UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"FENÓMENO DEL ROBO DE IDENTIDAD A TRAVÉS DE DISPOSITIVOS ELECTRÓNICOS EN LA CIUDAD DE GUATEMALA"

TESIS DE GRADO

ARELY MARISOL ZEA WELMANN
CARNET 24079-07

GUATEMALA DE LA ASUNCIÓN, ENERO DE 2016
CAMPUS CENTRAL

UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"FENÓMENO DEL ROBO DE IDENTIDAD A TRAVÉS DE DISPOSITIVOS ELECTRÓNICOS EN LA CIUDAD DE GUATEMALA"

TESIS DE GRADO

TRABAJO PRESENTADO AL CONSEJO DE LA FACULTAD DE
CIENCIAS JURÍDICAS Y SOCIALES

POR
ARELY MARISOL ZEA WELMANN

PREVIO A CONFERÍRSELE

EL TÍTULO Y GRADO ACADÉMICO DE LICENCIADA EN INVESTIGACIÓN CRIMINAL Y FORENSE

GUATEMALA DE LA ASUNCIÓN, ENERO DE 2016
CAMPUS CENTRAL

AUTORIDADES DE LA UNIVERSIDAD RAFAEL LANDÍVAR

RECTOR:	P. EDUARDO VALDES BARRIA, S. J.
VICERRECTORA ACADÉMICA:	DRA. MARTA LUCRECIA MÉNDEZ GONZÁLEZ DE PENEDO
VICERRECTOR DE INVESTIGACIÓN Y PROYECCIÓN:	ING. JOSÉ JUVENTINO GÁLVEZ RUANO
VICERRECTOR DE INTEGRACIÓN UNIVERSITARIA:	P. JULIO ENRIQUE MOREIRA CHAVARRÍA, S. J.
VICERRECTOR ADMINISTRATIVO:	LIC. ARIEL RIVERA IRÍAS
SECRETARIA GENERAL:	LIC. FABIOLA DE LA LUZ PADILLA BELTRANENA DE LORENZANA

AUTORIDADES DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DECANO:	DR. ROLANDO ESCOBAR MENALDO
VICEDECANA:	MGTR. HELENA CAROLINA MACHADO CARBALLO
SECRETARIO:	MGTR. ALAN ALFREDO GONZÁLEZ DE LEÓN

NOMBRE DEL ASESOR DE TRABAJO DE GRADUACIÓN

LIC. JAIME ARIEL ECHEVERRIA MERLO

TERNA QUE PRACTICÓ LA EVALUACIÓN

ING. ERICK ISRAEL AGUILAR PAAU

Arg.

Guatemala, 23 de noviembre del 2015

Señores
Consejo de Facultad
Facultad de Ciencias Jurídicas y Sociales
Universidad Rafael Landívar

Señores:

Por este medio hago de su conocimiento que, de acuerdo con el nombramiento recaído en mi persona como asesor del trabajo de tesis titulado "**FENÓMENO DEL ROBO DE IDENTIDAD A TRAVÉS DE DISPOSITIVOS ELECTRÓNICOS EN LA CIUAD DE GUATEMALA**" elaborado por la estudiante **ARELY MARISOL ZEA WELLMANN** con número de carné 2407907.

Después de efectuada la revisión y solicitud de correcciones al estudiante, las cuales fueron entregadas en tiempo establecido, se considera que el contenido de la tesis se encuentra realizada conforme a los requerimientos y regulaciones descritos en el instructivo de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Rafael Landívar.

Por lo anteriormente expuesto emito **DICTAMEN FAVORABLE** a efecto que la estudiante **ZEA WELLMANN** continúe con los procedimientos y requisitos establecidos por la Universidad Rafael Landívar.

Atentamente,

Licenciado Jaime Ariel Echeverría Merlo
Asesor de Tesis

Guatemala, 11 de Enero de 2016.

Señores
Consejo de Facultad
Facultad de Ciencias Jurídicas y Sociales
Universidad Rafael Landívar

Señores:

Por este medio hago de su conocimiento que, de acuerdo con el nombramiento recaído en mi persona como revisor de fondo y forma del trabajo de tesis, **"FENÓMENO DEL ROBO DE IDENTIDAD A TRAVÉS DE DISPOSITIVOS ELECTRÓNICOS EN LA CIUAD DE GUATEMALA"**, elaborado por la estudiante **ARELY MARISOL ZEA WELLMANN** con número de carné 2407907.

Después de efectuadas las correcciones por la estudiante y la revisión que lleve a cabo, las cuales fueron realizadas en el tiempo establecido, se considera que el contenido de la tesis se encuentra conforme a los requerimientos y regulaciones descritos en el instructivo de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Rafael Landívar.

Por lo anteriormente expuesto emito **DICTAMEN FAVORABLE** a efecto que la estudiante **ZEA WELLMANN** continúe con los procedimientos y requisitos establecidos por la Universidad Rafael Landívar.

Atentamente,

Erick Israel Aguilar Paau
Ingeniero
Asesor de Tesis

Universidad Rafael Landívar
Tradición Jesuita en Guatemala

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
No. 07781-2016

Orden de Impresión

De acuerdo a la aprobación de la Evaluación del Trabajo de Graduación en la variante Tesis de Grado de la estudiante ARELY MARISOL ZEA WELMANN, Carnet 24079-07 en la carrera LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE, del Campus Central, que consta en el Acta No. 0711-2016 de fecha 11 de enero de 2016, se autoriza la impresión digital del trabajo titulado:

"FENÓMENO DEL ROBO DE IDENTIDAD A TRAVÉS DE DISPOSITIVOS ELECTRÓNICOS EN LA CIUDAD DE GUATEMALA"

Previo a conferírsele el título y grado académico de LICENCIADA EN INVESTIGACIÓN CRIMINAL Y FORENSE.

Dado en la ciudad de Guatemala de la Asunción, a los 13 días del mes de enero del año 2016.

MGTR. ALAN ALFREDO GONZÁLEZ DE LEÓN, SECRETARIO
CIENCIAS JURÍDICAS Y SOCIALES
Universidad Rafael Landívar

AGRADECIMIENTO Y DEDICATORIA

A MIS HIJOS:

Por la paciencia de mi ausencia para terminar los estudios, por sus risas, por motivarme con su hermosa existencia.

A RONALDO:

Mi amor, mi cómplice, mi apoyo, por recordarme que puedo lograr lo que quiero.

A MIS PADRES:

Por sus enseñanzas y su amor.

A MIS HERMANAS Y HERMANO:

Porque son hermosos compañeros de vida y grandes seres humanos, porque buscan aportar cada día.

A LA POLICIA NACIONAL CIVIL:

A los agentes y subcomisarios que me brindaron información y apoyo, conscientes de su deber de informar para colaborar con la lucha contra el crimen y que padecen la falta de presupuesto y apoyo por parte del Estado, pero que hacen muy bien su trabajo.

A TODAS LAS MUJERES VICTIMAS DE VIOLENCIA Y SUS FAMILIAS:

Que sus hijos reciban consuelo y resignación, para que puedan tener una vida mejor, y que logremos superar el machismo, la misoginia y la impunidad.

RESPONSABILIDAD: “la autora será la única responsable del contenido y conclusiones de la tesis”

LISTADO DE ABREVIATURAS

DEIC	Dirección Especial de Investigación Criminal
DPI	Documento Personal de Identificación
ENCOVI	Encueta Nacional de Condiciones de Vida
FODA	Fortalezas, Oportunidades, Debilidades y Amenazas
ICEFI	Instituto Centroamericano de Estudios Fiscales
IDPP	Instituto de la Defensa Pública Penal
IMEI	*International Mobile SystemEquipmentIdentity*, Sistema Internacional para la Identidad de Equipos Móviles
INACIF	Instituto Nacional de Ciencias Forenses
IVE	Intendencia de Verificación Especial
MINGOB	Ministerio de Gobernación
MP	Ministerio Público
OJ	Organismo Judicial
PNC	Policía Nacional Civil
RENAP	Registro Nacional de las Personas
SAT	Superintendencia de Administración Tributaria
SIT	Superintendencia de Telecomunicaciones
UDT	Unidad de Decisión Temprana del Ministerio Público

RESUMEN EJECUTIVO

La presente tesis “fenómeno de robo de identidad mediante dispositivos electrónicos en la ciudad de Guatemala” busca informar sobre las características del fenómeno y la forma en que el Estado responde a la población. En Guatemala no está tipificado el robo de identidad, el Estado no cuenta con la tecnología suficiente, ni la capacitación de recurso humano, para la investigación de delitos informáticos. En seis capítulos se presentarán las definiciones en cuanto al robo, los delitos informáticos, el delincuente informático, el robo de identidad en Guatemala, la Criminalística e informática Forense, Derecho comparado, el sistema de Justicia frente a fenómeno del robo de identidad mediante dispositivos electrónicos, el fenómeno criminal del robo de identidad a través de bibliografía. Además, el resultado de encuestas de victimización a usuarios de dispositivos, profesionales del derecho y un profesional experto en cibernética que describen las vulnerabilidades y riesgos de padecer el robo de identidad y la falta de interés por parte del Estado en prevenirlo, investigarlo e impartir justicia. La relevancia radica en que se analizan las fortalezas, debilidades, los desafíos y las oportunidades del Estado frente a éste hecho ilícito, se propone una hoja de ruta para el fortalecimiento de las instituciones de justicia y seguridad. Se entrevistó a miembros de la Policía Nacional Civil (PNC) y Ministerio Público (MP) encargados de darle seguimiento a casos de robo de identidad mediante dispositivos electrónicos describiendo las modalidades que hoy se denuncian en la ciudad de Guatemala, constituyéndose como las únicas secciones en la república que velan por la investigación de delitos informáticos, quienes describen el modo en que operan para esta circunstancia.

ÍNDICE

INTRODUCCIÓN

Este trabajo de investigación busca dar respuesta, a las siguientes preguntas: ¿Cómo se manifiesta el robo de Identidad mediante medios electrónicos en Guatemala? Y, ¿Está preparado el Estado para enfrentar los delitos informáticos que derivan en el robo de identidad mediante dispositivos electrónicos en Guatemala?

Para lograr determinarlo se analiza la legislación actual en materia de Registros Informáticos del Código Penal de Guatemala en su artículo 274 "F" y su aplicación en Guatemala. Además de los mecanismos del Estado para el tratamiento de dichos delitos que derivan en un robo de identidad mediante dispositivos electrónicos.

La presente tesis tiene como objetivo principal describir el fenómeno del "Robo de identidad" en la ciudad de Guatemala a través de dispositivos electrónicos.

Sus objetivos específicos son, la identificación de las fortalezas, amenazas, oportunidades y debilidades del Sistema de Justicia frente a los delitos que se tipifican en el artículo 274 del inciso A al inciso G, del Código Penal guatemalteco, que derivan en el robo de identidad de usuarios de dispositivos electrónicos. Así mismo, identificar los mecanismos por medio de los cuales se realizan los delitos bajo el título de "Destrucción de registros informáticos" tipificados en el artículo 274, incisos A a la G, del Código Penal y a través de qué dispositivos electrónicos se logra, con el objeto de robar la identidad de otra persona, que generalmente deriva en la consecución de otro delito o el despojo monetario a un usuario de sistemas financieros o de sistemas de redes. Se detalla el manejo actual de los delitos informáticos en Guatemala. El combate de los delitos es responsabilidad del Estado, por lo que se Identificará si existe la coordinación institucional para prevenir o investigar los casos que deriven en el Robo de identidad de usuarios de dispositivos electrónicos y el papel del Estado respecto de la prevención, al usuario de dispositivos electrónicos, para el resguardo de

sus datos personales e identificativos, ¿hay suficiente información respecto de los peligros y vulnerabilidades con los dispositivos electrónicos?

Derivado de la investigación desarrollada que, luego, se contrasta con bibliografía, se proponen acciones para las instituciones del Estado, vinculadas al tratamiento, prevención o investigación de delitos informáticos en Guatemala para integrar acciones para la prevención e investigación de delitos informáticos en Guatemala, para combatir el robo de identidad mediante dispositivos electrónicos.

En la actualidad, miles de personas se ven afectadas en Guatemala, derivado del robo de información, que luego es utilizada para robar la identidad de cualquier usuario de aparatos electrónicos, ya sea que lo adquieran de un celular, cámara digital, dispositivo móvil, laptop, correo electrónico, red social o cualquier servicio electrónico.

Para los delincuentes, los datos personales robados pueden ser útiles para adquirir préstamos, inscribir empresas, emitir facturas y cometer hechos ilícitos, ya que si a una persona le roban su teléfono celular, en un momento, el delincuente tendrá acceso a: pines de seguridad, teléfonos de familiares, acceso a correos electrónicos y redes sociales que pueden ser vendidos a personas inescrupulosas.

Ya sea por medio de correos falsos, mediante un ataque planeado o de forma personal el delincuente puede aprovechar la ventaja de la información. El robo de información, la estafa electrónica, el robo de identidad y el fraude en línea, tipificados en otras legislaciones, son algunos de los problemas que nuestro país afrontará y que conllevan el cuidado de la privacidad y dignidad de la persona. Sin embargo, es a través de dispositivos electrónicos como: celulares, dispositivos móviles, chips, tarjetas electrónicas o tarjetas de crédito o débito que se abre una oportunidad para los conocedores de métodos de evadir la seguridad de los dispositivos.

Actualmente se han desarrollado, en otros países, las herramientas necesarias no sólo para brindar seguridad sino para rastrear cada una de las órdenes que se dan al computador o dispositivo.

En Guatemala, si a una persona le roban su documento personal de identificación, no existe un mecanismo, dentro de las instituciones del Estado,que garantice al usuario que ese dispositivo será bloqueado para que sea inservible a los delincuentes. Las instituciones de justicia no cuentan con unidades especializadas para detectar a tiempo a estos criminales. Y las unidades que se encargan de investigar lo concerniente a la investigación del fenómeno de robo de identidad mediante dispositivos electrónicos en Guatemala, no cuentan con la tecnología, capacidades o institucionalización mínima para combatir éste tipo de delitos.

El estudio se realizó mediante el uso de bibliografía, de entrevistas, encuestas de victimización y ejemplos de políticas públicas de otros países para la visualización del fenómeno del robo de identidad. La identificación de las fortalezas y amenazas del Sistema de Justicia, frente a este delito, permitirán trazar una hoja de ruta para el tratamiento de dichos delitos por parte del Estado de Guatemala, para que el legislador tome en cuenta a la hora de tipificar el delito en nuestro Código Penal.

El aporte consiste en que será de utilidad para profesionales, ya sean abogados, jueces, fiscales, consultores técnicos, legisladores, peritos, técnicos de escena del crimen, ingenieros en sistemas, así como para estudiantes de carreras de Ciencias Jurídicas,que de alguna manera se vean involucrados como sujetos activos o pasivos en delitos sobre registros informáticos en Guatemala y la posibilidad de que estos sean utilizados para el robo de la identidad de un usuario de dispositivos electrónicos.

También va dirigido a todo aquel que se relacione en la vida cotidiana con un dispositivo electrónico en el que almacene datos sensibles y confidenciales que le puedan representar, de caer en manos equivocadas, perjuicio a un bien jurídico tutelado, ya que en la mayoría de los casos se reflejará en perdida de dinero. Aportará

también un esquema de cómo el Estado articula a sus instituciones para prevenir o contrarrestar el robo de identidad por medios electrónicos.

El límite que puede tenerse para la realización de esta investigación es la falta de capacitación y conocimiento respecto del tema de parte del personal asignado para desempeñar la investigación de los delitos informáticos, la falta de capacidad instalada y de tecnología, el desinterés del Estado, reflejado en planes operativos que pretenden planificar el fortalecimiento de las instituciones pero que luego carecen de presupuesto y asignación.

Otro límite es la ineficiencia de las unidades de acceso a la información de las instituciones del Estado, encargadas de la administración de justicia, pues aunque todas las instituciones tienen personal asignado a ellas, no ofrecen responder preguntas directas, más bien, quieren otorgar solamente datos estadísticos.

Las unidades de análisis para la presente investigación fueron leyes vigentes guatemaltecas, bibliografía y como instrumentos se utilizaron diversas entrevistas semiestructuradas a funcionarios de la Policía Nacional Civil (PNC), Ministerio Público y Organismo Judicial. Así mismo, formato de encuesta cerrada para los usuarios de dispositivos electrónicos, solicitud mediante la ley de acceso a información pública para la determinación de los procesos que se siguen en las instituciones de justicia, entrevista a profesionales del derecho, encuesta cerrada a un experto en ingeniería en Sistemas.

CAPITULO I

Delitos Informáticos en el mundo

1.1 Definiciones

Criminalística: Según Castellanos "es la disciplina por medio de la cual se aportan las pruebas materiales, con estudios técnicos científicos, para probar el grado de participación del o de los presuntos autores y demás involucrados".[1]

Delito Informático: Tellezdefine como delito informático "las actitudes contrarias a los intereses de las personas en que se tiene las computadoras como instrumento o fin o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin".[2]

Hacker"Persona muy aficionada y hábil en informática que entra ilegalmente en sistemas y redes ajenas".[3]:

Identidad: Entre los conceptos clásicos, se puede citar un importante fallo de la Corte Suprema Italiana, en el cual se expresó que la identidad era "el conjunto de atributos, calidades, caracteres y acciones que distinguen a un individuo con respecto a cualquier otro y que conforma su derecho a ser reconocido en su 'peculiar realidad' ".[4]

Ingeniería Social:"El acto demanipular a una persona para que lleve a cabo una acción que, puede ser o no, lo más conveniente para cumplir con cierto objetivo.

