piratería informática no tenía nada que ver con la violación de la ley ó el daño a los sistemas. "Los primeros hackers que surgieron en el Instituto Tecnológico

[20] http://www.solon.com.

de Massachussets en los años 60's estaban impulsados por el deseo de dominar las complejidades de los sistemas computacionales y de empujar la tecnología más allá de "sus capacidades conocidas".

La ética del hacker, que es un dictamen aún sin escribir y que gobierna el mundo de la piratería, dice que un hacker no hará daño. Pero esto no lo podemos comprobar, así que mientras estemos en la red, estamos "a su disposición". Existe por la red un documento llamado "Hacker manifiesto. Si una persona tiene motivos políticos contra alguna empresa y decide estropear su página Web solo tiene que entrar en línea y aprender como hacerlo.

"Como pasa a menudo no existe una definición unívoca y universalmente aceptada de lo que se entiende por hacker. Si se fija en el origen del término quizás se pueda definirlo mejor, y de esa manera se pueda entender principalmente desde el aspecto jurídico penal y desde la perspectiva de la criminalidad".[21]

"A finales de los años cincuenta y durante los años sesenta, en los laboratorios del MIT (Massachusetts Institute Of. Technology) se empezaba a trabajar con los ordenadores, que entonces eran grandes maquinas que requerían habitaciones enteras, con cientos de transistores, válvulas y tarjetas perforadas. Consumían ingentes cantidades de electricidad y desprendían tanto calor que necesitaban una refrigeración exclusiva para ventilarlos En 1959 la institución ofreció el primer curso de programación y un grupo de alumnos quedaron literalmente prendidos de los ordenadores y de lo que se podía llegar a hacer con ellos. Este grupo de

[21] Miguel Ángel Davara Rodríguez. **Derecho Informático.** Pág. 33

alumnos pertenecía en su mayoría al TMCR (Tech Model Railroad Club o Club de Modelo de Trenes) y por la complejidad de los primeros computadores pocas veces podían acceder directamente a ellos. Poco después llegó al MIT el TX-0, un ordenador novedoso para la época y Jack Dennis, antiguo miembro del TMCR y profesor del MIT facilito a sus alumnos un acceso ilimitado a este ordenador. Este ordenador tenía un teclado para introducir datos, y no las tediosas tarjetas perforadas que hasta entonces se hacían servir. El teclado supuso un avance extraordinario, ya que permitía interactuar directamente con el ordenador y ver inmediatamente el resultado del trabajo. El grupo de alumnos cada vez pasaba más tiempo con el ordenador y empezaron a hacer cosas que ni los ingenieros que habían diseñado el ordenador nunca habían soñado.

"A partir de este momento es cuando el término hacker se empieza a aplicar a un grupo de alumnos fanáticos de los ordenadores que empiezan a desarrollar un trabajo que va más allá de lo que entonces se creía posible. Piensan por si mismos, exploran los límites y descubren nuevos horizontes, empezando a perfilar una manera de trabajar nueva, unas nuevas normas y reglas, e inconscientemente una nueva ética".[22]

Otros autores señalan que el origen de los hackers hay que buscarlos en el "mundo de las comunicaciones, en los laboratorios de la Bell Telephone. Algunos técnicos de estos laboratorios empezaron a desarrollar unas técnicas y unos inventos que revolucionaron el mundo de las comunicaciones y la informática.

La historia, o quizás más bien la leyenda indica que la etimología hacker nace cuando un operario de telefonía daba un golpe seco y contundente al aparato de teléfono (un Hack o hachazo) y conseguía que funcionara. "El término hacker es un término de argot de imposible traducción.

[22] Hermilio Azpicueta. **Derecho Informático.** Pág. 30

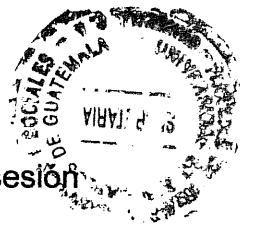
De estos antecedentes se deduce que un hacker es una persona técnica, con grandes y amplios conocimientos, un experto, apasionado por la informática, los computadores y los lenguajes de programación, pero que sustancialmente desafía a los límites y que quiere ir más allá, investigar, trabajar y descubrir. Sus características fundamentales también estriban en que tiene una pasión por el conocimiento fundamentada en la diversión y la satisfacción personal, y que cuando descubre que esa diversión y satisfacción personal le puede producir mayores ingresos, poder económico, usa ese ingenio para lograrlo.

"Los hackers son en un primer momento, en su sentido original unos entusiastas de la informática con un enorme interés, a menudo pasión, en aprenderlo todo de los sistemas informáticos, superar sus límites teóricos y usarlos de formas innovadoras. Un hacker es un profundo conocedor de una tecnología, que tiene ansia por saberlo todo y desafía a los límites".[23]

Una de sus características fundamentales es su ansia de conocimiento y su contrariedad en aceptar limites o cualquier tipo de restricciones a las posibilidades de conocimiento, y es posible que ello, también permita que no entienda sobre limites, sobre prohibiciones e incluso, aspectos éticos que debe observar "Existe un texto clásico en este mundo, escrito por Eric S. Raymond, uno de los pioneros y más emblemáticos hackers, se define a los mismos como alguien que reúne varias de las siguientes característica.

1-. Es una persona que disfruta investigando sistemas operativos, lenguajes de programación y sabe sacarle el máximo provecho. Se diferencia del usuario normal porque estos se limitan a conocer lo mínimo e imprescindible de un programa.

[23] Blossier Manzini Juan José. **Descubriendo los Delitos Informáticos**. Pág. 290



2-. En general es un entusiasta de la programación, y a veces llega a tener obsesión por ella.

3-. Alguien que aprecia el valor de hackear, entendiendo por ello el buscar un uso no documentado o previsto de algo.

4-. Cualquiera que sea muy bueno programando.

5-. Gran experto en un programa o sistema operativo concreto (p.e. Unix).

6-. Experto o entusiasta de cualquier clase.

7-. Alguien que disfruta con un reto intelectual y lo intenta resolver de forma autodidacta, creativa y lúdica. "En 1984 se publicó un trabajo por Levy, formula seis normas que deben estar en la base de todo aquel que se considere hacker. Estas son:

a.- Entrégate siempre al imperativo de transmitir! El acceso a ordenadores y a cualquier otra cosa que pueda enseñarte como funciona el mundo debe ser ilimitado y total.

b.- Toda la información debe ser libre

c.- Desconfía de la autoridad. Promueve la descentralización.

d.- Los hackers deben ser juzgados por su hacking (entendiendo por tal su manera de hacer, sus acciones), no por criterios falsos como títulos, edad, raza o posición.

e.- Puedes crear arte y belleza en un ordenador.

f.- Los ordenadores pueden cambiar tu vida a mejor.

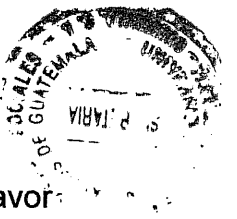
"Otro texto fundamental en el ideario hacker es "La Catedral y el Bazar", probablemente el ensayo más importante para entender un fenómeno como el del

código abierto. Escrito en 1997 por Eric Raymond ha sido revisado a principios de 2001. El texto parte de la contraposición entre dos modelos de desarrollo. En sus origines Raymond pensaba que el desarrollo de cualquier programa informático debía seguir un método similar a la construcción de una catedral."[24]

Esto es, en la construcción de un templo pequeños grupos de artesanos, vidrieros, marmolistas, picapedreros, escultores realizan su parcela de trabajo de manera aislada e independiente, sin ninguna interrelación entre ellos, y la suma de todos los trabajos es la catedral. Pensaba que en el desarrollo de un programa el mejor método de trabajo era el de los sabios individuales o pequeños grupos de trabajo realizasen su trabajo aisladamente, sin publicar ninguna beta. Pero el desarrollo especialmente del lenguaje Linux le hace cambiar totalmente de planteamiento.

Raymond citado por Carlos María Correa. Derecho informático en América, consta que la interrelación, el fin del aislamiento, el intercambio constante, casi la promiscuidad entre los miembros del grupo de trabajo, da mejores frutos. A partir de la metáfora del bazar afirma que el éxito de un proyecto se fundamenta en el intercambio permanente, en una relación ruidosa, alegre, desordenada y eficiente de todos los que trabajan en un proyecto. Afirma que es mucho más eficaz el modelo del bazar que el de la catedral, esto es, resulta más productivo desarrollar programas o cualquier proyecto informático en un entorno de comunidad abierta que en un sistema cerrado. La colaboración y la revisión crítica constante por múltiples interlocutores aseguran una calidad final incomparablemente superior.

[24] Jargón File. Raymund Eric, citado por Blossier,. Manzini, **Ob. Cit.** Pág. 292



"Este texto se ha convertido en una de las piedras angulares del movimiento a favor del código abierto, que pretende cambiar radicalmente el modelo imperante de desarrollo tecnológico del software. El movimiento de código abierto parte de la premisa que nadie es propietario del código fuente del programa, que cualquier usuario puede utilizarlo, mejorarlo y redistribuirlo y se contrapone al modelo del código propietario, donde el usuario no tiene ningún derecho sobre un programa, simplemente un derecho de uso. Este es un debate apasionante entre el modelo Linux y el modelo Microsoft, los dos extremos más emblemáticos de cada línea, "con importantísimas implicaciones económicas, políticas, de seguridad y prácticamente de política internacional".[25]

2.2 Procedimientos para el control automatizados de los delitos del uso de la Internet.

Estos son mecanismos que deben emplear los estados, precisamente para resguardar una serie de derechos que le asisten a los usuarios de Internet y que de alguna manera a través del uso de este sistema de redes también se puede contrarrestar, se deben identificar tres tipos de tecnologías para combatir la delincuencia: de identificación, de vigilancia y de investigación. Las principales tecnologías de identificación son las contraseñas, los cookies y los procedimientos de autenticidad. Las contraseñas son los símbolos convenidos que el usuario utiliza para entrar en esta red. Los cookies son marcadores digitales que los Web cites así equipados insertan automáticamente en los discos duros de los ordenadores que los conectan. Una vez que un cookie entra en un ordenador, todas las comunicaciones de dicho ordenador en la red son automáticamente registradas en el Web cite originario del cookie.

[25] Hackers, Héroes de la Revolución. Citado por Blossier Manzini Ob. Cit. Pág. 284

"En este caso, los procedimientos de autenticidad son firmas digitales que permiten a los ordenadores verificar el origen y características de las comunicaciones recibidas. Generalmente, utilizan tecnología de encriptación. Trabajan por niveles, de modo que los servidores identifican a usuarios individuales y las redes de conexión identifican a los servidores. ". [26]

"Las tecnologías de vigilancia permiten interceptar mensajes, insertar marcadores gracias a los cuales se puede seguir la comunicación de un ordenador o un mensaje marcado a través de la red; también consisten en la escucha continua de la actividad de comunicación de un ordenador o de la información almacenada en dicho ordenador. El famoso programa Carnivore del FBI Permite analizar mediante palabras clave enormes masas de información de las comunicaciones telefónicas o Internet" [27] buscando y reconstruyendo en su totalidad aquellos mensajes que parezcan sospechosos (aunque algunas detenciones sobre esas bases resultaron bastante chuscas, arrestando a buenas madres de familia que comentaban electrónicamente el peligro del consumo de drogas en la escuela de sus hijos).

Las tecnologías de vigilancia permiten identificar el servidor originario de un determinado mensaje. A partir de ahí, por colaboración o coacción, los mantenedores de los servidores pueden comunicar al detentor del poder la dirección electrónica de donde provino cualquier mensaje.

Por ello, las tecnologías de investigación se organizan sobre bases de datos obtenidos del almacenamiento de la información resultante de las tecnologías de vigilancia. A partir de esas bases de datos se pueden construir perfiles agregados de usuarios o conjuntos de características personalizadas de un usuario determinado. Por

---

[26] Consulta internet Los Hackers wwwgoesjuridica.com htlm. Día de consulta 16-2-2009

[27] **Consulta Internet www.onu.com.htlm**. Problemática del Internet Ante la Amenaza criminal. Folleto informativo. Día de consulta: 16-1-2009

ejemplo, mediante el número de tarjeta de crédito, asociado a un número de carné de identidad y a la utilización de un determinado ordenador, se puede reconstruir fácilmente el conjunto de todos los movimientos que realiza una persona que dejen registro electrónico. Como eso es algo que hacemos todos los días (teléfono, correo electrónico, tarjetas de crédito), parece evidente que ya no hay privacidad desde el punto de vista de la comunicación electrónica. O sea, la combinación de las tecnologías de identificación, de vigilancia y de investigación configuran un sistema en que quien tenga el poder legal o fáctico de acceso a esa base de datos puede conocer lo esencial de lo que cada persona hace en la red y fuera de ella y esto es importante para las políticas de prevención que ostenta el Derecho Penal.

"Desde ese punto de vista' la red no se controla, pero sus usuarios están expuestos a un control potencial de todos sus actos más que nunca en la historia. Así pues, un poder político, judicial, policial o comercial (defensores de derechos de propiedad) que quiera actuar contra un internauta determinado puede interceptar sus mensajes, detectar sus movimientos y, si están en contradicción con sus normas, proceder a la represión del internauta, del prestador de servicios, o de los dos. Lo anterior denota que si efectivamente puede existir un control y no precisamente como aducen muchos, que el uso del Internet permite a su usuario mantenerse en el anonimato".[28]

Obviamente, el control de esa manera podría no solo provenir del gobierno y de la policía sino también de determinadas empresas privadas. Se ha sabido que algunas empresas vigilan rutinariamente el correo electrónico de sus empleados y también, se tiene conocimiento en el caso de las universidades, el de sus estudiantes, porque la protección de la privacidad no se extiende al mundo del trabajo, bajo el control de la organización corporativa, que si bien constituye un tema interesante de abordar, no será motivo de ello, por el enfoque que se pretende darle a la presente investigación.

[28] Robert Lessig El Internet. Pág. 6

Resulta entonces, muy difícil pero no imposible que basándose en el principio de libertad, en un mundo en que la tecnología puede servir para el control de las vidas de los seres humanos mediante su registro electrónico, y la tendencia al control ubicuo es ya de por si es irreversible. En sociedad, todo proceso está hecho de tendencias y contra tendencias, y la oposición entre libertad y control continúa sin fin, a través de nuevos medios tecnológicos y nuevas formas institucionales, basados en la necesidad de prevenir ilícitos que afecten precisamente a la sociedad y la tranquilidad de la misma dentro de un aspecto de la vida de los ciudadanos.

Por eso, como lo han establecido algunos tratadistas respecto del tema, que a las tecnologías de control y vigilancia se contraponen tecnologías de libertad. Señalan que por un lado, el movimiento para el software de fuente abierta permite la difusión de los códigos sobre los que se basa el procesamiento informático en las redes. Por consiguiente, a partir de un cierto nivel de conocimiento técnico, frecuente entre los centros de apoyo a quienes defienden la libertad en la red, se puede intervenir en los sistemas de vigilancia, se pueden transformar los códigos y se pueden proteger los propios programas. Naturalmente, si se pone un ejemplo de lo que se dijo anteriormente, el mundo en general, y en Guatemala no es la excepción, se acepta sin mayores complicaciones el mundo de Microsoft, aunque en muchos casos, a través de esta red, se acaba cualquier posibilidad de privacidad y por lo tanto, de libertad en la red, porque los usuarios se someten a las reglas de esta entidad para navegar en el Internet.

a) La ciencia de la Criptacion o Encriptación.

Este sistema se refiere a la utilización de impresiones digitales, firma digital o claves que constituyen procedimientos de verificación de identidad del emisor y destinatario. Si bien es cierto que, como toda tecnología, su relación con "la libertad es ambigua, como señala Lessig" porque, por un lado, protege la privacidad del mensaje pero, por otro, permite los procedimientos de autentificación que verifican la identidad del mensajero.

Sin embargo, en lo esencial, las tecnologías de encriptación permiten, cuando funcionan, mantener el anonimato del mensaje y borrar las huellas del camino seguido en la red, haciendo difícil, pues, la interceptación del mensaje y la identificación del mensajero. Por eso, la batalla sobre la encriptación es, desde el punto de vista técnico, es una batalla fundamental por la libertad en Internet.

b) El control de los hackers.

"Como se ha mencionado, los hackers son persona con conocimientos técnicos informáticos cuya pasión es inventar programas y desarrollar formas nuevas de "procesamiento de información y comunicación electrónica. Según este autor, para ellos, el valor supremo es la innovación tecnológica informática. Y, por tanto, necesitan también libertad. Libertad de acceso a los códigos fuente, libertad de acceso a la red, libertad de comunicación con otros hackers, espíritu de colaboración y de generosidad (poner a disposición de la comunidad de hackers todo lo que se sabe, y, en reciprocidad, recibir el mismo tratamiento de cualquier colega). Algunos hackers son políticos y luchan contra el control de los gobiernos y de las corporaciones sobre la red, pero la mayoría no lo son, lo importante para ellos es la creación tecnológica. Se movilizan, fundamentalmente, para que no haya cortapisas a dicha creación. Los hackers no son comerciales, pero no tienen nada contra la comercialización de sus conocimientos, con tal de que las redes de colaboración de la creación tecnológica sigan siendo abiertas, cooperativas y basadas en la reciprocidad."[29]

La cultura hacker se organiza en redes de colaboración en Internet, aunque de vez en cuando hay algunos encuentros presenciales. Distintas líneas tecnológicas se agrupan en torno a grupos cooperativos, en los cuales se establece una jerarquía tecnológica según quiénes son los creadores de cada programa original, sus mantenedores y sus contribuidores.

