UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de:

INGENIERO DE SISTEMAS

TEMA:

ANÁLISIS Y EVALUACIÓN DE LA PROPUESTA METODOLÓGICA IOCE, PARA LA CADENA DE CUSTODIA SOBRE LOS PROCESOS DE UN PERITAJE INFORMÁTICO

AUTOR:

JOSÉ PAÚL ROSERO QUIROZ

DIRECTOR DE TESIS:

Msig. Nelson Mora Saltos

GUAYAQUIL, ABRIL 2015

DECLARATORIA DE RESONSABILIDAD

Yo José Paúl Rosero Quiroz autorizo a la Universidad Politécnica Salesiana, la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaro que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad del autor.

Guayaquil, Abril del 2015

(f)----------

José Paúl Rosero Quiroz

CC: 0921973541

DEDICATORIA

A Dios, por haber guiado mi camino gracias porque siempre me has mostrado el camino de la paciencia y la verdad, reconozco que me has ayudado de manera muy especial y sobrenatural de poder cumplir cada una de mis tantas metas propuestas, desde que te acepte en mi corazón me llenó de fortaleza de emprender mi objetivo de ser un profesional, buen hijo y sobretodo un buen hermano, nunca dejare de agradecerte porque cada día que despierto estoy en tu misericordia.

A mi familia, a mi padre por ser mi amigo, le agradezco por sus sabios consejos, mi madre por ser tan extraordinaria, con múltiples virtudes te agradezco por tu infinito amor.

José Rosero Quiroz

AGRADECIMIENTO

A mi tutor Nelson Mora por haberme asistido con la guía necesaria para elaborar mi proyecto de grado, también a todos los ingenieros que impartieron sus clases en su debido momento, les agradezco por compartir sus conocimientos, experiencias laborales y guiar mi carrera profesional.

José Rosero Quiroz

CERTIFICADO

Certifico que el presente trabajo fue realizado por el Sr. José Rosero Quiroz, bajo mi supervisión.

Guayaquil, Abril del 2015

Msig. Nelson Mora Saltos

DIRECTOR DE TESIS

ÍNDICE GENERAL

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

AUTOR: José Rosero Quiroz

TESIS UPS-G: CARRERA DE INGENIERIA DE SISTEMAS

TEMA: "ANÁLISIS Y EVALUACIÓN DE LA PROPUESTA METODOLÓGICA IOCE, PARA LA CADENA DE CUSTODIA SOBRE LOS PROCESOS DE UN PERITAJE"

RESUMEN

El presente estudio tiene como objetivo brindar un panorama global sobre la administración de justicia que existe en Ecuador, donde constantemente existen problemas en manipular la evidencia digital, la lentitud en manejar procesos de delitos informáticos, como objetivo de este proyecto consiste en definir los lineamientos operativos que ofrece IOCE al momento de manipular la evidencia digital, donde brinda recomendaciones de forma sistemática al recabar pistas en una investigación forense sea este una computadora hasta un dispositivo móvil, esto nos va a permitir en un futuro prolongado dentro de la indagación descubrir cualquier suceso. En el primer apartado del proyecto se introducirá sobre las consecuencias que llevan estos tipos de delitos informáticos, conocer sobre algunos casos que se han escuchado en nuestro país en donde se necesita la rama de la informática forense. En el segundo capítulo consiste en describir definiciones que están relacionados con el marco del proyecto, herramientas que son útiles para la recolección de evidencia, regulación del marco legal de nuestro País donde son penalizados estos crímenes. En el tercer capítulo se va reseñar sobre el aspecto metodológico para poder hallar toda información relevante para el sustento de este trabajo introduciendo de cómo se va realizar la recolección de datos, a quien y a donde se va obtener la información. En el cuarto capítulo consiste sobre el análisis de resultados de las encuestas y entrevistas realizadas, describir objetivos de las diversas entidades que hacen frente a estas amenazas cibernéticas. En el quinto capítulo implica algunas conclusiones y recomendaciones basado en los objetivos planteados. Finalmente, el capítulo sexto es el más importante porque se va analizar y explicar en qué consiste IOCE, la metodología y su estructura para realizar un análisis forense en un

delito informático, herramientas desde licenciados hasta software libre, de cómo se va extraer la información importante para hallar las pistas necesarias, para así brindar un informe técnico y ejecutivo que sirva de soporte.

PALABRAS CLAVES:

Peritaje Informático, cadena de custodia, metodología IOCE, análisis forense.

AUTHOR: José Rosero Quiroz

UPS-G THESIS: SYSTEMS ENGINEERING CAREER

TOPIC: "ANALYSIS AND EVALUATION OF METHODOLOGICAL PROPOSAL IOCE, FOR CHAIN OF CUSTODY ON THE PROCESS OF A COMPUTER EXPERTISE"

ABSTRACT

The current study has as an objective provide a global situation on the administration of justice that exists in Ecuador, where constantly exists problems in handling the digital evidence, slowness in handling cybercrime processes, the objective is to define the operational guidelines offered IOCE when handling digital evidence, provides recommendations for a systematic review to gather information in a forensic investigation it can be from a computer to a mobile device, this will allow us in a prolonged future in the investigation discover any facts. The first paragraph of project will be introduced on reality and consequences that carry these types of crimes, know some cases about that have been heard in our country, where is needed the branch of computer forensics, the past that support the researches with theoretical basis supporting the work. The second chapter is to describe definitions that are related to the project, tools that are useful for collecting evidence, regulation of the legal framework of our country where these crimes are punishable. In the third chapter will review about the methodological aspect to find all the relevant information, to sustain this work, introducing about how it will perform data collection, who and where you will get the information. In the fourth chapter is about the analysis and results of the interviews and surveys conducted, to describe objectives of the different entities facing these types of threats. In the fifth chapter involves the initiatives that users must manage some conclusions and recommendations, based on the objectives. Finally, the sixth chapter is the most important because it will analyze and explain what IOCE, methodology and structure that provides for forensic analysis in a cyber-crime, tools from graduates to

free software, where they will perform forensic analysis of how to find important information to find the necessary clues, in order to provide technical and executive report that serves as support.

KEYWORDS:

Computer Evaluation, chain of custody, IOCE methodology, forensic analysis.

INTRODUCCIÓN

El proyecto consiste en definir y analizar las múltiples circunstancias de los problemas cibernéticos en nuestra sociedad actual. En los últimos 10 años, se ha escuchado a través de casos denunciados sobre la tendencia que origina los delitos informáticos en nuestro país y en toda parte del mundo, el alcance y pérdidas que trae como consecuencia estas amenazas. A medida que surgían estos problemas, el país no contaba con leyes necesarias para penalizar a estos delincuentes. Por lo tanto cometerlos era un tema que no podían ser sancionados, existía muchas vulnerabilidades y falencias en las leyes de Ecuador, no existía aún mucha información sobre dónde acudir, muchos de los jueces no conocían sobre el tema del crimen cibernético y los procesos de estos delitos eran demasiado lentos y muy poco solucionados. A medida que avanza la tecnología, los delitos informáticos también, se puede hallar gran cantidad de información de cómo causar daño a través del internet, manuales, sitios dedicados donde se puede aprender diferentes métodos de ataques. Ecuador ha sufrido muchos incidentes por intromisiones informáticas como son: fraudes bancarios, violación a la privacidad de datos y extorsiones a través de redes sociales.

Ante la falta de un proceso legal no había sanción tipificada para estos delincuentes informáticos, tampoco los recursos tecnológicos y personal necesario para poder llevar una indagación respectiva. Actualmente ya existen profesionales encargados para realizar estas investigaciones, como son los profesionales llamados peritos informáticos. Un peritaje informático consiste en precautelar la evidencia digital, para que a lo largo de la búsqueda pueda descubrir las pistas necesarias para hallar aquellos hechos que dejo el atacante informático, este investigador utiliza un conjunto de técnicas para poder encontrar información necesaria. El experto informático actúa después que haya sucedido un siniestro con la autorización del fiscal respectivo, en el que puede verse afectado una persona natural o jurídica. Existen Leyes y Regulaciones sobre los delitos informáticos que se encuentran homologados en el Código Orgánico Integral Penal entre ellos tenemos:

- ✓ Destrucción Maliciosa de Documentos.
- ✓ Falsificación, estafa electrónica.

- ✓ Sabotaje o daños informáticos.
- ✓ Producción y distribución de imágenes pornográficas.

Entre los temas escuchados sobre investigación forense en nuestro País, expuestos por los diferentes medios de comunicación son los siguientes:

- **Clonación de tarjetas:**

  La gran mayoría de las personas han sido víctimas de clonación de sus tarjetas bancarias, éste es un delito muy frecuente que está tomando mayor impulso hoy en día, donde los atacantes utilizan un dispositivo llamado Skimmer del cual es una herramienta que permite capturar toda la información que hay en la tarjeta en cuestiones de segundos, donde el usuario no se da cuenta porque el dispositivo es muy fácil de ocultar.

- **Caso Chucky Seven:**

  Es un caso que por falta de evidencias fue cerrado, del cual consistió en realizar una investigación forense para encontrar información de un disco duro, sobre una sentencia que llevaba este pseudónimo.

Con el objetivo de descubrir quién era el que realizó la sentencia sobre el caso "EL UNIVERSO".

Esta propuesta permite identificar un marco global sobre los delitos informáticos, objetivos, la importancia sobre normativas y procedimientos operativos. Donde la metodología IOCE implica procesos para mantener en un buen recaudo la cadena de custodia ante el proceso de una investigación.

CAPÍTULO 1

PLANTEAMIENTO DEL PROBLEMA

1.1 Enunciado del problema

La preparación y capacitación que tienen algunos miembros de la Fiscalía en Ecuador sobre la tecnología es escasa por lo tanto no pueden ser de gran ayuda para la ciudadanía. Actualmente el incremento de los delitos informáticos ha aumentado de forma drástica como son: la violación a la intimidad personal, extorsiones, pornografía online y amenazas virtuales.

El Fiscal Provincial del Guayas Abg. Paúl Ponce, comunico en el diario "HOY", que estos actos no son frecuentemente denunciados por las personas, porque no poseen el conocimiento de que existe un área de investigación según las estadísticas, el 1% de cada 600 casos son denunciados, al parecer es un índice bajo de denuncias presentadas por los ciudadanos. Por lo general, cuando un individuo se dedica hacer el mal uso de la tecnología siempre deja rastros, ya sea el proceso de cómo realizó la intrusión informática, qué tipo de herramienta usó para ingresar al sistema, con estos datos el especialista forense informático en pleno indicio sabrá cómo actuar durante la investigación, decidiendo qué procesos se deben mantener intactos en la cadena de custodia para conservar la integridad de aquellas pruebas, de esta manera dejar bien expuesto sus informes ante el fiscal, donde el Juez actuará sobre el caso en particular. Es imprescindible destacar que pocas universidades añaden en su malla curricular sobre esta nueva profesión, como es el peritaje informático en la rama de derecho, como la de sistemas.

Factores estructurales – causas

En nuestra sociedad como cualquier parte del mundo, se comenzó a conocer el significado de estos temas por los actos dolosos que cometían algunos

delincuentes a través de internet, utilizando ataques de denegaciones de servicios, robo de información confidencial a organizaciones. El año en que las autoridades de nuestro país dieron una voz de alerta sobre los delitos informáticos fue en el año 2008, donde surgieron pérdidas cuantiosas de dinero afectando algunos usuarios en sus cuentas bancarias. Entre los diferentes factores estructurales tenemos los siguientes:

- Factores de ataques externos.
- Factores de ataques internos.

Factores de ataques externos: Donde el atacante con la finalidad de comprometer un sistema informático usa el anonimato qué por lo general es utilizado para evitar la ley del propio País y no pueda ser penalizado, entre uno de los ataques que se puede mencionar es el Malware que consiste en dañar o infiltrarse a una computadora.

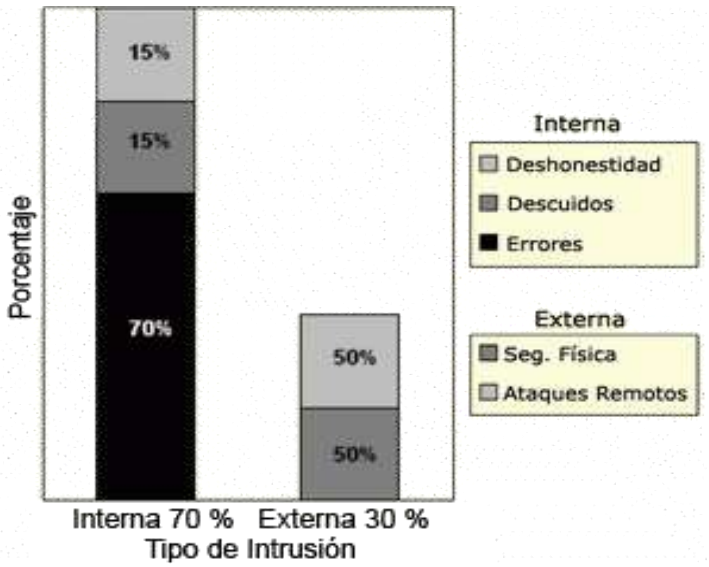
Factores de ataques internos: La gran mayoría de los usuarios son fácilmente atacados por no tener algún tipo de conocimiento relacionado sobre el manejo de la seguridad referente a las diversas herramientas de tecnología de la información.

Un análisis breve sobre los ataques internos, fueron realizados a través de ingeniería social que se conoce como la habilidad y la facultad de obtener información fácilmente de los usuarios a través de llamadas, correo electrónico, mensajes de texto, donde puede ser la organización con la mejor estructura tecnológica, pero si no se capacita las medidas de prevención a los trabajadores puede ser un objetivo fácil para aquellas personas que son expertas en recoger datos, que en un futuro pueden ser utilizados para un beneficio mal intencionado como son:

- Robos de identidad.
- Espionaje organizacional.
- Comprometer redes empresariales.

- Obtener información sobre tarjetas bancarias.
- Empleados deshonesto.
- Imprudencia del personal laboral.
- Ex empleados enojados o mal remunerados.

Figura 1: Intrusiones reportadas

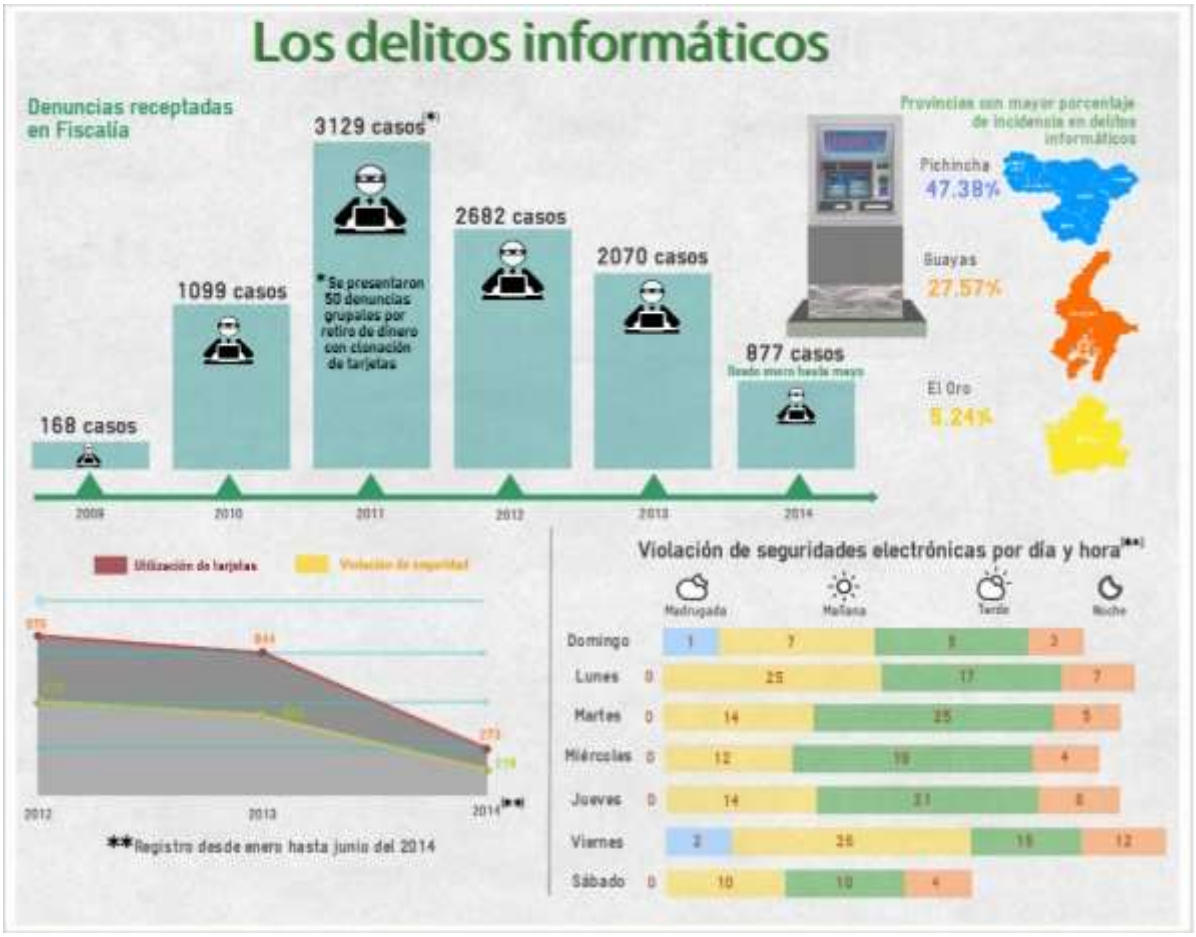


Fuente: CYBSEC

Factores intermedios – Rasgos del problema

Los procesos de los delitos informáticos son atendidos lentamente en la Fiscalía por múltiples causas: algunos funcionarios desconocen del tema, lentitud en asignar un perito informático y la poca gestión sobre los procedimientos operativos de la cadena de custodia. Sin embargo una de las mayores molestias por los ciudadanos que al realizar sus denuncias, hay poca información sobre estos delitos informáticos, por parte de los servidores judiciales en la fiscalía.