[1]Castellanos Tena, Fernando. Lineamientos elementales del Derecho Penal. Editorial Porrua. México 1977 Pág. 29
[2]Tellez Valdés, Julio. Derecho Informático. México. Pág. 163
[3]Manual de investigación policial, procedimientos y técnicas científicas, tomo III de investigación. Sigma Editores. Primera edición, página 1195
[4]Corte Suprema italiana, 13 VII 71, Foro Italiano, 1972 I 432

Este puedeser la obtención de información, conseguir algún tipo de acceso o logarque se realice una determinada acción".[5]

Phishing: " Es un tipo de robo de identidad en línea. Usa correo electrónico y sitio web fraudulentos que son diseñados para robar datos o información personal, tales como números de tarjeta de crédito, contraseñas, datos de cuenta u otro tipo de información".[6]

Robo de Identidad, suplantación de identidad mediante un dispositivo electrónico:"Es cualquier clase de fraude que origine la pérdida de datos personales, como, por ejemplo, contraseñas, nombres de usuario, información bancaria o números de tarjetas de crédito. Sucede cuando un tercero se apropia ilegalmente de información personal mediante engaños o ingeniería social".[7]

Skimmer:"Dispositivo electrónico que colecta una copia idéntica de otro dispositivo electrónico con banda magnética, en el que se puede almacenar hasta 3000 datos de bandas magnéticas y que proporciona la información privada que resguarda el dispositivo".[8]

Diferentes tesis han concluido que la ausencia de legislación específica sobre los delitos que se cometen en el ámbito informático y cibernético deja un gran vacío legal que debe ser llenado.

"Asimismo, hay ausencia de normas vigentes positivas aplicables a relaciones o casos jurídicos determinados, especialmente ante un planteamiento litigioso. Por otro lado, en este país, como en muchos países en vías de desarrollo y de pobre

[5] Hadnagy, Christopher. Ingeniería Social el Arte del Hacking Personal. Editorial Anaya. Pág. 215
[6] www.microsoft.com/es-es/security/online-privacy/phishing-faq.aspx
[7] www.mircrosoft.com/es-es/security
[8] Delitos Informáticos. Recuperado el 13 de Abril del 2014;
http://www.delitosinformaticos.com/10/2012//fraudes/tarjetas-bancarias-consumo-y-fraude

tecnología, se manifiesta por la inadvertencia reguladora en los legisladores, es decir, por desconocimiento"[9]

Debido a que, en materia penal, está excluida la posibilidad de utilizar el principio de analogía para la interpretación o tipificación de una figura delictiva, donde claramente establece "art. 7 Exclusión de Analogía: por analogía, los jueces no podrán crear figuras delictivas, ni aplicar sanciones"[10], se hace necesario promover las reformas legislativas correspondientes para establecerlos en la legislación guatemalteca.

El uso de la información, como se tipifica en el Código Penal de Guatemala, es el acto delictivo sancionado en el que el uso ilegal de datos e información pertenecientes a un tercero, que posee carácter de confidencial y no de dominio público, conlleva un valor monetario, una pérdida de dinero, además de la violación de información privada. Para evitar que se violente dicha privacidad, se han creado marcos jurídicos internacionales, que prevén que esas actividades ilegales sean perseguidas por las autoridades.

1.2 Marco Legal Internacional de los Delitos Informáticos:

Derivado de que el delito cibernético, en el cual se incluye el robo de identidad utilizando medios electrónicos, ha tenido un crecimiento impresionante y que no requiere de un determinado lugar físico para realizarse y cuenta con la tecnología, que no tiene fronteras, como aliada, los países agrupados en diferentes organizaciones internacionales han promovido los siguientes instrumentos:

[9] López García, Elmer Yovani, *Inclusión de los delitos informáticos, que se cometen en internet dentro del Código Penal Guatemalteco* Tesis, Guatemala: Universidad de San Carlos de Guatemala 2011
[10] Código Penal de Guatemala, Decreto 17-73. Guatemala 2012. Artículo 7. Página 4

1.2.1 La Organización de las Naciones Unidasha considerado los siguientes delitos, alertando a sus países miembros que se vele por ellos a través de la legislación:

A.” Fraudes cometidos mediante manipulación de computadoras:

1. Manipulación de datos de entrada

2. Manipulación de programas

3. Manipulación de datos de salida

4. Fraude por manipulación informática

B. Fraudes informáticos

1. Como objeto

2. Como instrumento

C. Daños y modificaciones de programas o datos computarizados”[11]

[11] Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, que entró en vigor en septiembre de 2003. *Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos.*Recuperado de https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

1.2.2 El Convenio sobre la Ciber-criminalidad:

Firmado en Budapest, Hungría, el 23 de Noviembre de 2001, por los países integrantes de la Unión Europea y Estados participantes , en la que emite sus recomendaciones sobre el trato que deberá llevarse frente a los Delitos Informáticos, en el cual sus principales objetivos son:

- “Reafirmar la estrecha unión entre las naciones de la Unión Europea y países firmantes para enfrentar la Cibercriminalidad.

- Intensificar la cooperación con los estados miembros.

- Prioridad en unificar una política penal para prevenir la criminalidad en el ciberespacio con una legislación apropiada y mejorar la cooperación internacional.

- Concientizar a los Estados miembros de los cambios suscitados por la convergencia y globalización de las redes.

- Concientizar sobre la preocupación del riesgo de las redes informáticas y la informática electrónica de ser utilizadas para cometer infracciones penales, ser almacenados y exhibidos.

- Fomentar la cooperación entre los Estados e industrias privadas en la lucha contra la cibercriminalidad y la necesidad de protección del uso de la Informática para fines legítimos al desarrollo de la tecnología.

- Concientizar que la lucha contra la Criminalidad requiere la cooperación internacional en materia penal asertiva, rápida y eficaz.

- Persuadir sobra la necesidad de un equilibrio entre los intereses de la acción represiva y el respeto de los Derechos del Hombre garantizado en el convenio para la protección de éstos derechos y libertades fundamentales y reafirmar el derecho de no ser perseguido por la opinión pública, la libertad de expresión, libertad de búsqueda y el respeto a la vida privada.

- Complementar los convenios anteriores, relacionados con la materia o que otorguen soporte, con el fin de hacer más efectiva la investigación, procedimientos penales y recolección de pruebas electrónicas.

- Persuadir sobre la necesidad de mantener y proteger la confiabilidad, integridad y disponibilidad de los sistemas de cómputo, bases de datos, computadoras y redes".[12]

1.3 Marco Legal en Guatemala de los delitos Informáticos:

El Código Penal de Guatemala tipifica las acciones que derivan en el Robo de Identidad;

1.3.3 "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.

La pena se agravará en un tercio cuando se trate de la información necesaria para la prestación de un servicio público o se trate de un registro oficial.

Artículo 274 "B". Alteración de programas:

[12] Convenio de Budapest 2001. Recuperado de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

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

Artículo 274 "C".Reproducción de instrucciones o programas de computación:

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

Artículo 274 "D".Registros prohibidos:

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

Artículo 274 "E". Manipulación de información:

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

Artículo 274 "F". Uso de información:

Se impondrá prisión de s eis 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.

Artículo 274 "G". Programas destructivos:

Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación."

1.3.2 El Robo en Guatemala

El Robo, art. 251 del Código Penal.

"Quien sin la debida autorización y con violencia anterior , simultánea o posterior a la aprehensión, tomare cosa, mueble total o parcialmente ajena será sancionado con prisión de tres a doce años".

Robo agravado "Art. 252. Es robo agravado: 1o. Cuando se cometiere en despoblado o en cuadrilla 2o. Cuando se empleare violencia, en cualquier forma, para entrar al lugar del hecho. 3o. Si los delincuentes llevaren armas o narcóticos, aun cuando no hicieren uso de ellos. 4o. Si los efectuaren con simulación de autoridad o usando disfraz. 5o. Si se cometiere contra oficina bancaria, recaudatoria, industrial, comercial o mercantil u otra en que se conserven caudales o cuando la violencia se ejerciere sobre sus custodios. 6o. Cuando el delito se

cometiere asaltando ferrocarril, buque, nave, aeronave, automóvil u otro vehículo. 7o. Cuando concurriere alguna de las circunstancias contenidas en los incisos 1o., 2o., 3o., 6o., 7o., 8o., 9o., 10 y 11 del Art. 247 de este Código. El responsable de robo agravado será sancionado con prisión de seis a quince años".

Cuando se realiza una denuncia por robo o hurto de documentos, en Guatemala, no se coordina ninguna institución de justicia de inmediato para articular la novedad de que a alguien le robaron su información personal, vital, la que le da su identidad.

1.4 Robo de Celulares en Guatemala:

Desde hace más de diez años el robo de teléfonos celulares fue creciendo, de manera tal que muchas personas han sido asesinadas con tal de despojarles de sus dispositivos. Como consecuencia, se ha legislado al respecto.La Ley de registro de terminales telefónicas móviles robadas o hurtadas (Decreto 9-2007), prevé castigo para la alteración fraudulenta del registro que active el dispositivo móvil con cualquiera de las empresas de telefonía móvil para su aprovechamiento. El objeto de la ley es "normar el bloqueo de equipos terminales móviles por causas de robo o hurto, establecer condiciones de activación de tales equipos en la provisión de servicios de telefonía móvil y regular la creación de una base de datos de teléfonos robados".[13]

Sin embargo, no prevé nada en cuanto a la información confidencial que se traslada a manos de un criminal que puede hacer uso dañino con ella. Tampoco impone a las empresas la responsabilidad sobre la educación del usuario respecto de su información confidencial. En su momento el espíritu de la ley es disuadir ladrones de celulares, que en Guatemala hasta cobra vidas. Según el

[13] Decreto 9-2007 República de Guatemala

informe 2012 de la Superintendencia de Telecomunicaciones[14], hay más celulares que personas; 20.7 millones de usuarios registrados hasta diciembre del 2012 en un país en donde la última encuesta realizada por el Estado (la ENCOVI 2006, Encuesta nacional sobre condiciones de vida) se estimó que el 53% de la población vive en la pobreza.[15]

1.4.1 Procedimiento en caso de robo de teléfono celular

Los esfuerzos del Estado en el combate al robo de aparatos electrónicos han derivado en mesas de coordinación, interinstitucional, entre el Ministerio Público, la Policía Nacional Civil y la Superintendencia de Telecomunicaciones que generaron las siguientes procedimientos en el caso de que una persona sufra del robo o hurto de su aparato celular:

A. Tras sufrir un robo, hurto o pérdida del dispositivo el usuario deberá contactar a la empresa telefónica que le provee el servicio y reportar el incidente. Se suministrará el número de celular, nombre del usuario y número de IMEI (código de registro de cada aparato celular, que permite el bloqueo del servicio.

B. Interponer una denuncia en la Policía Nacional Civil o el Ministerio Público como requisito de reposición o trámite para recuperar el número de celular y adquirir otro dispositivo.

C. La denuncia será presentada a la compañía telefónica que ratificará el bloqueo.

[14] http://www.prensalibre.com/noticias/justicia/Vigente-ley-robo-celulares_0_1007899230.html
[15] Instituto Nacional de Estadísticas. ENCOVI 2011. Recuperado de http://www.ine.gob.gt/sistema/uploads/2014/12/03/qINtWPkxWyP463fpJgnPOQrjox4JdRBO.pdf

En materia de comunicación, también se han impulsado campañas de información y presión de medios de comunicación se han dado a conocer los procedimientos,

Las empresas telefónicas detallan los procedimientos en sus páginas de internet, por ejemplo, la empresa Telefónica ofrece un formulario base de denuncia, que luego será incluido en una base de datos, negra, de teléfonos robados.

Existe un procedimiento que borra los registros identificativos de los dispositivos, permitiéndole el acceso a cualquier servicio telefónico, denominado *flasheo*, que todavía a finales de Noviembre del 2013 se ofrecía en *kioskos* de centros comerciales. No es sino a raíz de la implementación de la ley de equipos terminales móviles, decreto 8-2013, que se define una sanción penal a quien procure el *flasheo* de celulares y a las empresas que no bloqueen e inhabiliten los dispositivos. Es así que en las calles comienza a percibirse la medida y hay más cautela para las bandas dedicas a tráfico de dispositivos y, por qué no, de datos privados de usuarios.

CAPITULO II

2.1 Los delitos Informáticos

Según Rafael Garófalo un delito es “la violación de los sentimientos altruistas fundamentales de benevolencia o piedad y probidad o justicia en la medida media en que se encuentran en la sociedad civil, por medio de acciones nocivas para la colectividad”

Tellezdefine a la Sociedad de la Información como: "el uso masivo de tecnologías de la información y comunicación para difundir el conocimiento e intercambio de la sociedad”.[16]

2.1.2 El Robo de Identidad

El increíble avance en el desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos, información personal, mediante los cuales es posible obtener grandes beneficios económicos y causar perjuicios materiales o morales. La diferencia se basa en que es más difícil de descubrir, porque éste tipo singular de delincuentes es capaz de borrar sus huellas del hecho.

El robo, hurto o apropiación de la identidad de una persona se utiliza, siempre en perjuicio de la víctima, pues el acceso es ilegal y sin permiso. La falta de protección al consumidor de servicios de comunicación mediante dispositivos electrónicos vulnera indiscriminadamente a los usuarios de cualquier dispositivo electrónico.

[16] Julio Tellez Valdez “Derecho Informàtico. Mexico. Pág. 6

En Guatemala se atraen potenciales víctimas, mediante la utilización de la tecnología y los medios electrónicos robándoles sus claves, identidad o extorsionándole para perjudicarles y pedir dinero a cambio de terminar éstas acciones. En el caso específico del fenómeno del Robo de identidad en Guatemala es importante analizar el alto índice de robo de dispositivos móviles o dispositivos electrónicos y con ello la muy probable comercialización, dado que se brinda la oportunidad, de bases de datos, información, fotografías, claves, pines, contactos y un sin número de datos importantes en materia de seguridad para el usuario del medio electrónico.

Dado el creciente número de denuncias de incidentes relacionados con el Robo de identidad, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica y campañas para prevenir a los usuarios con la aplicación de medidas técnicas a los programas. Sin embargo, hasta el momento en Guatemala, el Estado no cuenta con una institución, dirección o unidad que vele por el bienestar del consumidor, cliente/usuario de la red.

La clasificación estadística en el Ministerio Público respecto del fenómeno del robo de identidad mediante dispositivos electrónicos en Guatemala se contabiliza en los Delitos Informáticos, se trata básicamente de los delitos contenidos en el Código Penal de Guatemala en el artículo No. 274 de los delitos relativos a la destrucción de datos informáticos.

Tabla No. 1

Estadísticas del Ministerio Público sobre delitos informáticos, tipificados en el artículo 274 de la A a la G del Código Penal

Reporte Estadístico a Nivel Nacional de Denuncias Relacionadas a Delitos Informáticos, correspondientes a los años 2012, 2013 y al 24 de Noviembre del 2014.

	Año	Total
Delitos Informáticos	**2012**	432
	2013	707
	2014	417
	Total general	1556

Fuente: Unidad de Acceso a la información pública, Ministerio Público, CD-ROM, Guatemala, 2014

El robo de identidad se constituye en uno de los hechos ilícitos más populares en ésta era de tecnificación. La educación que recibe la ciudadanía (usuarios de internet) respecto a la seguridad de sus datos y movimientos en internet es casi nula. Las personas ofrecen información en la red, en su computador, en su dispositivo móvil, o en su celular, mediante el chip de su tarjeta o la banda de su tarjeta de crédito.

La imaginación del delincuente no descansa y a cada paso se inventan dispositivos que vulneran la seguridad del usuario, exponiendo sus datos a delincuentes, pues quien ejerza esta intromisión no tiene un propósito amigable con los datos de la víctima.

Muchos son los delitos que pueden generarse del robo de identidad y muy sencillas las amenazas y forma de controlar a su víctima. El usuario se puede ver amenazado de las siguientes maneras.

- Vigilancia en Redes Sociales.
- Información en Internet.
- Minería de Datos.
- Como objetivo fijo.
- Difusión de todo absolutamente, todo lo que hemos dejado publicado en la red.
- Adquisición de dispositivos electrónicos como, aparatos celulares, memorias USB, computadoras personales, etc. son un medio para adquirir datos e información confidencial de cualquier persona, ya sea que se haya adquirido por un robo, un *hackeo* o la adquisición de bases de datos. Todos estos elementos serán de vital importancia a la hora de examinar el fenómeno del robo de identidad mediante medios electrónicos en Guatemala.

2.3 Riesgos derivados del extravío, robo o hurto de un dispositivo electrónico

1. Recuperación de claves de correo electrónico y acceso a Bancos o Cuentas bancarias: Los teléfonos celulares cuentan con planes permanentes de

internet para actualizar la información que se trafica mediante correo electrónico. Múltiples denuncias sobre robo de identidad dan cuenta de correos que fueron enviados al banco para actualización de datos personales, acceso a banca en línea y con ellos a transacciones monetarias.

2. Alteración o venta o publicación de fotografías personales.

3. Utilización de los datos del individuo para extorsionarle. Contactos de familiares.

Un delito cibernético consiste en el uso sin autorización y de manera abusiva de alguna base de datos, información o datos propiedad de un tercero y que por el conocimiento de este pueda realizar alguna actividad determinada imposible hasta antes del momento de su conocimiento.

2.4 Elementos del robo de la identidad

a) La existencia de un acceso no autorizado a un sistema de tratamiento de información; o un dispositivo ajeno.

b) Su finalidad es lograr una satisfacción de carácter intelectual, pues busca tener la identidad de otro sujeto o equivocar a algún sujeto pasivo, ya sea individual, público, jurídico y/o comercial.

Cuáles son los bienes que se afectan con el Robo de la Identidad?

Los bienes que pueden ser afectados a través del robo de identidad, en Guatemala, son diferentes al delito “tradicional”, pues no afecta exclusivamente bienes materiales sino, también, inmateriales como:

- Bases de datos,
- Registros electrónicos
- Inscripciones regístrales
- Propiedad intelectual

2.5 Seguridad de los dispositivos electrónicos:

Los dispositivos electrónicos, cuando se adquieren nuevos, no cuentan con un sistema de seguridad que resguarde adecuada y cuidadosamente los datos que contiene dicho dispositivo.

2.5.1 Herramientas Anti Robo de identidad:

Hay varios programas informáticos antirrobo de identidad disponibles: La mayoría de estos programas trabajan identificando contenidos propios del robo de identidad en sitios web y correos electrónicos; algunos *software* anti-*pishing* pueden por ejemplo integrarse con los navegadores *web* y cliente de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los

phishers, ya que reducen el número de correos electrónicos relacionados con el *Phishing* recibidos por el usuario.

González Juárez, Diego Dante y Peña Enríquez, José Antonio. *Estudio del Impacto de la ingeniería Social- Phishing.* México Universidad Nacional Autónoma de México, [17] en su Estudio del impacto de la ingeniería social- *phishing* para optar al grado de Ingeniero en Computación a través de un trabajo de monografía, realiza un análisis histórico, inductivo y deductivo que le permite definir que en el desarrollo de un delito cibernético, como el *Phishing* (robo de identidad) es necesaria la aplicación metodológica de la Ingeniería Social, y ésta debe de tomarse en cuenta para la tipificación del delito como tal. Analiza casos reales de empresas que han sido utilizadas como gancho para obtener información útil de las personas, como su número de cuenta, accesos y otros, que luego se pueden utilizar para defraudar o suplantar a otro.