[29] Levy Raimond. **Los Hackers En La Internet**: Pág. 98

En virtud de la habilidad que tienen estos personajes y de la forma en que se introducen en las fuentes de información y de comunicación, a pesar de que favorece el principio de libertad, este debe ser restringido por el principio de seguridad, por ello, se ha establecido especialmente en la legislación que se ha analizado en este trabajo, la necesidad de que se regule su intervención, porque a pesar de la habilitad técnica que estos tienen y de la forma en que se introducen también existe el peligro de que provoquen ya no actos que tiendan a la aspiración de libertad, sino que sus fines sean puramente criminales.

Este autor, a manera de ejemplo, se refiere lo sucedido con uno de los movimientos más representativos de lo que realizan los hackers en el mundo, cuando trata lo relativo al movimiento hacker más político (en términos de política de libertad tecnológica) que fue el creado por Richard Stallman, un programador de MIT, que constituyó en los años ochenta la Free Software Foundation para defender la libertad de acceso a los códigos de UNIX cuando ATT trató de imponer sus derechos de propiedad sobre UNIX, el sistema operativo más avanzado y más compatible de su tiempo, y sobre el que se ha fundado en buena parte la comunicación de los ordenadores en la red. A tal grado llegó la intervención de este hacker que sustituyó el copy right por el copy left. Es decir, que cualquier programa publicado en la red por su Fundación podía ser utilizado y modificado bajo licencia de la Fundación bajo una condición: difundir en código abierto las modificaciones que se fueran efectuando.

Dentro de los hackers más destacados a nivel mundial se señalan a los siguientes:

a) Grace Hooper:

La graduada en matemáticas y física en el Vassar College Grace Hooper se asimiló en la Marina de Guerra de los Estados Unidos, llegando a ascender al grado de Almirante. Grace Hooper, en forma infatigable se dedicó a investigar acuciosamente las posibilidades de programación en las computadoras, de la Primera y Segunda

Generación. Sus compañeros de trabajo comentaban que ella trabajaba como un "hacker".

Durante la segunda guerra mundial, trabajando en su computadora Mark la almirante Hooper se dedicaba a sus investigaciones y experimentos, incluso fuera de su horario de trabajo o hasta en días festivos. Grace Hooper creó el lenguaje Flowmatic, con el cual desarrolló muchas aplicaciones y en 1951 produjo el primer compilador, denominado A-0 (Math Matic). En 1960 presentó su primera versión del lenguaje COBOL (Common Business-Oriented Language).

Paradójicamente, recibió entre muchos reconocimientos y condecoraciones, el título de Hombre del Año en Ciencias de la Computación, otorgado por la Data Processing Managment Association. También fue la primera mujer nombrada miembro distinguido de British Computers Society y hasta el día de hoy es la primera y única mujer con el grado de Almirante de la Marina de Guerra de su país. Grace Hooper falleció en 1992. La almirante Grace Hooper recibió el apelativo de "The Amazing Grace" (la asombrosa Grace) y es considerada la primera hacker de la era de la computación.

b) Kevin Mitnick

Como hacker, su carrera comenzó a los 16 años cuando, obsesionado por las redes de ordenadores, rompió la seguridad del sistema administrativo de su colegio. Para Kevin, el quehacer diario en sus últimos diez años fue el explorar y "explotar" computadoras ajenas y sistemas telefónicos. ¿Su profesión? "hacker", y sin duda muy bueno. Según el Departamento de Justicia de los Estados Unidos, este "terrorista

electrónico", conocido como "el Cóndor", fue capaz de crear números telefónicos imposibles de facturar, de apropiarse de 20.000 números de tarjetas de crédito de habitantes de California y de burlarse del FBI por más de dos años con sólo un teléfono celular apañado y un ordenador portátil. Un tipo fino.

Mitnick ya fue arrestado en 1988 por invadir el sistema de Digital Equipment. Fue declarado culpable de un cargo de fraude en ordenadores, y de uno por posesión ilegal de códigos de acceso de larga distancia. Adicionalmente a la sentencia, el fiscal obtuvo una orden de la corte que prohibía a Mitnick el uso del teléfono en prisión alegando que el prisionero podría obtener acceso a ordenadores a través de cualquier tel%eacute; fono. A petición de Mitnick, el juez le autorizó a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela, y sólo bajo la supervisión de un oficial de la prisión.

Después de varios intentos infructuosos, buscando perlas de telefonía, se encontró con la computadora de Tsutomu Shimomura, a la cual accedió en la Navidad de 1994. Shimomura es un físico, programador y experto en sistemas de seguridad del San Diego Supercomputer Center, y también muy buen hacker, aunque forma parte de los llamados "chicos buenos" y ejerce de consultor de seguridad informática. Y, tal como se cuenta en Takedown, al "malo" le llegó su hora; tras una ardua persecución, le pillaron. Aquí está la impresionante acusación federal a Mitnick.

c) Vladimir Levin

Un graduado en matemáticas de la Universidad Tecnológica de San Petesburgo, Rusia, fuŕ acusado de ser la mente maestra de una serie de fraudes tecnológicos que le permitieron a él y la banda que conformaba, substraer más de 10 millones de dólares, de cuentas corporativas del Citibank".[30]

En 1995 fue arrestado por la INTERPOL, en el aeropuerto de Heathrow, Inglaterra, y luego extraditado a los Estados Unidos. Las investigaciones establecieron que desde su computadora instalada en la empresa AO Saturn, de San Petesburgo, donde trabajaba, Levin irrumpió en las cuentas del Citibank de New York y transfirió los fondos a cuentas aperturadas en Finlandia, Israel y en el Bank Of. América de San Francisco, Estados Unidos.

A pesar de que la banda substrajo más de 10 millones de dólares al Citibank, Levin fué sentenciado a 3 años de prisión y a pagar la suma de US $ 240,015 a favor del Citibank, ya que las compañías de seguros habían cubierto los montos de las corporaciones agraviadas.

d) Ian Murphy

Conocido entre sus amistades como "Capitán ZAP", fue el primer cracker en caer tras las rejas. Murphy ingresó de manera ilegal en los computadores de AT&T en 1981 y cambió la configuración de los relojes internos encargados de medir los tiempos y tarifas a cobrar. Así, hubo miles de personas que se sorprendieron al recibir

[30] Correa Carlos María. **El Derecho Informático en América latina**. Pág. 98.

la cuenta y comprobar que tenían grandes descuentos por llamadas realizadas en horario nocturno cuando en realidad lo habían hecho en pleno día.

Caso contrario con respecto a los que llamaban a media noche con el pretexto de ahorrar, porque recibieron abultadas e inexplicables facturas. Murphy, ahora gerente general de IAM/Secure Data Systems, fue la inspiración para la película "Sneakers"

e) Robert Tappan Morris.

El 2 de noviembre de 1988 Robert Tappan Morris conocido como el gusano Morris diseñó un gusano que fue capaz de botar 1/10 de la Internet de entonces (lo que significa que inhabilitó cerca de 6 mil computadores).

El sujeto cometió el error de hablar en los Chat sobre su creación meses antes de llevar a cabo el plan. De esta manera, no fue muy complicado para la policía dar con su paradero.

Robert Morris fue el primer individuo en ser procesado bajo el Acta de Fraude y Abuso Computacional de EE.UU., pero sólo se vio obligado a realizar servicios comunitarios y a pagar la fianza, todo bajo el pretexto de que el virus de su creación no había destruido los archivos de las maquinas afectadas. Sin embargo, el costo de erradicar el gusano de los computadores infectados fue de US $ 15 millones. El "Gusano Morris" fue determinante a la hora de fundar el "Equipo Anticiberterrorista CERT" (Computer Emergency Response Team), que se encargaría de lidiar con futuros problemas de similares características.

f) Los escuadrones mod. Y Lod

En 1993, los Maestros de Decepción (Masters Of. Deception) fueron los primeros crackers en ser capturados gracias a la intervención de líneas telefónicas. Tipos de gran fama por tener numerosas formas de evitar el pago de llamadas telefónicas de larga distancia, los MOD además podían escuchar conversaciones privadas e incluso crear enormes líneas multiconferencias que compartían con sus amigos. Junto con pasarlo bien a través del teléfono, hachearon muchas bases de datos, incluyendo la de la National Security Agency, AT&T y la del Bank Of. América. También pudieron acceder a los registros de la Credit Record Repoting Agency y de esta manera "ojear" los registros de los ricos y famosos.

Como si fuera poco, los MOD tienen más credenciales que mostrar. Famosas fueron las guerras contra la Legión de Doom (LOD), otro grupo de crackers que tenía la reputación de ser la guarida de los elementos de elite de este mundo subterráneo.

El nacimiento de los MOD se remonta a un tiempo de intensas disputas internas entre los miembros de LOD. Uno de sus líderes, el hacker Phiber Optik, dejó dicha comunidad y formó MOD. Desde ese momento se sucedieron una serie de batallas por obtener el título de "Cracker King", hasta que la mayoría de los integrantes de ambos bandos fueron capturados en 1993.

Son muchos los testimonios que aseguran que ningún miembro de MOD habría sido castigado si no hubiesen participado en los constantes enfrentamientos contra la LOD.

g) Chen Ing-Hua.

Conocido en el mundo como el creador del virus Chernobyl o CIH, este joven taiwanés de 25 años dijo a las autoridades de su país que difundió el programa informático el 26 de abril de 1999 para que coincidiera con el decimotercero aniversario del desastre nuclear ocurrido en la antigua URSS.

Licenciado en ingeniería informática, Chen Ing-Hua aseguró que usó las iniciales de su nombre (CIH) para denominar técnicamente al virus, mientras estudiaba en la Universidad de Tan Tung, en Taipei.

"Diseñé el virus porque estaba enojado y porque todos los programas antivirus existentes en Internet son ineficaces", dijo en su momento Chen Ing-Hua a las agencias internacionales de noticias. También precisó que no pensó que su creación pudiera causar tanto daño.

Por este hecho, la universidad lo denunció en el mes de mayo de 1999 ante las autoridades estatales de Taipei, tras paralizar centenares de miles de ordenadores en el sudeste asiático. El virus causó importantes daños en Corea del Sur, aunque el impacto fue mucho menor en Europa y prácticamente nulo en los Estados Unidos.

h) David Smith

Nacido en Aberdeen (New Jersey), David L. Smith de 31 años de edad, fue acusado de crear el virus Melissa que se propagó rápidamente en centenares de millones de

ordenadores de todo el mundo. Apareció por primera vez ante las cámaras de televisión y los fotógrafos de las agencias de noticias, cuando salió de la Corte Superior del condado de Monmouth, tras enterarse de los cargos de que era inculpado: interrupción de las comunicaciones públicas, conspiración para cometer el delito y robo de servicios de ordenadores en tercer grado De prosperar las denuncias que enfrenta, Smith podría pasar por lo menos 40 años en prisión y sería obligado a pagar una multa de más de 400.000 millones de dólares. Este programador informático admitió ante el alto tribunal de justicia de haber accedido de forma ilegal a América Online con el propósito de enviar el virus a través de Internet.

i) Onel e Irene De Guzmán

Esta pareja de hermanos filipinos reconoció durante una rueda de prensa realizada en su país que había difundido el virus I Love You de manera accidental. En el caso de Onel De Guzmán, de 22 años, ex-alumno de la Universidad de Informática AMA y principal sospechoso de haber creado este programa, adujo que su actuación fue una señal de censura por que el servicio de Internet en su país es costoso para los jóvenes, en lugar de se gratuito.

Pese a las acusaciones de las que han sido objeto los hermanos De Guzmán, las autoridades de filipinas se encuentran en un serio dilema, en virtud a que legislación no tipifica como delito la piratería informática. Por esta situación, no pueden ser calificados de sospechosos y, por lo tanto, no se les puede citar a declarar de forma legal, indicó su abogado personal.

2.3 Perfil criminológico del hacker.

Los hackers son auténticos genios de la informática, entran sin permiso en ordenadores y redes ajenas, husmean, rastrean y a veces, dejan sus peculiares tarjetas de visita.

a) Hacker: es la persona que disfruta explorando detalles de los sistemas programables y aprendiendo a usarlos al máximo o el que programa con entusiasmo (al borde de la obsesión) o aquel que se divierte más programando que haciendo teorías sobre programación.

b) Cracker: es aquel que rompe con la seguridad de un sistema.

c) Preacker: arte y ciencia de crackear la red telefónica para obtener beneficios personales (por ejemplo llamadas gratis de larga distancia).

d) El hacker en general utiliza reglas gramaticales y particulares, juega y crea un lenguaje propio con la intención de confundir y diferenciarse para obtener así cierto poder.. Los piratas jamás trabajan bajo su verdadero nombre sino que lo hacen empleando seudónimos.

e) Detrás de un hacker adolescente hay un autodidacta, se auto considera su mejor motivación, aunque a veces es motivado por otro hacker.

f) Es inteligente, desaliñado, intenso, abstraído y sorprendentemente se inclinan por una profesión sedentaria. Poseen un alto coeficiente intelectual, curiosidad y facilidad para las abstracciones intelectuales.

2. 4 Análisis de la legislación en materia de los hackers

Republica de Argentina

Este país ha tenido que propiciar en la actualidad cambios legislativos especialmente en el orden penal, para sancionar conductas que no eran típicas respecto a los delitos informáticos.

Algo fundamental que ha sido de interés para quien escribe, es lo que representó una sentencia de la Corte Suprema de Justicia, que precisamente por la intromisión de un hacker afectó "su sistema de seguridad . El debate suscitado en los últimos días a nivel nacional e internacional en materia de delitos informáticos, tomó un nuevo rumbo como consecuencia del reciente fallo en la Argentina sobre el hackeo a la Página de Internet de la Corte Suprema de este país.

El fallo ha sorprendido a algunos, ha sido criticado por otros y se ha constituido en un serio llamado de atención para los legisladores por la falta de tratamiento de estas cuestiones. Argumentos esgrimidos en la resolución judicial: El Juez Argentino en lo Criminal y Correccional, ha fallado en el sentido de no encuadrar la acción de hackeo dentro de los tipos penales punibles en nuestro ordenamiento jurídico.

Para ello se ha sostenido que el concepto de corporeidad no es unánimemente reconocido por la doctrina, ya que para algunos existe la ocupación de un lugar en el espacio, concepto sostenido por Soler mientras que para otros resulta ser condición suficiente su materialidad, de manera que bastaría que un objeto pueda ser detectado materialmente para que sea considerado "cosa" criterio adoptado por Núñez.

El juez advierte que tanto en uno como otro concepto, una página Web no puede asimilarse al significado de cosa Ello así, en tanto y en cuanto por su naturaleza no es un objeto corpóreo, ni puede ser detectado materialmente. Cabe destacar que una interpretación extensiva del concepto de cosa, a punto tal que permita incluir a la página Web dentro del mismo, comprendería una acepción que implicaría un claro menoscabo al propio principio de legalidad establecido en el artículo 18 de la Constitución Nacional de la Republica de Guatemala.

En esta inteligencia, el Juez fundamenta su decisión en que nos encontramos ante un vacío legal. Y que conforme se desprende de los proyectos y anteproyectos de ley que se han presentado en las Cámaras del Congreso intentando tipificar dichas acciones, el delito como tal no existe para la legislación Argentina.

Entre los proyectos de ley se menciona el del Senador Antonio Berhongaray, el cual en el capítulo titulado "Daño a datos informáticos", reprime con prisión de seis a tres años a quien "sin expresa autorización del propietario de una computadora o sistema de computación y del propietario de los datos, o excediendo los límites de la autorización que le fuera conferida, ya sea a través del acceso no autorizado, o de cualquier otro modo, voluntariamente y por cualquier medio, destruyere, alterare en cualquier forma, hiciere inutilizables o inaccesibles, o produjera o diere lugar a la pérdida de datos informáticos.

En este encuadre legal si se tipificará la acción penal punible, tal cual se advierte en el anteproyecto de ley, se crea una figura penal, símil al daño previsto por el artículo 183 del Código Penal Argentino, pero que tenga como objeto del delito, ya no a la "cosa", sino a datos o sistemas informáticos.

Por ello concluye, que el hecho no tiene encuadre legal en figura penal alguna prevista en el Código Penal de la Argentina ni en las leyes complementarias.

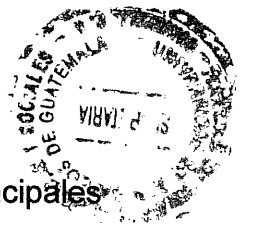
Más allá de los argumentos jurídicos sobre el caso, es interesante advertir la falta de tratamiento legislativo sobre los temas que hoy son moneda corriente en materia de delitos y seguridad pública.