Figura 2: Denuncias reportadas delitos informáticos



Fuente: Fiscalía General de Estado

En consideración sobre la publicación que realizó la Fiscalía General del Estado basados en hechos estadísticos reportados desde el año 2009 hasta Mayo del 2014, se observa que existen muchas denuncias presentadas por los internautas por la utilización de tarjetas bancarias, la provincia con mayor porcentaje de denuncias presentadas fue la de Pichincha con 47.38%.

Factores inmediatos – Consecuencias

Las diferentes consecuencias provocadas por ataques informáticos pueden ser las siguientes:

- No tener acceso a cuentas electrónicas.

- Publicaciones falsas en redes sociales.
- Robo y suplantación de identidad.
- Pedofilia.
- Fraude bancario.
- Sabotaje industrial y organizacional.
- Intercepción de redes informáticas.

Los usuarios cuando son afectados por estas circunstancias tienen algunas interrogantes sobre dónde y cómo exponer su caso:

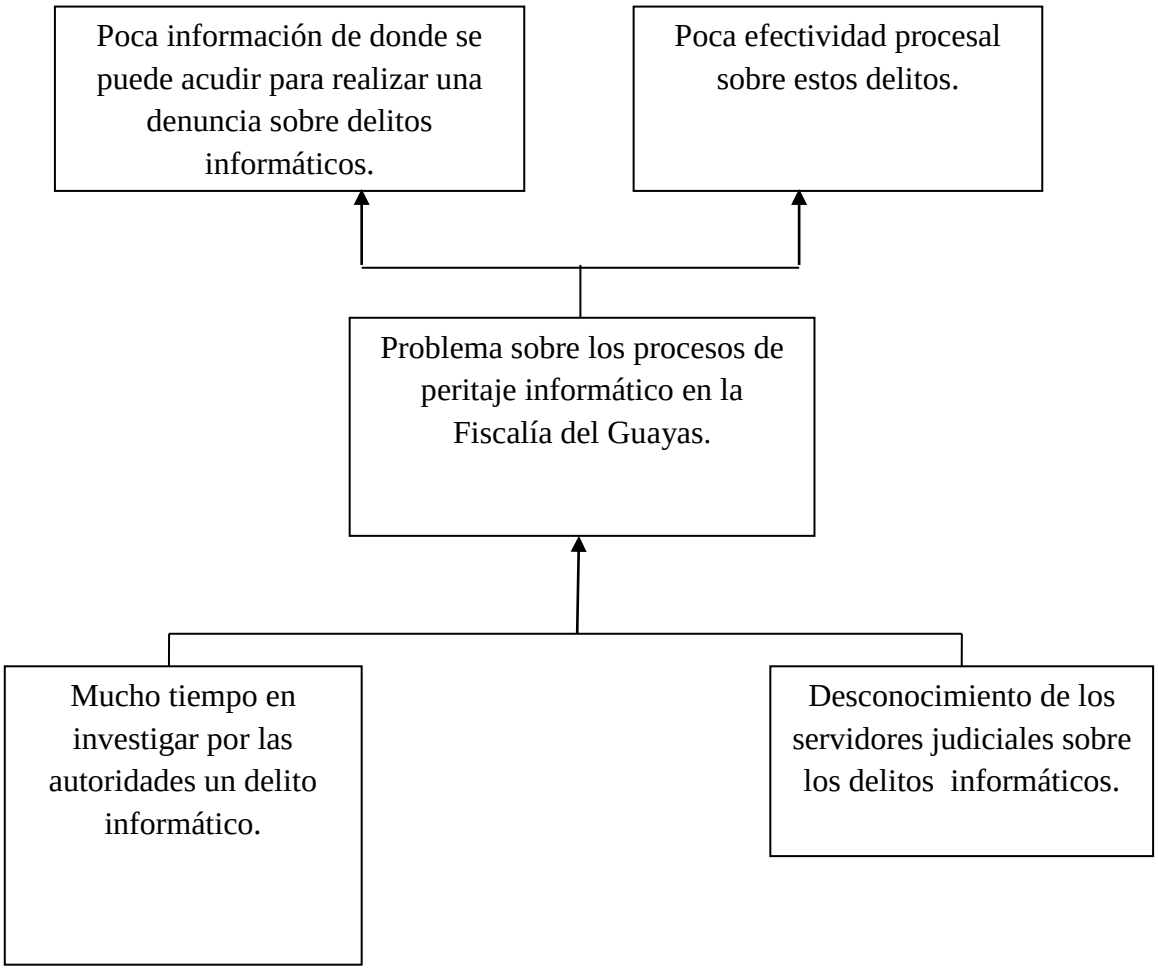
- ¿Cómo puedo prevenir un ataque informático?
- ¿Dónde puedo acudir si he sido víctima de un ataque informático?
- ¿En qué parte de la ley me puedo guiar para presentar mi denuncia?
- ¿Cómo expongo mi denuncia?

1.2 Formulación del problema de investigación

Como primer índice de investigación se va considerar como punto de partida la siguiente pregunta:

- ¿Qué aspectos inciden en el Ecuador, sobre la falla de los procedimientos en manejar la cadena de custodia, de un peritaje informático?

1.2.1 Árbol del problema



1.2.2 Sistematización del problema de investigación

- ¿Tienen los fiscales y jueces los conocimientos necesarios para poder enfrentar los delitos informáticos?
- ¿Cómo se podría reducir el tiempo de asignación para un perito informático?
- ¿Cuáles son los planes de acción para resolver un delito informático?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Analizar la propuesta metodológica IOCE sobre la cadena de custodia, lo cual incluye sugerencias sobre cómo se debe manejar las evidencias digitales en una investigación.

1.3.2 Objetivos específicos

- Describir la importancia de los delitos informáticos que enfrenta la Fiscalía del Guayas.
- Reducir el tiempo de asignación de los delitos informáticos para la atención en la fiscalía.
- Aplicar metodología para el manejo de la cadena de custodia en la evidencia digital.

1.4 Justificación

La importancia de este proyecto es poder conocer un poco más a fondo sobre la metodología que ofrece la organización IOCE relativo a procedimientos de cómo manejar la estructura analítica de la investigación digital, cuales son las buenas prácticas para mantener intacta la cadena de custodia, profundizar cuáles son los pasos que se debe realizar en una investigación forense, como manejar el proceso de la documentación al momento de analizar cualquier tipo de dispositivo del cual se va a extraer la información.. Como aporte es generar un documento que permita brindar un soporte de información para conocer a fondo sobre los delitos informáticos en nuestro País, con la finalidad de brindar una guía de dónde poder acudir, realizar sus respectivas denuncias, informar sobre él Marco Legal. Es importante que los profesionales de sistemas conozcan sobre el área de los delitos informáticos que

existe en el Ecuador con el objetivo de que puedan aplicar cargos de peritos informáticos acreditados por la Fiscalía, lo que permitirá que estos ataques tecnológicos puedan ser investigados con mayor eficiencia. La informática forense permite esclarecer cualquier tipo de delito con claridad y precisión, la opinión de un perito es muy importante ante un caso, para así poder descubrir la búsqueda de los datos importantes en la evidencia digital. Los principales beneficiarios es la población donde conocerán un poco sobre aquellas amenazas tecnológicas y los miembros que administran la justicia al momento de dar el respectivo soporte al denunciante.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Antecedentes investigativos

Dentro de este capítulo se describen los diferentes conceptos encontrados en guías de lectura referentes a lo que conlleva la investigación forense, lo cual fundamenta el estudio de la investigación para que se conozca un poco más sobre éstos delitos informáticos, se da a conocer definiciones terminologías de peritajes informáticos y también se explica el marco legal de nuestro país.

2.1.1 Metodología

"Es el estudio de los componentes que conlleva la investigación científica por ello es que dichos componentes se ponen en práctica y esto da el resultado al diseño o proyecto de la investigación" (REZA, 1997).

- **Análisis metodológico:** Es un examen detallado para extraer conclusiones en la cual está derivado por dos eventos como es la descriptiva, que permite compilar la información y una técnica sobre las herramientas a utilizar.

- **Evaluación metodológica:** Está vinculada con el proceso del caso a evaluar, del cual está compuesta de la siguiente forma:
  - ✓ Criterios de evaluación
  - ✓ Enfoques de la evaluación

2.1.2 Criminalidad informática

Como define Davara, "Es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos." (DAVARA, Miguel, 1990).

La criminalidad informática es toda acción que implique la utilización indebida de ordenadores o la utilización de cualquier medio de tecnología, herramientas virtuales, con el fin de cometer un perjuicio para obtener toda la información necesaria del usuario comprometiéndolo fácilmente por el atacante, robo de dinero en sus cuentas bancarias, extorsiones a través de publicaciones dolosas y comprometedoras, falsificación, robo de propiedad intelectual.

2.1.3 Cómputo forense

Es la ciencia ordenada que se objeta sobre los fundamentos de indagaciones y hechos predeterminados donde el perito tendrá que incursionar y trabajar para recoger indicios para luego poder analizarlos, donde el evento puede ser cualquier medio electrónico sea que esté encendido o apagado, esta ciencia ha venido creciendo de manera exponencial en el mercado laboral desde algunos años, donde conlleva todo el proceso de identificación, preservación, análisis y presentación de la evidencia que se encuentra almacenada en los dispositivos de almacenamientos con la finalidad de poder hallar los culpables involucrados en el caso.

El autor Dave Kleiman lo define como, una serie metódica de técnicas y procedimientos para la obtención de pruebas, a partir de los equipos informáticos y varios dispositivos de almacenamiento y los medios digitales, que se pueden presentar en un tribunal de justicia en un formato coherente y significativo (KLEIMAN, D., 2007).

Como base fundamental a la informática forense se lo podría denominar como:

- Auditorias e inspecciones a medios electrónicos.
- Técnicas de ingeniería social.
- Precisión y determinación con los propietarios de sitios web, blogs.

2.1.4 Objetivos de la informática forense

La informática forense tiene 3 objetivos claros:

1. La compensación de los daños causados por los criminales o intrusos.

2. La persecución y procesamiento judicial de los criminales.

3. La creación y aplicación de medidas para prevenir casos similares.

2.1.5 Usos de la informática forense

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense (López Oscar, Amaya Haver & León Ricardo, 2001):

- **Prosecución Criminal:** Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

- **Litigación Civil:** Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.

- **Investigación de Seguros:** La evidencia encontrada en computadores puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

- **Temas corporativos:** Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
- **Mantenimiento de la ley:** La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

2.1.6 Cadena de custodia

Consiste en los procedimientos sistemáticos para conservar la evidencia digital ante una fase judicial. Al manejar la cadena de custodia se debe considera lo siguiente:

- Mantener la integridad de la evidencia.
- Documentación
- Limitar las personas en manejar la evidencia digital en primera instancia.

2.1.7 Evidencia digital

Casey lo define como, "Cualquier dato que puede establecer que un crimen se ha ejecutado puede proporcionar un vínculo entre un crimen y su víctima o un crimen y su autor." (CASEY, 2011).

- Recuperar los datos.
- Analizar los datos más relevantes.
- Examen de sistema.

2.1.8 Delito informático

Es aquella forma ilícita de destruir y dañar ordenadores, medios electrónicos y redes de internet entre sus características son:

- Es muy complicado encontrar las pruebas después del siniestro.
- Tienden a proliferar y expandirse en ataques.
- Recuperación de información.
- Descifrado de claves criptográficas.

Por sus partes los señores Huerta y Líbano sostiene que, son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso

de un sistema de tratamiento de información y destinadas a producir un perjuicio (HUERTA, M., y LÍBANO, C., 1996).

Hoy en día ser ciudadanos digitales es una necesidad tan indispensable, pero a medida que avanza la misma, la delincuencia también se moderniza, existen gran cantidad de denuncias de los delitos informáticos en el país y toda parte del mundo, es la razón que exista la ciencia de la informática forense y que tenga gran aceptación en la sociedad, actualmente estos delitos ya están regulados por nuestro Código Integral Penal. Toda acción de un delito cometido a través de la red deja una huella digital, entre lo más comunes que se puede citar en nuestro entorno son:

- Acoso en redes sociales.
- Pedofilia.
- Robo de información de contenido industrial.
- Actividades terroristas.
- Acceso a información personal.
- Fraude.
- Ataques de denegación de servicio.

Por lo tanto nuevos delitos requieren nuevas técnicas de investigación.

2.1.9 Clasificación de los delitos informáticos

Como instrumento o medio: Consiste en temas relacionados como son: la falsificación electrónica, robo, amenazas, muertes, interceptación en redes de información y divulgación.

Con fin u objetivo: Está vinculado con sabotajes, accesos ilícitos, programaciones de ataques, etc.

2.1.10 Perito Informático

Es aquella persona con conocimiento técnico y analítico, que se encarga de tomar las pruebas respectivas del caso a ser tratado, hallar pistas que ha dejado la intrusión, realiza informes para que sirva de soporte en la declaración ante los tribunales para brindar una gestión más clara al fiscal, consta de tres etapas como son:

- Toma en contacto
- Desarrollo de la Investigación, elaboración de informes.
- Declaración ante tribunales.

2.1.11 Funciones en el área de peritaje informático

- Identificación y recolección de evidencias.
- Análisis forenses en dispositivos.
- Análisis de paquetes de datos.
- Reconstrucción de la escena del crimen.
- Rastros de mensajerías y ficheros.
- Análisis de malware.
- Seguridad y hacking ético.

El trabajo del perito informático tiende hacer muy complejo en diferentes casos al momento de encontrar las huellas para poder capturar a los delincuentes, el investigador busca los principales indicios referentes a cualquier tipo de delito informático de las cuales son las siguientes:

- Código mime que contiene del correo electrónico para determinar el remitente del mensaje que está causando el acoso.
- Por medio de un mensaje queda registrado la dirección IP.
- Análisis de llamadas telefónicas, pero esto se lo puede realizar por medio de una orden judicial.

2.1.12 Estándares en el peritaje de gestión

- ISO 9001: Calidad en procesos.
- COBIT
- ISO 27000: Sistemas de Gestión de Seguridad de la Información
- CMMI: Desarrollo de soluciones
- PMI: Gestión de proyectos
- ITIL: Gestión de servicios
- ISO/IEC 27037

2.1.13 Fases del análisis forense de la Cadena de Custodia

Existen cuatro fases presentes en este tipo de análisis como son (López Delgado, M, 2007):

- **Identificación del incidente:** Esta fase es cuando ocurre el hecho, en la cual se reporta a un perito, donde este debe adquirir la información utilizando las metodologías correspondientes para mantener intacta la cadena de custodia.

- **Preservación de la evidencia:** Implica realizar imágenes forenses, en que el perito debe trabajar con aquella imagen sin alterar la cadena de custodia.

- **Análisis de la evidencia:** Permite seguir un estudio de los eventos, registros, paquetes, etc. De la cual nos va ayudar sobre cómo se llevó a cabo el delito.