Utilizando como fuente los datos de empresas de seguridad informática, de talla mundial como, *Karspersky Lab* se apoya para concluir que el *Phishing* es el principal delito de estafa a través de la red en la actualidad, que se realiza al momento de obtener información de algún usuario y suplantar su identidad en diversos medios como son entidades bancarias en línea, servicios de pagos a través de la red, acceder a diversos tipos de redes sociales, etc. Asimismo, concluye que mientras más avanzan las tecnologías de comunicación, la gente descuida más su información y esto se debe a que los usuarios dejan toda la responsabilidad de seguridad a herramientas dedicadas a este fin, sin embargo, un pequeño descuido por parte del usuario es una puerta abierta para el criminal

[17] González Juárez, Diego Dante y Peña Enríquez, José Antonio. *Estudio del Impacto de la ingeniería Social- Phishing.* México Universidad Nacional Autónoma de México, 2012.

Campuzano, Cuamatzi y Sánchez[18] en su tesis para optar al grado de Licenciado en ciencias de la Informática en el Politécnico de México, a través de un trabajo de grado cualitativo, concluyeron, respaldados en las investigaciones que sobre el tema ya han efectuado empresas como *Symantec y Microsoft* –expertas en *software*- que aunque se tienen avances tecnológicos y empresas dedicadas a la creación y actualización de herramientas de seguridad los esfuerzos no son suficientes si las empresas que prevén servicios de comunicación o software, no realizan esfuerzos comunicacionales efectivos para informar sobre los riesgos existentes.

Con el fin de confirmar su hipótesis de que ciudadanos más informados son menos vulnerables a los delitos informáticos, se realizó una investigación en una empresa de 80 trabajadores. Se seleccionó a la mitad y, tras realizarle dos cuestionarios, se concluyó que se vieron beneficiadas en aspectos tales como:

1. El conocimiento que adquirieron para tomar decisiones con mayor responsabilidad al utilizar Internet.

2. Los lugares adecuados para realizar operaciones bancarias.

3. Las medidas de seguridad identificables en los sitios web.

Se concluyó, además, que la cultura informática en cada uno de los usuarios de la red, las políticas empresariales aplicadas al pie de la letra, el establecimiento de controles necesarios y útiles en los corporativos y una legislación informática que este a la vanguardia tecnológica, son puntos clave para minimizar en gran medida esta creciente problemática.

[18]Campuzano Aguilar, Eduardo Alejandro. Cuamatzi Saucedo Ana Lilia. Sánchez López, Jesús Eduardo. *Phishing; Amenaza y factores de riesgo en las tecnologías de la información del mundo empresarial*. México. Instituto Politécnico Nacional. 2009

Los programas de seguridad más conocidos son pagados. Sin embargo, mediante organizaciones que promueven el "*Software* libre", se puede adquirir protección de sus datos sin costo alguno. Ésta opción la conocerá solamente alguien con muy buena educación en redes, tecnología y software.

Debemos cuestionarnos sobre la responsabilidad que el Estado le debe otorgar a las empresas de *software* en cuanto a la seguridad de sus usuarios.

El portal digital del gobierno de los Estados Unidos[19], indica que si otra persona obtiene su información personal, es posible usar su nombre, fecha de nacimiento, número de pasaporte, número de tarjeta de crédito u otra información personal para cometer fraudes o robos.
Aconseja lo siguiente:

- No lleve su tarjeta del Seguro Social en su billetera ni la escriba en sus cheques. Sólo dé el número cuando sea absolutamente indispensable.
- Mantenga en secreto su PIN. Nunca escriba el PIN en una tarjeta de crédito o débito, ni en un trozo de papel que guarde en su billetera.
- Esté atento a las personas que miran por encima de su hombro cuando utilice teléfonos públicos y cajeros automáticos. En esos casos, proteja el teclado numérico con su mano libre.
- Proteja su correspondencia. Cuando viaje y no pueda recoger su correspondencia, solicite a la oficina local del Servicio Postal que no haga entregas hasta el día en que regrese.
- Esté atento a sus ciclos de facturación. Una factura faltante podría significar que un ladrón se ha apropiado de su cuenta.
- Guarde sus recibos. Solicite todas las copias de los comprobantes de compra aunque hayan sido anulados por algún error. Revise que no haya ningunatransacción no autorizada.

[19] www.Usa.gov

- Rompa o triture los recibos, ofertas de crédito, estados de cuenta, tarjetas vencidas, etc. que ya no necesite para evitar que los ladrones encuentren información en la basura.
- Guarde su información personal en un lugar seguro tanto en casa como en el trabajo. No la deje a la vista.
- No responda a ofertas no solicitadas que le piden su información por correo, teléfono o Internet.
- Instale un cortafuegos o "*firewall*" y programas de protección antivirus en su computadora personal.
- Controle su reporte crediticio una vez al año. Revíselo con mayor frecuencia si cree que alguien ha obtenido acceso a su información bancaria. Lea la sección sobre informes de crédito.

En cuanto al seguro que se ofrece en Estados Unidos por parte de las compañías contra el robo de identidad, el portal advierte que estas pólizas son más valiosas para la compañía que las vende que para los usuarios. Hacen una invitación a que antes de comprar uno de estos planes de protección de crédito, lea la letra pequeña, porque puede estar en una mejor situación siguiendo los consejos de prevención que se ya detallados.

Aconsejan que en caso de convertirse en víctima de fraude, la denuncia sea realizada por el usuario mismo, ya que muchas compañías y autoridades del orden público solo van a tratar con usted (en lugar de con una compañía de seguro que lo represente).

2.5.2 La Contraseña:

El nivel primario, de seguridad, que ofrecen los dispositivos electrónicos es el de la "Contraseña" o "*Password*". Sin embargo, los expertos en cibernética pueden evadir cualquier contraseña, por lo que pasos sencillos pueden ayudar al usuario a crear contraseñas seguras. Muchos sitios web, ya sea redes sociales, entidades bancarias, buscadores y empresas que proveen correos electrónicos, exigen que las personas creen una cuenta utilizando un nombre de usuario y una contraseña para proteger su privacidad e información personal.

El usuario, para simplificarse la vida puede utilizar la misma contraseña para varios sitios en internet, pero se convierte en un factor de vulnerabilidad, pues no todos son seguros. Para obtener la máxima protección posible hay que utilizar diferentes contraseñas en cada sitio, y cambiarlas periódicamente. El nivel de dificultad de la contraseña será un obstáculo para el delincuente informático, por tal razón las recomendaciones básicas son las siguientes:

- Usar una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.

- Mientras más larga sea la contraseña, mejor.

- No usar su nombre, fecha de nacimiento, equipos deportivos favoritos u otros datos que son fáciles de averiguar.

- Cambiar las contraseñas a cada cierto tiempo.

- No compartir contraseñas con otras personas, pueden no tener el mismo cuidado que usted como dueño de la información.

2.6 Mecanismos para el robo de identidad a través de dispositivos electrónicos:

En Guatemala, la clonación de tarjetas es la acción que más denuncias acumula en la Policía Nacional Civil y el Ministerio Público, ambos operadores afirman que hay varias maneras en que una persona puede adueñarse ilegalmente de información sensible para derivar en el perjuicio de las finanzas de esa persona. La capacidad del delincuente para manipular, determinar o lograr que otra persona le otorgue información sensible e importante juega un papel determinante en la consecución de los delitos informáticos.

Casos en los que, por medio de un *Skimmer,* un cajero o cobrador realiza una copia de la banda magnética que después vende o comparte con otra persona que se encargará de realizar la clonación (copia idéntica) de la banda magnética, que contiene los datos personales e identificativos del usuario y tener acceso a operaciones financieras.

CAPITULO III

3.1 El delincuente informático:

Usualmente cuando se trata de delitos cibernéticos[20], el delincuente es;

i. Es un conocedor del sistema

ii. Posee un plan para ingresar al sistema

iii. Borra su rastro y

iv. Consigue su objetivo

Robo de información: ¿Cuál es la razón para que exista el robo de información?

a. Poder

b. Control

c. Publicidad

d. Facilidad de accesos

e. Facilidad de localización

f. Atentados y extorsiones

[20]Dr. Sebastian Gòmez, Perito informàtico Oficial. “Actuaciones en delitos informáticos”

3.2 El delincuente informático y su impacto social

Una de las características de los delitosinformáticos radica en que quien lo realiza no necesita contar con una ubicación física determinada para realizar el robo de la identidad o, como se conoce en Guatemala, el Uso de la Información[21].

En ésta era de la tecnificación en que el cibercriminal se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, regularmente un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas, a veces sin dejar rastro, se pueden identificar varios tipos de intrusos:

A. El *Hacker*, según teóricos, es aquella persona que de una u otra manera puede demostrar las vulnerabilidades en los sistemas de información que existen en la actualidad. Puede mejorar los sistemas ya que muestra las fallas de cierta tecnología. Actualmente el *hacking* no se ve con los mismos ojos, es decir, su causa ya no es noble. Hoy en día el *hacking* lo entienden como el robo de contraseñas, la incursión en sistemas privados o cerrados, de seguridad, de la banca, el robo de información, el sabotaje y espionaje electrónico y muchas situaciones más.

B. Los *Script Kiddies*: Jóvenes curiosos y seguidores de los pasos de los hackers. Su fin es sacar provecho de las acciones de los hackers.

C. El Intruso Interno: Su motivación puede ser monetaria o personal, se encuentra dentro de la organización y posee conocimientos esenciales para vulnerar la seguridad de los sistemas informáticos.

D. Los *Crackers*: Son los delincuentes que reciben remuneración económica alrededor de la tecnología. Sus propósitos son; búsqueda, destrucción,

[21] Código Penal de Guatemala. Art. 274 F.

interrupción de sistemas y robo con motivaciones financieras. Pueden aprovecharse de personas, instituciones, organizaciones e incluso el gobierno. Tienen mecanismos eficientes para borrar su rastro.

E. El *phishing* o suplantación de identidad, es un término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada de tarjetas de crédito y otra información bancaria).

Según TELLEZ[22], este tipo de acciones presenta las siguientes características principales:

- Son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.

- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se haya trabajado.

- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios económicos " al hechor.

- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

[22] Tellez Valdés, Julio. Derecho Informático. México

- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

- Son muy sofisticados y relativamente frecuentes en el ámbito militar.

3.2.1 Criminalidad Informática:

Según Tiedemann la expresión criminalidad mediante computadoras se aluda a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.
Al hurtar o robar un dispositivo móvil o cualquier medio electrónico que contenga información confidencial sensible al interés de personas inescrupulosas, el usuario se arriesga a que cierto tipo de delincuentes obtenga acceso a su información más importante.[23]

Investigación Forense en delitos informáticos:

Montaño (2008)[24] realiza una reseña sobre "la problemática a la que se han enfrentado las investigaciones de los delitos informáticos, tales como:

- Uniformar disposiciones sobre los delitos informáticos.

- Facultad de especialización en los órganos de procuración y administración de justicia para el tratamiento de los delitos informáticos.
- La ausencia en la creación de órganos auxiliares en la procuración de justicia para la adecuada investigación de los delitos informáticos, tales

[23] Tiedemann, Klaus, Poder informático y delito, Barcelona, España. 1985
[24] Montaño Álvarez, Alejandro Armando. *La problemática jurídica en la regulación de los delitos informáticos.* México. Universidad Nacional Autónoma de México, 2008.

como una policía especializada, así como un cuerpo de expertos en la materia.

- El carácter transnacional de las múltiples operaciones realizadas a través de los sistemas computacionales.

- Ausencia de tratados internacionales para resolver múltiples problemas relacionados con los delitos informáticos , que van desde la celebración de convenios internacionales de colaboración , así como de extradición o de intercambio de reos por estos delitos.

- Escaso control de las compañías de computadores, así como de sus servicios como el de Internet.

El avance en la tecnología propicia que en los países que carecen de reglamentación, leyes y procedimientos específicos, la población se vea azotada por una serie de delitos en las que se encuentra en total desamparo ya que se desconoce, no solo sobre el tema cibernético, sino que se ve seriamente fracturada su privacidad, su identidad y hasta sus cuentas bancarias.

Según el Manual de Investigación Criminal, algunos de los medios utilizados para engañar a las personas y robarles sus datos son:[25]

- Por medio de correos falsos: Esta técnica permite pasar a un atacante por una organización, banco o empresa reales para obtener información que garantice acceso a algún recurso que usted utilice en esa organización, banco o empresa.

[25] Manual de Investigación Criminal y Forense. Tomo 2. Colombia

- De forma personal: Información que una persona escucha sobre otra, brindándole detalles valiosos sobre sus datos.

- Mediante un ataque organizado: Cualquier atacante podría intentar superar la seguridad de un banco, empresa u organización para obtener información personal de los clientes para luego acceder a algún recurso de esa empresa.

- A través de ataque a servidores de almacenamiento de información online: El atacante puede tratar de obtener datos de un servidor de almacenamiento de datos en la nube; obteniendo contraseñas, DNI, cuentas bancarias, etc.

CAPITULO IV

Articulación del Estado en contra del Robo de identidad mediante dispositivos electrónicos en Guatemala

4.1 Antecedentes:

Luego de tres décadas de conflicto armado interno, en 1996, llega finalmente “la paz firme y duradera”, el cese al fuego, la firma de la paz. Una serie de compromisos, firmados en los “Acuerdos de Paz” para terminar con la inequidad y exclusión de sectores en Guatemala, fueron firmados por funcionarios del Estado y de Contrainsurgencia. En ése mismo tiempo de la historia el gobierno vendió los activos del Estado como: La empresa estatal de telefonía, de luz y algunos silos (que protegen semilla vital).

La dinámica de guerra llega a su fin y la proliferación de delitos comienza su ascenso. En dicho tiempo, donde el presidente era Álvaro Arzú, el delito que proliferó fue el secuestro (los secuestros fueron mecanismo regular de presión por parte de los involucrados durante el conflicto armado interno). Contrariamente al fortalecimiento que debió recibir el Estado como encargado de la Administración de la Justicia, se vio perjudicado. Durante éste gobierno se suprimió el Delito de Enriquecimiento Ilícito y se implementó el Secreto Bancario, bajo el argumento de que vulneraba a las personas.

4.2 Secreto Bancario

Se regula en el artículo 63 del Decreto 19-2002, Ley de Bancos y Grupos Financieros, de la siguiente manera:

“Confidencialidad de operaciones. Salvo las obligaciones y deberes establecidos por la normativa sobre lavado de dinero u otros activos, los directores, gerentes,

representantes legales, funcionarios y empleados de los bancos, no podrán proporcionar información, bajo cualquier modalidad, a ninguna persona, individual o jurídica, pública o privada, que tienda a revelar el carácter confidencial de la identidad de los depositantes de los bancos, instituciones financieras y empresas de un grupo financiero, así como las informaciones proporcionadas por los particulares a estas entidades.

Se exceptúa de la limitación a que se refiere el párrafo anterior, la información que los bancos deban proporcionar a la Junta Monetaria, al Banco de Guatemala y a la Superintendencia de Bancos, así como la información que se intercambie entre bancos e instituciones financieras.

Los miembros de la Junta Monetaria y las autoridades, funcionarios y empleados del Banco de Guatemala y de la Superintendencia de Bancos no podrán revelar la información a que se refiere el presente artículo, salvo que medie orden de juez competente.

La infracción a lo indicado en el presente artículo será considerada como falta grave, y motivará la inmediata remoción de los que incurran en ella, sin perjuicio de las responsabilidades civiles y penales que de tal hecho se deriven"

Entonces, el secreto bancario es uno de los principales derechos que nace en las relaciones comerciales adquiridas entre los bancos y sus clientes, que obligan a las entidades a no divulgar, ni revelar aquella información sobre sus clientes y las operaciones que han realizado o han estado a punto de realizar con sus clientes.

En Guatemala, el secreto bancario se convierte en un obstáculo para los funcionarios encargados de las investigaciones ya que los bancos no les proporcionan información de sindicados, valiéndose de esta norma y, según manifiestan los agentes investigadores de la PNC, los fiscales del Ministerio

Público no realizan las peticiones ante juez para que mediante orden judicial se obligue a los bancos a entregar información a la Policía.

El Instituto Centroamericano de Estudios Fiscales (ICEFI) a través del observatorio Fiscal No. 19 Época II determina como un factor de riesgo existente y una deficiencia el hecho de que el Secreto Bancario no permite a las instituciones fiscalizadoras investigar preventivamente, ni siquiera después de varios delitos identificados, en contra de delitos como fraude y evasión fiscal.

Hasta el momento, las instituciones de justicia, según sea la "relevancia" que le otorguen al caso (por ejemplo, si salió en un medio de prensa o afecta a alguien importante) de delito cibernético, deben contratar a expertos externos que se incorporen al proceso para asesorar a las víctimas o al ente de administración de justicia, ya que no se cuenta, a nivel de institución del Estado, con un cuerpo profesional y capacitado para realizar el peritaje. El INACIF, hasta el momento sólo brinda ayuda en casos en donde se vulnere la vida de las personas.

Actualmente se han desarrollado, en otros países, las herramientas necesarias no sólo para brindar seguridad sino para rastrear cada una de las órdenes que se dan al computador. Los dispositivos móviles, en otros países, cuentan con aplicaciones que promuevan la conservación de los dispositivos haciéndolos completamente personales e identificables.

Cuando ocurre un ataque cibernético, el administrador de justicia debe cuidar la recolección de rastros para que la prueba pueda ser útil y pertinente. Es mediante un análisis forense que se recoge, analiza, preserva y presenta, a través de técnicas y herramientas, la información. El principal componente de dicho análisis deberá ser; la lógica, la coherencia y el sustento.

La falta de capacitación de los funcionarios de la administración de justicia en los temas de delitos cibernéticos provoca la poca atención de los juzgados, el

Ministerio Público y la Policía Nacional Civil. Dicho extremo se manifiesta en que no se cuenta con unidades especializadas y capaces de atender situaciones de delitos cibernéticos.