Se advertía que desde el año 1998, los organismos de seguridad de los Estados Unidos habían aumentado su capacidad operativa y de gestión en la prevención de esta modalidad delictiva. El FBI ha incrementado su personal en la prevención y castigo de los delitos cometidos por intermedios de las redes informáticas y en particular con Internet.

En la agenda del organismo de seguridad de los países más desarrollados del mundo se encuentra la prevención y castigo del uso de las redes informáticas, pero antes de ello fue adaptado el régimen legal para punir tales acciones.

En países como Italia se ha modificado desde el año 1997 el concepto de "cosa" ampliando su alcance para objetos inmateriales.

También se ve que en España recientemente el Consejo de Ministros del Gobierno de España aprobó el Proyecto de Ley de Servicios de la Sociedad de la Información y Comercio Electrónico. Según el texto, el objetivo de la norma es "establecer las garantías jurídicas necesarias para potenciar el desarrollo del comercio electrónico y de los servicios ofrecidos a través de Internet". Para ello, se buscó fijar un marco legal



seguro para los proveedores de servicios y los usuarios. Algunos de los principales aspectos de la norma son los siguientes.

En relación con los derechos de los usuarios y obligaciones de los prestadores de acceso se establecen obligaciones básicas respecto a la información que debe facilitarse a los usuarios por parte de los ISP. Se recogen en el texto las obligaciones que en materia de contenidos se consideran esenciales para la persecución de los delitos cometidos a través de Internet. También se establece especial cuidado en el cumplimiento de las obligaciones cuando pudieran afectar la intimidad de las personas, la protección de los datos personales o la libertad de expresión. En relación con el envío de Spam, se los prohíbe, salvo que previamente hubieran sido autorizados por los destinatarios. Para resguardar la Contratación por vía electrónica, se asegura a los usuarios el derecho a disponer de información sobre el contrato, las condiciones aplicables al mismo y el procedimiento que deben seguir para ordenar sus pedidos. Se declara la validez de los mismos aplicando las normas de fondo de Derecho Español.

La ventaja de contar con un plexo normativo que englobe el conjunto de cuestiones que hacen al interés de los prestadores de servicios, de los consumidores de productos y al público en general, es algo muy positivo. Argentina debería en la actualidad contar con un régimen que contemple estos aspectos, hoy dispersos o inexistentes. La defensa de los derechos de los consumidores, el derecho de la intimidad, la protección de los derechos intelectuales y los aspectos contractuales, deberán ser adecuados y repensados para un nuevo ámbito del derecho. Mientras esto no ocurra el fallo dictado en la Argentina es correcto. A pesar de los debates y conflictos que toda nueva norma genera es preferible un sistema discutible a no contar con ninguno.

Republica de Bolivia

En Bolivia, en el año de 1989, se consideró el análisis y tratamiento sobre Legislación Informática concerniente a contratación de bienes y servicios informáticos, flujo de información computarizada, modelización del aparato productivo nacional mediante la investigación científico- tecnológica en el país y la incorporación de nuevos delitos emergentes del uso y abuso de la informática.

Este conjunto de acciones tendientes a desarrollar de manera integral la informática, se tradujo en el trabajo de especialistas y sectores involucrados, representantes en el campo industrial, profesionales abogados y especialistas informáticos, iniciándose la elaboración del Proyecto de Ley Nacional de Informática, concluido en febrero de 1991.

Asimismo, el Código Penal Boliviano, texto ordenado según ley No 1768 de 1997, incorpora en el Título X un capítulo destinado a los Delitos Informáticos (16). Ambos cuerpos legales tratan de manera general los nuevos delitos emergentes del uso de la informática.

La Ley No 1768, no obstante de no estar exenta de la problemática actual, al abordar en el Capítulo XI la tipificación y penalización de delitos informáticos, no contempla la descripción de estas conductas delictivas detalladas anteriormente. Por consiguiente, la atipicidad de las mismas en nuestro ordenamiento jurídico penal vigente imposibilita una calificación jurídico-legal que individualice a la mismas, llegando a existir una alta cifra de criminalidad e impunidad, haciéndose imposible sancionar como delitos, hechos no descriptos en la legislación penal con motivo de

una extensión extralegal del ilícito penal ya que se estaría violando el principio de legalidad expreso en la máxima "Nullum crime sine lege" Así mismo resulta imposible extender el concepto de bienes muebles e inmuebles a bienes incorporales como ser los datos, programas e información computarizada. Según lo que regula esta ley pues está contemplado en los siguientes artículos.

Capítulo XI

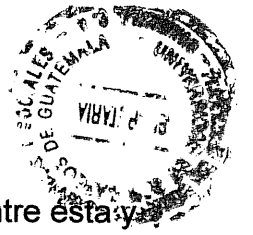
Delitos informáticos

Art. 363° bis.- (Manipulación Informática). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuy resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Art. 363° ter.- (Alteración, Acceso y uso indebido de datos Informáticos).

El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

Delitos Informáticos [31] en nuestro país, el fenómeno de la criminalidad informática o de los llamados delitos informáticos, en nuestro entorno mucho sobre esta clase de infracciones a pesar del efecto de aldea global que estamos viviendo, y la razón de que esta nueva forma de lesión a bienes jurídicos tutelados no sea tomada en cuenta, es



porque se ha perdido por parte de la legislación penal nacional la conexión entre ésta y la realidad social actual. (Problema que no solo es en el área Penal si no en todo el ordenamiento jurídico nacional).

En primer lugar existe una confusión terminológica y conceptual presente en todos los campos de la informática, especialmente en lo que dice relación con sus aspectos criminales, es por eso que es menester desenmarañar el intrincado debate doctrinario acerca del real contenido de lo que se ha dado en llamar los delitos informáticos. Desde esta perspectiva, debe reinar la claridad más absoluta respecto de las materias, acciones y omisiones sobre las que debe recaer la seguridad social que aporta el aparato punitivo del estado. La mayúscula trascendencia inherente a los delitos informáticos merece que toda persona que opere en el mundo del derecho se detenga a meditar sobre el lugar conceptual del espacio de lo jurídico-criminal en que tales agresiones se suceden "*con el uso de la internet con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al* Los Delitos Informáticos, *o a las tecnologías de la información.*" *para referirse a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o se* De ahí que se hable más bien de criminalidad informática que de delitos informáticos propiamente tales. Es por eso que resulta extremadamente complejo buscar un concepto técnico que comprenda todas las conductas ilícitas. Por tanto diremos que el nacimiento de esta nueva tecnología, está proporcionando a nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, *como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas*

informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la

En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos. Por tanto podemos decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos, en tal sentido de María Luz Gutiérrez Francés, respecto de la figura del fraude informático nos dice que: "*las conductas de fraude informático presentan indudablemente un carácter pluriofensivo. En cada una de sus modalidades se produce una doble afección: la de un interés económico (ya sea micro o macro social), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macro social vinculado al funcionamiento de* tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como.

a) El Patrimonio, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.

b) La Reserva, La Intimidad y Confiabilidad de los Datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.

c) La Seguridad o Fiabilidad del trafico Jurídico Probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.

d) 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 de daños y el llamado terrorismo informático. Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas

informáticos donde esta se almacena o transfiere. El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir –ya que constituye la razón de ser del delito– y no suele estar expresamente señalado en los tipos penales.

Dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción.

En fin la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de "dañosidad" o "lesividad". Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada. Así inspira tanto a la criminalización como a descriminalización de conductas. Sin circunscribirnos así a términos rígidos, como sería por ejemplo delitos informáticos. En tal razón diremos que "Delincuencia informática es todo acto o conducta ilícito ilegal que puede 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 *del estudio de la delincuencia vinculada a la informática o tecnologías de la información. En este sentido, es irrelevante que el computador sea instrumento u objetivo de la conducta, y que ésta esté criminalizada o merezca serlo por consideraciones político criminal.*

Republica de México

En el mundo virtual de Internet, es un "paraíso" para los delincuentes cibernéticos. Los vacíos legales y el retraso en avances tecnológicos son los principales factores que hacen a México un blanco para realizar conductas ilícitas en la red de información.

"A través de este sistema, el año pasado se detectaron fraudes que ascienden a más de 700 millones de dólares y en este momento hay un banco que está perdiendo 10 millones de pesos por semana; (...) en México no se persiguen este tipo de delitos.

"En México se registran delitos cibernéticos, pero no se investigan, esa es la verdad; en México hay una carencia importante en lo que es la falta de una unidad especializada en los delitos cometidos en Internet, no hay una especialidad para ese tipo de cosas, lo que sucede en Internet nadie lo investiga", aseguró Gabriel Cámpoli, académico e investigador del Instituto Nacional de Ciencias Penales (Inacipe).

México tiene un mercado potencial de transacciones, a través de Internet superior a los 14 mil 300 millones de dólares anuales, pero en la práctica las operaciones sólo llegan al 17.7 por ciento, es decir, 2 mil 384 millones, por el temor de los usuarios al fraude.

Prueba de ello es que, durante 2006, el fraude cibernético ascendió a 7 mil millones de pesos; la Asociación Mexicana de Internet (Amipci) advirtió que 31 por ciento de los 3.4 millones de usuarios del servicio en el país desconocen las medidas de seguridad para realizar transacciones a través de Internet; el 14 por ciento no saben como usarlas.

Excélsior publicó, en su edición del pasado 12 de noviembre, que cárteles de la droga en México y Colombia han aprovechado las ventajas y el anonimato que ofrece Internet para lavar dinero.

Utilizando transacciones en mundos virtuales, como es el sitio electrónico Second Life que, se "ofrecen a los traficantes oportunidades únicas para lavar dinero", según revela la edición 2007 del National Drug Threat Assesment, elaborado por el Departamento de Justicia estadounidense.

El doctor en legislación y sistemas cibernéticos de seguridad detalló que, en nuestro país, los delincuentes cibernéticos enfocan sus esfuerzos en tres rubros: el mercado de fraudes con automóviles; fraudes con créditos, ya sea tarjetas departamentales o tarjetas de crédito; el tercero, es el tema de lavado de dinero.

"Hay una legislación para todos los delitos, de hecho, el artículo 403 del Código Penal Federal te pediría investigarlo, que es el de operaciones con recursos de procedencia ilícita o lavado de dinero, como quieras llamarle.

"La SSP tiene la unidad de delitos cibernéticos; sin embargo, la Constitución mexicana permite que la policía investigue; lo que hace falta es un equivalente en la PGR".

Un especialista del Inacipe agregó que en nuestro país se han desaprovechado experiencias internacionales en el combate a este tipo de hechos ilícitos; la investigación persiste en Europa, a través de la Europol, y países como Estados Unidos, Venezuela, y Colombia.

"México no aplica este tipo de investigaciones porque no hay consciencia de la gravedad de este tipo de delitos, porque los consideran menos graves; de hecho, cuando se dice delitos informáticos o delitos cibernéticos, al común de la gente le suena al menor que se metió a la computadora de fulanito y hasta ahí llegan, de hecho no hay una especialización para el combate de estas conductas".

En el país, hubo falta de voluntad y estudio del problema; sin embargo, la solución es muy simple: la elaboración de un acuerdo para la creación de una fiscalía especializada en este tema.

"Además de voluntad haría falta tomar consciencia de la gravedad de estos delitos; cuando tú no persigues el lavado de dinero, lo que genera es un sistema de impunidad".

"Básicamente lo que se esta haciendo al no perseguir este tipo de delitos, estamos favoreciendo a la delincuencia porque si ellos pretenden lavar su dinero a través del sistema financiero o de los mecanismos de Internet y no los va a perseguir nadie, obviamente lo que van a hacer es llevarlo a esos sistemas. En teoría, México está en peligro de convertirse en un paraíso de delitos cibernéticos de este tipo".

Legislación Nicaragüense ante los delitos informáticos

Ley especial sobre delitos informáticos
Abril 2005

Secretaría Ejecutiva
Ley especial sobre delitos informáticos

El presidente de la Republica de Nicaragua
Hace Saber al pueblo Nicaragüense que:

La Asamblea nacional de la Republica de Nicaragua
En uso de sus facultades:
Ha dictado

La Siguiente:
Ley especial sobre delitos Informáticos.

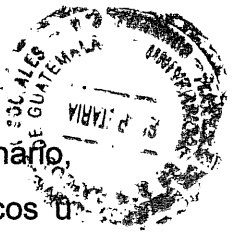
Capítulo I

Disposiciones Generales

Arto. 1.- Objeto de la ley. La presente ley tiene por objeto prevenir y sancionar los delitos cometidos en contra de los sistemas informáticos integrados en equipos físicos o datos e información almacenada en archivos, registros, bases o bancos de datos automatizados.

Arto. 2.- Ámbito de aplicación. Las disposiciones de la presente ley serán aplicables en todo el territorio nacional a las personas naturales que utilizan equipos físicos con sistemas informáticos integrados.

Arto. 3.- Definiciones. Para los efectos de la presente ley, se entiende por: a. Datos: símbolos o caracteres representados apropiadamente para que sean difundidos o procesados por equipos electrónicos a los cuales se les asigna un significado. b. Computador: dispositivo o unidad funcional que acepta datos, los procesa de acuerdo con un programa guardado y genera resultados. c. Hardware: componentes físicos de un sistema informática. d. Información: procesamiento de datos realizado por una persona a los cuales se les asigna un significado. e. Software: Registro de rutinas o



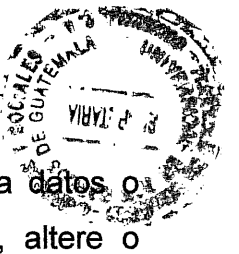
secuencia de instrucciones, de carácter lógico que, codificados en sistema binario, residen o se archivan en forma electrónica e intangible, en soportes magnéticos u ópticos, decodificados, interpretados y reproducidos, de cualquier forma a través de un computador o sistema informático. f. Sistema informático: comprende al hardware local y remoto conectado o no por una red telemática y al software residente en soportes electrónicos u ópticos, fijos o móviles, que dependen de el para realizar un trabajo en particular o resolver un problema dado. g. Virus informático: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un software o componente del sistema.

Capítulo II

De los Delitos y las penas

Arto. 4.- Acceso indebido de datos. Comete delito de acceso indebido de datos el que sin el debido consentimiento, accede, intercepta, interfiere, copia o desvía datos o información almacenada en archivos, registros, bases, bancos de datos o en equipos físicos que útil izan sistemas informáticos, será sancionado con la pena de seis meses a dos años de prisión. El que revele o difunda los datos o información obtenida indebidamente descrita en el párrafo anterior del presente artículo, será sancionado con la pena de seis meses a tres años de prisión. Cuando el autor sea funcionario público en ejercicio de sus funciones, será sancionado con inhabilitación especial para el desempeño de cargos públicos por el doble de tiempo que el de la condena.

Arto. 5.- Alteración de documentos. Comete delito de alteración de documentos, el que utilizando equipos físicos con sistemas informáticos integrados, altera, modifica, borra, suprime o lo sustituye con otro en parte o en su totalidad el contenido de un documento Público o privado almacenado o no en dicho sistema, será sancionado con la pena de tres a seis años de prisión. Si de tal acto, resultare en perjuicio a un tercero, la pena se aumentará en un tercio de lo dispuesto en el presente artículo.



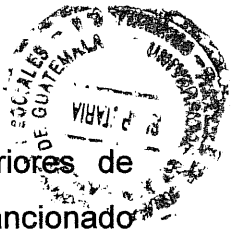
Arto. 6.- Daño a datos o sistemas informáticos. Comete delito de daño a datos o sistemas informáticos, el que sin la debida autorización destruya, dañe, altere o inutilice los datos o funciones de los sistemas informáticos integrados en equipos físicos, será sancionado con la pena de uno a tres años de prisión. Si los efectos indicados en el presente artículo se realizaren por medio de un virus informático o programa similar, será sancionado con la pena de cinco a diez años de prisión.

Arto. 7.- Sabotaje informático. Comete delito de sabotaje informático, cuando los hechos descritos en el articulo anterior recaigan sobre los datos o sistemas informáticos de los archivos, registros, bases, bancos de datos que almacenan datos o información de carácter destinada a las funciones publicas, será sancionado con la pena de hasta diez años de prisión.

Arto. 8.- Fraude informático. Comete delito de fraude informático el que con ánimo de lucro, para sí o para un tercero, mediante el uso de equipos físicos que utilizan sistemas informáticos, inserte información falsa, manipule o modifique los programas existentes, procurando el traslado no consentido de cualquier activo patrimonial en perjuicio de otro, será sancionado con la pena de tres a ocho años de prisión.

Arto. 9.- Hurto informático. Comete delito de Hurto informático el que mediante equipos físicos que utilizan sistemas informáticos o medios de comunicación, se apodere de bienes tangibles o intangibles de carácter patrimonial, con el fin de tener un beneficio económico para sí o para un tercero, será sancionado con la pena de tres a seis años de prisión.

Arto. 10.- Espionaje informático. Comete delito de espionaje informático el que sin la debida autorización acceda y obtenga datos o información almacenada en equipos físicos que utilizan sistemas informáticos, con o sin intención de divulgarla, será sancionado con la pena de tres a ocho años de prisión. Si el delito cometido, se obtuviere datos o información considerada muy secreta, secreta y confidencial,



relacionada a la seguridad nacional, defensa o a las relaciones exteriores de Nicaragua, almacenada en bases de datos o sistema informáticos, será sancionado con la pena establecida en el arto. 541 del Código Penal. Si el autor del delito descrito en el párrafo anterior revelare o divulgare los datos o información obtenida, será sancionado con la pena establecida en el arto. 542 del Código Penal.