- **Documentación del incidente:** Sistematizar por medio de un informe técnico y ejecutivo, el cronograma que se llevó la investigación. Redactar de manera precisa y clara cada detalle, el investigador digital deberá presentar dos tipos de informes de las cuales son:

  - ✓ **Informe Técnico:** Describe la metodología que se utilizó para el proceso de la investigación, como el uso de herramientas forenses.

- ✓ **Informe Ejecutivo:** Es poder expresar aspectos no técnicos para que permita una mejor compresión en altos mandos, explicando las conclusiones de cómo se llevó la experticia.

2.1.14 Guías de gestión de evidencia digital

RFC 3227: Guidelines for Evidence Collection and Archiving (Brezinski, D., & Killalea, T., 2002). Consiste sobre guías de evidencias digitales, la recolección de información y archivamiento, en el proceso de que haya ocurrido un incidente informático, del cual explica sobre cómo mantener intacta la cadena de custodia ante una investigación forense.

IOCE – "International Organization on Computer Evidence": Guidelines for Best Practice in the Forensic Examination of Digital Technology (IOCE, 2002). Implica mejores prácticas sobre la investigación de manejo de evidencia digital, en la cual nos indican consejos sobre cómo mantener el flujo de trabajo realizándolo metodológicamente como por ejemplo: Búsquedas en la escena, evaluaciones, análisis de datos.

2.1.15 Empleos de formularios para el manejo de incidentes informáticos

El uso de formularios va permitir a la persona encargada, llevar un control sistemático sobre el proceso inicial de la investigación, hasta poder obtener un resultado:

- Documento donde se maneje la evidencia hacer incautada.
- Registro de formulación de incidencias.
- Formulario para medios magnéticos.

2.1.16 Entornos de trabajo de un análisis forense

- Forense en sistemas operativos Windows, Linux, MAC.
- Medios extraíbles como son discos externos, pendrive, etc.
- Forense en redes tanto locales, como redes inalámbricas.
- Smartphone.

2.1.17 Análisis forense en redes

El análisis forense sobre redes de comunicaciones, es un tenga muy amplio donde el tipo de investigación implica tener conocimientos básicos sobre TCP/IP, conocer sobre sistemas operativos Windows y Linux, consiste en analizar protocolos, configuraciones, cabeceras, capturas de paquetes de datos, conocimiento sobre infraestructuras de redes, donde el investigador deberá descubrir el origen de dónde provino el ataque o prevenir futuros incidentes. Es importante considerar al analizar cualquier tipo de red, se debe capturar toda la información en vivo, ya que su información es volátil. El objetivo de esta investigación es poder responder las siguientes analogías ante un desastre:

- ✓ ¿Cómo obtuvo el acceso?
- ✓ ¿De dónde proviene?
- ✓ ¿Cómo se produjo el ataque?

2.2 Fundamentación legal

2.2.1 Código Orgánico Integral Penal

Fue publicado el 10 de Febrero del 2014, el nuevo registro tiene como objetivo tipificar medidas de control y procedimientos para realizar el juzgamiento respectivo según sea la finalidad de los delitos informáticos. Las personas que han sido

vulneradas, ya pueden realizar sus respectivas denuncias, para que aquellos puedan ser penalizados, en el proyecto de grado se encuentran los siguientes artículos tipificados en el Código Integral Penal.

El código está formado por las siguientes secciones:

- **Diversas formas de explotación.**

  En el artículo 103, 104:

  En estos artículos consiste en la infracción enfocada sobre la pornografía infantil y adolescentes menores a 18 años, personas que reproduzcan, vendan y distribuyan, podrán ser penalizados de un aproximado de diez hasta dieciséis años. (COIP, 2014).

- **Delitos contra la integridad sexual y reproductiva.**

  En el artículo 173, 174:

  Consiste en que se realice contacto a través de medios electrónicos a menores de edad que se fundamente un encuentro sexual. También las ofertas de servicios sexuales a menores de edad, por medio de publicaciones en distintas redes sociales, blogs, serán sancionados de uno a seis años aproximadamente dependiendo del artículo. (COIP, 2014).

- **Delitos contra el derecho a la intimidad personal y familiar.**

  En el artículo 178:

  Esta ley implica sobre la violación de la intimidad personal, tiene una penalidad desde uno hasta tres años. (COIP, 2014).

- **Delitos contra el derecho a la propiedad.**

  En el artículo 186, 188, 190, 191:

  Los temas principales de estos apartados están enfocados a temas de intimidaciones, fraudes por medio de tarjetas bancarias, pagos, clonaciones. Manipulación o acceso permitido a terceros para destruir sistemas Telecomunicaciones. Apropiaciones fraudulentas por medios electrónicos manipulando o alterando, redes, datos, sistemas financieros. Reprogramación o modificación de móviles, todas estos apartados tiene una penalidad aproximada de seis meses hasta diez años. (COIP, 2014).

- **Delitos contra la seguridad de los activos de los sistemas de información y comunicación.**

  Desde el artículo 229 hasta el 234:

  Está vinculado directamente sobre temas como son de revelación de datos, intercepción, divulgación de información, transferencias electrónicas, clonaciones, ataques a sistemas informáticos y accesos no autorizados van a ser penalizados de tres hasta cinco años. (COIP, 2014).

2.2.2 Reglas del el área pericial

En el artículo 511del Código Orgánico Integral Penal, están citados los requisitos que deberán cumplir los peritos:

1. Ser profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia y especialidad, acreditados por el Consejo de la Judicatura.

2. Desempeñar su función de manera obligatoria, para lo cual la o el perito será designado y notificado con el cargo.

3. La persona designada deberá excusarse, si se halla en alguna de las causales establecidas en este Código para las o los juzgadores.

4. Las o los peritos no podrán ser recusados, sin embargo el informe no tendrá valor alguno si el perito que lo presenta, tiene motivo de inhabilidad o excusa, debidamente comprobada.

5. Presentar dentro del plazo señalado sus informes, aclarar o ampliar los mismos a pedido de los sujetos procesales.

6. El informe pericial deberá contener como mínimo el lugar y fecha de realización del peritaje, identificación del perito, descripción y estado de la

persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilustraciones gráficas cuando corresponda, las conclusiones y la firma.

7. Comparecer a la audiencia de juicio y sustentar de manera oral sus informes contestar los interrogatorios de las partes, para lo cual podrán emplear cualquier medio.

2.2.3 Esquema de penalidades informáticas

A continuación se describe un cuadro esquemático sobre la tipificación del CPP, de las sanciones pecuniarias y del encarcelamiento para aquellas personas que comentan estos delitos.

Tabla 1: Penalidades informáticas

PENALIDADES INFORMÁTICAS	REPRESIÓN	SANCIÓN PECUNIARIA
Delitos contra la información protegida (CPP Art. 202)		
1. Violentando claves o sistemas accede u obtiene información	6 meses a 1 año	$500 a $1000
2. Seguridad nacional o secretos comerciales o industriales	1 a 3 años	$1.000 - $1500
3. Divulgación o utilización Fraudulenta	3 a 6 años	$2.000 - $10.000
4. Obtención y uso no Autorizados	2 meses a 2 años	$1.000 - $2.000
Destrucción maliciosa de documentos (CCP Art. 262)	3 a 6 años	
Falsificación electrónica (CPP Art. 353)	3 a 6 años	
Apropiación ilícita (CPP Art. 553)	6 meses a 5 años	$500 a $2000
Estafa (CPP Art. 563)	5 años	$500 a $1000

Fuente: Código de Procedimiento Penal del Ecuador

2.3 Formulación de la hipótesis y variables

2.3.1 Hipótesis general

Algunos casos de delitos informáticos en etapa de investigación no llegan a tener validez legal, debido a la alteración de sus evidencias, ocasionado por el desconocimiento de ciertos fiscales, en los procedimientos de manejo de la cadena de custodia.

2.3.2 Hipótesis específicas

- Los fiscales y jueces deben tener la capacidad de resolver los delitos informáticos actuales.
- Tiempo excesivo que toma en ser asignado un perito informático en una denuncia.
- Carencia de procedimientos operativos para investigar los delitos informáticos.

2.3.3 Matriz Causa – Efecto

Tabla 2: Matriz Causa - Efecto

FORMULACIÓN DEL PROBLEMA	OBJETIVO GENERAL	HIPÓTESIS GENERAL
¿Qué aspectos inciden en el Ecuador, sobre la falla de los procedimientos en manejar la cadena de custodia de un peritaje informático?	Analizar la propuesta metodológica IOCE sobre la cadena de custodia, lo cual incluye sugerencias sobre cómo se debe manejar las evidencias digitales en la investigación.	Algunos casos de delitos informáticos en etapa de investigación no llegan a tener validez legal, debido a la alteración de sus evidencias, ocasionado por el desconocimiento de ciertos fiscales, en los procedimientos de manejo de la cadena de custodia.

SISTEMATIZACIÓN DEL PROBLEMA	OBJETIVOS ESPECÍFICOS	HIPÓTESIS ESPECÍFICAS
¿Tienen los fiscales y jueces los conocimientos necesarios para poder enfrentar los delitos informáticos?	Describir la importancia de los delitos informáticos que enfrenta la Fiscalía del Guayas.	Los fiscales y jueces deben tener la capacidad de resolver los delitos informáticos actuales.
¿Cómo se podría reducir el tiempo de asignación para un perito informático?	Reducir el tiempo de asignación de los delitos informáticos para la atención en la fiscalía.	Tiempo excesivo que toma en ser asignado un perito informático en una denuncia.
¿Cuáles son los planes de acción para resolver un delito informático?	Aplicar metodología, para el manejo de la cadena de custodia en la evidencia digital.	Carencia de procedimientos operativos para investigar los delitos informáticos.

Elaborado por: Autor

2.4 Señalamiento de variables

2.4.1 Variables independientes

- Procedimientos empleados para recoger pistas en el proceso de un peritaje informático.

2.4.2 Variables dependientes

- Se determina las funcionalidades de diferentes herramientas forenses.
- La importancia de los procedimientos que debe realizar un perito informático.

CAPÍTULO 3

MARCO METODOLÓGICO

3.1 Modalidad de investigación

Para esta evaluación se toma como ejemplo un caso similar sobre una denuncia presentada en la fiscalía del Guayas en indagación previa, permitiendo analizar y evaluar la metodología IOCE lo cual puede ser una guía para llevar a cabo una investigación forense, dentro de este proyecto se va a manejar las siguientes investigaciones:

- **Investigación descriptiva:** Para el desarrollo de este trabajo, se va a concretar sobre un delito informático basado en amenazas a través de redes sociales que se realizó la denuncia en la Fiscalía del Guayas (Edificio La Merced), debido que por medio de este estudio se detalla el proceso de la cadena de custodia hasta poder obtener los resultados que permitan encontrar un culpable o varios.

- **Investigación de campo:** Determinar por medio de encuestas el grado de conocimiento de diferentes personas sobre los diferentes tipos de delitos cibernéticos que existen actualmente. Se realizó entrevistas a profesionales que dominan el tema a ser investigado.

3.2 Método de investigación

Como sustento a ésta investigación sobre el análisis y la evaluación, se utilizó los siguientes métodos de investigación:

- **Método inductivo–deductivo:** Porque de un caso en general se debe determinar pistas para llegar a un informe final, donde se describe el fenómeno y cuál fue su alcance, sugerir recomendaciones para esquematizar

el mejor uso de las herramientas de tecnologías de la información, para prevenir ser víctima de un ataque informático.

- **Método Estadístico:** Se maneja las probabilidades a través de estadísticas llevadas a cabo por las encuestas realizadas, donde se va necesitar tabular datos y hacer mediciones de los mismos.

3.3 Población y Muestra

- **Población:**

  Es necesario conocer la factibilidad de la tesis, se tomará como población a las usuarios que van a realizar sus denuncias en la fiscalía del Guayas, también a expertos dedicados a este tipo de investigaciones.

- **Muestra:**

  Se tomó como muestra las encuestas de algunas personas de la fiscalía debido que debemos conocer la situación actual de los delitos informáticos. Para esto se realizó en unos dos días particulares, donde en un total de 40 personas estaban realizando denuncias en la fiscalía del Guayas (Edificio de la Merced).

Tabla 3: Cantidad de usuarios encuestados

GUAYAQUIL	
USUARIOS	40
TOTAL	40

Elaborado por: Autor

Expertos sobre Tecnología de información - Entrevistas

- Ing. Roberto Olaya – Jefe de la empresa HACK – SECURITY.
- Fiscal Patricia Morán – Unidad Especializada en Personas y Garantías.

- Lcda. Yelena Casanova – Perito Informática acreditación vigente.
- Dr. Santiago Acurio del Pino – Juez de la Corte Provincial de Pichincha.

3.3.1 Ecuación utilizada para obtener el tamaño de la muestra

Para el cálculo del tamaño de la muestra se realizó en dos días particulares a partir de las 14:30 hasta las 16:30, para obtener los datos finitos de la población que estaban realizando sus denuncias, la fórmula utilizada será la siguiente:

$n= (N* K^2*p*q)/ (e^2*(N-1)+ K^2*p*q)$

Donde:

n= Tamaño de la Muestra.

N= Número de Elementos de la Población.

K= Se determina a través del Nivel de Confianza

e= Error de muestreo.

p= Proporción esperada de éxito.

q= Proporción de fracaso.

Niveles de confianza

Tabla 4: Niveles de Confianza

Valor de *k*	1,15	1,28	1,44	1,65	1,96	2,24	2,58
Nivel de confianza	75%	80%	85%	90%	95%	97,50%	99%

Fuente: (Balestrini, 1997)

Elaborado por: Autor

Referencia de datos obtenidos a través de personas que van a realizar denuncias

N = 92

K = 1,96

e = 5% = 0.05

p = 5% = 0.05

q = 1-p = (1- 0.05) = 0.95

n= (92* $(1,96)^2$*0.05*0.95) / ($(0.05)^2$*(92-1)+ $(1,96)^2$*0.05*0.95)

n= 40

3.4 Operacionalización de variables e indicadores

Tabla 5: Operacionalización de Variables

VARIABLE	ÁMBITOS	DIMENSIONES	INDICADOR
Carencia de procedimientos y poco asesoramiento para el percance de los delitos informáticos denunciados, tardanza en la atención de un especialista forense en la fiscalía de la ciudad de Guayaquil.	Función Judicial	Informática forense	Competencias sobre: análisis forenses, cadena de custodia, metodologías, estándares, procedimiento operativo
Carencia de procedimientos y poco asesoramiento para el percance de los delitos informáticos denunciados, tardanza en la atención de un especialista forense en la fiscalía de la ciudad de Guayaquil.	Función Judicial leyes enfocado en tecnología de información	Instrucción fiscal	Conocimiento sobre: Código Integral Penal, Ley de Comercio Electrónico y firmas digitales, Código Procedimiento Civil y Penal, Penalidades

Carencia de procedimientos y poco asesoramiento para el percance de los delitos informáticos denunciados, tardanza en la atención de un especialista forense en la fiscalía de la ciudad de Guayaquil.	Función Judicial tecnología de información	Herramientas forenses	Conocer sobre: herramientas forenses informáticas, software licenciado y software libre
Carencia de procedimientos y poco asesoramiento para el percance de los delitos informáticos denunciados, tardanza en la atención de un especialista forense en la fiscalía de la ciudad de Guayaquil.	Función Judicial tecnología de información	Informática	Manejo de: herramientas ofimáticas, internet, correo electrónico

Elaborado por: Autor

3.5 Plan de recolección de información

El trabajo de tesis está direccionado dentro de los siguientes aspectos:

- En el primer periodo se va derivar en recolectar información a través de encuestas para conocer el grado de conocimiento de diferentes personas sobre los delitos informáticos.
- En el segundo, se hizo entrevistas a profesionales involucradas con el tema de los delitos informáticos.
- Otra manera de recolectar información es por medio de internet, libros o guías de estudio sobre análisis forense.

3.6 Plan de procesamiento de la información

- Organización y recopilación de datos obtenidos.
- Criterios de especialistas sobre los delitos informáticos.