Los Bancos, que pertenecen al sector privado, han implementado una serie de controles o pasos para validar la información que sus usuarios colocan en la red, con el único objetivo de proteger la información para que luego no sea utilizada para defraudar a los usuarios o al Banco.

En Guatemala, un delincuente de delitos cibernéticos tiene la gran ventaja de que la mayoría de la población no tiene educación sobre cómo mantener seguros sus datos. La ignorancia es la principal aliada del delincuente. Por ejemplo, si a una persona le roban su teléfono celular o dispositivo móvil, pueden tener en un lapso de tiempo, acceso a datos importantes sobre las personas; pines de seguridad, correos electrónicos, estados bancarios o manejo de cuentas bancarias, contraseñas, teléfonos celulares y con este contactos, redes sociales, etc. Vulnerando los datos del usuario y éstos pueden ser vendidos a personas inescrupulosas.

En la actualidad, en Guatemala se realizan investigaciones para ubicar a los responsables de 30 casos de robo de identidad en los que se utilizan los datos para adquirir préstamos bancarios, inscribir empresas, emitir facturas y cometer hechos delictivos. Dicha denuncia, publicada por todos los medios de comunicación, motiva la apertura de la sección de Delitos Económicos del Ministerio Publico y consecuentemente una Dirección de Delitos Económicos en la Policía Nacional Civil.

4.3 Las instituciones del Estado frente al robo de identidad mediante dispositivos electrónicos

En Guatemala, cuando se trata de un delito penal, las instituciones de justicia que participan son:

- Policía Nacional Civil, encargado de la seguridad, de realizar las investigaciones y realizar las capturas emanadas desde el Organismo Judicial.

- Ministerio Público, dirige la investigación y realiza la persecución penal.

- Organismo Judicial, encargado de impartir justicia dentro del sistema de administración de justicia guatemalteco.

- El Instituto de Ciencias Forenses (INACIF), encargado de los peritajes

- El perito y el consultor.

- El Instituto de la Defensa Publica Penal, otorga defensa al sujeto procesal, regularmente el sindicado.

Sin embargo no se ha articulado la cadena de justicia de tal forma que permita desplegar políticas de prevención del delito de Robo de Identidad. Ninguna de las instituciones de justicia cuenta con una unidad especializada en la delincuencia cibernética para combatirla. El extremo radica en que las propias instituciones de justicia no cuentan con la seguridad necesaria para mantener sus propios datos seguros. Dicho extremo se manifiesta a nivel noticioso, cuando han sido públicos cientos de “ataques cibernéticos” a instituciones como el Ministerio Público, Ministerio de Gobernación, entre otras instituciones del Estado.

4.4 Instancias del Estado que tienen banco de Dato:

- Registro Nacional de las Personas: a través del DPI
- Empresa Maycom: Extiende las licencias de conducir.
- Instituto Guatemalteco de Seguridad Social: a través del número de seguro social.
- Dirección General de Migración: Extiende los pasaportes de los ciudadanos guatemaltecos.

Instancias del Estado que registran datos:

- Registro Mercantil.
- Registro de la Propiedad.
- Departamento de tránsito a través de Maycom en la emisión de licencias de conducir.
- Registro de Marcas.

Algunas instancias particulares que registran datos:

- Entidades Bancarias
- Redes Sociales
- Páginas web
- Personas individuales
- Empresas de telefonía
- Infornet (empresa privada que trafica datos)
- Colegios profesionales
- Universidades, colegios y escuelas

4.5 La Corrupción en las instituciones de justicia

La desconfianza entre las instituciones se hace manifiesta, hasta en los medios de comunicación, que reflejan operaciones realizadas por el Ministerio Público, sin el conocimiento de la Policía Nacional Civil. Y es que, aunque en el Ministerio de Gobernación, Ministerio Público y Organismo Judicial (como principales instituciones del Estado, en los casos de robo de identidad mediante dispositivos electrónicos) cuentan con Oficinas de Inspectoría para la investigación de asuntos internos, éstas existen en papel, pero no cuentan con presupuesto asignado ni personal capaz de realizar todas las investigaciones. En el caso de la Policía de Guatemala, la Oficina de Responsabilidad Profesional procede luego de una denuncia contra un miembro de la institución, que luego será sometido al proceso disciplinario según llene las características tipificadas en el reglamento de la ley Orgánica de la Policía Nacional Civil.

Las múltiples noticias, expuestas en medios de prensa, sobre corrupción en las instituciones dan cuenta de que al menos el 25% de cada presupuesto, se utiliza en distintas formas de corrupción.

CAPITULO V

Derecho Comparado

5.1 Estados Unidos

En los Estados Unidos de América, derivado de la enemistad con sectores de diferentes países, por sus políticas pasadas e intervencionistas, se aprobó la Ley de transacciones de crédito justas y precisas, (*Fair and Accurate Credit Transactions Act* o FACTA, 2003)en la que la Comisión Federal del Comercio ha propuesto recientemente una definición de Robo de identidad que se suma a la ley de Robo de Identidad (1998)

Robo de identidad: todo fraude consumado o no consumado mediante el uso de información identificativa de otra persona sin permiso legal. En donde la información identificativa es cualquier nombre o número que pueda servir, de manera individual o junto con otra información, para la identificación de un individuo concreto, incluyendo:

> Nombre, número de seguridad Social, fecha de nacimiento, licencia de conducir, número de carne de identidad, ya sea expedido por el Estado o por Gobierno Federal, número de pasaporte, número de identificación fiscal. Datos biométricos (huella dactilar, imagen de la retina o el iris, registro de voz o cualquier otra representación de un rasgo físico intrínseco. Número de identificación, dirección o código de enrutamiento electrónico exclusivos. Información de identificación de telecomunicaciones o dispositivos de acceso.

5.2 Chile

En Mayo de 1993 se promulgó la Ley relativa a delitos informáticos, No.:19223, que establece:

"*Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.*
Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."

5.3 Holanda

El primero de marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

- El *hacking*.
- El *preacking* (utilización de servicios de telecomunicaciones evitando
- el pago total o parcial de dicho servicio).
- La ingeniería social (arte de convencer a la gente de entregar informaciónque n circunstancias normales no entregaría).
- La distribución de virus.

5.6 Los delitos Informáticos en América Latina:

La empresa *Symantec*, en el 2011 contactó a 250 empresas (de 5 a 5000 empleados) de varias industrias. De los entrevistados el 78% sufrió un ataque en el último año, incluyendo ataques de código malicioso, de ingeniería social y ataques externos malintencionados. El 95% de los que fueron atacados sufrió pérdidas debido a ciberataques, incluyendo tiempo de inactividad, *robo de identidad* de clientes y empleados y robo de propiedad intelectual. Por último, un 20% de los negocios perdió, por lo menos USD$181,220.00 (Q. 1,449,760.00). Además el 42% de los encuestados está aumentando los presupuestos de prevención de pérdida de datos y seguridad web

Nuestra tipificación difiere en el nombre que le acuña a los delitos, pero el espíritu de cada uno es singular y característico. Otros países, sin embargo, tienen institucionalidad en el combate a éstos delito. La diferencia se basa en que el Estado no se ha fortalecido con herramientas para el combate de éstos delitos. La diferencia entre la consecución de los delitos tipificados en el artículo 274 del Código Penal y el Robo de identidad es la vulnerabilidad específica a la dignidad y seguridad de las personas.

Por otro lado, la clonación de tarjetas en Guatemala necesita del Robo de la Identidad de otra persona a quien le serán vulnerados 7 incisos (A – G) del artículo 274 bajo el título de “destrucción de registros informáticos”, del Código Penal, con la consecuencia del apoderamiento de recurso financiero de la víctima. Es ese dinero que le roban al usuario, de una tarjeta, lo que motiva la denuncia, lo que determina el robo de la identidad mediante un dispositivo electrónico y que deriva en la vulneración a raíz de obtener una copia exacta de claves, datos y accesos que permiten la sustracción de dinero. En una tipificación de delito de clonación de tarjeta, habría que colocar la acción de sustracción de dinero del usuario del dispositivo, y si queremos ir más adelante, se coacciona la cooperación de entidades bancarias y se suprime el secreto bancario.

En muchos países de América Latina no se toma en cuenta la Ingeniería Social como objeto de estudio permanente, ni se penaliza. Ésta situación evidencia que la tipificación específica de ciertos delitos describiría con mejor detalle la violación a la privacidad que un individuo sufre por parte de un sujeto que mediante actos de persuasión, encanto o engaño obtiene información de un usuario de dispositivo.

CAPITULO VI

Desarrollo, resultados y análisis de la investigación

6.1 Sujetos

Los sujetos a los que se les solicitará su opinión en la investigación son:

- Agentes policiales, investigadores de la Policía Nacional Civil (PNC) de la Dirección Especializada de Investigación (DEIC)

- Cuarenta personas usuarias de dispositivos electrónicos que describan la forma en que protegen su información, si es que la protegen.

- Veinticuatro profesionales del Derecho.

- Funcionario del Ministerio Público que detalle el procedimiento utilizado en el dicha institución.

- Jefe de la sección de delitos económicos de la Dirección Especializada de Investigación Criminal y dos agentes investigadores de delitos de Robo de identidad mediante dispositivos electrónicos.

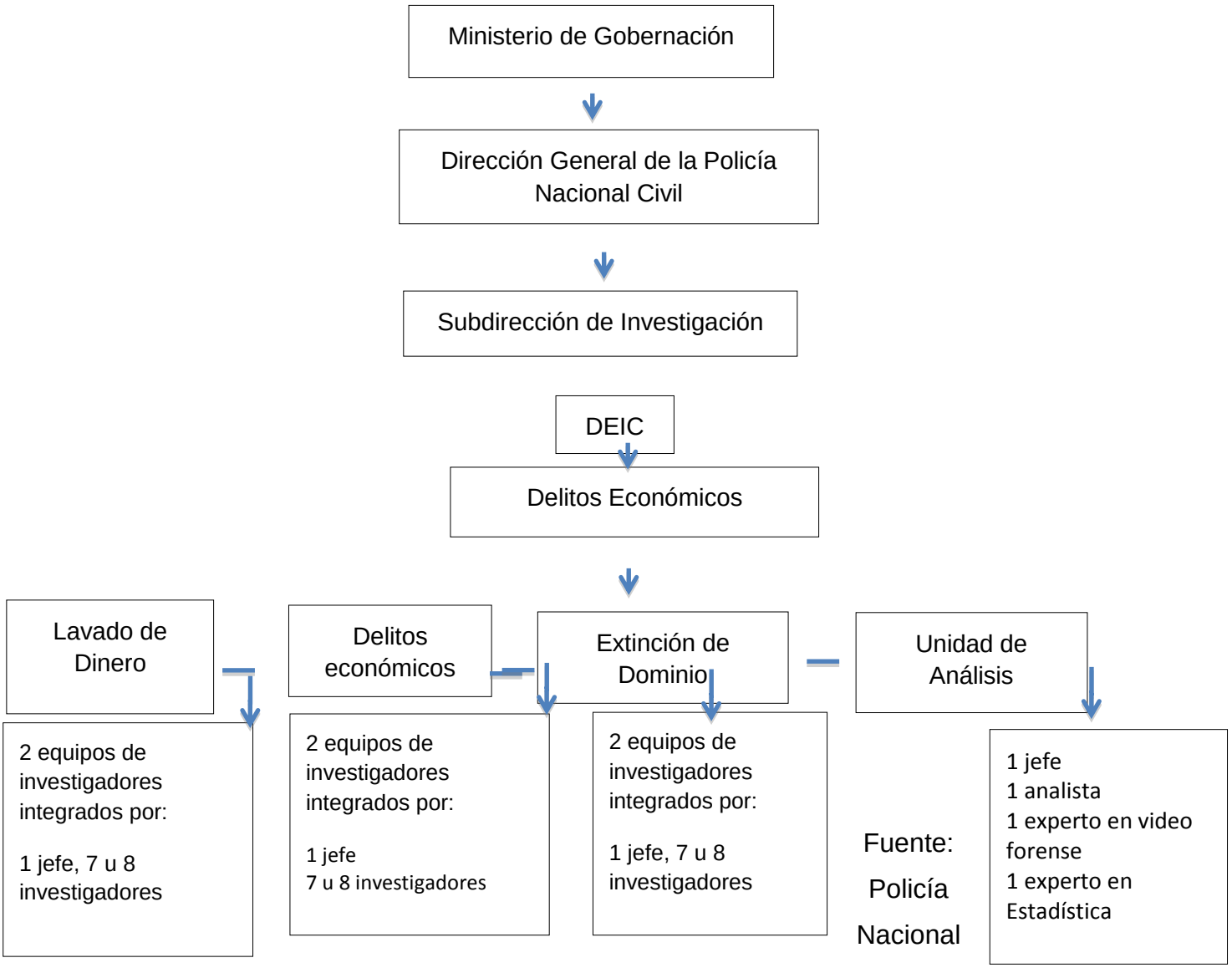
- Un experto en temas de delitos cibernéticos.

- Dos profesores de ingeniería en Sistemas o Seguridad de medios electrónicos.

Desarrollo de la Investigación:

6.1.1 Policía Nacional Civil:

Organigrama de organización de la Policía Nacional Civil, otorgado por el jefe de la Unidad de Delitos económicos derivada de la Dirección Especial de Investigación.



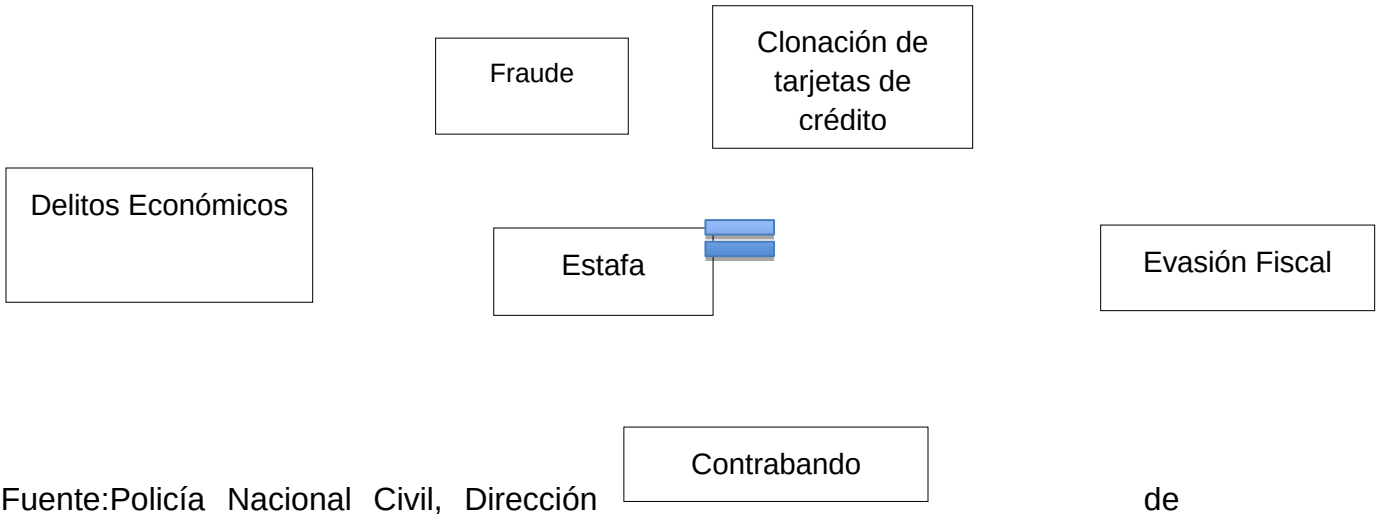
Fuente: Policía Nacional Civil, Dirección de Investigación Criminal, unidad de Delitos económicos, Oficial I Luis Alvarado, Guatemala 2014

A través de una entrevista semiestructurada al jefe de la sección de delitos económicos de la Dirección Especializada de Investigación Criminal (DEIC), que en la práctica, se encargan de la investigación de casos de robo de identidad y clonación de tarjetas de crédito o débito en la Policía Nacional Civil. Y, asimismo, la entrevista a 10 agentes de la sección que han tenido que investigar casos en que por medio de un dispositivo electrónico, una tercera persona obtiene los datos de otra persona y comete delitos, pretenden explicar el mecanismo de actuación de los funcionarios de administración de justicia en dichos casos.

En Guatemala, explica el jefe de la sección de delitos económicos de la Policía, el robo de identidad se utiliza para cometer delitos más graves como;

- Lavado de Dinero.
- Fraude
- Evasión Fiscal
- Falsificación Ideológica

Delitos que atiende la sección de Delitos Económicos de la División Especializada de investigación criminal



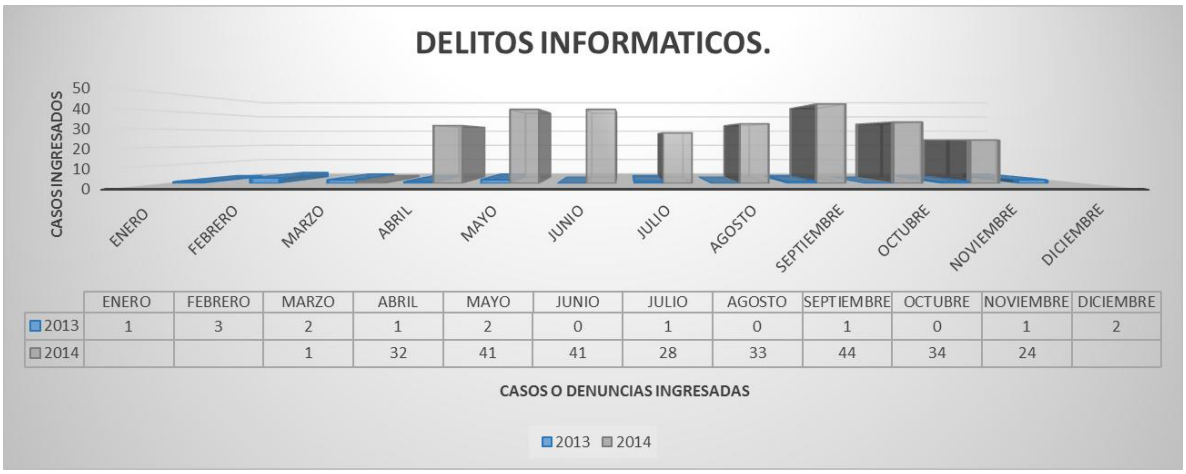
Fuente:Policía Nacional Civil, Dirección de

Investigación Criminal, unidad de Delitos económicos, Oficial I Luis Alvarado, Guatemala 2014

La sección de investigación de Delitos económicas tiene una única sede en la ciudad de Guatemala del departamento de Guatemala. En el resto del país no existen secciones de investigadores en delitos económicos, por lo que deben trasladarse a la capital.