Arto. 11.- Difusión pornográfica de niños, niñas o adolescentes. Comete delito de difusión pornográfica de niños, niñas o adolescentes, el que utilizando equipos físicos con sistemas informáticos integrados, soportes electrónicos y digitales, accede, imprime, copia, exhibe, distribuye, comercializa y difunde a través de cualquier medio material pornográfico con imágenes de niños, niñas o adolescentes que tuviere su origen en el territorio nacional, extranjero o desconocido, será sancionado con la pena de cuatro a ocho años de prisión. La pena del presente artículo se aumentará hasta diez años de prisión cuando el delito cometido sea con ánimo de lucro. El que facilite el acceso, impresión, copia, exhibición, distribución, comercialización y difusión, será sancionado con la pena de tres a seis años de prisión.

Arto. 12.- Creación y distribución de virus informáticos. Comete delito de creación y distribución de virus informáticos, el que maliciosamente cree o distribuya cualquier programa con el objeto de destruir, dañar, alterar o inutilizar el funcionamiento de los equipos físicos que utilizan sistemas informáticos, será sancionado con la pena de tres a ocho años de prisión.

Arto. 13.- Violación de las comunicaciones. Comete delito de violación de las comunicaciones, el que interfiere, intercepte, acceda, capture, desvíe o elimine señal de transmisión o mensajes de datos contenidos en equipos físicos electrónicos, sin la debida autorización de la persona o juez competente; será sancionado con la pena de dos a cuatro años de prisión.

Capítulo III

Disposiciones Finales

Arto. 14.- Vigencia. Esta Ley entrará en vigencia a partir de su Publicación en La Gaceta, Diario Oficial.

Republica de Colombia

"En el caso de este país, el Congreso Colombiano aprobó la ley que modifica el Código Penal para incorporar los delitos que violen la protección de la información y de los datos. Como lo señala el autor Luis Alcalá".[31] Veintidós años después de que Estados Unidos adoptó el Acta de Fraude y Abuso Computacional, y siete años después de que Europa firmó el Convenio de Ciber criminalidad, Colombia está contando actualmente con una legislación para combatir los delitos informáticos.

La plenaria del Senado de la República de Colombia aprobó la ley que modifica el Código Penal con el fin de crear una nueva serie de delitos en torno a la violación de la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. Los ajustes realizados a la regulación. Permitieron que el ordenamiento colombiano se sume a las políticas penales globalizadas en materia del combate frontal contra la llamada criminalidad en el ciberespacio y le brinde herramientas a la comunidad internacional para la persecución de estos flagelos.

Esta ley, establece penas de prisión de 4 a 8 años para los delincuentes informáticos y multas de 100 a 1.000 salarios mínimos mensuales, es decir de 46,1 a 461,5 millones de pesos.

[31] Legislación Colombiano en **Materia de Delitos Informáticos**. Pág. 63

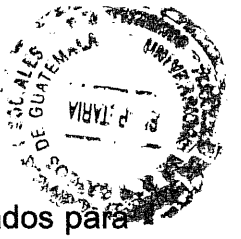
Entre las conductas tipificadas como delito están el acceso abusivo a sistemas informáticos, la obstaculización ilegítima de sistemas computacionales o redes de telecomunicaciones, la interceptación de datos informáticos, el uso de software malicioso, la violación de datos personales y la suplantación de portales de Internet para capturar datos personales, entre otras.

Mientras no existía esta ley, las personas que eran sorprendidas cometiendo este tipo de crímenes debían ser procesadas por delitos genéricos.

Dentro de las figuras que se encuentran en estas reformas a la ley penal, se encuentran:

Acceso abusivo a un sistema informático. Será sancionado quien sin autorización acceda a un sistema informático protegido o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.
Obstaculización ilegítima de sistema informático o red de telecomunicación. Se penalizará a quien impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

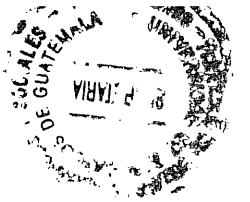
"Interceptación de datos informáticos. Bajo este delito serán castigadas las personas que, sin orden judicial previa, intercepten datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte. Daño informático. Se sancionará a quien, 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 lógico. Uso de software malicioso. El proyecto de ley señala que serán castigadas las personas que, sin estar facultadas para ello, produzcan, trafiquen, adquieran, distribuyan, vendan, envíen, introduzcan o extraigan del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

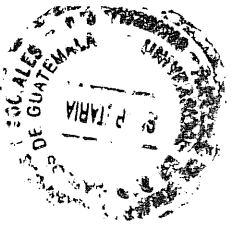


"Violación de datos personales. Este delito cobijará a quienes, sin estar facultados para ello, con provecho propio o de un tercero, obtengan, compilen, sustraigan, ofrezcan, vendan, intercambien, envíen, compren, intercepten, divulguen, modifiquen o empleen códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes".[32]

Suplantación de sitios Web para capturar datos personales. Será sancionado quien, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes. También quien modifique 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, siempre que la conducta no constituya delito sancionado con pena más grave. En este caso la pena se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena de los delitos.

[32] Blossiers Manzini, Juan José. **Descubriendo los Delitos Informáticos**: Pág. 98





CAPÍTULO III

3. Los Hackers en la Internet y las consecuencias penales, de la necesidad de que se regule en el Código Penal las conductas ilícitas.

3.1 Análisis del delito informático en el Código Penal

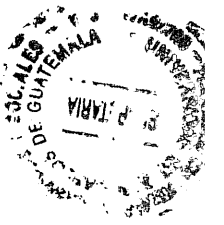
En materia propiamente de los delitos informáticos, el Capítulo VII se adicionaron algunas figuras delictivas en forma muy generalizada como se observará e incluidas dentro de los delitos contra los derechos de autor y propiedad intelectual, sin que puedan tener una relación directa entre éstos y los otros, tal como se observa con el análisis anterior, sin embargo, se han establecido y a continuación se describen las mismas.

Destrucción de registros informáticos

Artículo 274 "A". Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizare registros informáticos.

Alteración de programas

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



Reproducción de instrucciones o programas de computación.

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

Registros prohibidos

Artículo 274 "D". Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Manipulación de información

Artículo 274 "E". Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.

Uso de información

Artículo 274 "F". Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos.

Programas destructivos

Artículo 274 "G". Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o

instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.

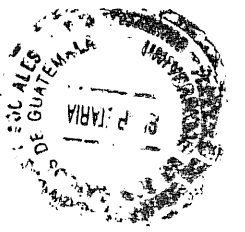
A consideración de quien escribe las figuras delictivas que se describen en el Código Penal son vigentes pero no positivas, por cuanto su redacción se ha hecho en términos muy generales, si se compara con lo que sucede con otras legislaciones como ya se ha visto específicamente en el tema del actuar de los hackers.

3.2 Las actividades de los hacker frente a los delitos informáticos en código penal

Existen una serie innumerable de actividades que puedan realizar los hackers, que están en la actualidad y que se pueden esperar en el futuro cercano. Dentro de las más importantes que se han podido determinar a efectos del presente trabajo, se encuentran las siguientes:

a) La introducción de virus

Los virus "son elementos informáticos que tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son, eventualmente, susceptibles de destrucción mediante un antivirus adecuados frente a los cuales pueden incluso desarrollar resistencias". Tienen formas variadas y se actualizan permanentemente. Los virus pueden ser a su vez, malignos y benignos, según si provocan daño o simplemente aparecen con el objeto de hacer notar algún acontecimiento ocupándonos por ahora solamente de los primeros Cuando el virus es maligno puede causar la destrucción o borrado de un software, sistema o banco de datos en la red.



b) Borrado o destrucción de un programa.

Esta conducta se realiza fundamentalmente cuando el propósito de borrar o destruir programas de computación, por cuanto esta claro que esta conducta como tal, no podría representar un delito, pero cambiaria la situación, si esto se hace con fines lucrativos. Incluso, en este caso, también podrían existir agravantes del mismo ilícito cuando el daño se ejecuta en archivos y registros digitales, bibliotecas digitales o cuando se refiera a registros públicos o estatales.

c) Piratería del Software y Banco de datos

"Como todo delito contra objetos protegidos por el derecho de autor, requieren inexcusablemente la existencia, en su aspecto subjetivo, del dolo del agente. Se tratan de delitos que involucran bienes jurídicos cuya protección por derechos de autor fue en algún momento, cuestionada. Se introduce como objeto de protección los derechos de autor. Violaciones a derechos morales y patrimoniales de otros objetos protegidos por el derecho de autor".[33]

Tal como se puede observar existe una red global de información de bienes protegibles por la ley de Propiedad Intelectual, las obras musicales, literarias, fotográficas, audiovisuales, plásticas, arquitectónicas, planos mapas, entre otros. También se puede encontrar actividades protegidas por los llamados derechos vecinos al derecho de autor, tales como el derecho de los intérpretes y de los productores de fonogramas que merecen una tutela de la ley y normas

[33] Guibour Ricrdo A. **Manual de Informatica Juridica**. Pág. 273

complementarias. Se puede decir, a sólo título ejemplificativo cuales son los ilícitos que se comente en violación a los derechos de autor y derechos conexos.

a) Editar, vender o reproducir una obra musical, texto original, imágenes estáticas y en movimiento el diseño de una página Web como todo su contenido sensible y original, sin autorización. Esta prohibición alcanza a las obras publicadas en la red como las inéditas que fueron obtenidas por violación de códigos de acceso.

b) Estos actos se llaman vulgarmente "piratería" significando toda reproducción no autorizada de una creación protegida.

c) Editar, vender o reproducir alguna obra protegida y editadas suprimiendo o cambiando el nombre de su autor, el título o alterando su texto. Sobre este caso se puede ejemplificar al que interfiere un sitio y altera los colores de las imágenes, se atribuyen la autoría de cualquier creación en el ciberespacio, y cambio de título de cualquier aporte creativo. Se encuentra con el supuesto de "plagio", un delito típico del derecho de autor que consiste en hacer que aparezca como propio lo que pertenece a otro, y representa la violación al derecho moral de paternidad del titular originario de la obra. También se encuentra en este supuesto la violación al derecho moral de integridad o respecto de la obra que consiste en la modificación, alteración, supresión de todo o parte de la creación. En consecuencia, es licito tomar parte de obras ajenas protegidas para realizar, notas, criticas comentarios para hacer más inteligible el propio o para sostener una investigación. También se provee el uso libre de las noticias de interés general indicando la fuente de ellas, la publicación de retratos con fines didácticos, científicos y de interés cultural estableciendo un plazo para solicitar sin autorización y los usos de obras musicales o dramáticas para establecimientos de enseñanza y en cumplimiento de dichos fines didácticos.

d) También la red es un terreno fértil para la comisión de delitos como los que son contra el honor, promoción y facilitación de la prostitución, violación de secretos, robo, estafa, corrupción de menores, contra la seguridad pública, instigación a cometer delitos, apología del crimen, etc.

3.3 Nuevas conductas criminales a través del uso de la Internet y la informática

Las diferentes formas que pueda adoptar el delito informático son de tal dimensión que para un profano prácticamente serían inimaginables limitados quizás únicamente por la astucia del autor, su capacidad técnica y las deficiencias de control existentes en la instalación invadida.

Para darse una idea del ámbito del problema conozcamos las diversas formas en las que el delito informático puede producirse sin que ello suponga de ninguna manera que estamos ante una lista cerrada sino tan sólo de una relación enumerativa de las situaciones más frecuentes.

Entre ellas, aparte de las ya citadas, se pueden señalar las siguientes:

a) Introducción de datos falsos a Data Diddling

Consiste en manipular las transacciones de entrada al computador con el fin de ingresar movimientos falsos total o parcialmente, o eliminar transacciones verdaderas que deberían haberse introducido. Es un método al alcance de muchas personas que desarrollan tareas en los servicios informáticos para lo cual no es necesario poseer conocimientos técnicos especiales sino tan sólo haber percibido las deficiencias de control que muestre un determinado sistema. La pregunta entonces, es que no más pueden hacer con fines criminales los hackers ante esta situación. "Un antecedente

muy publicitado es el Caso Blair, conocido por un delito cometido en Maryland en mayo de 1980. Janeth Blair, empleada de las oficinas de seguridad social, ingresaba desde su terminal informática, que se encontraba conectado con un computador central, transacciones falsas para producir la emisión de cheques fraudulentos, consiguiendo por este procedimiento apropiarse de cerca de Ciento Doce mil Dólares. Este delito fue descubierto de manera casual por el empleado del banco a cuyo nombre eran girados los cheques quien sospechó al verificar la existencia de gran cantidad de cheques con el mismo número de afiliación a la seguridad social pero expedido a" diferentes titulares

Según en este caso, la Señora Janeth Blair fue acusada de 43 cargos de falsificación y desfalco y fue condenada a ocho años de prisión con una multa de Quinientos Dólares, como conclusión del caso objeto de análisis.

b) El salame, redondeo de cuentas o "Rounding Down"

Es tal vez la técnica más sencilla de realizar y la que menos probabilidades tiene de ser descubierta. La modalidad consiste en introducir o modificar unas pocas instrucciones de los programas para reducir sistemáticamente una cantidad transfiriéndola a una cuenta distinta o proveedor ficticio que se abre con nombre supuesto y que obviamente la controla el defraudador.

Por ejemplo puede darse el caso de disminuir constantemente en unos céntimos las cuentas corrientes de un cliente bancario, pequeños saldos de proveedores, reducir los talones de impresión para el pago a acreedores, transfiriendo luego estas pequeñas cantidades a la cuenta particular del autor. También se suele aplicar esta modalidad cuando se calculan los intereses de cuentas corrientes bancarias, de libretas de ahorro, de depósitos a plazo o bien cuando se elabora el cálculo de la planilla de los trabajadores de una empresa, procediéndose a eliminar el criterio generalizado de redondeo de céntimos a la alza o a la baja de dinero en montos

exactos y a cambiarlo por la eliminación total de dichos céntimos que son transferidos a una determinada cuenta o a nombre de un empleado real o ficticio.

La razón principal por la que es tan difícil descubrir este tipo de hechos es porque las cuentas o el importe total del listado, siguen estando "cuadrados" por lo que no se deduce ninguna señal de alarma que pueda indicar lo que está sucediendo.

Por ejemplo se da el caso al redondear cuentas bancarias y acreditar los montos resultantes a una cuenta determinada repitiendo automáticamente la operación sin intervención posterior del autor. Un caso real se dio en los Estados Unidos donde un programador tenía bajo su responsabilidad el sistema mecanizado de personal en el cual introdujo pequeñas modificaciones en los cálculos del plan de inversiones corporativas.

La empresa había acordado con sus trabajadores que les retendría una pequeña cantidad de sus salarios para invertirlos en valores. Lo que realizó el programador fue retirar pequeñas cantidades de lo descontado cada empleado para transferirlo a su propia cuenta.

c) Uso indebido de programas o l "Superzapping"

"Es el uso no autorizado de un programa de utilidad para alterar, borrar, copiar, insertar o utilizar cualquier forma no permitida los datos almacenados en el computador o en los soportes magnéticos. El nombre proviene de un programa llamado "Superzap" y es una especie de llave que permite abrir cualquier rincón de una computadora por más protegida que pueda estar. Estos programas pertenecen al grupo de los llamados "Programas de Acceso Universal" de uso imprescindible en

cualquier instalación de ciertas dimensiones cuando fallan los procedimientos normales para recuperar o reiniciar "el sistema". [34]

Efectivamente, cuando un sistema informático almacena gran cantidad de información se hace necesario disponer de un mecanismo de emergencia que permita entrar a cualquier punto del sistema en caso que se produzca alguna avería o lo que normalmente se ha denominado "caída del sistema". Es por esta razón que se justifica la existencia de los llamados "Programa de Acceso Universal" (PAU) herramientas imprescindibles en cualquier instalación de ciertas proporciones cuando fallan los procedimientos normales para "recuperar" o "reiniciar" el sistema.

Los programas de utilidad son una herramienta valiosa y muchas veces imprescindible en los casos de caída del sistema pero igualmente un arma peligrosísima cuando se encuentra al alcance de personas que lo utilizarán con otras intenciones.

No es necesario insistir que su acceso debe ser restringido y con adecuados controles. No obstante suelen estar archivados en las librerías de producción junto con el resto de programas de uso común y generalizado, con lo cual cualquier técnico podría tener la posibilidad de utilizarlo indebidamente. Con la modalidad de súper zapping es posible alterar los registros de un fichero sin que quede constancia de tal modificación lo cual hace sumamente difícil descubrir y detectar el autor de tales eventos. Aparentemente se suelen registrar los ingresos a un sistema y las transacciones que se han procesado en una determinada operación actualizando los registros con un dato específico como por ejemplo la hora de ingreso.