CAPÍTULO 4

ANÁLISIS Y RESULTADOS

4.1 Análisis de la situación actual

Como instrucción se va identificar los inconvenientes al momento de enfrentar este tipo de investigaciones sobre el uso indebido de medios electrónicos en la fiscalía del Guayas, en lo que se genera diversas problemáticas en base a la situación actual de los delitos informáticos presentados. La gran mayoría de denuncias en cierta medida tiene responsabilidad la parte afectada por no tener el conocimiento sobre el correcto uso de la tecnología de la información, algunos usuarios desconocen que pueden presentar la respectiva denuncia ante un siniestro informático en donde se ve vulnerado sus derechos constitucionales. Entre las situaciones en las que se vieron afectadas muchas de las personas fueron las siguientes:

- Utilizar computadoras que no son de su propiedad, donde habían instalado Keylogger, esta herramienta permite capturar todo la información que digitan.
- Registrar sus claves de diferentes cuentas electrónicas en papeles.
- Conectarse a redes públicas en la que son blanco fácil por un atacante que puede utilizar múltiples ataques para poder capturar sus contraseñas.
- Virus, troyanos, etc.

Es necesario conocer las diversas problemáticas ante éste tipo de indagación pudiendo aplicar medidas de prevención para disminuir el índice actual de las infracciones informáticas en nuestro País.

4.2 Técnicas e instrumentos de evaluación

Como objetivo principal es analizar los diferentes puntos de información para así conocer sobre la problemática de los delitos informáticos en la sociedad, la

administración de justicia, el grado de afectación y el desconocimiento que tiene las diferentes personas, por consiguiente se va describir como se realizó la recolección de los datos:

a) Encuesta

Las encuestas fueron dirigidas a personas que estaban realizando algún tipo de denuncia en la Fiscalía del Guayas.

b) Entrevista

Se toma como referencia a cuatro profesionales involucrados en el análisis de los delitos informáticos.

La entrevista fue dirigida al Ingeniero Roberto Olaya, Jefe de la empresa HACK-SECURITY, quien está involucrado en la gestión de riesgo e investigación de estos delitos informáticos. Otra fue realizada a la Fiscal Abogada Patricia Morán ella está involucrada en la unidad Especializada en Personas y Garantías con la intención de conocer la situación actual de estas amenazas, medidas de control que se están tomando y los procedimientos para realizar una denuncia. También a la Perito Informática acreditada Lcda. Yelena Casanova y al Juez de la Corte Provincial de Pichincha Dr. Santiago Acurio del Pino.

4.3 Análisis de los resultados

4.3.1 Resultado de las encuestas:

Se procedió a encuestar a diferentes usuarios que estaban denunciando en la Fiscalía del Guayas (Edificio la Merced) con el objetivo de conocer la realidad social si conocen sobre los delitos informáticos. Para ello se efectuó la siguiente encuesta:

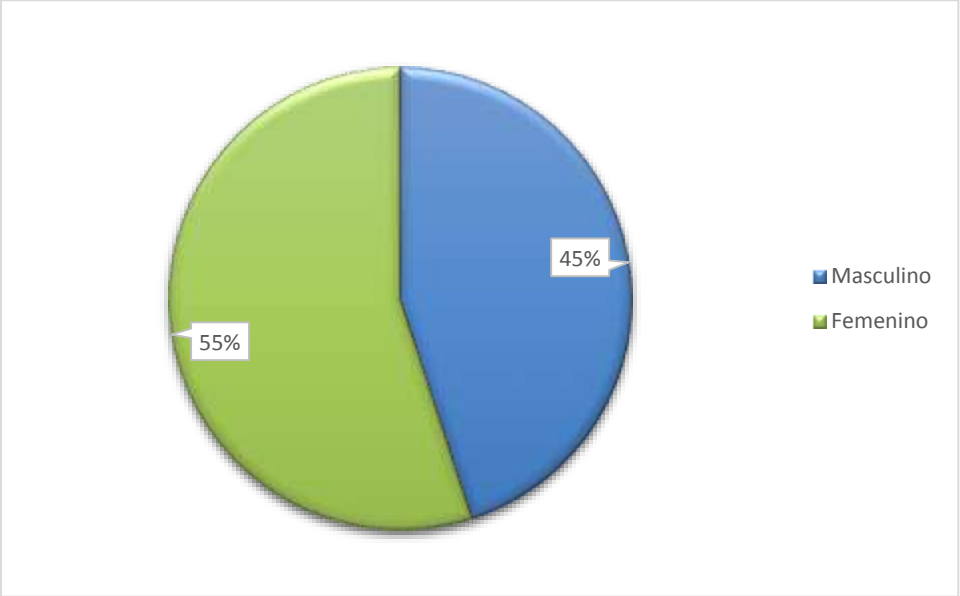
Tabla 6. Cantidad de Personas Encuestadas

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
	Masculino	18	45%
Sexo	Femenino	22	55%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 3: Cantidad de personas encuestadas



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

4.3.1.1 ¿Ha escuchado sobre los ataques informáticos en nuestro País?

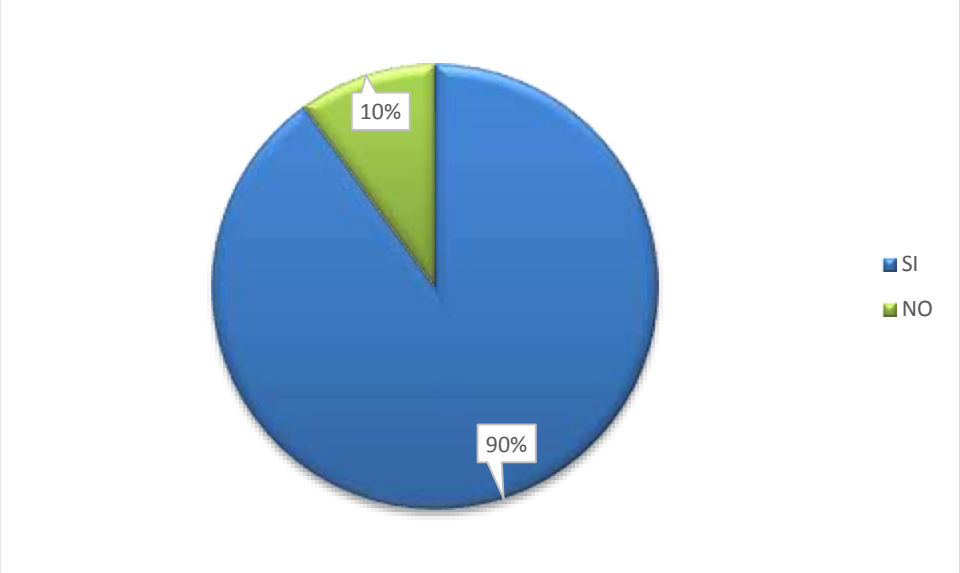
Tabla 7: Encuesta aplicada a pregunta 1

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Ha escuchado sobre los ataques informáticos en nuestro País?	SI	36	90%
	NO	4	10%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 4: Gráfico estadístico de la pregunta 1



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

OBSERVACIÓN: El gráfico sobre el indicador nos informa que:

- El 90% de 40 encuestados han escuchado o tiene noción sobre los ataques informáticos, donde se puede apreciar en primera instancia que tienen conocimiento sobre los ataques informáticos.
- El 10 % de 40 personas no han escuchado sobre estos ataques.

4.3.1.2 ¿Cuál es el tipo de delito informático que usted conoce?

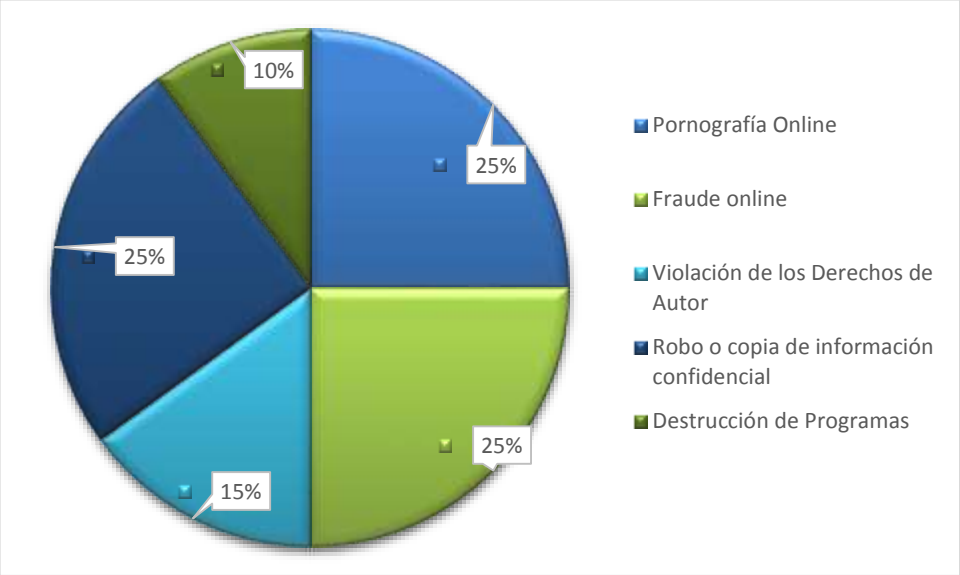
Tabla 8: Encuesta aplicada a pregunta 2

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Cuál es el tipo de delito informático que usted conoce?	Pornografía Online	10	25%
	Fraude online	10	25%
	Violación de los Derechos de Autor	6	15%
	Robo o copia de información confidencial	10	25%
	Destrucción de Programas	4	10%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 5: Gráfico estadístico de la pregunta 2



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

OBSERVACIÓN: El gráfico informa sobre los diferentes tipos de delitos informáticos que puede sufrir alguien, los de mayores índices obtenidos en las encuestas realizadas fueron del 25% como son: robo o copia de información confidencial, pornografía online y fraude online.

4.3.1.3 ¿Con qué frecuencia cambia las contraseñas de sus cuentas electrónicas?

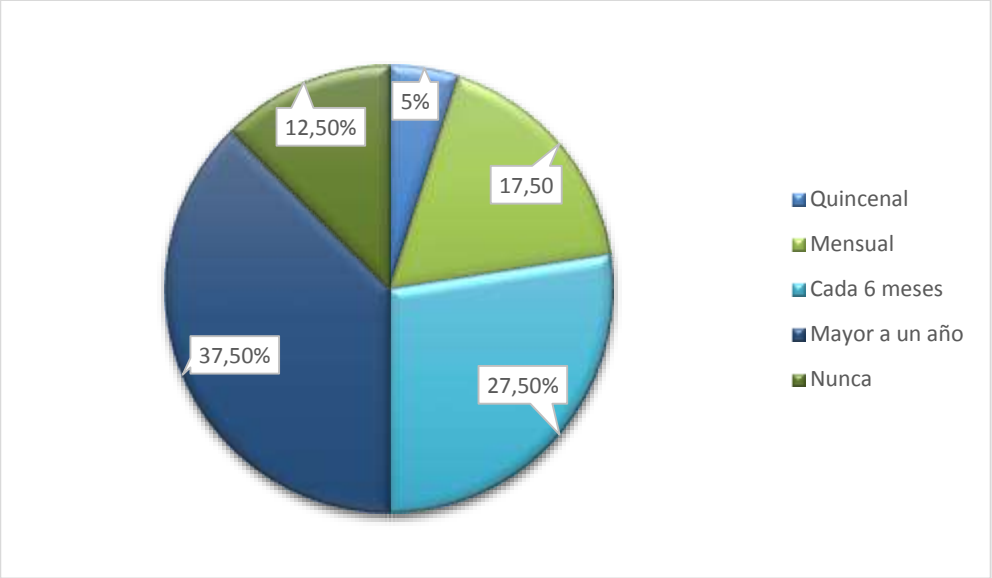
Tabla 9: Encuesta aplicada a pregunta 3

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Con qué frecuencia cambia las contraseñas de sus cuentas electrónicas?	Quincenal	2	5%
	Mensual	7	17,50%
	Cada 6 meses	11	27,50%
	Mayor a un año	15	37,50%
	Nunca	5	12,50%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 6: Gráfico estadístico de la pregunta 3



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

OBSERVACIÓN: La poca gestión que los usuarios realizan en sus cuentas electrónicas es interesante porque la gente no toma el debido tiempo para realizar los cambios constantes de sus contraseñas en sus cuentas pudiendo ser vulnerables, el 37,50% de los usuarios realizan cambios de sus contraseñas mayor a un año.

4.3.1.4 ¿Ha sido víctima de un ataque informático?

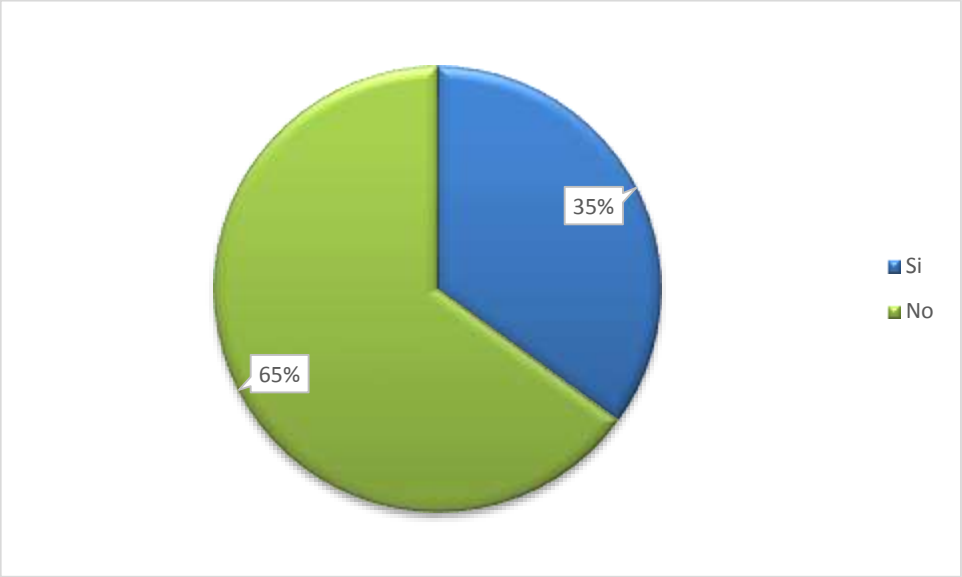
Tabla 10: Encuesta aplicada a pregunta 4

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Ha sido víctima de un ataque informático?	Si	14	35%
	No	26	65%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 7: Gráfico estadístico de la pregunta 4



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

OBSERVACIÓN: El 35% de los encuestados han sido víctimas de un ataque informático siendo un estadística baja, es muy preocupante porque han vulnerado sus derechos a la privacidad de su información, sin embargo el 65% no han sufrido algún tipo de ataque informático.

4.3.1.5 ¿Conoce sobre los perjuicios que ocasionan estos ataques informáticos?

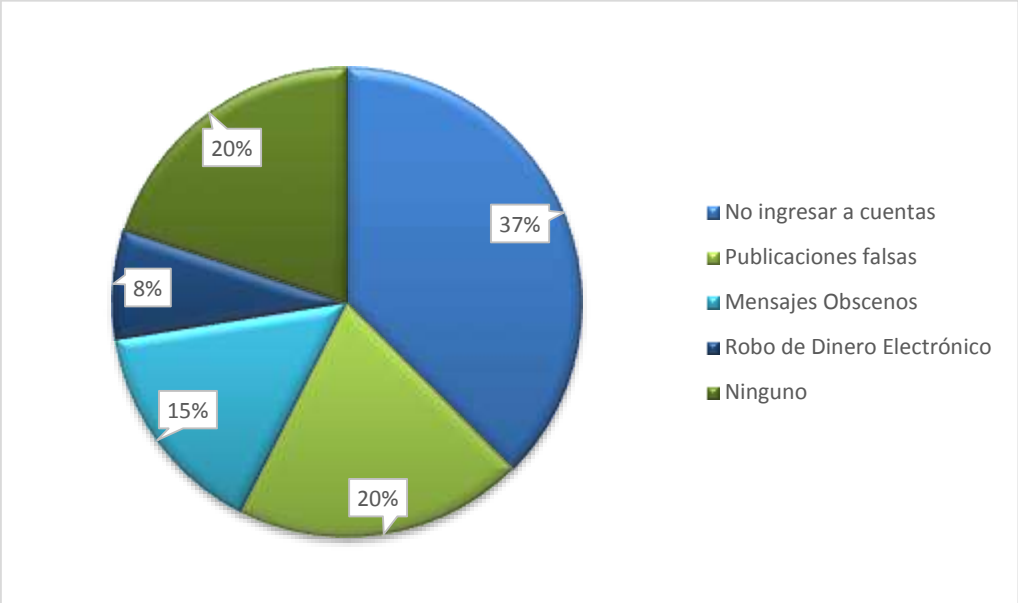
Tabla 11: Encuesta aplicada a pregunta 5

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Conoce sobre los perjuicios que ocasionan estos ataques informáticos?	No ingresar a cuentas	15	37%
	Publicaciones falsas	8	20%
	Mensajes Obscenos	6	15%
	Robo de Dinero Electrónico	3	8%
	Ninguno	8	20%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 8: Gráfico estadístico de la pregunta 5



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

OBSERVACIÓN: Por medio de este indicador se pudo obtener el resultado de los perjuicios ocasionados por un ataque informático:

- El 37% de los usuarios no pudieron ingresar debido que fueron cambiadas sus contraseñas en sus cuentas electrónicas.