Gráfica No. 1

Número de denuncias recibidas por la de la Policía Nacional Civil por delitos que implican el robo de identidad de una persona, mediante dispositivos electrónicos.



	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
2013	1	3	2	1	2	0	1	0	1	0	1	2
2014			1	32	41	41	28	33	44	34	24	

Fuente: Unidad de delitos económicos de la DEIC, PNC, CD-ROM Guatemala 2014

La amplia brecha en el número de denuncias recibidas todos los meses, respecto del año 2013 se debe a que hasta el 2014 se implementó un sistema estadístico que identifica por sus características, los delitos informáticos que necesitan del robo de la identidad de una persona, y se realiza mediante algún dispositivo electrónico. La clonación de tarjetas de débito o crédito son un ejemplo. Hasta el momento, los casos registrados en los que usuarios de dispositivos electrónicos

se vieron afectados por el robo de su identidad fueron producto en la sustracción monetaria a usuarios de tarjetas de crédito.

La tecnología de la Policía Nacional Civil:

Cada turno de 8 días de trabajo por 4 de descanso cuenta con 40 investigadores, todos dotados de computadora de escritorio, internet y teléfono celular. Al menos, la mitad poseen además una computadora personal. Sin embargo, no cuentan con ningún software de análisis, detección de malware (virus informáticos y de datos), *Software* para la obtención de claves, o acceso a múltiples bases de datos,directamente.

Para realizar capturas, que mayoritariamente se derivan de investigaciones previas y con orden de juez competente, cuentan con el apoyo del gabinete criminalística para comprobación de identidad de los sujetos.

Acción que desarrolla la PNC:

La Constitución Política de la República establece, que la seguridad interna de los ciudadanos guatemaltecos estará a cargo de la Policía Nacional Civil, quienes a través de la Ley Orgánica de la Policía Nacional Civil (Decreto 11-97) otorgan la labor investigativa. En consecuencia, la sección de investigación de delitos económicos de la Policía Nacional Civil, ofrece los siguientes servicios, para el caso del Robo de Identidad en Guatemala.

- Recepción de denuncias directas
- Requerimientos de investigación del Ministerio Público
- Capturas de los sindicados.
- Atender el llamado de la Subdirección de operaciones para festividades importantes.

- Búsqueda de documentos de identidad, propiedad, y otros elementos de prueba.

Principales avances:

A partir de la creación de la sección de investigación de delitos económicos dentro de las funciones de la Dirección Especializada de Investigación Criminal (DEIC), en 2010, como producto de la denuncia pública de una banda de asesinos que compraban propiedades de las personas que, acto seguido asesinaban. Sin embargo, según manifiestan los agentes entrevistados, es hasta hace unos 4 meses (Julio del 2014) que se realizó una reingeniería total en la sección. Consistente en:

- La reorganización y estratificación de la sección

- La desarticulación de bandas

- Adecuación de instalaciones, dignificando el lugar de trabajo, que en opinión del oficial, jefe de la sección es fundamental para el buen desempeño de las labores.

- Adquisición de vehículos para realizar investigaciones y traslados, la sección no contaba con ninguno

- Fortalecimiento y seguimiento a la coordinación interinstitucional para obtención de resultados a través de reuniones con Fiscalía para la revisión de casos.

- Aunque no son estadísticas formales dentro de la organización policial, se cuenta ahora con un registro de casos manejados.

- En Octubre del 2014 se aprueba la nueva orden general de la Policía Nacional Civil que ordena la creación de una sección de investigación contra delitos informáticos dentro de la Dirección Especializada de Investigación Criminal (DEIC).

Principales desafíos:

- A través de la entrevista, el jefe y los agentes de investigación concuerdan que la ausencia de legislación es un factor importante de retraso y complicación, principalmente a la hora de la persecución penal.

- El secreto Bancario es un obstáculo, los bancos no proporcionan información a la policía y los fiscales no hacen requerimiento a juez.

Figura 1: *Skimmer*, dispositivo electrónico a través del cual se obtiene una copia exacta de la banda magnética de otro dispositivo electrónico (tarjeta de débito o crédito) que luego se utiliza para clonar una copia exacta de la banda magnética robada o hurtada, para luego sustraerle su dinero. Foto otorgada por DEIC, PNC.

6.1.2 Ministerio Público

El Ministerio Público, a través de la sección de delitos contra el robo de radio frecuencias, atiende los delitos relacionados con el robo de identidad y clonación de tarjetas.

La información pública emanada de dicha institución indica que no cuentan con una sección de delitos informáticos, dichos casos son atendidos en la fiscalía Metropolitana, es decir, se da cobertura a la ciudad capital.

Tabla No. 2

Reporte Estadístico de Denuncias en las Cuales se dé el hecho de Clonación de Tarjetas de Crédito o Debito de los años 2012, 2013 y al 24 de Noviembre de 2014 a Nivel Nacional.

	AÑO	TOTAL
Clonación de Tarjetas de Crédito	2012	4885
	2013	4118
	2014	3150
	Total General	12153

Fuente: Unidad de acceso a la información pública del Ministerio Público, Reporte estadístico de denuncias en las cuales se dé el hecho de Clonación de Tajetas de Crédito o Débito de los años 2012,2013 al 24 de noviembre del 2014. Guatemala 2014.

La clonación de una tarjeta de crédito o de débito se realiza con el fin de sustraer dinero de la cuenta de la persona a la que le fue robada su identidad, a través de

un dispositivo electrónico, que se aloja en la banda magnética o el *chip*de su tarjeta de pago.

Mediante una entrevista realizada a la auxiliar fiscal, encargada de la investigación de aproximadamente 1500 casos de clonación de tarjetas, pudimos determinar lo siguiente:

a. El Ministerio público no cuenta con equipo especial, capacitado y articulado para investigar y perseguir los delitos informáticos.

b. La ausencia de legislación apropiada no permite que se proceda de manera directa. Por ejemplo: explica el fiscal, no existe el delito de clonación de tarjetas, por lo que deberemos procesarle por; uso de información, asociación ilícita, falsificación, fraude de documentos, etc. Y probar cada una para que se haga justicia. Con esto queda atrás aquel dicho de que "en Guatemala no hay cárcel por deuda" pues si les comprueban alguno de éstos delitos, irán a la cárcel.

c. El personal de dicha sección del Ministerio Público desconoce si en otras fiscalías se atienden, también investigaciones por clonación de tarjetas y robo de identidad por dispositivos electrónicos.

d. No existe un protocolo de actuación para delitos informáticos en Guatemala.

Tabla No. 3

Reporte Estadístico de Denuncias en los Cuales se dé el Hecho de Clonación de Tarjetas de Crédito o Debito de los Años 2012, 2013 y al 24 de Noviembre de 2014 a Nivel Nacional.

ESTADO	AÑO			Total General
	2012	2013	2014	
EN INVESTIGACIÓN	580	848	921	2349
SENTENCIA	11	9	3	23
Total general	**591**	**857**	**924**	**2372**

Fuente: Unidad de acceso a la información pública del Ministerio Público, Reporte estadístico de Clonación de tarjetas del 2012 al 2014. CD-ROM. Guatemala 2014.

La tabla anterior describe que, por ejemplo, en el año 2013 se investigaron 848 casos de clonación de tarjetas. Ese mismo año se recibieron 4118 denuncias por clonación de tarjetas y en consecuencia Rodo de identidad mediante un dispositivo electrónico y se obtuvieron 9 sentencias.
Ni en el sistema de información, ni a través del sistema estadístico del Ministerio Público se orienta sobre los números que observamos. No se especifica si se agruparon en bandas criminales, si se desestimaron porque los usuarios recibieron su dinero de vuelta por parte de las aseguradoras y ya no “quieren perder su tiempo” en el proceso penal y juicio contra los delincuentes o qué número de bandas e integrantes se condenaron en las sentencias.

6.1.3 Instituto Nacional de Ciencias Forenses (INACIF)

El Instituto Nacional de Ciencias Forense de la ciudad de Guatemala, tiene como visión fortalecerse mediante la mejora continua de sus procesos, en una institución

del Sector de Justicia autónoma, independiente y confiable; que busca mediante el esfuerzo conjunto, servir a la sociedad guatemalteca en forma efectiva y eficiente en el ámbito de la investigación científico forense.
La misión, del INACIF, es convertir los indicios en elemento útil al Sistema de Justicia, mediante la realización de análisis técnico científicos en materia forense y estudios médico legalesapegados a la objetividad, transparencia y autonomía, fundamentados en ciencia o arte y basados en el trabajo en equipo[26].

Desde el 2012 cuenta con una sede en cada departamento de Guatemala (22 sedes), ´ésta no tiene cobertura en todos los municipios, sólo cabeceras y en algunos municipios de Guatemala como Mixco y Villa Nueva, por lo el acceso a la justicia, se ve interrumpido a menos que se traslade a las sedes. Los servicios que ofrece INACIF en la ciudad capital son:

- Reconocimientos Clínicos
- Reconocimiento médico forense
- Toma de muestras
- Levantamiento de indicios
- Reconocimientos Post mortem
- Necropsias medico legales
- Exhumaciones médico legales
- Reconocimietnos Psicológicos
- Reconocimientos Psiquiatricos
- Reconocimientos Odontológicos
- Reconocimientos Antropolígicos
- Balistica identificativa
- Balística informática
- Fisicoquímica
- Toxicología

[26]Misión del Inacif, Portal. http// www.inacif.gob.gt

- Sustancias Controladas
- Serología
- Hispatología
- Dactiloscopia
- Peritaje de Vehículos
- Impresiones de neumáticos y calzado
- Lingüística
- Acústica
- Reconstrucción de trayectorias
- Grafotécnia
- Impresiones y autenticidad de documentos y moneda
- Toma de muestras
- Embalaje y cadena de custodia.

Durante 4 años, desde su creación (2010) el Instituto Nacional de Ciencias Forenses ha sido fortalecido pobremente, la ejecución presupuestaria del año 2010 y 2011 es de 45%[27] denotando ineficiencia en el gasto y en consecuencia el recorte de presupuesto en futuros años, desde el Congreso de la Republica a través de la Comisión de Finanzas.

Sin embargo, los avances hasta hoy, no contemplan la implementación de unidades de peritaje para delitos informáticos y con ello el Robo de identidad mediante dispositivos electrónicos. Por lo que difícilmente se logra la prueba necesaria para juzgar y probar los delitos informáticos.

En Guatemala, si alguien necesita un peritaje para probar delitos informáticos lo deberá realizar en el ámbito privado.

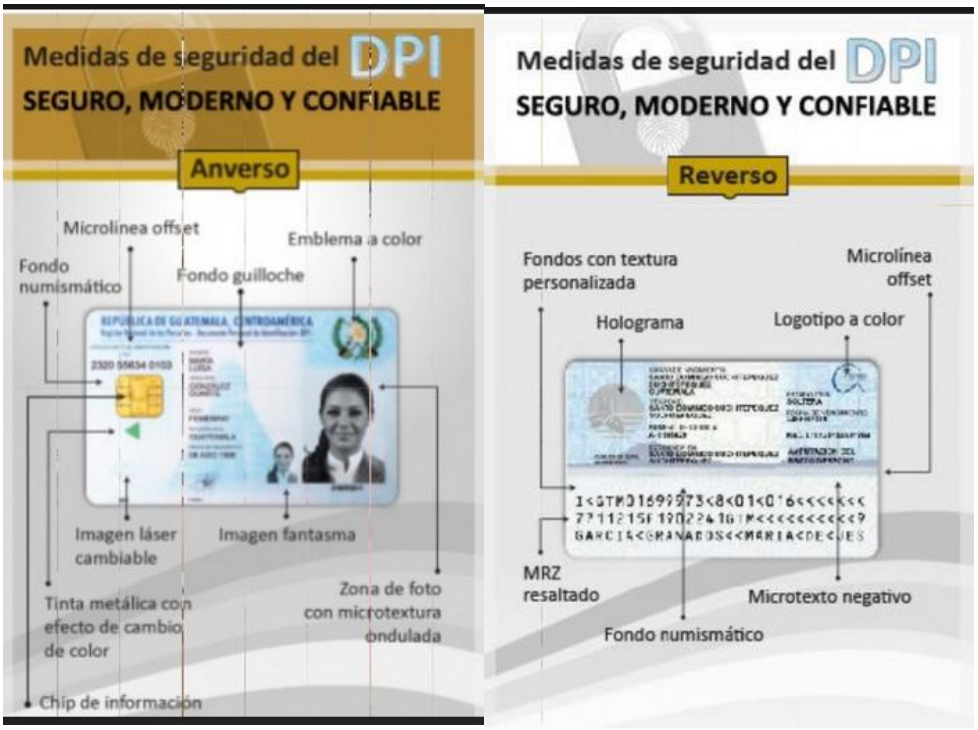
[27] Fundesa. Desafios actuales de la justicia penal. Asociación de investigación y estudios sociales. 2011

6.1.4 Registro Nacional de las Personas

La ley del Registro Nacional de las Personas regula la organización, funciones y obligaciones del Estado respecto del resguardo de información identificativa de sus ciudadanos.

El DPI, constituye el único Documento Personal de Identificación para todos los actos civiles, administrativos y legales, y en general para todos los casos en que por ley se requiera identificarse. Es también el documento que permite al ciudadano identificarse para ejercer el derecho de sufragio.

Medidas de seguridad del Documento Personal de Identificación: El portal electrónico del Renap informa sobre las siguientes medidas de seguridad del DPI



Registro Nacional de las Personas. (2015) *Medidas de seguridad del DPI*[Ilustración]. Recuperado de www.renap.gob.gt/medidas-de-seguridad-del-dpi

El banco el GyT Continental y el Banco Industrial tienen departamentos específicos de seguridad contra delitos informáticos, clonación de tarjetas y demás

delitos informáticos. Los bancos del Estado, el Banco de Desarrollo Rural, S.A y el Crédito Hipotecario Nacional

6.1.5 Asociación de Medios de Pago

Debemos mencionar a la Asociación de medios de pago, haciendo la salvedad de que no se trata de una organización del Estado, pero su relevancia al mencionarlo radica en la información que aglomeran con sus miembros.

Es la asociación que, derivado de miles de casos de clonación de tarjetas, ha creado los medios necesarios para tener acercamiento con las autoridades. La información que manejan los bancos consiste en; bases de datos con información sensible y privada de los usuarios, transacciones financieras con ubicación, establecimiento, monto y hora en que ocurren, dispositivos de seguridad (cámaras) de entidades bancarias, y otros.
El problema radica en que dicha asociación no proporciona la información al Ministerio Público, puede ser desconfianza y, manifiestamente, el secreto bancario del cual se escudan y también se protegen.

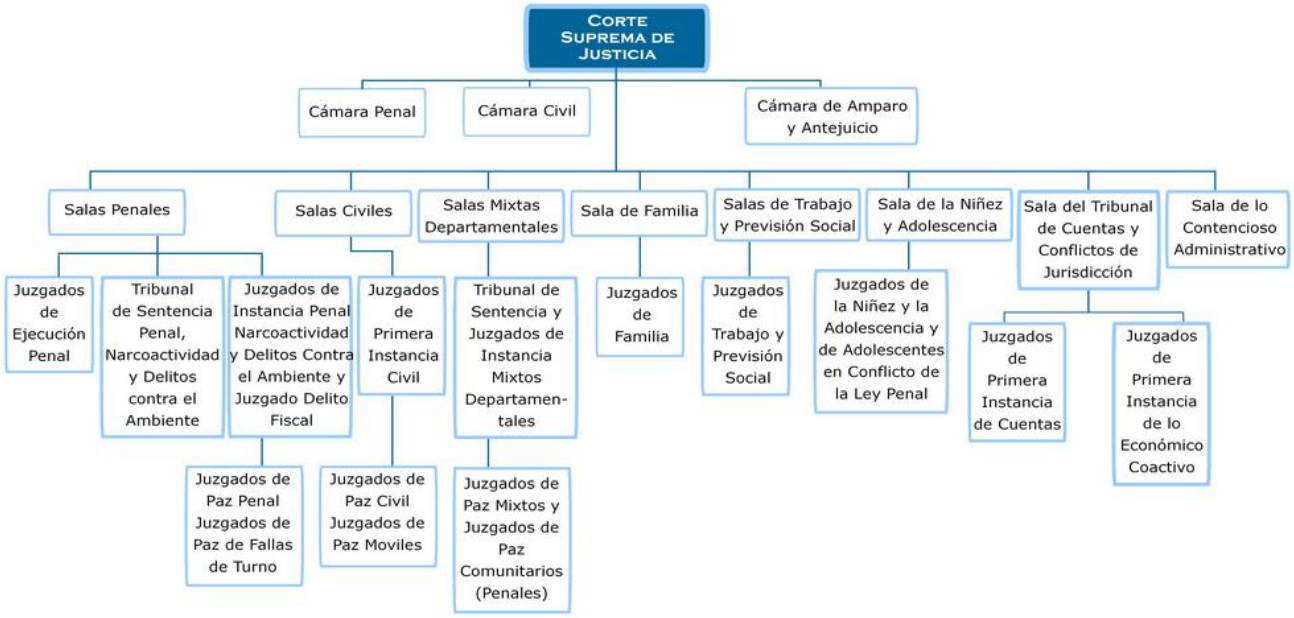
El hecho de que los investigadores no tengan acceso rápido y total de los movimientos que puede otorgar la asociación de medios de pago solo provoca;

- Trabajar más difícilmente el seguimiento de una investigación.
- Desperdicio de recursos del Estado.
- No se pueden identificar bandas criminales ya que se deberá investigar caso por caso, es decir individualmente los casos de clonación de tarjetas, por lo que llevará más tiempo concluir la investigación.

6.1.6 Organismo Judicial

Según la Constitución Política de la República el Organismo Judicial se encarga de impartir y juzgar,los actos u omisiones tipificados, a través de sus jueces y tribunales.