Sin embargo los programas de acceso universal -permiten modificar directamente la información sin activar los programas de actualización ni introducir ninguna operación al computador. Aún más, sin dejar rastro si la persona que lo está usando

[34] Blossiers Manzini, Juan José. **Delitos Informáticos**. Pág. 98

sabe como realizarlo. Bastaría con hacer coincidir el momento de la modificación no autorizada con el comienzo o el final de la ejecución del programa verdadero de actualización y algún error intencionado en el sistema que requiera la utilización del programa de acceso universal.

En ese preciso momento se tendrá cargado en el sistema el fichero que se quiere modificar y el programa que permite modificar no registrándose por lo tanto su utilización no justificada ni del fichero, ni del programa de utilidad

Cuando se descubran las alteraciones de los datos se pensará que ha sido un funcionamiento erróneo del programa de actualización, un funcionamiento inadecuado del computador o una transacción errónea y en esas direcciones se encaminará la investigación las cuales seguramente no abordarán a ningún puerto.

En el mejor de los casos si se descubre como se realizó la alteración de datos será muy difícil probarlo. Un conocido caso con el método del "súper zapping ocurrió New Jersey en donde el autor comenzó a desviar fondos desde las cuentas de diferentes clientes hacia la de unos amigos sin que quedara en el sistema ninguna evidencia de las modificaciones efectuadas en los saldos de cuenta corriente. El delito se descubrió por los reclamos efectuados por uno de los afectados lo cual motivó una investigación que culminó con la detención del sujeto.

b) Puestas falsas o " Traps Doors"

Es una costumbre en el desarrollo de aplicaciones complejas que los programas permitan introducir interrupciones en la lógica de los desarrollos del mismo, con el objeto de chequear por medio de los procesos informáticos si los resultados intermedios son correctos, producir salidas de emergencia y de control a fin de guardar resultados parciales en ciertas áreas del sistema para comprobarlos después.

Inclusive algunas veces este procedimiento se enlaza con rutinas del sistema operativo para facilitar una puerta de entrada al programa que no estaba prevista, pero de esta manera facilitan la labor de desarrollo y prueba de programas. El problema radica en tener la seguridad de que cuando los programas entran en proceso de producción normal todas esas "puertas falsas" hayan desaparecido. Y aunque parezca mentira, las puertas creadas no se eliminan, permitiendo a su paso puertas de acceso al programa con el agravante que por ser elementos temporales creados por la computadora no constan en la documentación del sistema. Es de uso frecuente para posibles recuperaciones en caso de "Caída del Sistema" a mitad de un proceso ir grabando en cinta resultados intermedios o copia de las transacciones procesadas, o incluso ciertas áreas de memoria para la recuperación más rápida y sencilla.

Las puertas falsas son: Por personas que no las crearon, pero que una vez descubiertas se aprovechan de ella sin necesidad de poseer una formación informática profunda. Tal es el caso de unos ingenieros en una fábrica de automóviles en Detroit que descubrieron una puerta falsa en una red de servicio publico de time-sharing de Florida.

Después de una serie de intentos consiguieron ingresar con una llave de ingreso de alto nivel, según parece la del propio presidente ejecutivo de la compañía y utilizándola pudieron apoderarse de diferentes programas clasificados de carácter reservado y archivados en el computador bajo la denominación de secreto comerciales, al mismo tiempo que utilizaban la red sin cargo económico alguno.

e) Bombas Logicas o "Logic Bombs"

"Previamente debe señalarse que este tipo de delito se ejecuta para producir daños sin otro beneficio que el placer de perjudicar, en muchos casos. El método consiste en introducir en un programa un conjunto de instrucciones no autorizadas para que en una fecha o circunstancia predeterminada se ejecuten automáticamente desencadenando el borrado o la destrucción de información almacenada en el computador, distorsionando el funcionamiento del sistema o paralizaciones intermitentes".[35]

Un conocido caso de bomba lógica se presentó en septiembre de 1981 y tuvo como protagonista un programador de computadoras de 26 años de edad que trabajaba para el departamento de defensa en Washington D.C. en los Estados Unidos de Norteamérica. Resulta que el programador se sintió frustrado y discriminado al no recibir una promoción que supuestamente le correspondía, por lo que decidió vengarse. El trabajo de este empleado consistía en el mantenimiento de las nóminas del sistema de personal lo que le permitía tener acceso a todos los programas y a la información contenida en la base de datos de dicho sistema.

Decidido a vengarse escribió unas rutinas para incluir en los programas que a cierta señal se borren y destruyan gran parte de la información que él procesaba en los sistemas. Posteriormente comenzó a buscar otro trabajo para lo cual solicitó vacaciones en su empleo siendo así que consiguió un nuevo trabajo. Unos días después que recibió la confirmación de su nuevo empleo, y en ese mismo momento aprovechando la hora del almuerzo, introdujo la rutina que tenía programada, incluyendo un control que se activaría seis meses desde la fecha de su salida de su anterior empleo.

[35] Blossiers Manzini, Juan José. **Ob. Cit.** Pág. 287

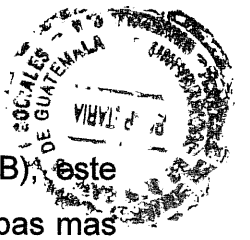
En efecto, seis meses después de haber abandonado a su anterior trabajo cuando se estaban procesando las nóminas de personal la rutina introducida por él funcionó como había previsto su autor, borrando la mayor parte de información de los registros de personal.

Dada que el programa había estado funcionando largo tiempo y nadie dudaba de su funcionamiento se volvieron a probar con las copias de seguridad las que también resultaron dañadas. El descubrir el motivo de los daños al sistema y recomponer la información requirió gran esfuerzo de personal y de tiempo lo que puede dar una idea del costo que se supuso, pero no fue posible probar la autoría del hecho, aunque las sospechas recayeron sobre su verdadero autor, el que nunca fue acusado formalmente. ni juzgado ni castigado.

Esta modalidad es una forma bastante extendida, utilizada por muchos fabricantes de paquetes de software con el fin de asegurar el importe de los mismos. Consiste en programar una instrucción que revisa la fecha del día, lo que permite una fecha de caducidad oculta que ha introducido el fabricante del software al instalarlo en el computador del cliente y que no será eliminada o prorrogada hasta que el cliente pague los nuevos derechos. Esto constituye una verdadera forma de coacción ilegal pero que es utilizada por una falta de protección adecuada de sus derechos de autor.

f) Eliminar el blanco o pong mortal.

Algunos ataques eliminan el blanco en lugar de inundarlo con trabajo. Un ejemplo de este tipo es el ping mortal, un paquete pin ilícitamente enorme, que hace que el equipo de destino se cuelgue. Muchas implementaciones de routers, la mayoría de los Unix y todas las versiones de Windows mostraron vulnerables a este ataque cuando se lo descubrió por primera vez hace un par de años. A pesar de que los vendedores lanzaron parches de inmediato, hay todavía cantidades significativas de hosts "no corregidos" en la redes de producción (en especial, las que corren bajo el



Windows 95). TSP/IP permite un tamaño de paquete de 64 kilobytes (KB), este máximo esta dividido en piezas más pequeñas a través de protocolos de capas más bajas.

g) Ataques asincrónicos o "Asynchronoc Attacks"

Los sistemas informáticos en la mayoría de casos funcionan ejecutando más de dos comandos u órdenes a la vez o en otras circunstancias una instrucción sucesiva de la otra en forma secuencial".[36]

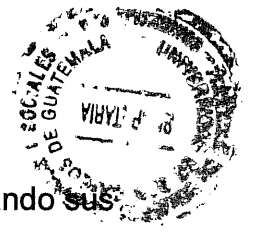
Cabe recordar que el sistema operativo es el conjunto de programas que controlan el funcionamiento del computador y todos sus dispositivos periféricos (discos, cintas, impresoras), la entrada de los datos procesados por el programa, la ejecución de los programas de las diferentes aplicaciones y la salida de la información elaborada hacia los dispositivos exteriores.

El sistema operativo es imprescindible para el funcionamiento del equipo y su desarrollo es responsabilidad del fabricante. Una de las principales funciones del sistema operativo de las computadoras es controlar la ejecución simultánea de varios programas a la vez. Otra función fundamental del sistema operativo es optimizar la ocupación de memoria central reasignando áreas en función de las necesidades de cada uno de los programas que están ejecutando en cada momento.

De otro lado el sistema operativo asigna a los programas otras funciones de clasificación, intercambio, etc. Por lo tanto el sistema operativo es quien controla y maneja todos los errores que pueden producirse tanto en la computadora como en los programas que se están ejecutando, avisando al operador por medio de mensajes de cualquier situación anormal que se produzca.

---

[36] Blopssier Manzini, Juan José. **Ob. Cit.** Pág. 281



"Pues bien, los programas funcionan en forma sincrónica, es decir, ejecutando sus instrucciones en un orden fijo predeterminado de nivel en nivel, en tanto que el sistema operativo funciona en forma asincrónica es decir ejecutando sus órdenes de manera independiente, en función de una gran cantidad de factores ajenos a él. Esto produce rigurosidad en los programas en ejecución conformando las llamadas "Colas de Espera" que se van a ir desbloqueando en función de la disponibilidad de los datos o comandos que estaban esperando. Uno de los típicos casos en el que puede producirse es en los llamados puntos de recuperación del sistema".[37]

Cuando se procesan programas complejos y de larga duración se establecen puntos de recuperación cada cinco o diez minutos por ejemplo gravando en soporte magnético externo (diskettes) el estado del programa, lo que implica que si el sistema "SE CAE ", es decir, que se interrumpa el proceso por una situación de error no recuperable, por ejemplo falta de energía eléctrica no es necesario retroceder desde el principio del programa sino bastará hacerlo desde el último punto de recuperación ya que todo se encuentra grabado, reiniciando de esta manera el proceso.

Pues bien, si entre dos puntos de recuperación se provoca voluntariamente una "caída del sistema" y en el intermedio se manipula los parámetros en que se va a apoyar el sistema operativo para reiniciar resulta obvio que las condiciones en que se ejecuten serán distintas a las originales por lo que sus resultados serán por lo menos diferentes, fraudulentos o erróneos .

[37] Blossier Manzini, Juan José Ob. Cit. Pág. 281

h) Recojo de información residual o "Scavenging"

Este procedimiento se basa en aprovechar los descuidos de los usuarios ya que la información ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con la debida autorización.

"La denominación proviene del anglicismo" [38] "to scavengeque significa recogerla basura. Simplemente se va aprovechando las finalizaciones de los trabajos reales en el computador para obtener la información residual que ha quedado en la memoria. La modalidad más frecuente es la "Impresión Diferida" preparando la unidad para que posteriormente imprima sin ningún tipo de protección siendo fácilmente recuperable sin necesidad de utilizar ninguna clave de acceso. Tiene dos formas bien definidas: scavenging físico y scavenging electrónico.

a) El Scavenging Físico: Consiste en recoger el material de desecho que se abandona en las papeleras, encima de las mesas, en el suelo, etc., y que frecuentemente incluye listados de pruebas de programas, documentos conteniendo información de entrada a un programa de la computadora, copias de apoyo que no han sido repartidas, etc.

c) El Scavenging Electrónico: Consiste en aprovechar las finalizaciones de las ejecuciones de los programas realizados en el computador para obtener la información residual que ha quedado en la memoria o en soportes magnéticos. Una de las formas más simples del scavenging electrónico es cuando se ordena la impresión diferida ya que en la computadora queda preparada la información que posteriormente se imprimirá sin ningún tipo de protección, siendo sumamente fácil recuperar la información sin la necesidad de utilizar ningún tipo de clave o cualquier procedimiento.

[38] www.onu..com.htlm.

de seguridad. El caso más célebre de scavening ocurrió en Los Ángeles por un estudiante de ingeniería eléctrica. El estudiante simultáneamente trabajaba como vendedor de equipos de comunicaciones lo cual le permitió adquirir un conocimiento bastante profundo de como operaban los sistemas mecanizados de la empresa.

Al haber recogido cada mañana los papeles que depositaban en el exterior del centro de procesamiento de datos de la compañía. El estudiante simulando ser un publicista convenció a los directivos de la empresa para lanzar un boletín que reforzaría considerablemente la imagen de la compañía. Esto le permitió recopilar información, añadida a la compra de una camioneta en una subasta de la propia compañía. El estudiante pidió telefónicamente mercadería para una empresa que había seleccionado previamente. Para ser despachada por la noche por la cantidad de 30 mil dólares, lo que hizo fue recoger la mercadería y distribuirla a diferentes compradores.

"El estudiante fue descubierto al ser denunciado por su ayudante a quien se negó a aumentar el dinero que le pagaba por sus servicios especiales. El estudiante fue acusado de varios delitos y el 5 de julio de 1972 fue condenado por el Juez M. Deal a dos meses en una correccional, 500 dólares de multa y tres años de "libertad vigilada.

i) Divulgacion no autorizada de datos o "Data Leakcage"

Consiste en sustraer información confidencial almacenada en un computador central desde un punto remoto, accediendo a ella, recuperándola y finalmente enviándola a una unidad de computador personal, copiándola simultáneamente.

La sustracción de información confidencial es quizás uno de los cánceres que con mayor peligro acechan a los grandes sistemas informáticos. Se ha empleado también bajo la denominación de espionaje industrial, pues sería particularmente débiles al sustraerse aspectos claves de su actividad empresarial, como por ejemplo estrategias de mercado, nuevos productos, fórmulas de producción, etc. Inclusive hay cierto tipo

de empresas que dependen de la privacidad de su información como las empresas de publicidad directa en donde tiene ficheros completos de su público objetivo.

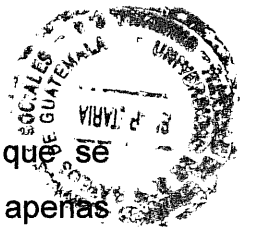
j) Accso a areas no autorizadas o "Piggyn baking"

Pese a no tener una traducción específica consiste en acceder a áreas restringidas dentro de la computadora o de sus dispositivos periféricos como consecuencia de puertas abiertas o dispositivos desconectados. Se da también cuando el usuario que está trabajando en un terminal en un nivel autorizado que le permite realizar ciertas funciones reservadas deja el Terminal conectado, con lo que cualquier otra persona puede continuar trabajando sin necesidad de identificarse pudiendo efectuar operaciones que en condiciones normales no le estarían permitidas.

k) Suplantación de la personalidad o "Impersonation"

Puede ser entendida como la suplantación de personalidad fingiendo ser una persona que no es imitándola e inclusive remedándola. Algunos sistemas requieren la identificación con una clave para acceder al sistema. Más adelante se ha requerido la posesión de algo pudiendo ser una llave o tarjeta magnética. Y aún podríamos complicarlo aun más si se adiciona dispositivos de reconocimiento biométrico como identificación con la palma de la mano o dactilográfica, scanners de retina o del iris, reconocimiento de voz, etc. Un caso muy frecuente de Impersonation o suplantación de personalidad se da en el robo de las tarjetas de crédito y de cajeros automáticos.

Los autores del delito se hacen pasar por un empleado de la central de tarjetas de crédito, llamando telefónicamente al titular para solicitarle que con el objeto de anular la posibilidad de utilización fraudulenta de la tarjeta robada le revele su clave secreta o personal. Como es fácil advertir, una vez descubierta la clave a la persona desconocida que las ha llamado utilizan la tarjeta para sacar el dinero de los cajeros automáticos hasta su límite máximo de crédito. También aprovechan las repeticiones



automáticas de los proceses de computo es una técnica especializada que se denomina técnica del salchichón "en pequeñas rodajas muy finas" apenas perceptibles de transacciones financieras, se van sacando de una cuenta y se trasfieren a otra. Esta es una alerta para aquellos que realizan compras mediante la modalidad de debito. Fraude por duplicidad de tarjeta cuando se opera bajo la modalidad de debito en cuenta maestra, este consiste en instalar un Past Net o sea (lector de tarjeta) falso, el cliente que se presenta en el negocio realiza su compra mediante la utilización de su tarjeta y al momento del pago lee en la banda que ingrese su PIN. El empleado le informa al cliente que se ha producido una falla que el equipo no funciona o que existe un problema, a consecuencia de ello la transferencia se cancelo. Por lo que debe repetir la operación en otra terminal. Es esa operación supuestamente fallida en la cual el equipo no esta conectado a ningún sistema informático, captura la banda y PIN. Con esta información se logra generar una tarjeta melliza.