4.3.1.6 ¿Ha escuchado hablar sobre los peritos informáticos?

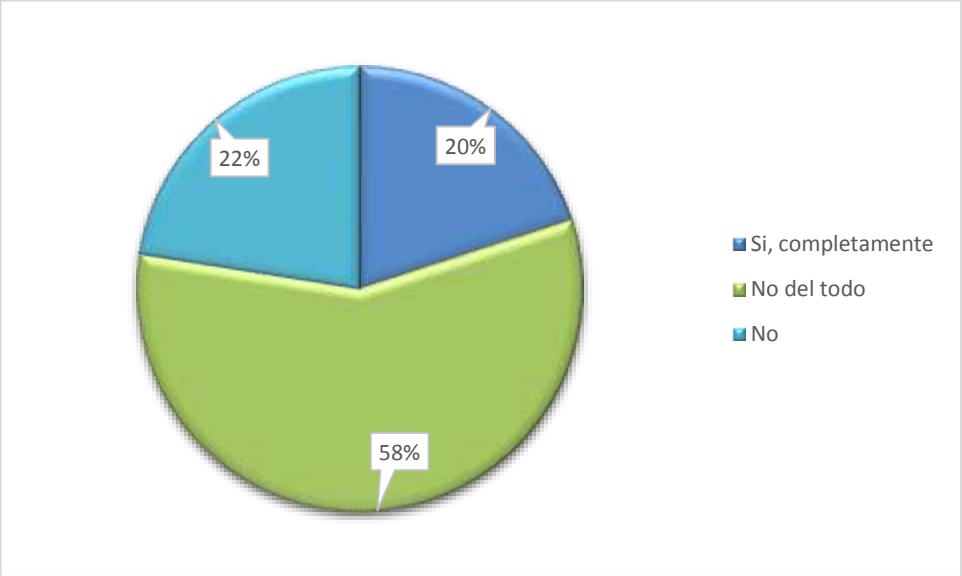
Tabla 12: Encuesta aplicada a pregunta 6

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Ha escuchado hablar sobre los peritos informáticos?	Si, completamente	8	20%
	No del todo	23	58%
	No	9	22%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 9: Gráfico estadístico de la pregunta 6



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

OBSERVACIÓN: El gráfico informa que las personas no tienen un conocimiento definido sobre el tema, el 58% no conocen si existen profesionales especializados en el País para poder analizar su situación ante un ataque informático y encontrar de dónde provino el ataque de aquella intromisión.

4.3.1.7 ¿Conoce si en la fiscalía existe un departamento que investiga éstos tipos de delitos?

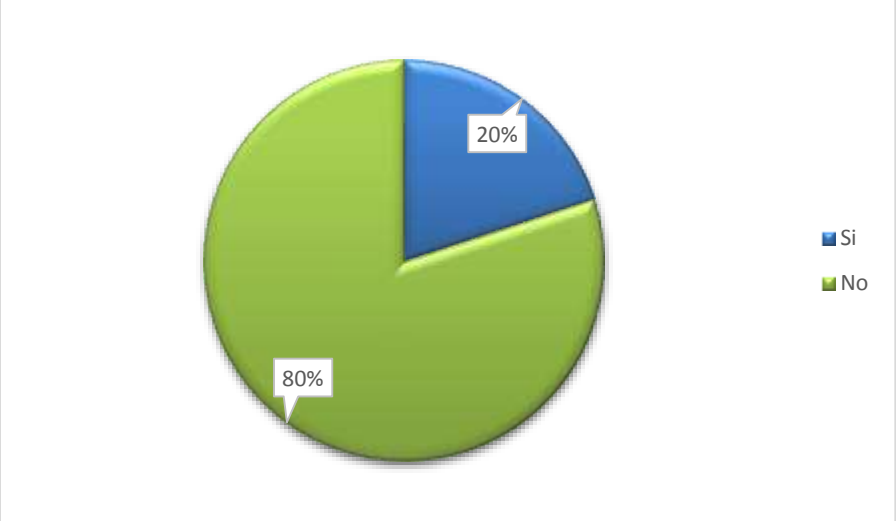
Tabla 13: Encuesta aplicada a pregunta 7

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Conoce si en la fiscalía existe un departamento que investiga éstos tipos de delitos?	Si	8	20%
	No	32	80%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 10: Gráfico estadístico de la pregunta 7



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

OBSERVACIÓN: El 80% de las personas encuestadas no conocen cuáles son los departamentos involucrados que se encargan de investigar estas operaciones delictivas, considero que en la Fiscalía del Guayas (Edificio La Merced) se brinda poca información concreta de las diferentes unidades operativas de justicia.

4.3.1.8 ¿Conoce cuáles son los procedimientos para realizar este tipo de denuncia?

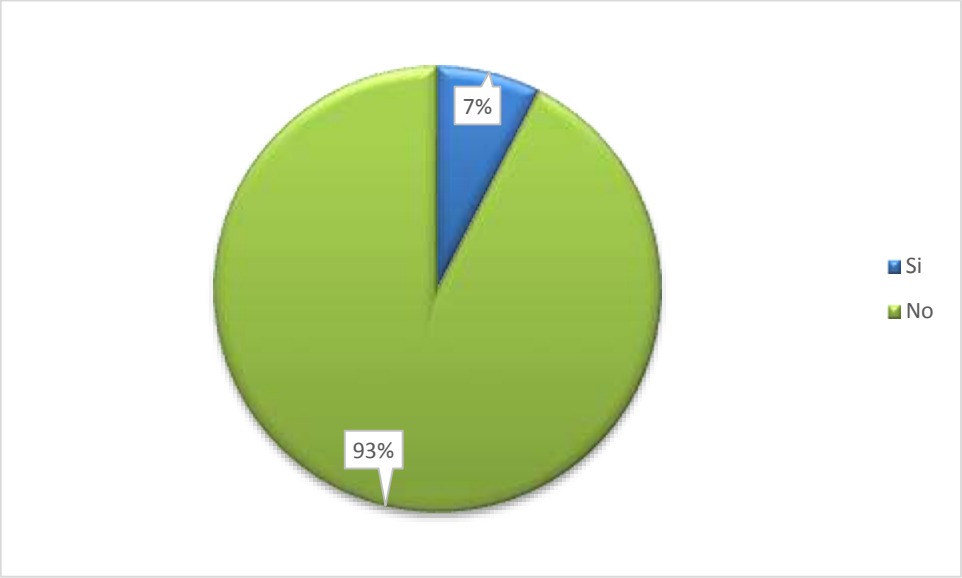
Tabla 14: Encuesta aplicada a pregunta 8

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Conoce cuáles son los procedimientos para realizar este tipo de denuncia?	Si	3	7%
	No	37	93%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 11: Gráfico estadístico de la pregunta 8



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

OBSERVACIÓN: El análisis porcentual es alto en este indicador con un 93%, considero que al no tener información de los procedimientos no fueron resueltas y quedaron sus denuncias en el olvido.

4.3.1.9 ¿Cree usted que deberían existir campañas de prevención para éste tipo delito?

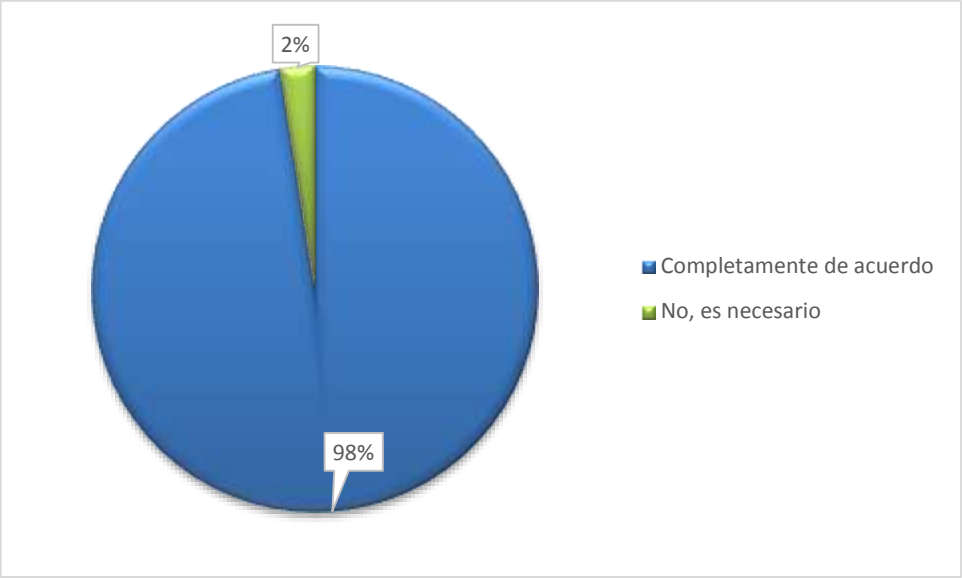
Tabla 15: Encuesta aplicada a pregunta 9

INDICADORES	PARÁMETROS	CANTIDAD	PORCENTAJE
¿Cree usted que deberían existir campañas de prevención para éste tipo delito?	Completamente de acuerdo	39	98%
	No, es necesario	1	2%
TOTAL		40	100%

Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

Figura 12: Gráfico estadístico de la pregunta 9



Fuente: Datos de personas encuestadas que realizaban alguna denuncia en la Fiscalía del Guayas.

Elaborado por: Autor

OBSERVACIÓN: El 90% de las personas, les interesaría recibir charlas para no ser víctimas de algún tipo de ataque que esté vinculado con la informática y conocer más a fondo sobre las unidades investigativas de la fiscalía.

4.4 Entrevistas

- **Entrevistado: Ing. Roberto Olaya - Jefe de la empresa HACK - SECURITY**

Entrevista

¿Con qué frecuencia las personas le piden asesoría por temas de delitos informáticos?

En un promedio semanal, tres personas vienen a mi oficina con algún problema referente a delitos informáticos, al momento de realizar la investigación el usuario tienen que firmar un contrato de confidencialidad.

¿Cuáles son los casos más frecuentes de asesoría reflejado en la anterior pregunta?

- Espionaje
- Fraude Bancario
- Extorsión Marital

¿Cuáles son las áreas de investigación en el Ecuador para estos delitos informáticos?

- Área policial.
- Área de función judicial.
- Consultores externos.

¿Qué objetivos tiene su empresa para resolver estos delitos informáticos?

- Proporcionar asesoría.
- Guiar al perjudicado sobre cómo debe realizar las denuncias respectivas en la fiscalía.
- Esclarecer quien es el culpable para que pueda realizar la denuncia respectiva en la fiscalía del cual el informe que se le brinda al perjudicado no tiene

ningún sustento legal por lo que tienen que comenzar de nuevo con la investigación cuando denuncie en la fiscalía.

¿Cómo considera usted la nueva reforma del Código Orgánico Integral Penal para castigar estos delitos informáticos?

Considero que en Ecuador se está tomando con mayor profundidad los temas de incidentes informáticos, existen leyes que ya penalizan a estos individuos.

¿Considera que ha cambiado la infraestructura tecnológica para investigar temas de delitos informáticos en Ecuador?

Considero que ha cambiado poco la infraestructura de investigación antes no se contaba con un área donde almacenar la evidencia, los procesos eran muy lentos, no existían muchos especialistas dedicados a realizar peritajes informáticos. Aunque falta por mejorar los procesos operativos para estas investigaciones.

- **Entrevistada: Fiscal Penal Patricia Morán – Unidad Especializada en Personas y Garantías**

<u>Entrevista</u>

¿Cuál es la situación actual de los delitos informáticos en el Ecuador?

Antes estos delitos no estaban tipificados, con la nueva reforma del Código Integral Penal, ya se puede penalizar a estos individuos inescrupulosos que buscan un bien común. En nuestro país se trabaja con personal muy competente como son los peritos informáticos acreditados, que son los encargados de analizar la evidencia digital para que el Juez pueda tomar las debidas decisiones.

¿Qué procedimientos considera como críticos frente una investigación forense?

- No mantener el procedimiento de cadena de custodia en el proceso de investigación.
- Que el sospechoso utilice el anonimato, eso dificulta en cierta medida al investigador digital.
- Recoger pistas, sin ninguna instrucción fiscal.

¿Cómo puedo realizar mi denuncia en la fiscalía ante un delito informático?

- Llevar su cédula de identidad
- En forma verbal o escrita mediante una narración breve de cómo sucedieron los hechos, fecha y lugar. Si se conoce a los presuntos autores, incluirá todos los datos que se conozca sobre los mismos.
- Acta de reconocimiento de la denuncia o reconocimiento de la firma.
- La persona encargada por medio de su testimonio la deriva al área correspondiente.
- Indagación previa.

¿Cuáles son los delitos más comunes presentados en la fiscalía?

- Cesión, publicación, utilización o transferencia de datos personales sin autorización.
- Robo bancario.

¿Los peritos informáticos acreditados en la fiscalía son capacitados constantemente por alguna entidad?

Actualmente el personal acreditado no recibe capacitaciones, ellos se capacitan por su propia cuenta para que puedan cumplir de manera eficiente su trabajo. El perito informático para poder ser acreditado, debe tener título profesional o dos años de experiencia en su profesión.

¿Cuáles son los sujetos que intervienen en un proceso penal?

- Juez.
- Fiscal.
- Ofendido.
- Procesado.
- Perito (en caso de ser necesario).
- Abogados.

¿Cuál es la clasificación de los delitos en la fiscalía?

- Delitos contra la Seguridad Pública.
- Delitos contra las Personas.
- Delito de Corrupción de Menores.
- Delitos de explotación sexual.
- Delito contra la propiedad.

Entre otros delitos tenemos:

- Delitos informáticos.

¿Cuáles son las etapas en el proceso penal?

- Instrucción fiscal
- Etapa intermedia
- El juicio
- La impugnación

- **Entrevistada: Licenciada Yelena Casanova – Perita Informática con acreditación vigente**

Entrevista

¿Después de que haya sido escogida durante la terna para investigar un caso de Cesión, Publicación, Transferencia de datos qué procedimiento sigue?

- ✓ Ponerme de acuerdo con la víctima.
- ✓ Hacer consultas de todos los sucesos que involucren al denunciante.
- ✓ Investigar perfiles de cuentas en redes sociales, que involucren al sospechoso.

¿Qué herramientas utiliza para realizar investigaciones forenses digitales?

Software libre que sean con conocidos y certificados en el medio tecnológico por ejemplo:

- ✓ Winmd5free.
- ✓ Kali.
- ✓ FTK IMAGER.
- ✓ AUTOPS, entre otros.

¿Qué tipo de casos de investigación se inclina usted?

Son muy pocos los casos de Cesión, Publicación, Transferencia de datos, porque el contenido a investigar es muy delicado pero me inclino más por auditorías informáticas forenses.

¿Qué opina usted sobre los casos de Cesión, Publicación o Transferencia de datos personales?

Considero que la ciudadanía debe utilizar las redes sociales de manera responsable para que no puedan sufrir ningún tipo de agravio, del cual no pueda estar involucrado su integridad personal y de sus familiares.

¿Trabaja en conjunto con un proveedor de servicio de internet para poder localizar al sospechoso?

Siempre y cuando exista una orden por parte del Fiscal encargado.

¿Qué aspectos considera usted, sobre la lentitud de los procedimientos legales de un peritaje informático?

- Falta de recolección de pistas.
- Las personas no denuncian.
- Asignación de un perito.
- Falta de conocimiento de los fiscales.
- Herramientas Tecnológicas.

- **Entrevistado: Dr. Santiago Acurio del Pino - Juez de la Corte Provincial de Pichincha**

Entrevista:

¿Qué opina sobre el delito de Cesión, Publicación o transferencia de datos personales?

Las redes sociales está tomando bastante aceptación por los internautas, por lo tanto los delitos de esta índole va aumentando cada vez más, donde existen muchas denuncias sobre estos casos.

¿Considera que en el País deben existir más centros de investigación para estos delitos?