Organigrama organizacional del Organismo Judicial



Fuente: Unidad de Acceso a la Información del Organismo Judicial enviada por archivo electrónico por Licda. Eloisa Amelia Yoc Smith, Coordinadora de Estadística OJ

El organismo Judicial no posee juzgados especializados en el tratamiento de delitos informáticos, pero se han atendido y se tiene sentencia para bandas que se ocupan de realizar estos delitos.

Según información obtenida a través de la unidad de acceso a la información pública, no se tiene registro sobre si se ha recibido capacitación en manejo de delitos informáticos por parte de los jueces.

Si se piden datos sobre delitos informáticos (art. 274 Código Penal) en el interior de la república, responden que no tienen registros.

Tabla No.4

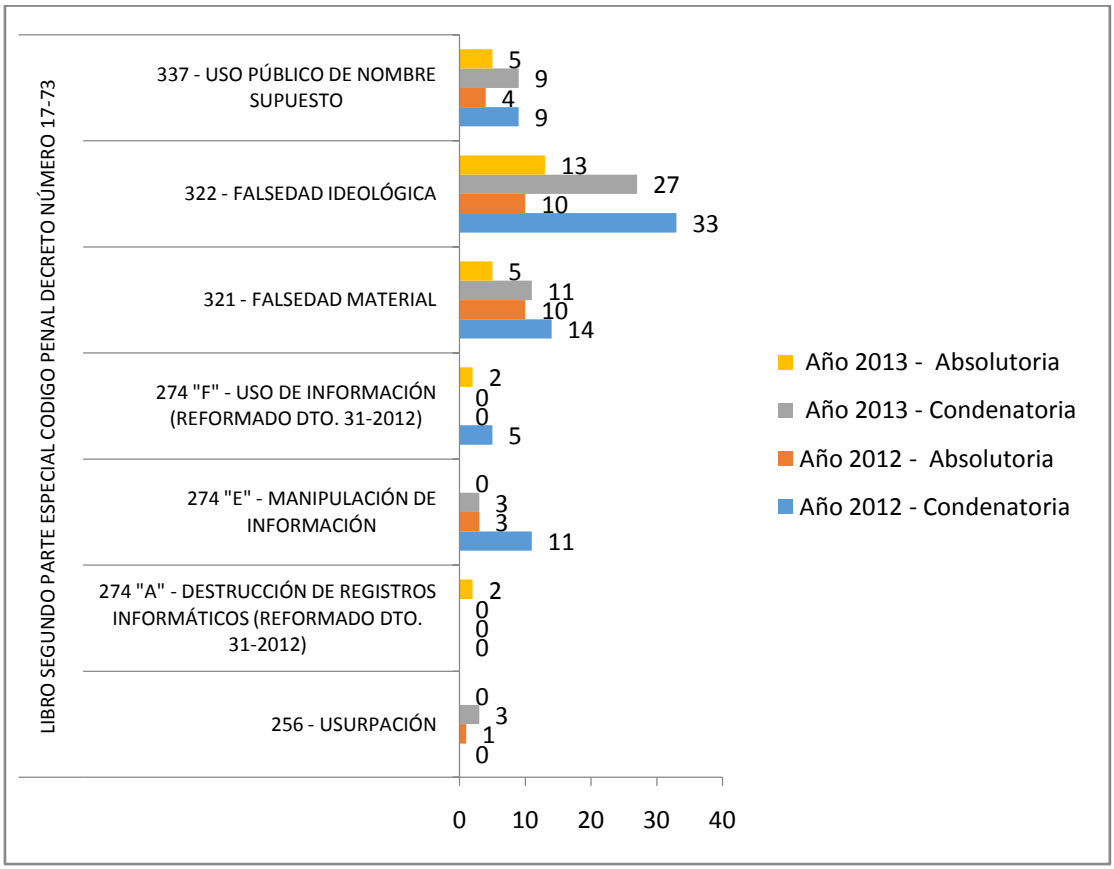
Casos de delitos cibernéticos con sentencia absolutoria o condenatoria del Organismo Judicial durante los años 2012 y 2013

Cantidad		TIPO DE SENTENCIA			
		Año 2012		Año 2013	
Ley	Articulo	Condenatoria	Absolutoria	Condenatoria	Absolutoria
LIBRO SEGUNDO PARTE ESPECIAL CODIGO PENAL DECRETO NÚMERO 17-73	256 - USURPACIÓN	0	1	3	0
	274 "A" - DESTRUCCIÓN DE REGISTROS INFORMÁTICOS (REFORMADO DTO. 31-2012)	0	0	0	2
	274 "E" - MANIPULACIÓN DE INFORMACIÓN	11	3	3	0
	274 "F" - USO DE INFORMACIÓN (REFORMADO DTO. 31-2012)	5	0	0	2
	321 - FALSEDAD MATERIAL	14	10	11	5
	322 - FALSEDAD IDEOLÓGICA	33	10	27	13
	337 - USO PÚBLICO DE NOMBRE SUPUESTO	9	4	9	5

Fuente: Unidad de acceso a la Información pública del OJ, Sentencias de Delitos Cibernéticos años 2012 y 2013, Archivo electrónico, Guatemala 2014. Licda. Eloisa Amelia Yoc Smith, Coordinadora de Estadística OJ.

Gráfica No. 2

Sentencias absolutorias y condenatorias sobre delitos cibernéticos del Organismo Judicial sobre delitos cibernéticos, años 2012 y 2014



Fuente: Unidad de acceso a la Información pública del OJ, Sentencias de Delitos Cibernéticos, Archivo electrónico, Guatemala 2014. Licda. Eloisa Amelia Yoc Smith, Coordinadora de Estadística OJ.

6.2 Coordinación Institucional

En la cadena de justicia, es imprescindible la buena coordinación interinstitucional. La correcta coordinación se incluye en las leyes y reglamentos de cada institución e indican, que sucedido un hecho delictivo, el Ministerio Público quien dirige la investigación, debe trabajar articuladamente con los investigadores de éstos delitos, en la Policía Nacional Civil.

Al suceder un delito, el investigador deberá recabar las pruebas necesarias y el Ministerio Público deberá requerir los peritajes necesarios para probar un hecho, al INACIF. Luego de que se recaban las pruebas, se procede a la formal acusación penal por parte del MP y éste caso entra al Organismo Judicial, en donde un juez determinará una sentencia. Es importante que se promueva la eficiencia y eficacia en la investigación de un hecho delictivo ya que para poder presentar un caso penal o civil se debe contar con la preparación y articulación previa de todos los sujetos involucrados.

6.3 Cómo se manejan los casos de robo de identidad en Guatemala:

1. Ya sea que el usuario de un dispositivo electrónico realice la denuncia a la Policía Nacional Civil, que luego traslada la denuncia al Ministerio Público, para su valoración o que la denuncia sea realizada directamente en el Ministerio Público, en ésta identidad se le dará el siguiente tratamiento.

2. Ingresa la denuncia a la Unidad de Decisión Temprana (UDT) en donde se determinará la relevancia del caso.

3. que luego trasladará a una agencia fiscal específica, mayoritariamente, la sección contra el robo de frecuencias radiales, ubicada en el zona 4 de la ciudad de Guatemala.

4. Una vez asignada la fiscalía que desarrolla la investigación el fiscal realiza los requerimientos al equipo de investigación de delitos económicos de la policía Nacional Civil detallando las diligencias a realizar.

5. La sección contra delitos económicos, en la DEIC (Dirección Especializada de investigación Criminal), realiza los requerimientos solicitados y recaba las pruebas que se detallan en un informe minucioso de actividades realizadas y sus resultados.

6. Seguidamente, el fiscal evaluará la solicitud ante el juez competente. Indican en el Ministerio Público que el Organismo Judicial no cuenta con juzgado especializado en delitos informáticos o similares. Sin embargo, luego de un proceso probatorio pertinente y exitoso se han logrado sentencias condenatorias exitosas y desarticulación de bandas.

6.4 FODA del Sistema de Seguridad y Justicia de Guatemala

A continuación identificaremos las fortalezas, oportunidades, debilidades y amenazas de las instituciones, operadoras de justicia, frente a los delitos tipificados en el Código Penal en el artículo 274 bajo el título de; “Destrucción de registros informáticos”, en Guatemala, que conforman el delito de Robo de identidad mediante dispositivos electrónicos.

Fortalezas

- Marco Legal establecido.
- El Plan Operativo se realiza anualmente, por lo que se puede presupuestar, en adelante, los renglones y el espacio presupuestario necesario para fortalecer el sistema de Justicia para los delitos relacionados a la destrucción de delitos informáticos que se utilizan como figura para conglomerar el Robo de Identidad, mediante dispositivos electrónicos en Guatemala.
- El gran desconocimiento de la mayoría de los usuarios de las vulnerabilidades pero así mismo de las ventajas u oportunidades que ofrecen los dispositivos electrónicos como fuente de información, hay un desconocimiento generalizado de la posibilidad de cometer dichos actos.
- Muchos países cuentan con experiencia que se puede trasladar a Guatemala para el adecuado tratamiento de los delitos, informáticos, que derivan en el robo de identidad de alguna persona.
- Existen manuales para el tratamiento de la evidencia, cadena de custodia y manejo de la prueba en casos de delitos informáticos. Es cuestión de voluntad el que se implementen a los funcionarios que trabajan dichos casos.

Oportunidades

- Existe un acuerdo Nacional para el avance de la seguridad y la justicia.
- Las universidades han implementado carreras sobre seguridad y justicia.
- Fortalecimiento a través de auditoria social, por parte de organizaciones de sociedad civil.
- Reingeniería y tecnificación de las instituciones.
- Firma de acuerdos interinstitucionales por los operadores de justicia.
- Implementación de nuevos y eficientes sistemas de control.
- Cooperación Internacional que traslade experiencia en el combate de los delitos contra los registros informáticos.

Debilidades

- Falta de capacitación de sus agentes policiales.
- Falta de Recursos.
- Falta de tipificación en nuestra legislación, sobre el robo de identidad mediante dispositivos electrónicos.
- Débil coordinación interinstitucional.
- Falta de Tecnificación de las instituciones de justicia para la persecución e investigación del robo de identidad mediante un dispositivo electrónico.
- Ausencia de políticas de informática y de seguridad de la información.
- Malos sueldos de los funcionarios de administración de justicia
- Las instituciones del Estado encargadas de la administración de justicia, ya sea la Policía Nacional Civil, el Ministerio Público, el Organismo Judicial, el INACIF, no cuentan con el presupuesto suficiente de inversión (aproximadamente 6% en promedio) por lo que la cobertura se implementará lentamente.
- El cambio de autoridades de gobierno no permite un carrera en materia de seguridad y justicia, en materia de dirección

- Falta de institucionalidad, pues aunque contamos con leyes, no se implementan a través de un presupuesto que garantice el adecuado desenvolvimiento de las funciones del estado en materia de Administración de Justicia.
- Débil articulación, dentro de las instituciones de administración de justicia, entre el plan operativo anual y su presupuesto.
- No existe la cultura de trabajo en equipo dentro de las instituciones, las encuestas dan cuenta de que los funcionarios de la administración justicia no se creen complementarios entre sí, sino rivales de competencia, pero increíblemente desproporcionados de herramientas.

Amenazas

- Tecnologías más avanzadas adquiridas por personas inescrupulosas que puede irrumpir o vulnerar dispositivos electrónicos.
- Falta de voluntad política para fortalecer las instituciones de justicia en el combate contra delitos informáticos.
- Impunidad.
- Crecimiento de delitos informáticos, derivado de la falta de tecnología y capacitación de los funcionarios que atienden los delitos informáticos que derivan en el robo de identidad.
- Falsificación de Documentos Personales de Identificación.
- Pérdida económica para ciudadanos, entidades bancarias o financieras y aseguradoras.
- Infiltración del crimen organizado dentro de las instituciones del Estado.
- Los operadores de justicia trabajan con agendas particulares y no cooperan entre sí, generado debilidad en la necesaria articulación.

6.5 Cómo integrar acciones para la prevención e investigación de delitos informáticos en Guatemala, para combatir el robo de identidad mediante dispositivos electrónicos.

A continuación se describirán mecanismos básicos para iniciar una ruta de fortalecimiento a las instituciones del Estado que deberán implementarse a través de las unidades pertinentes dentro de cada institución. Será necesaria la voluntad política de las autoridades principales de las instituciones operadoras de justicia y demás instituciones del Estado.

- Implementación de acciones, lineamientos, protocolos, comisiones específicas en la política criminal del Estado de Guatemala, para el combate de los delitos informáticos, para así garantizar el adecuado tratamiento de situaciones como el robo de identidad en Guatemala mediante dispositivos electrónicos.

- Conformación de una comisión multidisciplinaria para la formulación de un protocolo de actuación interinstitucional en casos de delitos relativos a la "Destrucción de Registros Informáticos" (delitos informáticos en general), integrada por:Policía Nacional Civil (PNC), Ministerio Público (MP), Instituto Nacional de Ciencias Forense (INACIF), Instituto de la Defensa Pública Penal (IDPP), Organismo Judicial (OJ), Banco de Guatemala, Registro Nacional de las Personas (RENAP), Instituto Nacional de Migración, Departamento de Tránsito, Superintendencia de Administración Tributaria (SAT), Intendencia de Verificación Especial (IVE), Secretaría Técnica del Sistema Nacional de Seguridad.

- Conformación de comisión, en alianza pública-privada, para la actualización de medidas de seguridad, en el sistema financiero y la banca. Dicha mesa debería estar integrada mínimamente por:

Jefe de la sección de investigación encargada de la investigación de los delitos relativos a la destrucción de registros informáticos.
Representante de la Asociación de Medios de Pagos.
Representante de Seguridad de Agencias Bancarias del sistema.

- Debe existir un protocolo, dentro de la Policía Nacional Civil y el Ministerio Público, para el embalaje de los dispositivos electrónicos en un comiso, allanamiento, etc.

- El INACIF debe implementar el departamento de peritaje de dispositivos electrónicos, para identificar y luego probar que dicho dispositivo se utilizó para la comisión de un delito. Esta sección de peritaje puede implementarse igualmente en la Policía Nacional Civil toda vez se tenga un protocolo de actuación y la debida cadena de custodia, necesaria para probar en un juicio, la implicación de un dispositivo como prueba de un delito.

- Integración en el Plan Operativo Anual de las instituciones de la administración de justicia que se articulan en casos de delitos informáticos que derivan en el Robo de Identidad. La implementación de unidades especializadas, debidamente equipadas y con suficiente personal capacitado para atender éstos casos.

- Coordinación estrecha, por parte de las instituciones del Estado encargadas de la administración de la justicia con el Registro Nacional de las Personas, RENAP y acceso a las bases de datos, de forma remota, con la autorización del Ministerio Público, para evitar pérdida de tiempo de los agentes en gestionar los datos. La tecnología apropiada garantizará el adecuado control de los operadores de justicia respecto de ésta información sensible.

- Campañas de comunicación informando al usuario de dispositivos electrónicos, de los peligros que enfrentan como potenciales víctimas del robo de identidad. Campañas de prevención e información.

- Controles de verificación en Instituciones públicas como el Registro Mercantil, etc. Existen dispositivos que corroboran la identidad de las personas en línea.

- Actualización tecnológica de dispositivos, de identificación (DPI, licencias, carnets) que posean chip y clave de identificación única para que se proceda a su inhabilitación al momento de denunciar su robo o pérdida. Esto ayudará a identificar qué uso se le quiere dar a los dispositivos una vez que son hurtados o robados.

- Mediante la normativa necesaria, obligar a las empresas de servicios o fabricantes de dispositivos a implementar medidas de seguridad básicas, ya que los equipos nuevos deberían incluirlo. En otros países, el Estado, obliga a dichas empresas a sostener medidas de protección.

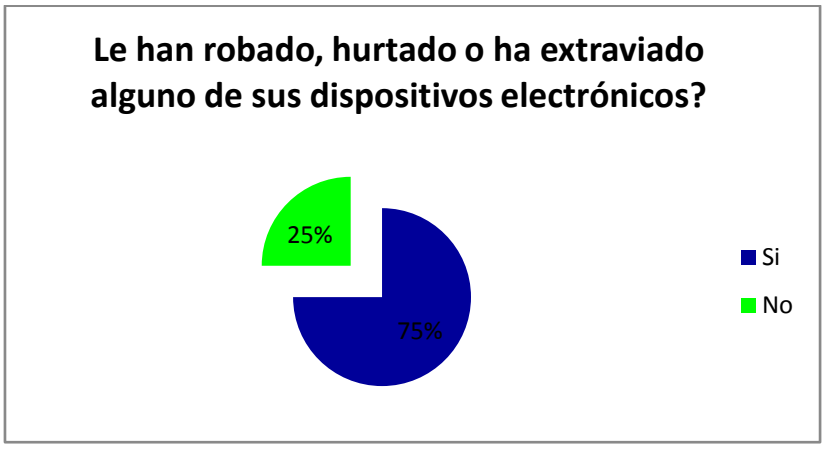
6.6 Resultados de las Encuestas a usuarios de dispositivos electrónicos en Guatemala.

A continuación se presentan los resultados de las encuestas realizadas a los sujetos de ésta investigación sobre el fenómeno del robo de identidad mediante dispositivos electrónicos en Guatemala**.**

Conoce la población la vulnerabilidad de los dispositivos?