Otro caso célebre es el que hicieron los estudiantes de una universidad norteamericana al mandar una carta en papel oficial a todos los usuarios de computadoras de la universidad advirtiéndoles que el número de conexión al sistema había sido cambiado, solicitándoles su número anterior. Posteriormente y debido a que lo primero pedía el sistema al conectarse era la clave de identificación, los estudiantes recogieron la clave e indicaron que hasta nueva orden volvieran a usar su número antiguo, obteniendo así el número clave de todos los usuarios del sistema, descubriendo todos los secretos de los estudiantes de la universidad. Una vez descubierto el procedimiento todas las claves fueron cambiadas.

l) Pinchado de linea informaticas "Wiretapping"

"Se trata de pinchar o interferir líneas de transmisión de datos y recuperar la información que circula en ellas generalmente se produce en el mismo origen de la transmisión. No es necesario tener equipo sofisticado, sólo se requerirá un pequeño cassette, una grabadora, una radio portátil AM-FM, un módem para demodular las señales telefónicas analógicas y convertirlas en digitales, y una pequeña impresora para listar la información que se hubiera captado. La forma de realizarlo depende del sujeto que lo ejecuta".[39]

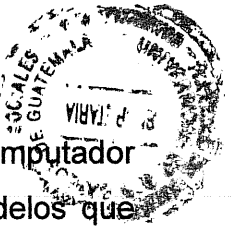
m) Hurto de tiempo

Se da cuando los empleados utilizan sin autorización las horas de la máquina del empleador por ejemplo para realizar trabajos particulares hurtando el tiempo del computador o del servicio de procesamiento de datos y por tanto incrimina un uso no autorizado.

n) Simulación e imitación de modelo o "simulation and modeling"

Se trata del uso de la computadora para simular y planificar la comisión de un delito antes de realizarlo. La utilización de la computadora se realiza de forma mediata para conseguir un fin ilícito como ejemplos se puede señalar desde la simulación del robo de una bóveda de un banco hasta el contador que contrató los servicios contables de una empresa para estudiar detenidamente las repercusiones de los asientos fraudulentos que pensaba realizar para sustraer una cantidad importante de dinero.

[39] Blossiers Manzini, Juan José. **Ob. Cit.** Pág. 283



Aquí se difiere de los anteriores tipos de delitos informáticos pues el computador que puede ser usado para simular situaciones previsibles o efectuar modelos que representen el comportamiento previsible de una empresa, una fábrica, una inversión, es utilizado equivocadamente con fines delictivos.

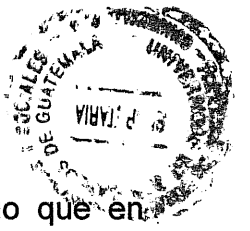
No obstante lo mencionado se considera que este tipo en particular por la finalidad distinta al uso normal de la computadora así como la escasez de los delitos cometidos por este método no sería recomendable su tipificación.

ñ) Los Virus

Son una serie de claves programáticas que pueden adherirse a otros programas, propagarse a otros sistemas informáticos. Un virus puede ingresar por una pieza de soporte lógico que se encuentre infectado desde una forma remota ingresando al programa.

1) El caballo de Troya o "Trojan Horse"

Este virus ha sido conocido en Guatemala por varias personas que manejan computadoras y precisamente porque la misma computadora señala el nombre del mismo. Fue inspirado en las épicas hazañas contadas por Homero en su obra "La Ilíada" que narra toma de Ciudad de Troya. Ulises mandó construir un enorme caballo de madera vacío el cual obsequió a los troyanos en señal de paz, sin embargo, en su interior ocultaba gran cantidad de soldados y pertrechos militares de la época, los cuales permanecieron ocultos hasta que se diera la orden a fin de sitiar la ciudad. Los habitantes de Troya al creer que habían ganado la guerra, introdujeron el caballo en la ciudad y celebraron el triunfo con una gran fiesta, pero durante la noche, cuando todos dormían confiados bajo los efectos del alcohol, los soldados de Ulises salieron del caballo y abrieron las puertas de la ciudad ingresando los soldados enemigos tomando la ciudad sin que los troyanos opusieran mayor resistencia.



Por esta razón, la denominación "Caballo de Troya" se aplica a algo que en apariencia es inofensivo para tranquilidad de la víctima, pero cuando desencadena su dañino potencial causa verdaderos estragos.

Luego de esta breve referencia mitológica que explica la razón de su nombre se puede precisar que este método consiste en la inclusión de instrucciones dentro del programa de uso habitual una rutina para que realice un conjunto de funciones desde luego, no autorizadas, para que dicho programa ejecute en ciertos casos de una forma distinta a como estaba previsto. Fácilmente puede decirse que el hacker puede hacer esto y recabar información sin la debida autorización para un beneficio económico o patrimonial e indiscutiblemente esta conducta debe estar prohibida porque es lesiva para la sociedad.

Dentro de los efectos de este, puede tratarse en determinados casos de la ejecución de cálculos erróneos por ejemplo aumentando el importe de la lista de un empleado, desviando ingresos hacia cuentas ficticias, etc. También puede presentarse cuando se imprimen documentos no autorizados o inclusive no imprimir documentos reales, por ejemplo emitir cheques a proveedores fantasmas o no imprimir cheques a proveedores reales cuando previamente se les ha cancelado su deuda, ya que se ha alterado la forma de pago transfiriendo los fondos a una cuenta que pertenece al defraudador. Un procedimiento usualmente utilizado en la banca es por ejemplo introducir una modificación al programa del tratamiento de cuentas corrientes para que siempre que se consulte un saldo lo multiplique por diez, por cien, por mil, por cien mil etc. con lo que es posible autorizar pagos, transferencias superiores a lo real.

Por sus características es necesario poseer una capacidad técnica suficiente al menos saber programar y además tener acceso al programa para poder manipularlo. Es importante agregar que en todo este tipo de ilícitos el programa manipulado ha

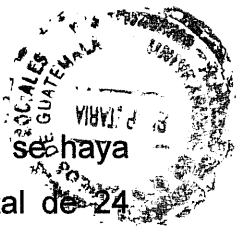
estado en funcionamiento habitual desde hace un buen tiempo y casi nunca se trataba de programa de nueva creación.

El motivo es muy simple, los programas nuevos suelen ser sometidos a procesos de revisión y chequeo para detectar cualquier anomalía que puedan afectarlos. Sin embargo un programa que ha estado en funcionamiento correctamente durante un prolongado tiempo no se cuestiona, y salvo casos absolutamente excepcionales, jamás sus resultados son sometidos a comprobación.

Debido a ello la modalidad de Caballo de Troya es una de las más peligrosas y al mismo tiempo difíciles de eliminar. Un ejemplo claro de este método es un caso real sucedido en una entidad de crédito al cual no se le dio publicidad y del que se desconoce incluso el nombre del autor.

Este caso ocurrió a fines de 1984 y el procedimiento utilizado por el autor, aparentemente un ex empleado de centro de cómputo de la entidad, fue el introducir una rutina en el programa de tratamiento de cuentas corrientes para que un determinado día, aproximadamente seis meses después de haber dejado su trabajo, y a una hora nocturna predeterminada se autorizase el pago a un talón de una cuenta corriente sin consultar el saldo. Posteriormente la misma rutina borraba parte del programa modificado con lo cual se eliminaba el rastro de la comisión del delito.

Otro caso similar en sucedió en 1985 en una importante entidad bancaria cuando en una oportunidad tres personas, supuestamente antiguos empleados de la institución, manipularon el sistema informático abriendo dos cuentas en diferentes oficinas de la ciudad con nombres distintos y falsos, lo que les permitió disponer de talonarios de cheques al mismo tiempo que las cuentas ingresaran al sistema del banco.



Pues bien, después de unos días de funcionamiento normal y sin que se haya explicación alguna, en las cuentas se hicieron asientos falsos por un total de 24 millones de dólares. Los malos elementos fueron detenidos al ser descubiertos después de haber cobrado cinco cheques y en posesión de documentos falsos que identificaban a las personas en cuyo nombre estaban abiertas las cuentas.

2) Gusanos

Se fabrica en forma análoga al virus con miras a infiltrarlo en programas normales de procesamiento de datos o para modificar o destruir la información, pero se diferencia del virus porque no puede regenerarse.

Si se asimilara a la medicina podría decirse que es una especie de tumor benigno. Ahora las consecuencias del ataque de un gusano pueden ser tan peligrosas como el de un virus.

Difusión de los virus

Si bien es un ataque de tipo tampering difiere de este porque puede ser ingresado al sistema por dispositivos externo (diskettes) o a través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su autoproducción, no necesita de mucho ayuda para programarse a través de una LAN o WAN rápidamente, si es que no esta instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e-mail. Existe distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe. com, bat, etc.) y los sectores de boot-partición de disco y diskettes, pero aquellos que causan en estos tiempos mas problemas son los macro-virus, que están ocultos en simples documentos o plantilla de calculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además

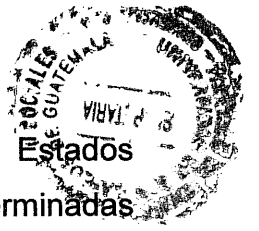
son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento de MS-Word puede ser procesado tanto en un equipo Windows 3.x/95/98, como en una Macintosh u otras.

Ciertos virus son descubiertos mes a mes, y técnicas mas complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puestas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

3.4 Necesidad de que se regule en el código penal

Tal como se ha venido describiendo en que consisten los denominados hackers, como iniciaron en el mundo, quizá de una manera no criminal, y que en la actualidad, si muchos de ellos, tienen esa característica, amerita que las legislaciones, como en el caso de Guatemala, y que en algunos países de Latinoamérica como se ha descrito anteriormente, han tomado las medidas necesarias para regular aspectos puntuales o concretos relacionados a tipificar los delitos que cometen los hackers para que cumpla los fines de prevención general y prevención especial conforme los principios inspiradores del Derecho Penal, específicamente en ejercicio del poder punitivo del Estado y de la protección que la sociedad necesita de los abusos y arbitrariedades que les puedan causar perjuicio moral, psicológico, patrimonial o económico.

Por eso se ha dicho que es un problema que cada día preocupa más en la sociedad de la información, y que por ello, ha aparecido la llamada ciber delincuencia, con delitos como el "blanqueado" electrónico de dinero, las actividades de juego ilegal, la piratería informática o la violación de los derechos de la propiedad intelectual, y otros como los ya señalados, lo cual pone a prueba los actuales sistemas de prevención, descubrimiento y persecución de delitos.



También es importante la conciencia a nivel internacional de los Estados organizados. La cooperación internacional ya está muy avanzada en determinadas áreas, como la lucha contra la delincuencia internacional organizada. Un ejemplo de lo anterior, es Europa, en un contexto internacional más amplio, se han creado grupos especiales y se ha reforzado la cooperación transfronteriza en áreas como la localización y seguimiento de delincuentes en línea y la búsqueda y confiscación de pruebas digitales.

El Consejo de Europa aprobó (con la firma de 30 estados miembros), el 23 de noviembre de 2001 el Convenio Europeo sobre Ciber crimen. Por su parte, en la Unión Europea y a raíz del Consejo Europeo de Dublín, se creó el Grupo de Alto Nivel, que está ultimando un plan de acción para luchar contra la ciber delincuencia. Estos esfuerzos revisten una importancia fundamental para incrementar la confianza en el comercio electrónico internacional.

Hay que tener presente que en los delitos cometidos por la Red es preciso determinar el lugar de comisión para establecer cuál es la legislación aplicable y la jurisdicción competente, lo que lleva, casi necesariamente, a tomar en cuenta el país en el que se halla el servidor y si pertenece a la categoría de los llamados paraísos informáticos, países que no han ratificado los convenios internacionales de propiedad intelectual o de auxilio a la administración de justicia y que suelen coincidir con los llamados paraísos fiscales. En el caso de Guatemala, la ley penal mantiene las características de la extraterritorialidad de la ley penal, en cuanto a los delitos, sin embargo, estos deben reforzarse para cumplir con el principio de legalidad y que como puede evidenciarse a través de lo que se ha hecho en este trabajo, la legislación penal guatemalteca, esta muy corta y posiblemente también pueda ser considerado como otros países como paraísos informáticos, en donde la comisión de hechos delictivos como conductas de los hackers están prácticamente permitida.

CAPÍTULO IV

4. Presentación de los resultados del trabajo de campo

4.1 Entrevistas

El trabajo de campo consistió en la realización de una entrevista dirigida a abogados y notarios respecto del tema del uso de las computadoras y los delitos informáticos, en especial para determinar el grado de conocimiento de los denominados hacker, por lo que se presenta a continuación los resultados.

4.2 Resultado de la encuesta

Cuadro No. 1

Pregunta: ¿Ha utilizado en su actividad profesional las computadoras para asuntos laborales y personales?

Respuesta	Cantidad
Si	10
No	02
Total:	12

Fuente: Investigación de campo, febrero del año 2009

Cuadro No. 2

Pregunta: ¿Cree usted que a través del uso de las computadoras se pueden cometer ilícitos penales?

Respuesta	Cantidad
Si	12
No	00
Total:	12

Fuente: Investigación de campo, febrero del año 2009.

Cuadro No. 3

Pregunta: ¿Tiene conocimiento que el código penal regula algunos delitos informáticos?

Respuesta	Cantidad
Si	12
No	00
Total:	12

Fuente: Investigación de campo, febrero año 2009.

Cuadro No. 4

Pregunta: ¿Considera que existen muchos mas delitos informáticos que el código penal no regula?

Respuesta	Cantidad
Si	12
No	00
Total:	12

Fuente: Investigación de campo, febrero año 2009.

Cuadro No. 5

Pregunta: ¿Ha oído mencionar en el ámbito informático a los hackers?

Respuesta	Cantidad
Si	02
No	10
Total:	12

Fuente: Investigación de campo, febrero año 2009.

Cuadro No. 6

Pregunta: ¿Cree usted que la habilidad y técnica que tienen los hackers en los programas de computación pueden se empleados con fines ilícitos?

Respuesta	Cantidad
Si	12
No	00
Total:	12

Fuente: Investigación de campo, febrero año 2009

Cuadro No. 7

Pregunta: ¿Considera que la conducta de los hacker esta regulada en el código penal?

Respuesta	Cantidad
Si	00
No	12
Total:	12

Fuente: Investigación de campo, febrero año 2009

Cuadro No. 8

Pregunta: ¿Dentro del mundo informático, considera que deben prohibir conductas ilícitas que lesionen bienes jurídicos tutelados en el ámbito informático?

Respuesta	Cantidad
Si	12
No	00
Total:	12

Fuente: Investigación de campo, febrero año 2009.

Cuadro No. 9

Pregunta: ¿Conoce de normas internacionales que regulen aspectos de los delitos informáticos?

Respuesta	Cantidad
Si	00
No	12
Total:	12

Fuente: investigación de campo, febrero año 2009.

Cuadro No. 10

Pregunta: ¿Cree usted que debiera regularse la conducta ilícita de los hackers en el código penal como parte de los delitos informáticos?

Respuesta	Cantidad
Si	12
No	00
Total:	12

Fuente: Investigación de campo, febrero año 2009

4.3 Base para el establecimiento de una reforma al Código Penal.

Dada la complejidad del delito informático y que además vulnera varios valores o bienes jurídicos protegidos por la sociedad, el tipo básico debería contener la delimitación precisa de lo que está penado con una pena privativa de la libertad o inhabilitación para acceder al servicio informático por un determinado plazo de tiempo.

Como se ha visto en este trabajo sobre nuevas tipologías, especialmente en el caso de la conducta criminal que realizan los hackers, el espectro es amplio y en mucho de los casos no ingresan en el tipo penal vigente por el Código Penal que nos rige.

Empezando porque no esta definido en el Código Penal Guatemalteco, el bien jurídico tutelado, estas abarcan varias, dentro de los más fundamentales y que deben tomarse en cuenta para las bases de su inclusión se encuentran:

a) El Patrimonio;

b) El Orden Económico

c) El Sistema Informático:

Por eso, la teoría de este delito informático vulnera no individualmente cada uno de estos bienes, sino todos en su conjunto, de tal suerte, la magnitud del problema y de la necesidad de su adecuación jurídica a través de reforma en el Código Penal guatemalteco.

a) La acción u omisión en las nuevas figuras delictivas informáticas

La acción u omisión del delito puede recaer en valores protegidos por la sociedad, de esta manera pueden ser motivo de protección el patrimonio, el orden económico, la intimidad. En el caso y en el caso especial de la destrucción de datos informáticos pueden catalogarse contra el sistema informática en su conjunto al poner en grave riesgo la información disponible en la red nacional o internacional de computadoras.

Pueden tratarse de delitos contra el patrimonio cuando se sustrae dinero o documentos que lo representen, mercaderías al adulterar inventarios, sustracción de valores negociables, etc. requiriendo que el autor se apropie de cosa mueble ajena generando algunos inconvenientes serios si se considera que muchas veces se trata de dinero contable, que en realidad es un crédito.

También puede vulnerar aspectos que atenta contra la libertad de la persona y a su intimidad como cuando se ingresa sin autorización al archivo documentario de una

persona natural o jurídica con la finalidad de conocer información que por la calificación de la víctima la va ha considerar reservada.

Sería un error por lo tanto tipificar esta nueva figura como un agravante del delito de hurto, cuando en realidad están en peligro bienes jurídicos protegidos tan importantes como del orden económico y personal como la intimidad. Parece ser que lo que en realidad vulnera esta novedosa tipología es una violación mixta de valores jurídicos que en algunos casos compromete tanto al patrimonio como la libertad de las personas o el sistema informático y la protección de datos, no sólo se vulneran valores de carácter económico sino de carácter tan valioso y personal como la intimidad, lo que hace imposible negar su existencia.

b) La importancia de que con la conducta de los hackers se vulnera el derecho a la intimidad de las personas .