Por su puesto, como Juez me he mantenido en la lucha constante para que se fomente centro de capacitaciones e unidades investigativas que sean específicos para estos delitos, para así poder brindar un soporte a todas las provincias de nuestro País.

¿Considera que el País deba constar un estándar de trabajo?

Aunque existe en el COIP en el artículo 500 una guía de proceso, aún falta un estándar operacional de trabajo.

¿Qué opina sobre la nueva reforma del Código Integral Penal?

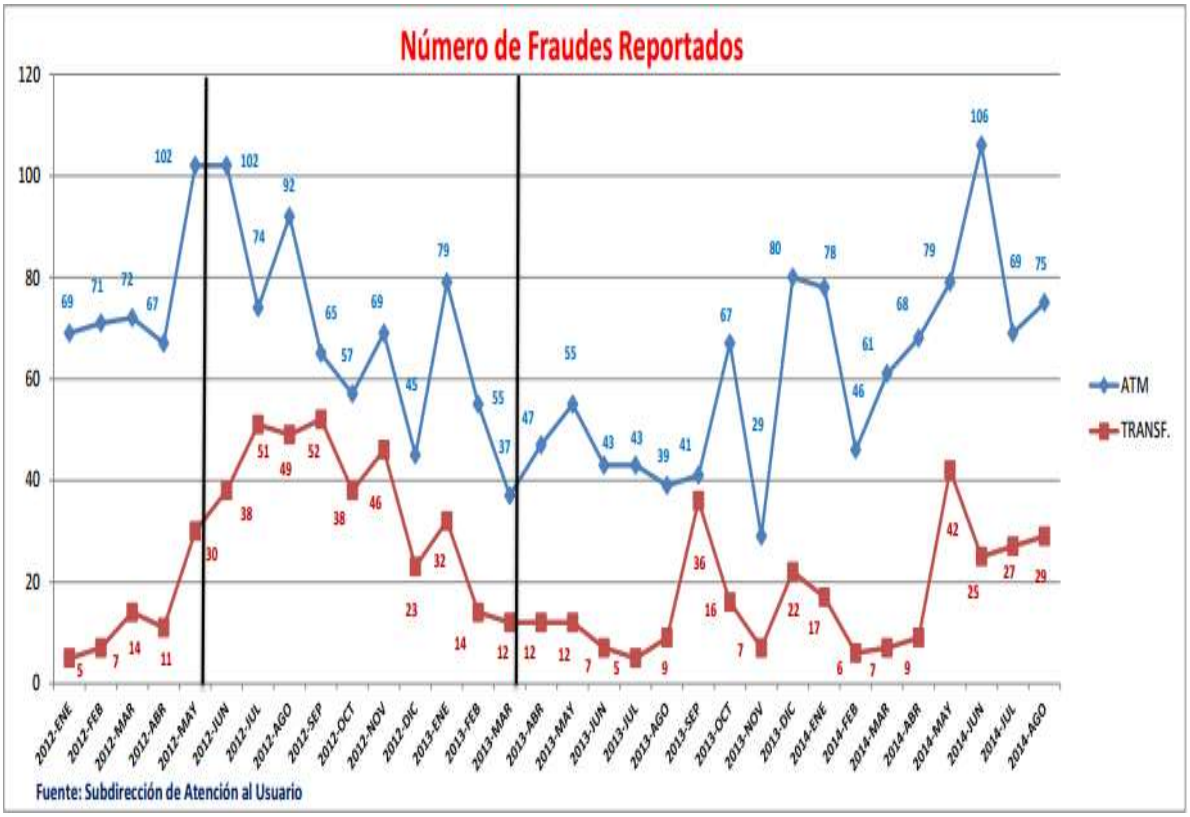
Es un cambio grande que ha tomado el País, porque ahora incluyen penalizaciones para los delitos informáticos.

- **Entrevista**

La información obtenida se lo realizó a través de una entrevista a una funcionaria pública de la Superintendencia de Bancos y Seguros, con la finalidad de brindar un soporte de veracidad al proyecto de Grado. Por motivo de confidencialidad se va reservar sus datos y su cargo laboral ya que el trabajo es estrictamente académico.

¿Estadística sobre los casos denunciados de delitos informáticos en la Superentendida de Bancos y Seguros del año 2012 hasta Agosto del 2014?

Figura 13: Fraudes Reportados S.B.S



Fuente: Superintendencia de Bancos y Seguros

¿Cuál es el departamento encargado en procesar estas denuncias?

La SBS recibe los reclamos por parte de los usuarios del sistema financiero que se sienten perjudicados, en este link:

http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_XX_cap_IV.pdf.

Se puede encontrar la norma vigente para la atención de reclamos, en la misma se indica que los reclamos serán atendidos por un delegado del señor Superintendente, actualmente el área que atiende estos reclamos es la Dirección Nacional de Atención y Educación al Usuario.

Las denuncias se realizan a través de la Fiscalía.

¿Con qué entidad del gobierno trabaja conjuntamente la S.B.S para poder resolver estos delitos?

Con la Fiscalía principalmente. De acuerdo al artículo 226 de la constitución podemos coordinar con cualquier institución del estado.

"...Art. 226 de la Constitución de la República, determina que: "Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la Ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución". "

¿Medidas de control que está tomando la S.B.S para los fraudes informáticos bancarios?

Las funciones que realiza la Superintendencia para mitigar los riesgos de fraudes informáticos en las entidades del sistema financiero controladas por dicho organismo de control, son:

1. La Superintendencia ha emitido normativa para mantener la seguridad en los canales electrónicos a través de los cuales las entidades financieras brindan sus servicios a sus clientes.
2. Realiza un seguimiento periódico del cumplimiento de la normativa por medio de reportes e información que las entidades tienen obligación de reportar al organismo de control
3. Realiza inspecciones o verificaciones en las instalaciones de las entidades controladas a fin de verificar el cumplimiento normativo.
4. Adicionalmente la Superintendencia ha emitido la normativa para la gestión del riesgo operativo que incluye el factor de riesgo tecnológico, gestión que se realiza a través de la identificación, medición, control y monitoreo de los riesgos operativos que ayuda a evitar o reducir pérdidas financieras por deficiencias en los factores de personas, procesos, tecnología de la información y eventos externos.

Normativa de riesgos en donde se puede encontrar la norma específica para la seguridad en canales electrónicos a partir del numeral 4.3.8.
http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/nueva_codificacion/todos/L1_X_cap_V.pdf

¿Magnitudes de control para la seguridad de información de los clientes bancarios?

Las entidades del sistema financiero están obligadas a cumplir con las siguientes disposiciones normativas, que es parte de la norma de riesgo operativo que te indiqué, específicamente en estos numerales:

"**4.3.8.22.** Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos;

4.3.8.23. Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos por la entidad;".

4.5 Verificación de hipótesis

Las encuestas y entrevistas realizadas permiten la verificación de las hipótesis planteadas.

4.5.1 Contestación de hipótesis

- **Los fiscales y jueces deben tener la capacidad de resolver los delitos informáticos actuales.**

En cuanto al conocimiento de un servidor Judicial deben conocer los delitos actuales "Informáticos", pero en la práctica carecen de tal aseveración debido a que la tecnología multimedia va creciendo día a día donde se maneja parte de una

comunicación abierta que las personas tienen acceso a los diferentes tipos de comunicación. Se necesitaría de un asesor informático en la fiscalía involucrado en estos tipos de delitos informáticos o especializar al fiscal o Juez sobre metodologías de informática forense.

- **Tiempo excesivo que toma en ser asignado un perito informático en una denuncia.**

Deben crear más unidades especializadas de investigación forense digital en cada provincia del País, donde la terna de peritos debería ser seleccionada por el Fiscal Provincial y no ser centralizado porque estos tipos de delitos deben ser tratarse manera sistemática para evitar el aglomera miento de casos no resueltos.

- **Encontrar el delito informático flagrante.**

La fiscalía debe constar con departamentos informáticos especializados en rastrear, monitorear los posibles fraudes a través de redes de comunicaciones informáticas como son: Convocatorias fraudulentas de puestos de trabajo, ventas piramidales de empresas fantasmas, venta de droga, casos sexuales de pornografía infantil y extorsiones maritales.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDADCIONES

5.1 Conclusiones

De las entrevistas realizadas a diferentes expertos los casos frecuentes son: fraudes bancarios relacionados con transacciones, páginas webs falsas, clonación de tarjetas bancarias. Otras como CESIÓN, PUBLICACIÓN, TRANSFERENCIA DE DATOS PERSONALES donde se ve afectado la integridad y la intimidad de la persona. Además no se cuenta con un estándar definido de trabajo para seguir este tipo de investigaciones. Entre las conclusiones que se pudo obtener en consideración a esta investigación fueron las siguientes:

- Las autoridades del Ministerio de Justicia deben redefinir la importancia de los delitos informáticos como un delito de fácil prescripción para que se pueda emitir su premisa y específicamente quienes resuelvan su situación conozcan que al investigarlos rápido pueden evitar que la evidencia digital desaparezca. Deben existir fiscales especializados para la investigación directa de la criminalidad informática ya que es similar a cualquier delito, las autoridades que legislan y administran la justicia de nuestro País, deben legislar con una visión en el marco global de internet.

- La fiscalía debería tener peritos expertos en la materia informática para derivar a los fiscales competentes.

- Se puede reducir el impacto de los delitos informáticos, haciendo uso de la tecnología de forma responsable y eficaz.

- No hay en el País un estándar metodológico sobre el manejo de la evidencia en la cadena de custodia, lo cual este trabajo permite fundamentar la importancia que brinda IOCE, como una organización que implica mejorar la estructura de procedimientos al manejar la evidencia digital.

- La importancia y los beneficios que brinda la informática forense tanto en la Policía y Fiscalía son de gran soporte, porque gracias a la extracción e investigación de cada escena del ilícito, se pueden hallar las pistas necesarias para encontrar cual fue el responsable de aquel delito informático.

5.2 Recomendaciones

Entre los objetivos planteados en esta tesis, es brindar algunas recomendaciones para minimizar el impacto de los delitos informáticos:

- Los fiscales, jueces y todos los miembros que administran justicia deben recibir capacitación constante sobre la tendencia que involucra los delitos informáticos, procedimientos operativos, normas y estándares relacionado con el manejo de la cadena de custodia.

- Las instituciones públicas dedicadas a este tipo de investigaciones, necesitan implementar campañas en las escuelas y en los colegios para concientizar el uso de herramientas tecnológicas para así disminuir el impacto de los delitos informáticos.

- Es necesario que las autoridades judiciales de la ciudad de Guayaquil donde se denuncien él delito de "Cesión y Publicación", se maneje de forma inmediata como delito flagrante, debido que la evidencia puede desaparecer, o el atacante puede deshabilitar la cuenta electrónica.

- Otro punto que debe cambiar en el país, que cada ciudad deba constar con departamentos especializados, para poder realizar este tipo de investigaciones tecnológicas. Áreas acopladas con los recursos tecnológicos, personal suficiente no limitado y herramientas forenses necesarias para mantener el resguardo de las evidencias digitales.

- Los lineamientos que ofrece IOCE, sobre el manejo de la evidencia digital, guía sobre los procesos desde el inicio de la recolección de evidencia, hasta los informes periciales. Como País es importante aprender de las experiencias de cómo otros analizan este tipo de escenas referente a los delitos informáticos.

CAPÍTULO 6

ANÁLISIS Y EVALUACIÓN IOCE DE UN PERITAJE INFORMÁTICO

6.1 Antecedentes de la propuesta

La tendencia de los crímenes cibernéticos en el País surgió desde el año 1999 donde no existía algún tipo de ley que permitiera una sanción para estos infractores, por lo que tampoco no se constaba con el personal capacitado y las herramientas e instalaciones tecnológicas para poder enfrentar estas amenazas, a medida del transcurrir de los años, las observaciones sobre estos delitos cibernéticos aumentaban sobre la banca electrónica así después de un tiempo el congreso aprobó la Ley de Comercio Electrónico, firmas digitales entre otros, donde aún existían falencias sobres las leyes establecidas. Donde poco a poco se capacitó al personal para que puedan ser un soporte en la administración de justicia, a su vez también hubo cambios en el Código Integral Penal. La principal diferencia que existe entre cualquier tipo de delito en común con el delito informático es que está relacionado con la evidencia en aspectos técnicos, donde el crimen a investigar que representa puede ser tornado en un marco global adjuntando un grado de responsabilidad, complejidad y de esfuerzo por parte del perito designado, en nuestro país existen pocos departamentos involucrados en esta área de investigación como es criminalística. El propósito no es preocuparnos por la tecnología, sino que hagamos conciencia sobre el buen uso de la navegación de manera responsable y adecuada sobre el manejo de correo electrónico, también en realizar nuestras transacciones, hacer actos más cuidadosos, para qué en un futuro no ser víctimas de un robo o fraude informático. En la presente tabla se muestra los actos ilícitos utilizando medios informáticos reportados en la Fiscalía del Guayas.

Tabla 16: Apropiación ilícita utilizando medios informáticos 2014

VALORES	TOTAL
Suma de NDD	323
Suma de SOLUCIONES PROCESALES	265
Suma de INDAGACIONES PREVIAS	296
Suma de INST. FISCALES	10
Suma de ACUSATORIO	12
Suma de ABSTENTIVO	1
Suma de MIXTO	1
Suma de EXTINCION DE LA ACCION	0
Suma de SOBRESEIMIENTO	0
Suma de SENT. CONDENATORIAS	5
Suma de SENT. ABSOLUTORIAS	1
Suma de SENTENCIA MIXTAS	0
Suma de DESESTIMACION	92
Suma de CONVERSION (F)	0
Suma de PROCEDIMIENTO ABREVIADO	3
Suma de ACUERDOS REPARATORIOS	1
Suma de SUSPENSIÓN CONDICIONAL	5
Suma de OPORTUNIDAD	3
Suma de SIMPLIFICADO (t)	0
Suma de ARCHIVO PROVISIONAL (F)	27
Suma de ARCHIVO DEFINITIVO (F)	127
Suma de DESPLAZAMIENTO POR NULIDAD	0
Suma de PRESCRIPCIONES	1
Suma de AUDIENCIAS REALIZADAS (PRELIMINARES)	10
Suma de AUDIENCIAS FALLIDAS (PRELIMINARES)	8
Suma de AUDIENCIAS REALIZADAS JUZG.	4
Suma de AUDIENCIAS FALLIDAS JUZG.	11
Suma de LLAMAMIENTO A JUICIO	8

Fuente: Fiscalía Provincial del Guayas, 2014

6.2 Objetivo

Realizar una investigación forense donde consiste en aplicar algunos tecnicismos siguiendo la metodología IOCE, con el propósito de poder normalizar los lineamientos operativos que nos permitan poder manejar las pistas necesarias para poder esclarecer el caso planteado y así hallar los hechos necesarios en la indagación, entre las cuales debemos tener presente algunos objetivos, con la finalidad de alcanzar con una mayor efectividad la parte investigativa:

- Detectar y preservar los indicios que el perito informático considere necesario.
- Asegurar la cadena de custodia y mantener en resguardo los medios electrónicos de información.
- Garantizar la efectividad de cada procedimiento.
- Realizar las imágenes forenses respectivas de los medios digitales para llevar a cabo el proceso de análisis.
- Identificación de los rastros en la escena del crimen del cual nos permitirá encontrar respuestas de que o quiénes fueron los responsables de aquel delito cometido.
- Redactar de manera eficiente los informes que será de soporte para el fiscal, donde se detalla como ocurrió el hecho, los procesos de las intromisiones y las herramientas forenses utilizadas.
- Medidas de prevención utilizando mecanismos de seguridad, que puedan ser utilizados como guía de sustento.

6.3 Análisis de la metodología IOCE

Es una organización dedicada a las buenas prácticas de metodologías, estándares y procesos para la recolección de evidencia digital, donde varios grupos de profesionales brindan información sobre el análisis forense, en la que están involucrados documentos, hardware, software y análisis de la evidencia digital, implica recomendaciones sobre cómo mantener la evidencia por parte del personal forense, abarca desde el inicio con procedimientos, conservación y análisis de la evidencia digital incautada hasta poder sustentarlo en una corte. Entre la estructura principal de esta documentación metodológica consiste en:

- Garantía de calidad (instrucción del personal, documentación y herramientas forenses).
- Determinación de los requisitos de examen del caso.
- Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, procesos y responsabilidad).
- Prácticas aplicables al examen de la evidencia de digital.