Gráficas. No. 3

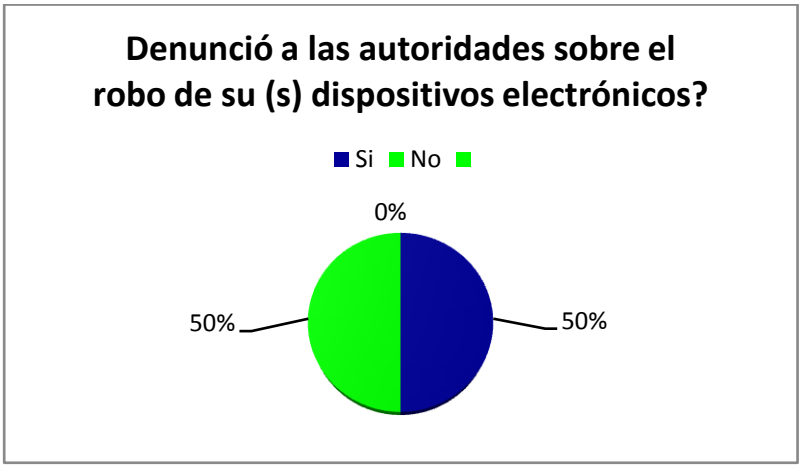
Encuesta de victimización



El 75% de los entrevistados ha sufrido el robo o el hurto de su(s) dispositivo electrónico

Gráfica No. 4

Encuesta a usuarios de dispositivos electrónicos

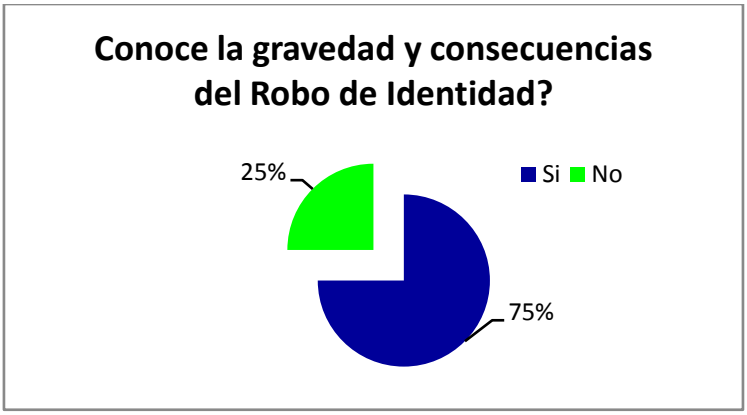


El 50% de las personas que sufrieron del robo o hurto de su dispositivo móvil, lo denunció a las autoridades policiales o Ministerio Público. El otro 50% no realizó ninguna denuncia

Encuestas a Usuarios de Dispositivos Electrónicos:

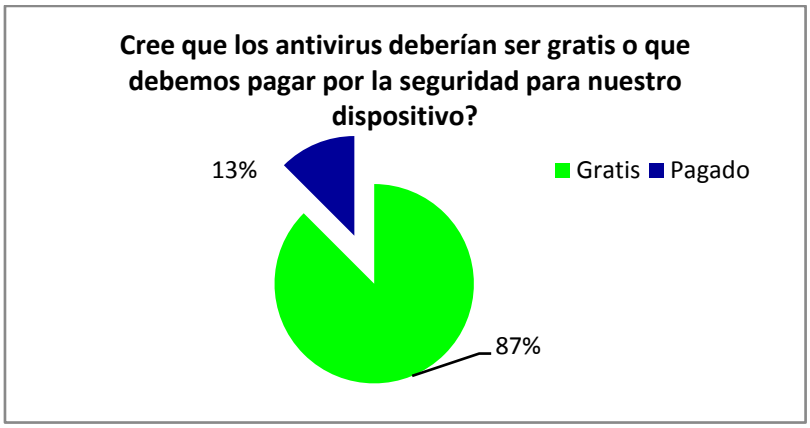
Gráfica No. 5

Encuesta realizada a usuarios de dispositivos electrónicos



Gráfica No. 6

Encuesta realizada a usuarios de Dispositivos electrónicos



El 87% de los encuestados opina que los antivirus deberían ser gratis para los dispositivos electrónicos, ya que ellos adquieren el dispositivo nuevo y, éste, debería incluir el mecanismo de seguridad que resguarde sus datos.

La encuesta también arroja como resultado que el 100% de los entrevistados ha pasado por un evento de destrucción de información en su dispositivo por virus.

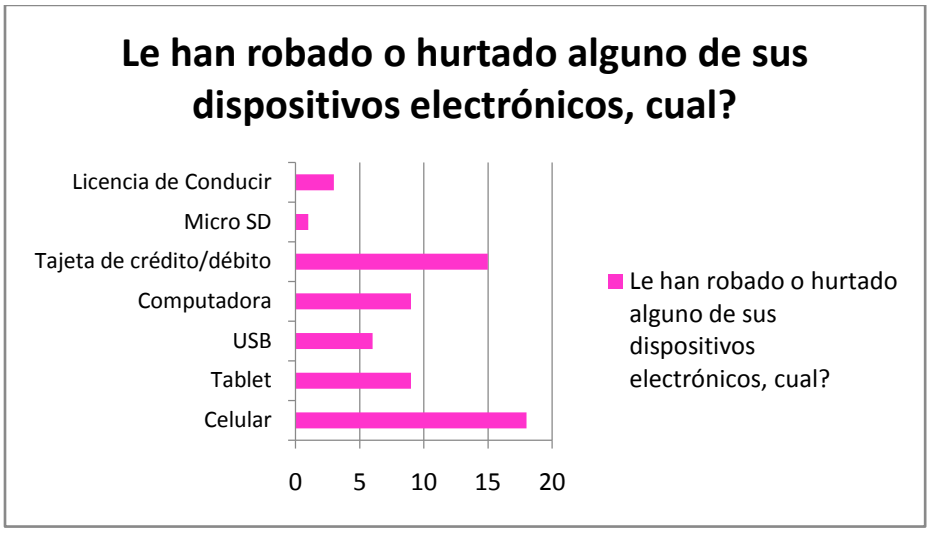
Asi mismo, el 100% de los encuestados como usuarios de dispositivos electrónicos opina que las autoridades no le dan la importancia necesaria al problema del Robo de Identidad que puede sufrir una persona al perder (que le roben o hurten) sus dispositivos electrónicos.

6.7 Resultados de la Encuestas a profesionales del derecho sobre el delito de robo de identidad mediante dispositivos electrónicos.

Encuestamos a veinticuatro profesionales del derecho que litigan en cualquiera de los ámbitos legales; el penal, mercantil o civil en la ciudad capital

Gráfica No. 7

Encuesta realizada a profesionales del derecho



Ante la pregunta “Le han robado o hurtado algún dispositivo electrónico, el 100% de los profesionales del derecho que ejercen en diferentes ámbitos pero que se dedican a litigar, contestó que sí. El teléfono celular es el dispositivo que más se ve afectado, o más es cotizado por los delincuentes. De veinticuatro encuestados, a dieciocho le robaron el celular, es decir, al 75% de los entrevistados. El dispositivo que le sigue es la Tarjeta de crédito o débito con 62% de entrevistados afectados en su patrimonio y por consiguiente en los datos que se manejaban en cada dispositivo.

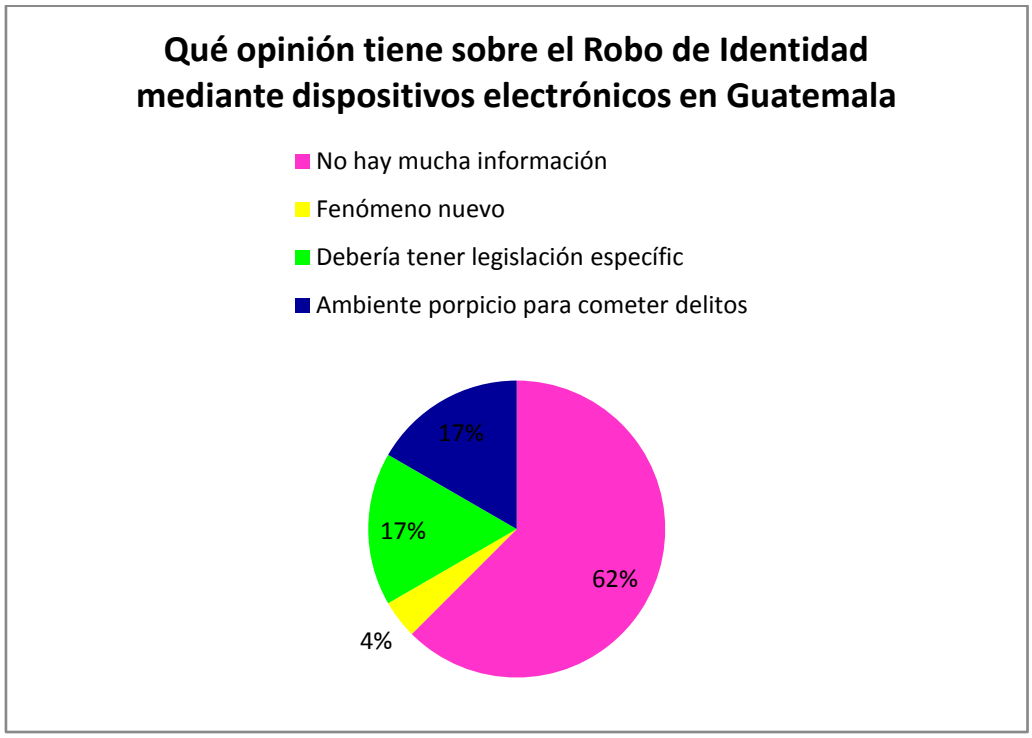
Cuando le preguntamos a los profesionales del derecho si habían realizado la denuncia a la Policía Nacional Civil o el Ministerio Público, el 50% de ellos no realizó la denuncia, dentro de algunas razones se encuentran; Las autoridades no

tienen como investigar estos delitos, sólo es un requisito para recuperar la línea de teléfono celular, puede representarles perder su tiempo.

Encuestas realizadas a profesionales del derecho sobre manejo de casos de robo de identidad:

Gráfica No. 8

Encuesta a profesionales del derecho sobre casos de Robo de Identidad



El 62%de los entrevistados manifiesta que no hay información sobre los delitos informáticos, tanto para el usuario en el uso y cuidado de sus datos, como en los profesionales del derecho. El 17% opina que debería tener legislación específica y el 4% que se trata de un fenómeno nuevo, del que no se tiene información y se conoce muy poco.

De los profesionales del derecho encuestados, solamente uno tiene más de doscientos casos de robo de identidad mediante dispositivos electrónicos, dos de ellos tienen tres casos y uno de ellos lleva dos, en promedio, por año. Todos relacionados a la clonación de tarjetas de crédito o débito.

6.8 Fenómeno Criminal del Robo de Identidad mediante dispositivos electrónicos en Guatemala.

- En su relación jurídica:

  En cuanto a la relación jurídica del fenómeno del robo de identidad, en Guatemala se tipifica a través del artículo No. 274 del Código Penal, bajo el título de “Destrucción de registros informáticos” en los que se describen en los incisos de la A a la G, siete modalidades de delito informático.
  Aunque se encuentra tipificado, institucionalmente no se ha fortalecido al Estado para el combate de dichos delitos. Las instituciones no tienen personal capacitado, presupuesto asignado a secciones especializadas (los delitos informáticos requieren de especialización)

- En su relación individual:

  El usuario de dispositivos electrónicos en Guatemala adquiere todos los dispositivos sin ningún programa de seguridad que resguarde los datos o información que se tendrán en dicho dispositivo.
  Además, no hay campañas de comunicación sobre los peligros del robo de identidad mediante algún dispositivo electrónico.
  Las empresas fabricantes de dispositivos tienen información sobre medidas de seguridad en sus páginas de internet, por lo que recibirán orientación y ayuda, los que tengan acceso a internet.

- En su relación social:

  La dinámica en la que se desenvuelve a sociedad guatemalteca, es de innovación y procesos de tecnificación, que aunque son más lentos que en otros países, el nivel de desconocimiento de la población sobre los peligros de manejar información en dispositivos que no la aseguran es una de las situaciones que preocupa a muy pocos. El experto consultado indica que el robo de identidad no discrimina a nadie. Cualquier persona que pierda sus dispositivos y contenga información, que carezca de seguridad o que sea manipulado mediante ingeniería social puede ser víctima del robo de la identidad.

  La ingeniería social, que es el arte de que una persona manipule un entorno para lograr lo que quiere ha sido elemental para cometer delitos informáticos.

  El Estado no se tecnifica, no se capacita y no informa de los peligros de la tecnología por lo que vulnera la seguridad de los ciudadanos.

  Los dispositivos electrónicos son esenciales para lograr comunicación y cualquier empresario debe disponer de un celular para poder tener más alcances.

CONCLUSIONES

1) En Guatemala se encuentran tipificados los delitos relativos a la destrucción de registros informáticos que componen varias modalidades de crimen como el robo de identidad mediante dispositivos electrónicos y que, en su mayoría, derivan en la clonación de tarjetas de crédito o débito para obtener un beneficio económico. Esta tipificación es suficiente para que, en un proceso penal, se compruebe la comisión de dichos delitos. Sin embargo, el Estado estará ausente respecto de la violación a la intimidad, de la acción de apropiación indebida de fondos monetarios ajenos, pues no se especifica en ninguna parte del Código Penal, aun así se logran penas de prisión.

2) Cuando hay consecución de delitos que derivan en el robo de identidad mediante dispositivos electrónicos con el fin de reproducir sus datos financieros, afectándoles económicamente, pero que son resarcidos antes del juicio, la víctima, pierde el interés por continuar la búsqueda de justicia y el castigo del delincuente. Según el jefe de la sección de delitos económicos de la Dirección Especializada de Investigación (DEIC) de la Policía Nacional Civil, sólo se obtiene denuncia y declaración escrita del afectado. Esta situación afecta el proceso de repartición de justicia.

3) El Ministerio Público, la Policía Nacional Civil y el Organismo Judicial proporcionaron estadísticas sobre delitos informáticos que implican el robo de identidad de una persona mediante dispositivos electrónicos, sin embargo, no coinciden, denotando la ya conocida falta de homogenización en los datos.

4) La extraterritorialidad que puede acompañar un delito informático, como el robo de identidad de una persona a través de un dispositivo electrónico,

tipificado en Guatemala mediante el artículo 274 del Código Penal, hace necesaria la capacitación de la interpol en Guatemala, pero sobre todo se debe ser específico en cuanto a las penas y jurisdicción.

5) La PNC tiene cobertura en la mayor parte del país, no sucede igual con el órgano encargado de la investigación, ni el que administra la justicia. La falta de cobertura, en el interior de la República, denota una deficiencia en cuanto al cumplimiento del principio constitucional de acceso a la justicia, pues el delito de Robo de Identidad, ya sea que se enmarque dentro de la falsificación ideológica, la usurpación, la destrucción de registros informáticos, manipulación de información, falsedad material, falsedad ideológica y uso público de nombre supuestopuede investigarse de manera óptimasólo, a nivel de la ciudad capital.

6) El Estado no está preparado para el abordaje del fenómeno de los delitos informáticos y en consecuencia contra el robo de identidad mediante dispositivos electrónicos. Esto se refleja en la ausencia de presupuestos de tecnificación y prevención.

7) Debido a que en el Congreso de la República no se han realizado las modificaciones pertinentes relacionadas con el secreto bancario, ésta se constituye como el principal obstáculo, para los investigadores, ya que en muchos casos no tienen acceso a cuentas bancarias para poder realizar análisis de flujo de dinero en delincuentes.

8) La falta de tecnología es un valladar para la Policía Nacional Civil, el INACIF y Ministerio Público.

9) En toda la República de Guatemala no se requieren peritajes, de delitos informáticos, al INACIF ya que no cuentan con una unidad capacitada para desarrollarlos.

10) El Estado de Guatemala es vulnerable a la destrucción o alteración de registros informáticos, provocando un ambiente de impunidad.

11) La falta de un protocolo de actuación, entendido como un conjunto de procedimientos específicos establecidos en un plan, en casos de delitos informáticos dificulta la labor investigativa y probatoria de las instituciones ya que no se da un adecuado embalaje de los indicios, no hay un resguardo efectivo de la cadena de custodia y con esto, se dificulta el éxito probatorio ante los tribunales o el juez.No se procuran medios de prueba pertinentes, eficientes y efectivos

12) Los funcionarios públicos en la Policía Nacional Civil, encargados de la investigación de delitos informáticos y los fiscales el Ministerio Público, consideran que se tiene mala coordinación y comunicación entre las instituciones mismas.

13) Derivado de que en Guatemala, el Código Penal en el artículo 7 prohíbe la aplicación del principio de analogía en materia penal para tipificar un delito, es necesario tener una tipificación específica.

RECOMENDACIONES

1. Se debe tipificar como figura delictiva, propia de estos delitos, la sustracción monetaria que tiene lugar como consecuencia del robo de su identidad mediante un dispositivo electrónico, pues estas acciones se realiza, en su mayor parte, con el objetivo de tomar dinero de otra persona sin que ésta se entere.

2. Las instituciones de justicia, Ministerio Público, Policía Nacional Civil y el Organismo Judicial, deben realizar un acuerdo de coordinación, con las diversas entidades que prestan servicios financieros, electrónicos y de comunicación, para perseguir eficazmente y ponerle fin a estos delitos, sin la cooperación de las antes mencionadas no se puede garantizar el verdadero combate del delito, ya que las mismas poseen bancos de datos personales.

3. Crear un sistema electrónico centralizado que recopile datos de la PNC, del MP y del OJ al cual tengan acceso los investigadores y público en general para así, crear estrategias de fortalecimiento a las instituciones y prevención de estos delitos.

4. Derivado de la sofisticación y los avances tecnológicos, los crimines pueden trascender fronteras por lo que debe fortalecerse el intercambio de experiencias y esfuerzos de investigación con otros países.

5. Un incremento en el presupuesto otorgado a la Dirección Especial de Investigación Criminal de la Policía Nacional Civil y la capacitación adecuada de los funcionarios de justicia respecto de la necesidad de

prevenir e investigar estos delitos a nivel regional para colaborar con los ciudadanos en el acceso a la justicia.

6. Existe falta de información y conocimiento sobre la incidencia de este delito y los montos altos que se defraudan, por lo que deberá cuantificarse el impacto real que tiene sobre la economía individual y colectiva para que se asignen recursos suficientes para trabajar en la prevención de dichos delitos y la adecuada investigación.

7. Aunque sería deseable que se modifique el Secreto Bancario, es posible que mediante la emisión de órdenes judiciales se puede acceder a la informaciónbancaria de sujetos investigados.

8. Incluir dentro de los Planes Operativos de las instituciones del Estado, encargadas de la administración de justicia, de bancos de datos, entidades financieras del Estado y otras, programas de seguridad contra delitos informáticos que protejan la información que administran. Dichos renglones deberán tener aumentos progresivos para el fortalecimiento tecnológico de las instituciones que, especialmente, tienen directamente relación a la investigación de los delitos informáticos.

9. Fortalecer al INACIF de manera tal que tenga capacidad de realizar peritajes relacionados con delitos informáticos o promover el convenio con alguna institución privada que los realice y que se pueda incluir como prueba. Seguidamente informar a la población sobre éste servicio y así puede utilizarse como prueba pertinente.