Como se ha revisado en la tipología esta clase de ilícitos atentan contra la intimidad de la persona e inclusive puede darse el caso de que la misma vea violada su intimidad sino que puede ser sustituida su identidad.

c) La tipicidad objetiva

La acción u omisión que afecte los componentes de la computadora tanto de hardware como del software, como medio o instrumento para perpetrar el delito.

d) En el caso del sujeto activo

Las personas que cometen este tipo de delitos son aquellas que poseen ciertas características que no presenta un delincuente común. Es decir, el denominador común es que poseen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos de manejo de información de carácter sensible, o más bien son hábiles en el uso de los

programas informáticos aunque no desarrollen actividades laborales, de manera que el sujeto activo está dado por la persona que "entra" a un sistema informática con intenciones delictivas, por ejemplo cuando desvía fondos de las cuentas bancarias de sus clientes.

Son personas listas, decididas y motivadas, dispuestas a aceptar el reto tecnológico, muchas veces un empleado del sector de procesamiento de datos. Sin embargo estudiosos en la materia lo han catalogado como "delitos de cuello blanco" término introducido por el criminólogo norteamericano Edwin Sutherland en 1943, cuando señala un sin número de conductas no tipificadas en los ordenamientos como delitos, como por ejemplo la violación de leyes de patentes, los derechos de autor, el contrabando o mercado negro, corrupción de funcionarios, evasión de impuestos, etc. Para el criminólogo norteamericano, el delito informática es cometido por un sujeto de cierto status socio- económico y su comisión se explica no por carencia económica sino por ambición .

Pueden ser por ejemplo, los operadores, programadores, analistas de sistemas, analistas en comunicaciones, supervisores, personal técnico y de servicio, funcionarios, auditores, bibliotecarios, personal de custodia o vigilancia, así como usuarios en general.

Entonces, a pesar de que puede ser cualquier persona, es una persona especial, hábil para el manejo de los sistemas de computación, aún más, el experto, habilidoso, técnico como el caso de los hackers que emplean ese conocimiento en perjuicio colectivo, debiera entonces, merecer una sanción con agravación.

e) En el caso del sujeto pasivo

En primer término tenemos que distinguir al sujeto pasivo de la víctima, que es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo.

En el caso de las víctimas pueden ser individuos, instituciones crediticias, gobiernos, que usan sistemas automatizados de información, generalmente conectados a otros sistemas. En este caso se encuentran personas naturales. De otro lado las personas jurídicas pueden constituirse como parte civil en el proceso así como parte agraviada, entre las que podemos citar bancos, compañías, etc.

f) Tipicidad objetiva:

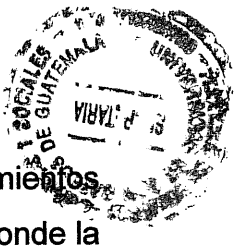
El caso de este tipo de conductas tanto por acción como por omisión deben realizarse en forma consciente y voluntariamente con el objeto de conseguir un provecho determinado.

g) La consumación y la tentativa

En este tipo de delitos no parece que debe perseguirse la tentativa, más si la consumación. Eso porque cuando se observa el resultado es que se puede determinar que ha habido una intromisión de un tercero no autorizado que ha hecho determinado acto que es lesivo.

h) Los hackers

La conducta de los hackers en español, se ha conocido también como "Pirateo Informático", consiste en entrar sin autorización a una computadora y explorar su interior. No existe aparentemente límite pudiendo acceder por vía remota a servicios de noticias, servicios financieros, información financiera, instalaciones universitarias,



correo electrónico, computadoras oficiales. Esta persona capaz, con conocimientos técnicos, y que esos conocimientos los emplea en perjuicio de terceros, es en donde la conducta de este hackers o pirata informático, debe ser regulado.

i) Los crackers

Como se dijo en un inicio de este trabajo, el típico Hacker el que no ingresa al sistema por curiosidad o porque le represente un reto para entender el funcionamiento de cualquier sistema. En realidad se refriere a la persona que conscientemente ingresa a un sistema con la finalidad de destruir información.

Existen dos vertientes:

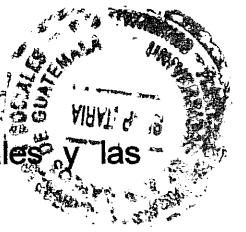
1) El que ingresa en un sistema informático y roba información produciendo destrozos en el mismo.

2) El que se dedica a desproteger todo tipo de programas, tanto para hacerlas plenamente operativas como para los programas que presentan anticopias.

En virtud de ello, también es una conducta que produce perjuicio a terceros, y por lo tanto, debe ser sancionado.

j) Los phreakers

Este es similar al hacker o crackers pero utilizando el teléfono por eso su nombre. Es el especialista en telefonía. Se le podría llamar el pirata de los teléfonos, sobre todo emplea sus conocimientos para poder utilizar las telecomunicaciones gratuitamente.



Los principales perjudicados son los usuarios nacionales e internacionales y las compañías telefónicas.

Existen muchos software que hacen posible la comunicación por computadora a un teléfono como el "Netphono!" creado por IDT Corporation que permite realizar llamadas internacionales desde una computadora personal a un teléfono fijo o celular a cualquier parte del mundo. El sistema se basa en la transmisión de la voz vía Internet. El software o programa digitaliza la voz para que viaje a través de la red. Esta nueva modalidad de comunicarse por teléfono se ha desatado con fuerza en los países donde la tecnología se encuentra en mayor desarrollo esta posibilidad estará disponible en mayor volumen en la medida que la tecnología derivada se extienda a otros, lo que permite comunicarse de una PC hacia un teléfono o de una PC hacia otra PC. Los usuarios no necesitan coordinar con su interlocutor la hora y el día para estar en línea en el momento de la llamada. Quien efectúa la llamada sólo necesita una PC con conexión a Internet para comunicarse con otra persona.

Como se observa, se trata de una conducta lesiva que aún no se regula en el Código Penal, de tal suerte que debe establecerse como parte de las reformas que se proponen a través de este trabajo.

CONCLUSIONES

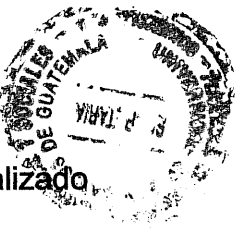
1-. Los hackers son expertos, personas con conocimientos en las tecnologías y programas de computación, surgen con ocasión de su interés en evolucionar positivamente, sin embargo, ha sido motivo o interés de otros en promover perjuicio a cambio de intereses patrimoniales o económicos, que han provocado grandes perjuicios a nivel mundial y en el caso de Guatemala, aun no se encuentra regulado estas conductas lesivas la sociedad.

2-. El desarrollo incesante de la informática estimulando básicamente por la competencia y las nuevas expectativas de los usuarios hace necesaria la protección del sistema informático que prevenga básicamente a nivel administrativo, en primer lugar y no castigue futuras acciones delictivas que ya se empiezan a observar y que atenta contra lo que se puede llamar el sistema informático.

3-. La problemática de los delitos informáticos requiere un estudio especial y multidisciplinario con vistas a determinar la medida en que las leyes penales vigentes constituyen un cuerpo normativo suficiente para prevenir este tipo de conductas elaborado por expertos y de carácter multidisciplinario que aborde el reto que plantean los delitos informáticos.

4-. El aparecimiento del internet como un sistema de redes de información que trascienden en fronteras entre los países por hacer que las comunicaciones entre las personas sea mucho mas cerca respecto de cualquier otro medio de comunicación, ha sido de beneficio para la sociedad humana.

5-. En el Código Penal guatemalteco, se encuentran reguladas algunas figuras delictivas que tienen relación con el uso de las computadoras y el internet, sin



embargo, tal como quedo establecido en el presente trabajo, su carácter generalizado no permite su encuadramiento eficaz de la ley.

RECOMENDACIONES

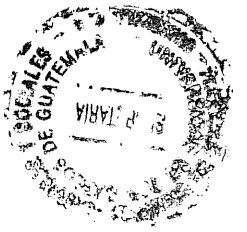
1-. Por el análisis efectuado no cabe duda que el camino que el legislador deberá seguir es la modificación del código penal vigente para adaptarse a estos nuevos tipos legales lo cual puede hacerse con la creación de un titulo especial que contemple los delitos informáticos de la manera como se propone en este trabajo.

2-. La conducta tan compleja que realizan los hackers en el mundo informático, amerita que previo a realizar las reformas legislativas, se realice un estudio por los legisladores, las conductas criminales que pueden ser tipificadas de acuerdo a la realidad Nacional, y esto es una obligación de la comisión respectiva del congreso de la república de Guatemala.

3-. Aparte de las conductas complejas que realizan los hackers, existen otros intervinientes como los crackers y otros que también deben ser objeto de estudio para su futura tipificación.

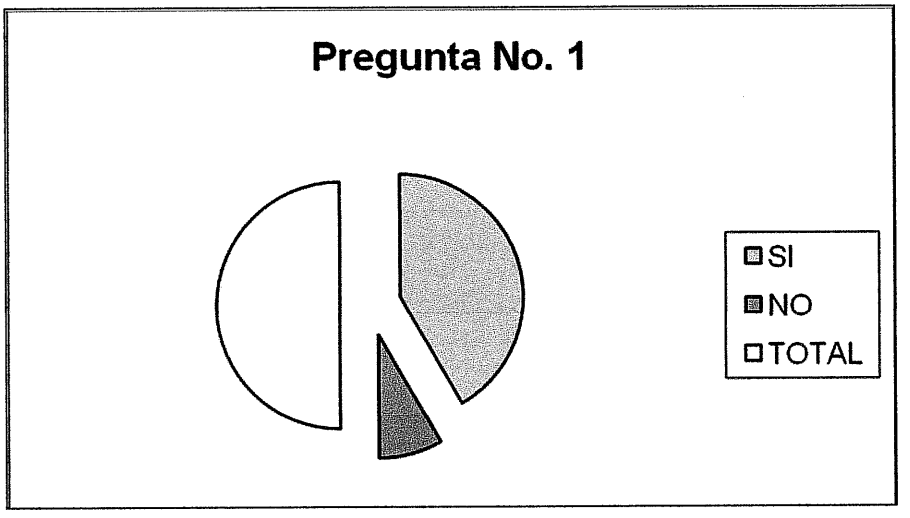
4.- Las autoridades estatales, especialmente la Corte Suprema de Justicia, el Ministerio Publico y la Defensa Publica Penal, tienen la obligación de brindar capacitaciones a su personal, en el tema de los hechos delictivos novedosos y complejos que se comete a través del dolo en el mundo informático que lesiona bienes jurídicos como los señalados, y que por lo tanto, son conductas criminales que comentes los llamados hackers.

5-. En virtud de que los ilícitos penales regulados en el Código Penal respecto a los delitos informáticos tienen carácter muy general, y por ello, podrían tornarse inaplicables y que tenga como consecuencia la impunidad y falta de justicia, se hace necesario que el Congreso de la Republica reforme el Código Penal y Código Procesal Penal del origen de la Internet. y crear una Ley específica al respecto.



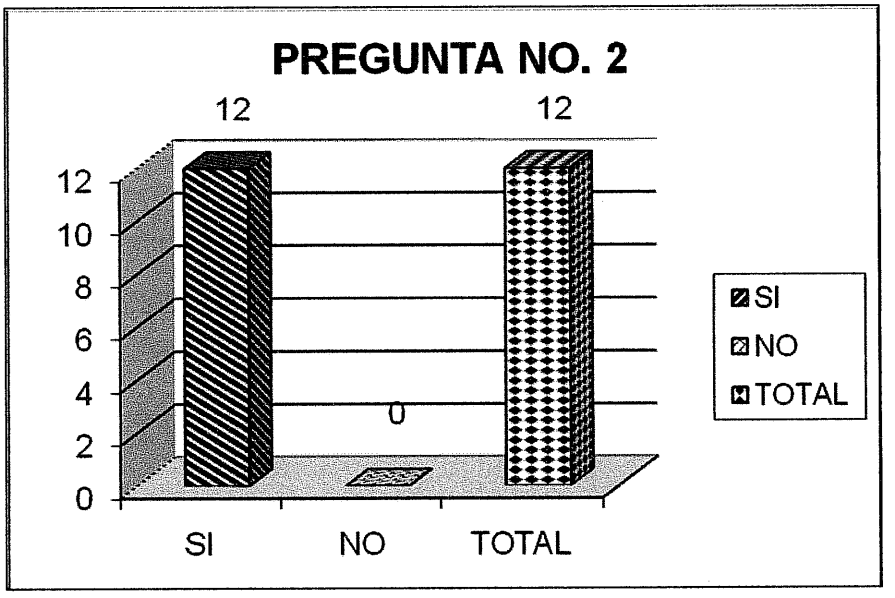
ANEXOS

RESPUESTA	CANTIDAD
SI	10
NO	2
TOTAL	12



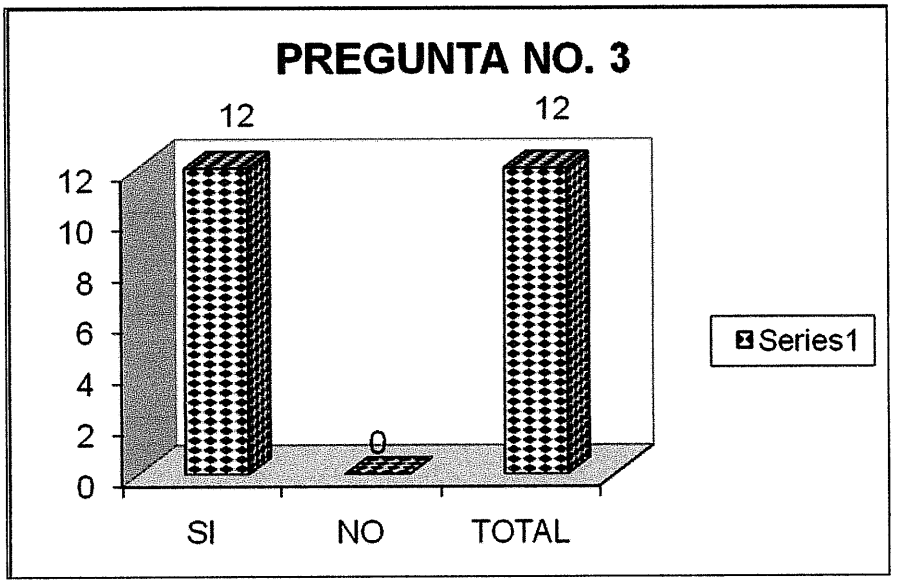
El 98% RESPONDIO SI PORQUE EN LA ACTUALIDAD ES UN MEDIO NECESARIO PARA LA ELABORACION DE DIVERSOS TRABAJOS.
EL 2% RESPONDIO QUE NO PORQUE NO TIENEN ACCESO A UNA COMPUTADORA.

RESPUESTA	CANTIDAD
SI	12
NO	0
TOTAL	12



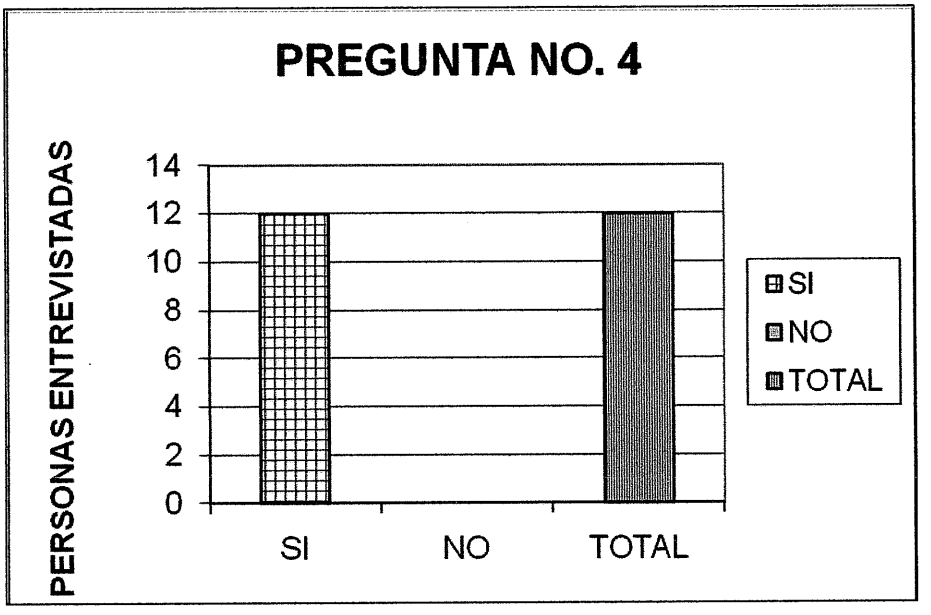
EL 100% CONTESTO QUE SI, PUES NO SE TIENE ACCESO A LA INFORMACION.