- Localización y recuperación de la evidencia en la escena: precauciones, búsqueda en la escena, recolección de evidencia, empaquetado, etiquetado y documentando.
- Priorización de la evidencia digital.
- Examinar la evidencia: protocolos de análisis y expedientes de caso.
- Evaluación e interpretación de la evidencia
- Presentación de resultados (informes).
- Revisión del archivo del caso: Revisión técnica y revisión administrativa.
- Presentación oral de la evidencia.
- Procedimientos de seguridad y quejas.

Entre los principales podemos tener:

- La persona encargada en recolectar y analizar la evidencia debe estar altamente capacitado.
- Toda acción que se realice, la evidencia no debe ser modificada, alterada o manipulada.
- Delegación de responsabilidad por el fiscal a la persona encargada en realizar el peritaje informático.
- La evidencia que se encuentre debe ser documentada, almacenada y debe estar disponible para su fututa revisión desde su fase inicial hasta la fase final.
- Debe cumplir fundamentos legales de investigación para obtener un reporte final.

La investigación permite fomentar la metodología consistente para la producción de resultados comparables, a fin de facilitar el intercambio de datos. Es importante la documentación y las guías que brinda esta organización porque abarca desde la investigación hasta la presentación de pruebas.

6.4 Análisis de factibilidad

El modelo de esta propuesta consiste en evaluar la factibilidad de poder realizar un peritaje informático, conociendo la estructura metodológica IOCE que ofrece algunos lineamientos sobre la recolección de evidencia digital, la justificación

necesaria para realizar un análisis forense, lo cual permite algunas recomendaciones de índole orientativa sobre el impacto social de este tipo de investigación, lo cual permite minimizar el impacto de los delitos informáticos, también está destinado a todos quienes llegan en primera instancia al lugar de la escena, entre los puntos necesarios tenemos los siguientes:

- Análisis de fase inicial.
- Diseñar el perfil del supuesto implicado.
- Recolección de evidencias.
- Flujo de trabajo de los objetivos de un caso.
- Plan de pruebas.
- Cronograma de actividades.
- Análisis y evaluación de evidencias.
- Almacenamiento de evidencias.
- Uso de herramientas forense.
- Asesoramiento integral a través de conclusiones de informes periciales.

6.5 Requerimientos del personal

Para la asignación de un caso, se debe tomar en cuenta las siguientes características que el profesional debe cumplir para que pueda ser apto para el perfil requerido de un caso, de las cuales son:

- Conocimientos técnicos en el manejo de evidencia digital.
- Nivel de competencia que tenga la persona por ejemplo: alguna certificación que aporte más a su perfil de investigador.
- Entrenamiento y evaluaciones periódicas.
- El individuo a realizar la extracción de información debe tener los permisos que está acreditado para realizar dicho trabajo.
- Proporcionar las prueba encontradas para que sea soporte del veredicto.

Cuando el perito llegue a la escena del crimen, debe cubrir la intangibilidad de los eventos que considere necesarios, definir cuáles son los indicios de mayor importancia, para lo cual es necesario que realice:

- Asentar la fecha, hora y lugar de la escena del crimen.
- Restringir el acceso a terceras personas.
- Documentar las diferentes opiniones que pueda tener la víctima.
- Registrar cada evidencia necesaria según lo observado.
- Evaluar la escena, cada dispositivo electrónico es de gran valor.
- Tomar un registro de cada persona que realice la recolección de la evidencia.

6.6 Fundamentación

Como procedimiento en este capítulo se va abordar la descripción de software libre y licenciado que pueden ser de gran utilidad para poder esclarecer algún tipo de ataque informático, a través de esto se va realizar un caso práctico de un delito que se ve muy frecuente y es denunciado en nuestra sociedad de la cual va consistir en simular el peritaje informático correspondiente: realizar una imagen forense, pasos para manejar la cadena custodia, hallar y esclarecer pistas, cronograma de eventos del imputado y como analizar la evidencia.

6.7 Perfil del Criminal

Para que el investigador pueda identificar el perfil del delincuente se puede utilizar dos tipos de métodos que son:

Inductivo: Se relaciona a través de crimines similares, perfiles de personas que han cometido el mismo acto, se aplica un estudio por medio de estadísticas del cual se obtiene los resultados esperados, pero este método no es tan específico para ese tipo de delito y pocas veces se puede descubrir al criminal ya que las variables son muy grandes.

Deductivo: Consiste en las comprobaciones observables que se pueda tomar en la escena para poder recoger datos generales y así brindar un gran soporte en la conclusiones. Para poder construir la escena del crimen hay que procurar seguir los siguientes pasos como son:

- Observación detallada del crimen.
- Segmentar y correlacionar patrones que nos permitan aclarar las ideas sobre el caso investigado.

6.8 SKRAM

Fue creada por Donn Parker, el lo cual nos permite crear una reseña del perfil del atacante entre las definiciones de sus siglas tenemos:

- **S:** Habilidades, está relacionado si el sospechoso tiene algún tipo de destreza con lo que respecta a términos de tecnología, evasión de sistemas, borrado de huellas digitales entre diversos temas más.
- **K:** Conocimiento, aunque es muy similar a las habilidades, este abarca temas generales, como una investigación, planificación de la víctima, el investigador debe descifrar como realizo el ataque y que competencia específica utilizo.
- **R:** Recursos, los componentes implicados en el proceso investigativo, el perito debe relacionar cada pista que tenga con cualquier red del implicado.
- **A:** Autoridad, investigar cómo pudo tener acceso esa persona, como el delincuente pudo obtener información que tipo de métodos utilizo para poder realizar su ataque.
- **M:** Motivo, analizar ciertas preguntas ¿Por qué lo realizó?, ¿Cómo lo hizo?, ¿Qué medidas utilizó?, ¿Qué ganancia pudo obtener?, entre otras temas más.

Ejemplo de SKRAM:

En la ciudad de Guayaquil la empresa "XT", contrata a un especialista dedicado a la investigación de computo forense, donde en el informe de denuncia presentada

indica que el jefe del departamento de contabilidad, le están borrando los balances o al parecer están cambiando los valores, donde se está alterando los sueldos, proveedores entre diversos contenidos más, este tipo de información es de gran importancia para la organización, se desconoce la hora que fue realizado el ataque pero el jefe nos explica que no ha ingresado a su máquina desde las 10:00 AM por motivos de una reunión, cuando regreso a sus itinerarios 3 horas después, encontró que ya no existía dicha información, cabe mencionar que la información se encontraba almacenada en una carpeta personal y en un archivo en Excel.

Como crear el perfil del atacante

SKILL

Utilización de computadora, redes, utilitarios de ofimática.

KNOWLOADGE

Información de la empresa, investigación exhaustiva del Jefe de aquel departamento, contraseñas, jerarquía de archivos.

RECURSE

Computadoras, redes de datos, software de acceso.

AUTHORITY

Nivel de permisos del atacante, si creó un usuario con privilegios administrativos o si pertenece a la empresa.

MOTIVE

Por alguna deuda pendiente, un empleado inconforme por su salario, algún tipo de venganza o por demostrar sus habilidades.

6.9 Línea de tiempo de la investigación

Consiste que el investigador desde una base inicial, mida tiempos, tome la evidencia necesaria para poder encontrar pruebas, para señalar en un futuro las conclusiones más relevantes, existen dos maneras de poner determinar las indagaciones:

- **Línea previa:** Implica cuales fueron los sucesos iníciales, entrevistas de las partes y recoger pistas que favorezcan a resolver el delito.

- **Línea exploración:** Pone mucho énfasis en lo que respecta al análisis, verificar cada detalle de ficheros, archivos, métodos para poder extraer información de la evidencia, determinar horas de actividad en la computadora al ser analizada y se basa en evaluaciones técnicas.

6.10 Identificación de la evidencia

Incidente: Cuando al tratar un acontecimiento sobre problemas de ataques de seguridad informática en una organización, es necesario realizar los análisis respectivos de la recolección de los dispositivos electrónicos. Al momento de realizar la entrevista a la persona encargada hay que formular las siguientes preguntas de acuerdo a los diferentes sucesos en que haya ocurrido el incidente de las cuales son básicamente las necesarias para poder obtener información.

- Tiene en su organización un firewall, ¿Cuál es?
- ¿Quién fue la persona que se dio cuenta del incidente?
- ¿Cómo departamento de sistemas, tiene manuales de políticas de seguridad?
- ¿Considera alguna persona que fue el que provoco el incidente?
- Como es su topología de red, accesos de intranet e internet.
- Mantiene actualizaciones de sus equipos informáticos.
- Cuál es la información más crítica para su organización.
- Realiza respaldos de todos sus sistemas.
- Manejan licenciamiento de software.

- Que plataformas de hardware están utilizando.
- Tiene las listas de las personas con sus accesos respectivos.
- Cuantos o cuales fueron los usuarios comprometidos por el acto cometido.
- Cuáles son las restricciones para los usuarios.
- Hay un manual de política del departamento de sistemas.
- Cuáles son los horarios de los trabajadores.

6.11 Manejo de evidencia Digital

La importancia de la protección inicial es de mucho valor, porque hay que mantener la conservación de todos los elementos digitales, con el fin de eludir cualquier alteración o mala manipulación. La evidencia digital exige establecer medidas necesarias para la preservación, la primera persona encargada de llegar será la responsable de mantener el lugar así sea por una orden o sentido común ya que por ser una fuente de información es muy frágil, delicada y puede dañarse por un algún tipo de manejo inadecuado. Por eso es necesario tener en consideración algunas de las precauciones al momento de realizar el peritaje informático, en base a esto podemos realizar algunos pasos básicos dentro de una indagación:

- Realizar, iniciar y evaluar la evidencia de acuerdo al marco legal del país.
- Llevar un registro de los instrumentos recogidos como hardware, software, tomar fotos de los equipos, series, facturas, etc.
- Priorizar los medios de almacenamiento para realizar la extracción de la información.
- Especificar y puntualizar las características de todo el proceso.
- Desconectar todos los equipos ordenadamente para que no pueda ocurrir algún daño en los medios.

La evidencia digital tiene algunas particularidades:

- Es volátil
- Fácil de alterar
- Manipulable
- Correos, mensajerías instantáneas.

- Documentos, archivos.
- Historiales de navegación.
- Historial de programas instalados.
- Conexiones USB, donde cada conexión del dispositivo se guarda en él equipo un registro identificador que está guardado en el registro del computador.
- Perfiles de usuarios (tipo de cuentas administrador, estándar).

Cadena de custodia

Se fundamenta 4 principios como son: identificación, preservación, análisis, presentación.

- Marco Legal.
- Documentar cada evidencia digita incautada.
- Grabar, tomar fotos en la escena del delito.
- Evitar cualquier tipo de negligencia en el proceso de la imagen forense.
- Detallar cada aspecto y hecho donde se encontraba la evidencia digital.
- Calcular el código hash de cada imagen forense.

6.12 Herramientas de análisis forense

Existen diversas herramientas que sirven para realizar una investigación forense dentro de diferentes entornos de las cuales tenemos desde software licenciado o GNU, entre las cuales tenemos:

Software Licenciados

OXYGEN FORENSIC

- Su precio está entre $490,00 y $7999,00.
- Herramienta para forense de dispositivos móviles.

Figura 14: Software OXIGEN FORENSICS

Fuente: http://www.oxygen-forensic.com/

UFED TK

- Su precio está entre $6000,00.
- Análisis forense de dispositivos móviles.
- Visualización y generación de informes.

Figura 15: Equipo UFED TK

Fuente: http://www.cellebrite.com/

Software GNU

AUTOPSY

- Contiene múltiples funciones, es una herramienta con gran velocidad para la extracción de imágenes forense.

SANTOKU

- Herramienta para auditoria informática.
- Permite realizar análisis forense en dispositivos móviles.

Figura 16: Software SANTOKU

Fuente: https://santoku-linux.com/

Entre otras herramientas forenses interesantes tenemos como son; DEFT, CAINE, KALI entre otros más

6.13 Equipos para una investigación forense

SHADOW 2

Permite tener el soporte magnético sin alterar su contenido, entre su característica principal es:

- Permite arrancar en caliente el sistema, analizar sin alterar su contenido.

HARDCOPY

- Clona discos a una velocidad de hasta un máximo de 5.5 GB por minuto, en condiciones óptimas.
- MD5 permitido en toda la imagen.
- Permite imágenes ISO.
- Puede trabajar con discos de hasta 2 TB de capacidad

6.14 Documentación

IOCE implica que debe haber un sistema de gestión de calidad referente con la documentación referente a la investigación al momento de realizar cualquier trabajo forense de tecnología digital al ser manipulados:

- Validación de herramientas forenses tanto hardware como software.
- Área física donde almacenar la evidencia.
- Seguridad para los dispositivos electrónicos.
- Detallar cada procedimiento realizado en el informe pericial.

Al utilizar los equipos forenses deben ser permitidos dentro del marco legal del País, aplicar el software licenciado, la validación de cada resultado debe ser fiable y reproducible además que realizar un peritaje es fundamentar cada procedimiento

realizado a través de un documento formal con la explicación de cada hecho utilizando un estilo no muy técnico de cómo se ha llegado a la resolución del caso. También es necesario que el perito realice un acta de incautación de que realiza la cadena custodia.

6.15 Espacio de trabajo

Es muy considerable tener un espacio físico para mantener intacta la cadena de custodia, se debe almacenar en sitios donde se encuentre seguro, que tenga todas las condiciones ambientales, adecuar el área con todo el equipamiento tecnológico necesario, controles de accesos, documentación y archivamiento.

6.16 Principios de la recuperación de la evidencia

Esta organización toma como eje las pruebas digitales que deben ser analizadas en un laboratorio de análisis forense.

- Las acciones que se manejen no deben alterar la evidencia.
- Un perito deberá tener los conocimientos necesarios para poder realizar la investigación forense.
- Utilizar formatos para llevar un registro de todas las evidencias.
- Firma de acta de confidencialidad por parte del perito asignado.

Cada organismo debe establecer un SOP que incluye la confiscación, el almacenamiento y los procedimientos del examen antes mencionado.

6.17 Recuperación de la evidencia

Esto dependerá de las leyes jurisdiccionales de cada país, el perito informático puede actuar sobre la evidencia del crimen o simplemente brindar la asesoría necesaria para que otras personas lo realicen.

- Todo material que se use el perito informático debe ser desechable como guantes, bolsas y etiquetas.
- Se debe tener en cuenta mucho la contaminación de la evidencia como por ejemplo huellas dactilares, ADN que nos puede brindar información, es necesario ser precavidos al momento de incautar la misma.
- Buscar evidencia que no sea tan solo digital, como testigos, documentos.

La recuperación de información en dispositivos consta de tres indicios:

- Registros almacenados en la evidencia (archivos ofimáticos, imágenes, correo e historiales de navegación).
- Registro de eventos, aplicaciones, log.
- Registro de archivos y aplicaciones ocultas.

6.18 Definir prioridades

Antes de realizar cualquier tipo de análisis es necesario priorizar el orden de trabajo para todo tipo de indagación:

- Línea de la evidencia.
- Definir tiempos establecidos.
- Establecer qué tipo de medio incautado, nos puede ayudar a obtener información primordial para la inclusión probatoria.
- Reportar cualquier tipo de anomalía, en que se encuentre la evidencia.
- Debe ser exacto el registro de toda la información para que en un futuro otro investigador pueda revisar sin ningún problema las pruebas encontradas, por lo tanto debe ser conveniente que todo deba estar bien detallado.
- La presentación de los resultados debe ser concisa, estructurada y sobre todo sin ambigüedades.

IOCE ofrece lineamientos que debe haber una revisión técnica y administrativa. Entre sus procedimientos de metodologías implica que haya un departamento de quejas que se pueda investigar cualquier tipo de problema.

Etapas de Preservación de la Evidencia:

1. Imagen forense bit a bit de la evidencia.
2. Cadena de Custodia.

Tabla 17: Prioridades forenses

Identificación de evidencia
Entrevista
Priorizar la evidencia para obtener información
Fotografiar el lugar que se encuentre la evidencia
Imagen forense
Procesos ejecutados
Conexiones de red
Puertos abiertos
Programas instalados, configuración de dispositivos
Contenidos de carpetas, archivos

Elaborado por: Autor

6.19 Resguardar dispositivo informático

Es necesario antes de cualquier investigación, la seguridad del perito es muy importante en cualquier escena del crimen, hay que siempre procurar cuando se va a resguardar la evidencia que no haga solo el perito es aconsejable por dos o más funcionarios que estén presentes, si el perito considera un dispositivo como evidencia para mitigar hallazgos, es primordial incautar aquel dispositivo. Es elemental seguir los procedimientos básicos:

- Grabar la escena del crimen, tomar foto a cada pista.
- Utilizar guantes, documentar cada registro de dispositivo.