10. Fomentar el fortalecimiento de la seguridad de los sistemas informáticos de las instituciones de justicia y bancos de datos para que no sean susceptibles de alteración por parte de intrusos u operadores del mismo sistema en detrimento de la verdad sobre cualquier hecho o dato.

11. Capacitar a los investigadores de la Policía para que puedan implementar un protocolo de actuación policial en casos de Delitos informáticos y que, dicho protocolo, sea socializado con los fiscales del MP para garantizar las pruebas en estos casos.

12. Mejorar la comunicación entre los funcionarios de justicia a través de una mesa de coordinación interinstitucional, con reuniones periódicas y un plan de trabajo, para promover desde ahí, el conocimiento de estos delitos y su prevención.

13. Es necesario promover ante el Congreso de la República la inclusión de delitos informáticos como la Clonación de tarjetas para que se pueda juzgar de manera justa a estos delincuentes.

REFERENCIAS

Referencia Bibliográfica

Andrew, A (1999) *Crimes related to the computer network. Threats and opportunities: a criminological perspective*.Helsinki, Finlandia.

De Miguel Asencio, P.A (2002), *Derecho Privado de Internet,* 3ra. Edición, España, Civitas

Enciclopedia CCI, (2010), *Manual de investigación policial, procedimientos y técnicas científicas, tomo III de investigación*.. Primera edición, página 1195, Sigma Editores. Colombia.

Francesc Canals, (2008).*El libro rojo del cibercrimen*,Barcelona, España.

Furnell, S. (2002) Cybercrime. *Vandalizing the information society*. Addison Wesley. London, London.

Gòmez, S. Perito informàtico Oficial. *Actuaciones en delitos informáticos,* Madrid España.

Hadnagy, C. (2011), *Ingeniería Social el arte del hacking personal*. 1ra. Edición. Estados Unidos, Editorial Anaya..

Osterburg, J. y Ward, R. (2000), *Criminal investigation*. 3erd. Edition. Anderson Publishing Co.Ney York city, United States.

Reyes Calderón, J.C. (1997). *Seguridad Bancaria 2000*. Primera edición, México, Cárdenas editor.

Téllez Valdez, J. (2005), *"Derecho Informàtico*", 3ra. Edición, México. Editorial Mc Graw Hill.

Tiedemann, Klaus,(1985)*Poder informático y delito*, Barcelona, España.

Referencia electrónica

Criptored. Acurio del Pino, S.M. *Manual de manejo de evidencias digitales y entornos informáticos.* Diciembre de 2009.www.criptored.upm.esFecha de Consulta: Enero del 2014

Justice, Minister of public safe an emergency preparadness Canada and the Attorney General of the United States, *Report on Pishing*, October 2006. http://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf Fecha de consulta: Enero del 2014

Software Engineering Institute*,* Friedberg, R. *What is Network Situational Awareness*www.cert.orgFecha de consulta: Enero del 2014

Delitos Informáticos, García Nogera, N. Gallo Ruiz, G. Curvo Gonzalez, O.*Uso fraudulento de tarjetas bancarias,*Noviembre 2003. http://www.delitosinformaticos.com/estafas/estafa_tarjeta.shtml Fecha de consulta: Enero del 2014

Carrier Brian, D. Dr. *Basic Digital Forensic Investigation Concepts,* June 2006 http://www.digital-evidence.org/di_basics.htmlFecha de Consulta: Enero del 2014

Carrier Brian, D. Dr.Defining *Digital Forensic Examination and Analysis Tools*, August 7, 2002 http://www.digital-evidence.org/papers/dfrws_define.pdfFecha de Consulta: Enero del 2014

FBI en español, *Los delitos cibernéticos más recientes*,https://www.fbi.gov/espanol/historias/los-delitos-ciberneticos-mas-recientesconsultado en: Enero del 2014

Referencia del Marco Legal

Código Penal de Guatemala, Decreto 4-2010 Reforma al Código Penal, Diario de Centroamérica, Guatemala 2010.

Constitución Política de la República de Guatemala Reformada en Acuerdo legislativo No. 18-93, Diario de Centroamérica, Guatemala 1993 .

Ley de equipos terminales móviles.Decreto 8-2013, Diario de Centroamérica, Guatemala, 2013.

Ley De La Policía Nacional Civil Decreto Número 11-97, Diario de Centroamérica, Guatemala, 1997.

Ley Marco del Sistema Nacional de Seguridad de Guatemala, Decreto 18-2008, Diario de Centroamérica, Guatemala, 2008.

Organización Y Designación De Funciones De La División Especializada En Investigación Criminal Subdirección General De Investigación Criminal De La Policía Nacional Civil .Orden General No. 12-2009. Diario de Centroamérica, Guatemala, 2009.

Régimen Interior De La Academia De La Policía Nacional Civil De Guatemala Acuerdo Ministerial No. 299-97. Diario de Centroamérica, Guatemala, 1997.

Reglamento Disciplinario De La Policía Nacional Civil Acuerdo Gubernativo Número 420-2003. Diario de Centroamérica, Guatemala, 2003.

Reglamento De Organización De La Policía Nacional Civil Acuerdo Gubernativo No. 662-2005, Diario de Centroamérica, Guatemala, 2005.

Reglamento Del Sistema De Clasificación De Cargos O Puestos Y Remuneraciones De La Policía Nacional Civil Acuerdo Gubernativo Número 409-2006. Diario de Centroamérica, Guatemala, 2006.

ANEXOS

Modelos de Instrumentos

BOLETA DE RECOPILACIÓN DE DATOS DE EXPEDIENTES

TESIS DE LICENCIATURA: ROBO DE IDENTIDAD MEDIANTE MEDIOS ELECTRÓNICOS EN GUATEMALA. UNIVERSIDAD RAFAEL LANDÍVAR, FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ESTUDIANTE: MARISOL ZEA WELLMANN
CARNE:2407907

MODELOS DE INSTRUMENTO

Modelo de Encuesta 1

Diseñada para público usuario de dispositivo electrónico

¿Es Ud. Usuario de dispositivos electrónicos?

¿Cuáles?:

- Celular
- Dispositivo móvil (ipad) (android)(tablets)
- USB
- Correo Electrónico
- Otros:

¿Sabe usted lo que es el Robo de identidad?

¿Se le ha extraviado a usted la cédula de vecindad o el documento de identificación personal?

¿Cuando alguien le solicita sus datos de identificación, usted pregunta con qué fin necesitan esos datos?

¿Ha presentado la denuncia al Ministerio Público o a la Policía Nacional Civil?

¿Conoce usted la gravedad y las consecuencias del robo de Identidad?

¿Cree usted que las autoridades le dan la suficiente importancia al delito de robo de identidad, si ni siquiera está tipificado?

¿Considera que es necesario que se le dé la importancia necesaria al delito de Robo de Información?

¿Alguna vez ha suministrado información personal (de carácter confidencial) por teléfono, como parte de una encuesta u otras?

BOLETA DE RECOPILACIÓN DE DATOS DE EXPEDIENTES

TESIS DE LICENCIATURA: ROBO DE IDENTIDAD MEDIANTE MEDIOS ELECTRÓNICOS EN GUATEMALA. UNIVERSIDAD RAFAEL LANDÍVAR, FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ESTUDIANTE: MARISOL ZEA WELLMANN
CARNE:2407907

Modelo de Encuesta 2

Dirigida a profesionales del Derecho.

¿Le han robado o hurtado algún dispositivo electrónico?

Si

No

Cuáles?

¿Cuantas denuncias se han presentado en su despacho derivado del robo de identidad?

¿Ha escuchado incidentes sobre el robo de identidad en su medio?

¿Cree usted que se investigan lo suficiente éstos casos?

¿Conoce de alguna persona que haya sido sentenciada por el delito de Robo de Identidad?

¿En su condición de profesional, le han suplantado alguna vez la firma?

¿Cree usted que es necesaria la tipificación del delito de Robo de Identidad en Guatemala?

¿Cree que el delito de Uso de Información abarca, en cuanto a tipificación y castigo, el fenómeno del Robo de Identidad?

¿Cree usted que debería sancionar con penas más rigurosas?

BOLETA DE RECOPILACIÓN DE DATOS DE EXPEDIENTES

TESIS DE LICENCIATURA: ROBO DE IDENTIDAD MEDIANTE MEDIOS ELECTRÓNICOS EN GUATEMALA. UNIVERSIDAD RAFAEL LANDÍVAR, FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ESTUDIANTE: MARISOL ZEA WELLMANN
CARNE:2407907

MODELO DE ENCUESTA No. 3

Encuesta de Víctimización dirigida a víctimas de Robo de Identidad

¿Hace cuánto tiempo fue víctima de robo de identidad?

¿Sabe a través de que medio consiguieron sus datos personales?

¿Cree que los legisladores deberían incluir el delito de robo de Identidad en la legislación guatemalteca?

¿Cree que el Estado debe brindar información al respecto de los peligros del robo de información importante?

¿Su caso fue asignado a alguna fiscalía, a cuál?

BOLETA DE RECOPILACIÓN DE DATOS DE EXPEDIENTES

TESIS DE LICENCIATURA: ROBO DE IDENTIDAD MEDIANTE MEDIOS ELECTRÓNICOS EN GUATEMALA. UNIVERSIDAD RAFAEL LANDÍVAR, FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ESTUDIANTE: MARISOL ZEA WELLMANN
CARNE:2407907

MODELO DE ENTREVISTA No. 1

Dirigida al investigador en Jefe del delito de Robo de Identidad, por medio de dispositivos electrónicos, sección de investigación de delitos económicos de la Dirección Especial de Investigación Criminal, de la Policía Nacional Civil, de la ciudad de Guatemala, Departamento de Guatemala

Entrevista a Jefe de sección de Investigación

1-¿Cuál es la cobertura de la división? ¿Qué delitos? ¿Cuánto personal tiene?
2-¿Cuentan con presupuesto designado?
3-¿Qué capacitación recibe un agente investigador de esta sección?
4- ¿Cuántas denuncias reciben, al día, de casos de robo de identidad?
5- ¿Cuántas de estas denuncias fueron de, delitos de robo de identidad, concretados a través de dispositivos electrónicos?
6- ¿Qué tipos de dispositivos se utilizan para concretar el robo de identidad?
7- ¿Cuál es el dispositivo más popular o más vulnerable?
8-¿Cuentan con protocolo de actuación, para casos de delito de robo de identidad, cuál es?
9-¿Cuáles son sus avances?
10- ¿Con qué instituciones coordinan y de qué manera?

11- ¿Tienen algún tipo de coordinación con abogados privados o individuales, representantes legales o sujetos jurídicos que intercedan por casos de robo de identidad?

12- ¿Cuáles son los desafíos de la sección?

13-¿Qué tecnología poseen para investigar estos delitos?

14- ¿Cuántos casos, sobre robo de identidad mediante dispositivos electrónicos, maneja cada agente investigador?

15- ¿Cuál es el delito al que se le da prioridad, ya sea institucionalmente, presupuestariamente o por cooperación internacional?

16- ¿Hay algún sector que se vea más afectado por el delito de robo de identidad en Guatemala? ¿Qué características reúnen las víctimas?

17- Como calificaría la relación de coordinación de dicho delito con el Ministerio Público? Excelente Buena Regular Mala

18- Como calificaría la relación de coordinación de dicho delito con el Organismo Judicial? Excelente Buena Regular Mala

19- Qué nivel de seguridad deberían ofrecerle al usuario las empresas de comunicación, respecto de sus datos?

BOLETA DE RECOPILACIÓN DE DATOS DE EXPEDIENTES

TESIS DE LICENCIATURA: ROBO DE IDENTIDAD MEDIANTE MEDIOS ELECTRÓNICOS EN GUATEMALA. UNIVERSIDAD RAFAEL LANDÍVAR, FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ESTUDIANTE: MARISOL ZEA WELLMANN
CARNE:2407907

MODELO DE ENTREVISTA No. 2

Dirigida a investigador encargado de delitos de Robo de Identidad por medios electrónicos, de la sección de investigación de delitos económicos de la Dirección Especial de Investigación Criminal, de la Policía Nacional Civil, de la ciudad de Guatemala, Departamento de Guatemala

Que debe hacer una persona para denunciar el robo de su identidad?

¿Cuál es el horario, los turnos, en ésta sección de investigación de delitos económicos?

¿Cuál es su grado en la PNC?

¿Cuál es su grado académico?

¿En qué consiste su labor?

¿Qué diligencias realiza?

¿Cuántos casos se atienden por turno?

¿Cómo describiría su coordinación con el Ministerio Público, éste le aporta la apertura necesaria para agilizar los casos?

¿Cuál es el delito al que se le da prioridad?

¿Cuántos casos manejan por cada investigador?

¿Hay algún obstáculo, técnico, metodológico, legal, etc. que impida que cumplan su labor investigativa?

¿Cómo calificaría la coordinación con el Ministerio Público? Excelente.Buena.Regular. Mala

BOLETA DE RECOPILACIÓN DE DATOS DE EXPEDIENTES

TESIS DE LICENCIATURA: ROBO DE IDENTIDAD MEDIANTE MEDIOS ELECTRÓNICOS EN GUATEMALA. UNIVERSIDAD RAFAEL LANDÍVAR, FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ESTUDIANTE: MARISOL ZEA WELLMANN
CARNE:2407907

MODELO DE ENTREVISTA No. 3

Dirigida a auxiliar fiscal encargado de delitos de Robo de Identidad por medios electrónicos, del Ministerio Público, de la ciudad de Guatemala, Departamento de Guatemala

Cuantas denuncias han recibido sobre robo de identidad en la ciudad?

Cuántos de esos casos ya tienen sentencia?

Cuántos casos maneja cada oficial o auxiliar?

Qué tipo de diligencias se realizan en caso de robo de identidad mediante dispositivos electrónicos?

Cree usted que la población está protegida de este delito?

¿Hay algún sector que se vea más afectado por el delito de robo de identidad en Guatemala? ¿Qué características reúnen las víctimas?

¿Cuántas de estas denuncias fueron de, delitos de robo de identidad, concretados a través de dispositivos electrónicos?

¿Qué tipos de dispositivos se utilizan para concretar el robo de identidad?

¿Cuál es el dispositivo más popular o más vulnerable?

¿Cuentan con un protocolo de actuación en caso de que se realice, una estafa, un fraude mediante el robo de identidad de alguna persona?

Cuentan con un protocolo de actuación en caso de que se realice, una estafa, un fraude mediante el robo de identidad de alguna persona, si este se concreta con dispositivos electrónicos?

Con qué instituciones se coordina en el caso de un delito de robo de identidad?

Cuáles son los avances de la Unidad?

Cuáles son los desafíos?

Cómo calificaría la relación de coordinación de dicho delito con la Policía Nacional Civil? Excelente Buena Regular Mala

Cómo calificaría la relación de coordinación de dicho delito con el Organismo Judicial? Excelente Buena Regular Mala

¿Tienen algún tipo de coordinación con abogados privados o individuales, representantes legales o sujetos jurídicos que intercedan por casos de robo de identidad?

¿Cuenta la Policía Nacional Civil con estadísticas oficiales respecto de delitos económicos?

¿Cuál es la modus operandi del delincuente en el caso de robo de identidad mediante tarjeta de crédito?

¿Cuál es el modus operandi del delincuente en el caso de robo de identidad a través de correo electrónico?

¿Modus operandi de otro delito que incluya el robo de identidad mediante dispositivos electrónicos?

¿Cuál es la circunstancia de vulnerabilidad que permite el robo de identidad?

BOLETA DE RECOPILACIÓN DE DATOS DE EXPEDIENTES

TESIS DE LICENCIATURA: ROBO DE IDENTIDAD MEDIANTE MEDIOS ELECTRÓNICOS EN GUATEMALA. UNIVERSIDAD RAFAEL LANDÍVAR, FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ESTUDIANTE: MARISOL ZEA WELLMANN
CARNE:2407907

MODELO DE ENTREVISTA No. 4

Dirigida a Juez encargado de delitos de Robo de Identidad por medios electrónicos, Organismo Judicial de la ciudad de Guatemala, Departamento de Guatemala

¿Qué delitos se atienden en éste juzgado?
¿Qué capacitación ha recibido en cuanto a delitos de robo de identidad?
¿Cuántas denuncias reciben sobre el delito de robo de identidad?
¿Cuántos casos de robo de identidad derivan en un delito mayor?
¿Qué dispositivos considera que son los más populares para los delincuentes, en el delito de robo de identidad por dispositivos electrónicos?
¿Cree que la población está protegida o prevenida de las vulnerabilidades de los dispositivos electrónicos?
¿Cree que hay suficiente legislación respecto del delito de robo de identidad, y especialmente mediante dispositivos electrónicos?
¿En su opinión, el Estado es capaz de combatir dicho delito?
¿Cuáles son los avances en el Organismo Judicial, respecto de dicho delito?
¿Cuáles son los desafíos?
¿Cómo considera la coordinación entre Policía Nacional civil y ministerio Público en los casos de robo de identidad? Excelente Buena Regular Mala

BOLETA DE RECOPILACIÓN DE DATOS DE EXPEDIENTES

TESIS DE LICENCIATURA: ROBO DE IDENTIDAD MEDIANTE MEDIOS ELECTRÓNICOS EN GUATEMALA. UNIVERSIDAD RAFAEL LANDÍVAR, FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

ESTUDIANTE: MARISOL ZEA WELLMANN
CARNE:2407907

MODELO DE ENTREVISTA No. 5

Dirigida a experto en delitos de Robo de Identidad por medios electrónicos.

¿Qué opinión le merece el fenómeno del robo de identidad en Guatemala?

¿Cree que el ciudadano esta protegido de ser víctima de dicho delito en Guatemala?

¿Cuál es, según su opinión, el sector más afectado por dicho delito?

¿Qué opina de la seguridad que ofrecen las telefónicas al usuario?

¿Los fabricantes de dispositivos, ofrecen seguridad al usuario, sobre su información personal?

¿Qué puede hacer una persona con los datos de otra persona?

¿Considera que el Estado está preparado y articulado para contrarrestar esa problemática?

¿Cree que la legislatura actual es suficiente para prevenir o castigar los delitos económicos?

¿Qué instituciones cree usted que enfrentan un desafío mayor en cuanto a la persecución de los delitos económicos?

¿Qué sector social, considera usted que es más vulnerable de delitos económicos?

¿Qué implicaciones tiene que el Estado no esté preparado para contrarrestar dicho delito.