RESPUESTA	CANTIDAD
SI	12
NO	0
TOTAL	12



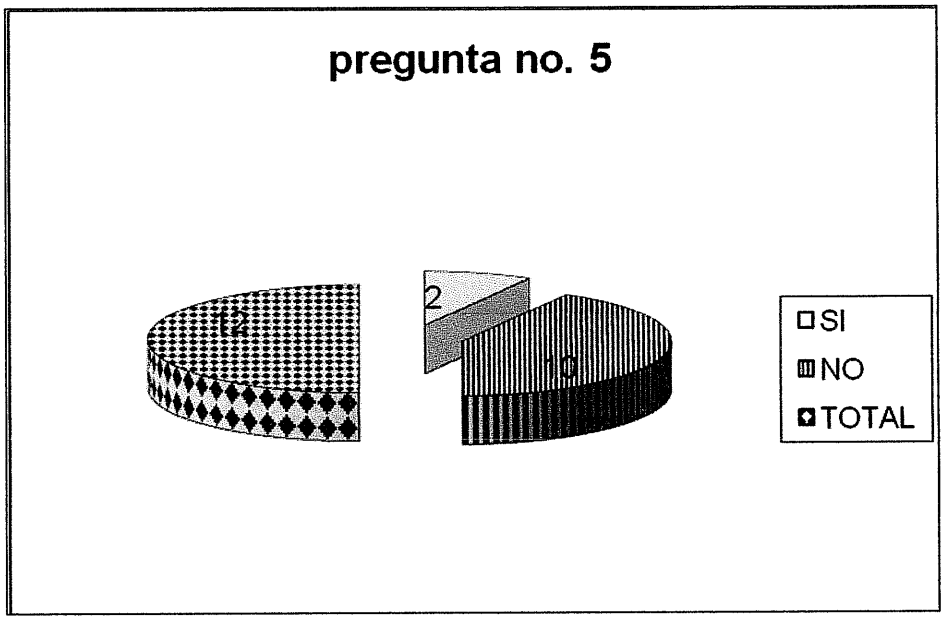
EL 100% RESPONDI QUE SI YA QUE TIENEN CONOCIMIENTO A LAS LEYES QUE REGULA EL CODIGO PENAL

RESPUESTA	CANTIDAD
SI	12
NO	0
TOTAL	12



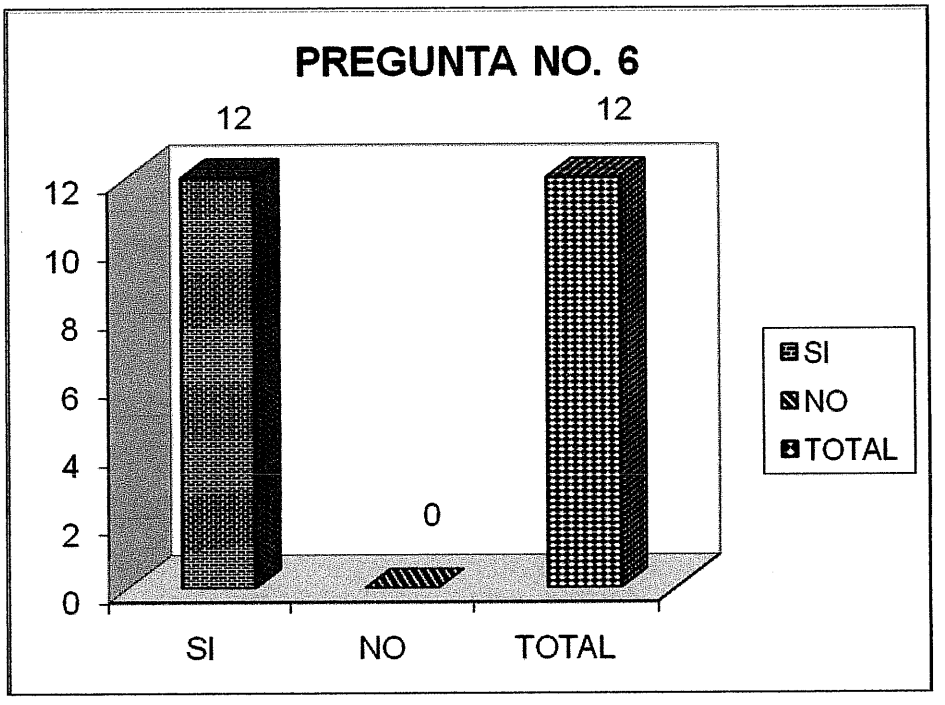
EL 100% RESPONDIO QUE SI PORQUE EN NUESTRO ACTUAL SISTEMA POLITICO SE DEDICA A REGULAR LAS LEYES SIN RELEVANCIA

RESPUESTA	CANTIDAD
SI	2
NO	10
TOTAL	12



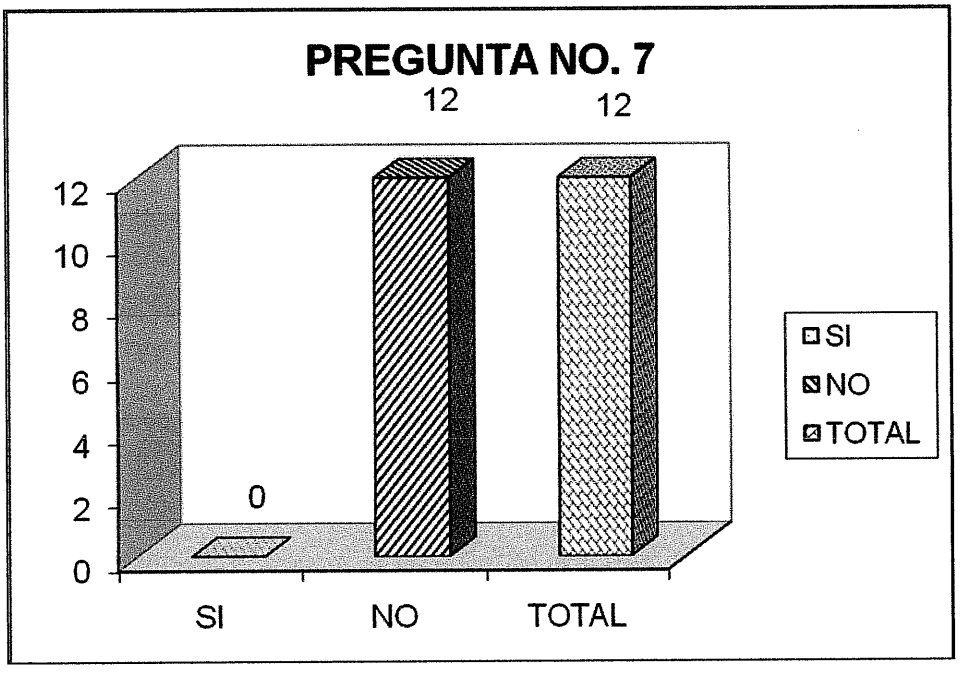
EL 2 % RESPONDIO QUE SI YA QUE HAN INGRESADO A DIVERSOS PROGRAMAS DE INFORMACION POR INTERNET.
EL 98% RESPONDIO QUE NO UNICAMENTE SE DEDICAN A UTILIZAR ESTOS MEDIOS DE INFORMACION COMO UNA HERRAMIENTA DE TRABAJO .

RESPUESTA	CANTIDAD
SI	12
NO	0
TOTAL	12



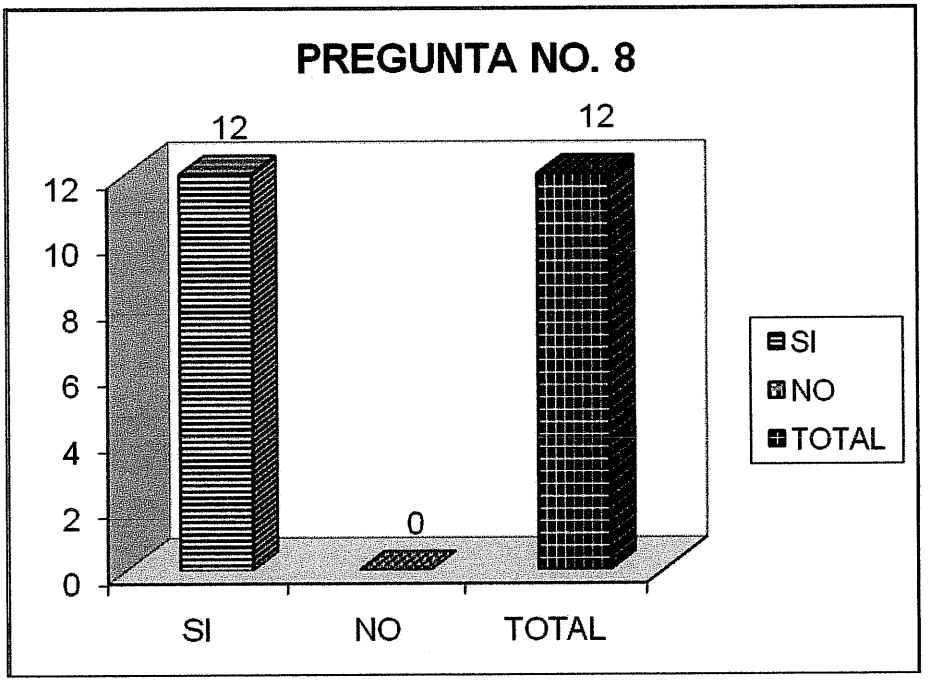
EL 100% RESPONDIO QUE SI, PORQUE INGRESAN A PROGRAMAS VIOLANDO LA PRIVACIDAD DE ALGUNAS INSTITUCIONES DEL ESTADO COMO PRIVADAS.

RESPUESTA	CANTIDAD
SI	0
NO	12
TOTAL	12



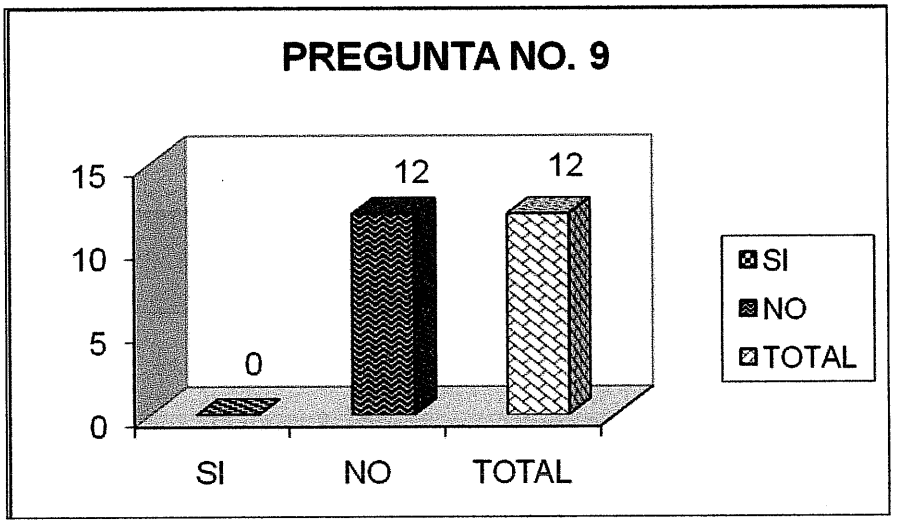
EL 100% RESPONDIO QUE SI PORQUE REALMENTE NO EXISTE UNA LEY QUE LO REGULE

RESPUESTA	CANTIDAD
SI	12
NO	0
TOTAL	12



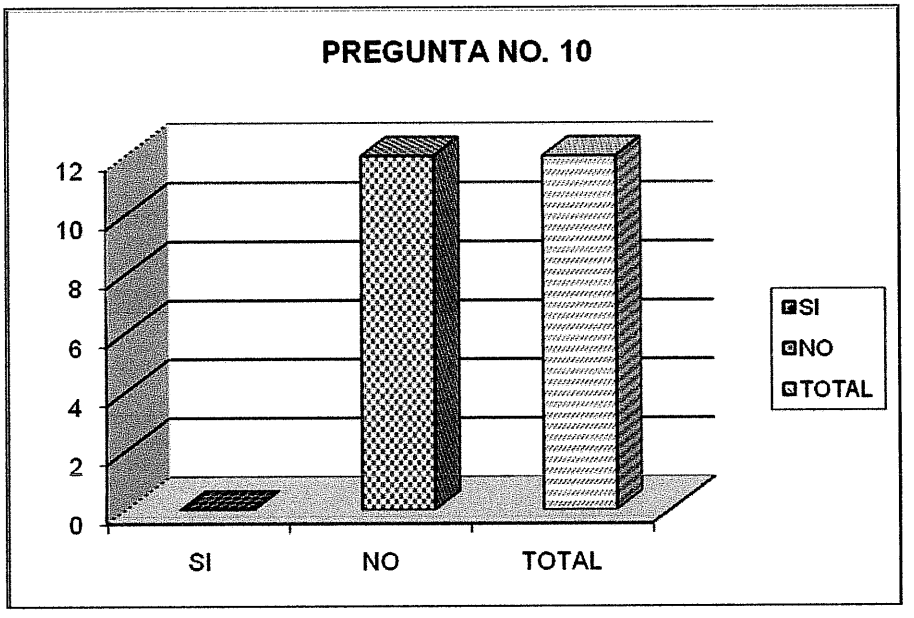
EL 100% RESPONDIO QUE SI DEBIDO ES ESTO. LA LEY ES ULTRAJADA POR LOS HAKERS EN LA INFORMATICA.

RESPUESTA	CANTIDAD
SI	0
NO	12
TOTAL	12



EL 100% RESPONDIO QUE SI PUES EL ESTADO NO PROMUEVE LA SUFICIENTE INFORMACION A LA POBLACION GUATEMALTECA.

RESPUESTA	CANTIDAD
SI	0
NO	12
TOTAL	12



EL 100% RESPONDIO QUE SE DEBIDO A LA EXISTENCIA DE LOS HAKERS SE DEBEN CREAR LEYES QUE REGULEN LA MATERIA

BIBLIOGRAFÍA

ALCALA-Zamora, L. **Derecho Procesal Penal**. Enc. Jur. Omeba Buenos Aires,1945.

BLOSSIERS MANZINI, Juan José. Los **Delitos Informáticos**. Editorial Porrúa, Mayo 1998 Perú.

BUSTAMANTE Alsina, J., **La Informática** y la Protección del Secreto de la Vida Privada, Editorial Porrúa. Madrid, España, 2000

CARNELUTTI, Francesco. **Las miserias del proceso penal**. Editorial Ejea. Buenos Aires Argentina 1959

CARRANCA y TRUJILLO, Raúl. **Derecho Penal Mexicano**. Parte General. Editorial Porrúa S.A. México 1977

CORREA, Carlos María. **El derecho informático en América Latina**. En Derecho y Tecnología Informática, Editorial Themis 1990. Bogotá Colombia.

COSSIO y CORRAL, Alfonso de. **Instituciones de derecho civil**. Tomo Responsabilidad civil, Editorial Civitas, S.A. 9191

FENECH, Miguel. **Derecho Procesal Penal**. Editorial Labor, S.A. Barcelona, 1960

DAVARA RODRIGUEZ, Miguel Ángel. **Derecho informático**. España, Editorial Aranzadi, 1993.

GARCIA RAMIREZ, Sergio. **Derecho Procesal Penal.** Editorial Porrúa, México, 1974.

GUIBOUR Ricardo A. Jorge O. Alende y Elena M. Campenella. **Manual De Informática Jurídica.** Tomo 280 Editorial Themis, Bogotá Colombia, 2002

Enciclopedia de Consulta En carta 2002

LEDESMA, J., **La Piratería en el Campo de la Informática** Editorial Lasner 2000.

IPSZYC, D., Protección del software, **Revista Jurídica** del Centro de Estudiantes España 1998.

MAROTTA, B. D., **El Delito Informático**: Consideraciones sobre la Defrau7dacion Informática, I congreso Iberoamericano y Ix Latinoamericano De Derecho penal y Criminología.

MUÑOZ CONDE, Francisco. Introducción al **Derecho Penal**. Barcelona Editorial Busch 1975.

SÁEZ Capel, J., Existe el delito Informático?, **Revista del Colegio Público** de Abogados de la Capital Federal nro.21 Buenos Aires 1999.

SÁEZ Capel, J., Lecciones y artículos sobre **Elementos de Derecho Penal** Y Procesal Penal, Ed. Estudio, 1999.

SOLER, S., **Derecho Penal Argentino,** t. II, p.42, t. IX, p. 115, 2da reimpresión Ed. Tea Buenos Aires, 1953.

MANZINI Vicenco. Tratado de **Derecho Penal**. Tomo I, Italia l933.

SÁEZ JIMÉNEZ, Jesús y EPIFANIO LÓPEZ FERNÁNDEZ de Gamboa. Compendio De **Derecho Procesal Civil y Penal**. Volumen I Editorial Santillana, S.A. Madrid 1966

SICHES Recanses. Vida humana, **sociedad y derecho.**

SILVIA MALERO, Valentín. **Revista de Legislación** y Jurisprudencia. Editorial Revista De derecho privado, Madrid 1950

Legislación:

Constitución Política de la República de Guatemala, Asamblea nacional Constituyente, 1986.

Código Civil, Decreto Ley 106 Enrique Peralta Azurdia, Jefe de Gobierno de la Republica de Guatemala, Decreto numero 107-92, 1992.

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

Código Procesal Civil y Mercantil, Enrique Peralta Azurdia, Jefe de Gobierno de la Republica de Guatemala. Decreto número 107-92, 1992.

Código Penal, Republica de Guatemala, Decreto numero 17-73, 1973

Código Procesal Penal, Congreso de la Republica Decreto número 51-92, 1992.