- Incautar con precaución cada medio digital, si el computador esta encendido, realizar un volcado de memoria RAM.
- Preservar la evidencia, transporte adecuado.

En teléfonos celulares es necesario seguir las instrucciones para no alterar la cadena de custodia:

- No manipular el dispositivo sin ningún tipo de orden.
- Tomar foto del dispositivo incautado, registrar modelo, marca, serie.
- No apagar el dispositivo.
- Guardar en una bolsa de Faraday o una bolsa que le permita al dispositivo desconectarse de la red.
- No utilizar el dispositivo para realizar llamadas, tampoco para enviar mensajes.
- Realizar la imagen forense respectiva.

Caso Investigación forense

Propuesta práctica de un peritaje informático

Por medio de un entorno práctico se va realizar un caso parecido a lo que se vive hoy en día acerca de un delito en particular denunciado en la fiscalía del Guayas, por motivo de confidencialidad se mantendrá el anonimato de la persona denunciante y al presunto implicado, tanto como sus direcciones IP, su fecha de denuncia, entre diferentes puntos más que relacionen a las persona investigadas, en lo general estas denuncias se llevan muy frecuente en la fiscalía, se lo va realizar la parte práctica de la siguiente manera:

6.20 Caso Planteado: Formulación de problema.

Relato de los hechos:

Es el caso señor Fiscal que el día 2 de Diciembre del 2014 en la noche he empezado a recibir mensajes de acosos, llamadas, extorsiones por parte de mi ex enamorado, éste comienza sustrayendo mis fotos a través de mi computador para publicarlas en redes sociales y enviando a su entorno social, utilizando mensajes obscenos que perturban mi integridad personal con índole maliciosa. Señor Fiscal ahora que corroboré que era él que comenzó a enviar mensajes de amenazas donde me exige que vuelva con él, me indico por mensaje que si no regresaba publicaría fotos intimas, donde inmediatamente acudo a usted señor Fiscal para presentar la respectiva denuncia formal. Es tan indignante la actitud de este sujeto, esto es todo lo que puede decir en honor a la verdad.

El fiscal de turno le asigna el caso al departamento correspondiente a fin de iniciar el campo de la investigación sobre este delito, el cual toma el nombre de CESIÓN, PUBLICACIÓN, TRANSFERENCIA DE DATOS en nuestro país es considerado como un delito penal. Al comenzar el proceso de investigación se realiza las principales indagaciones, inmediatamente incautan sus equipos informáticos, su celular, su unidad extraíble para realizar una investigación previa del cual se identificará si él presunto sujeto está difundiendo las fotos de la actora.

El marco como se va manejar el peritaje se lo va estructurar de la siguiente manera.

- Metodología.
- Antecedentes del caso.
- Recolección de datos.
- Descripción de la evidencia.
- Análisis de la evidencia.
- Descripción de los hallazgos.
- Posibles víctimas y rastros del sospechoso.
- Informes periciales.

Alcances:

- ✓ Analizar el entorno del delito informático: Windows XP, MEMORIA RAM, FLASH MEMORY, de esta forma para poder recabar información.

Por medio del caso práctico se debe realizar los siguientes eventos:

- ✓ Cadena de custodia.
- ✓ Análisis de metadatos.
- ✓ Dumpeo de memoria RAM.
- ✓ Recuperación de archivos a nivel forense.

Objetivos:

- Informe de procedimiento técnico y ejecutivo.
- La relación que tiene las pruebas con él delito cometido.

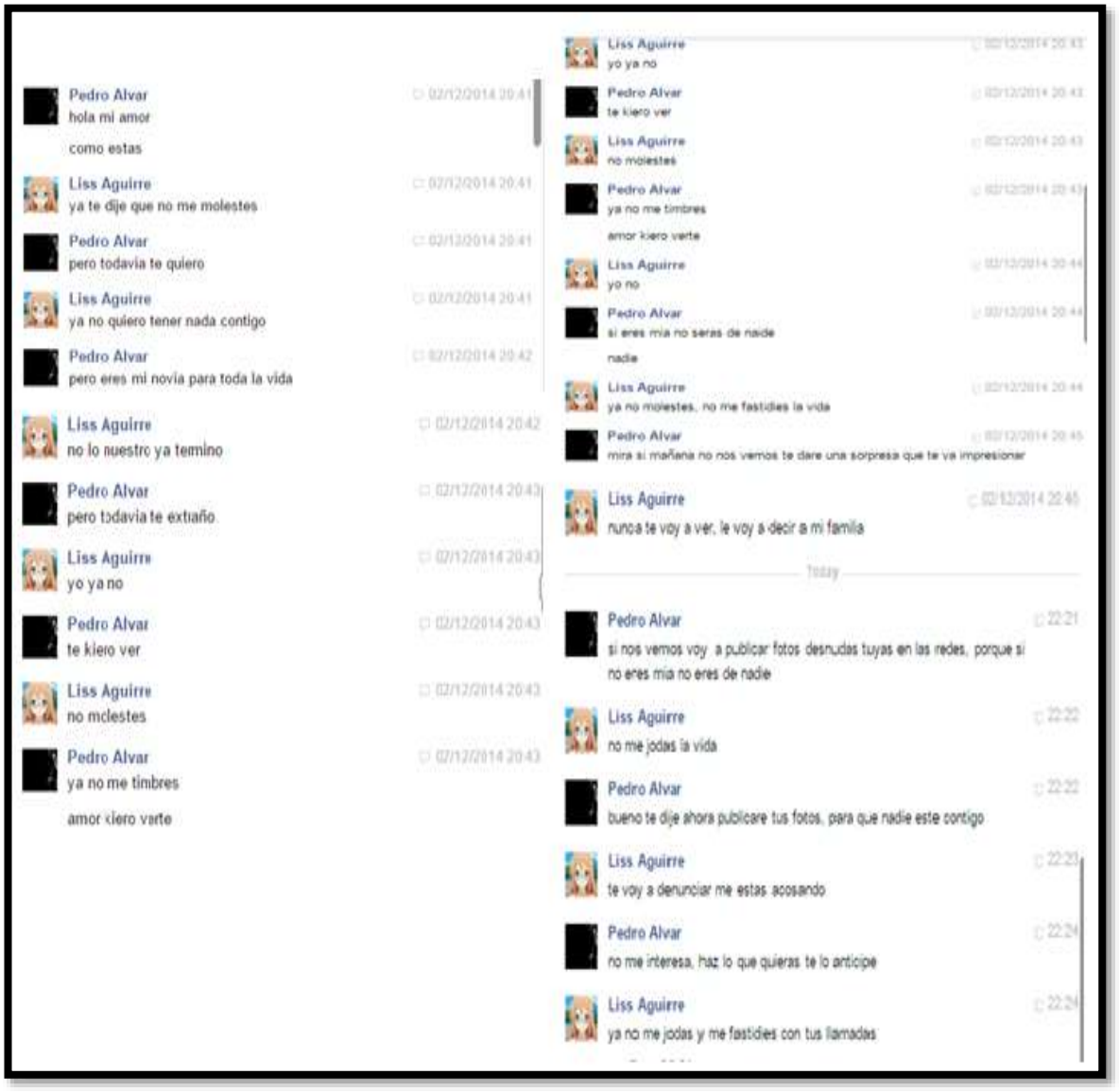
Antecedentes del caso

- Denuncia Formal - Oral
- Acta de reconocimiento de la denuncia
- Indagación previa
- Terna de peritos informáticos

La Sra. Lissette Aguirre adjunta en la denuncia las impresiones de pantalla respectivos a la red social, que el supuesto denunciado le mandaba mensajes de acosos. Para lo tanto el perito informático deberá realizar el análisis respectivo para poder encontrar los respectivos hechos sobre el caso.

Amenazas sobre redes sociales, capturas de pantalla por parte de la denunciante

Figura 17: Captura 1, historial presentada en la denuncia



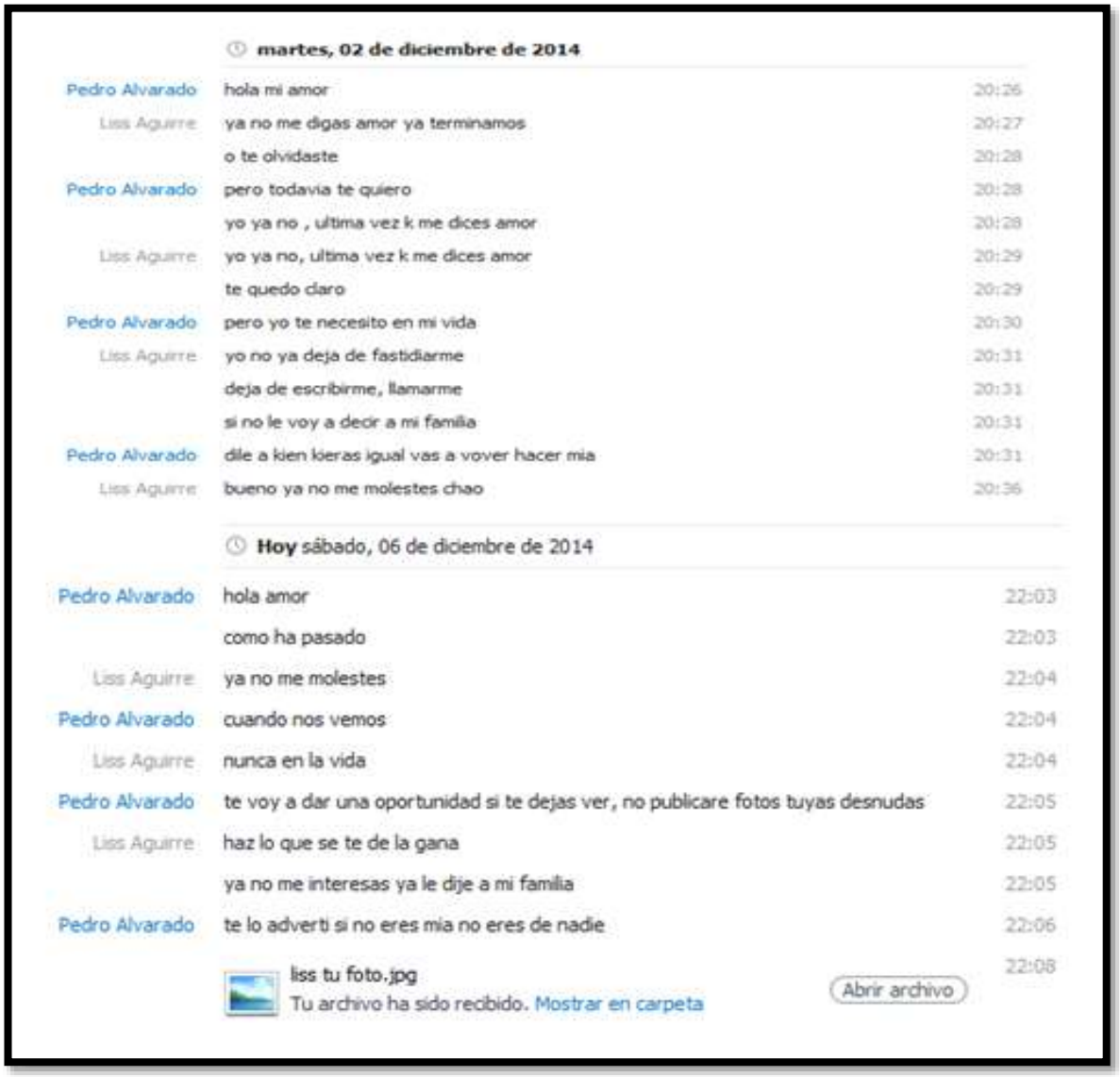
Fuente: Fiscalía del Guayas, 2014

Elaborado por: Autor

Observación: Por motivo de confidencialidad las imágenes de las personas no serán publicadas con el objetivo de mantener el anonimato.

Amenazas adjuntada sobre Skype, del cual presenta la denunciante

Figura 18: Captura 2, historial presentada en la denuncia



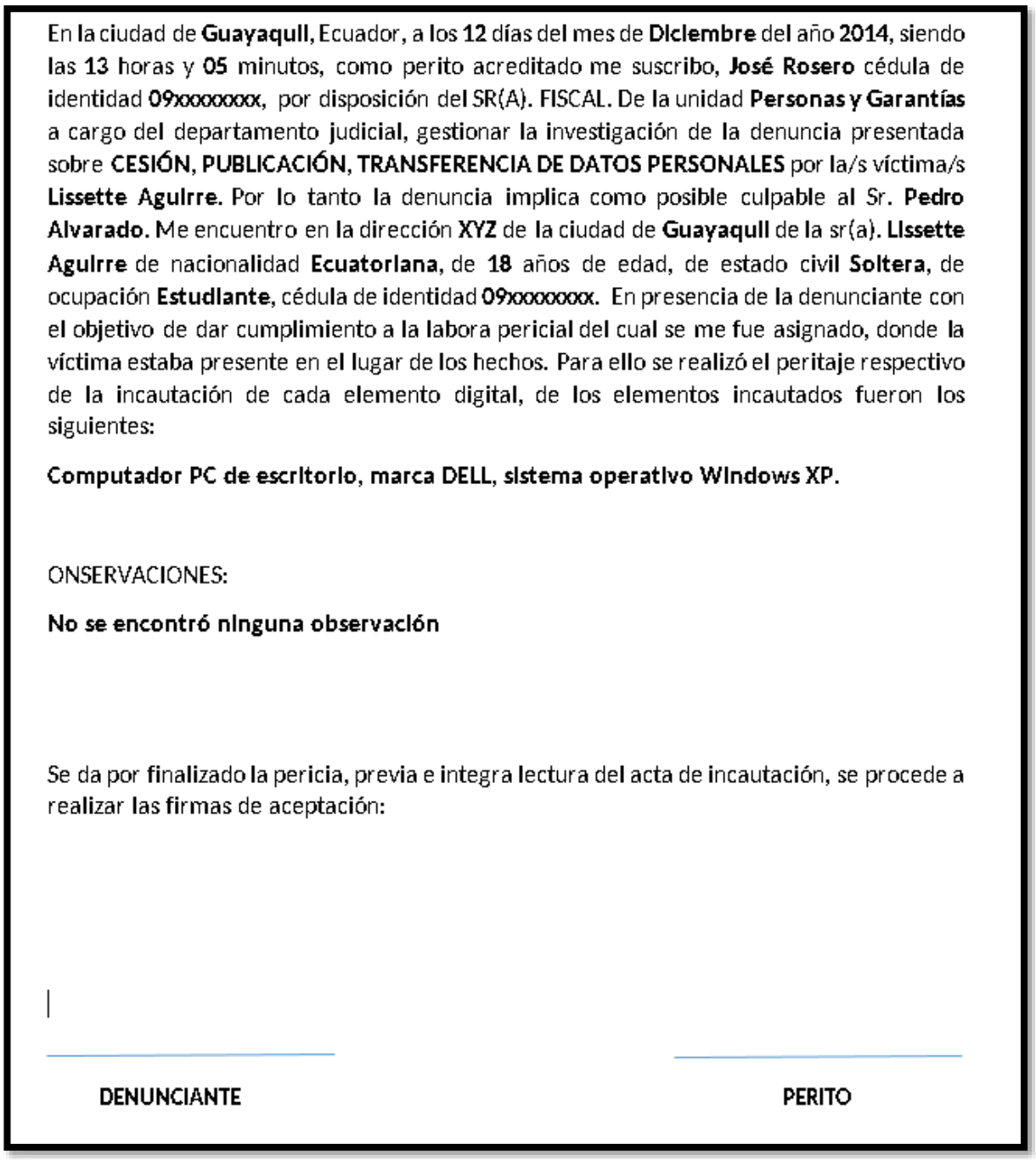
Fuente: Fiscalía del Guayas, 2014

Elaborado por: Autor

INFORME TÉCNICO DENUNCIANTE

Propuesta de informe de acta de incautación

Figura 19: Acta de incautación



En la ciudad de **Guayaquil**, Ecuador, a los **12** días del mes de **Diciembre** del año **2014**, siendo las **13** horas y **05** minutos, como perito acreditado me suscribo, **José Rosero** cédula de identidad **09xxxxxxxx**, por disposición del SR(A). FISCAL. De la unidad **Personas y Garantías** a cargo del departamento judicial, gestionar la investigación de la denuncia presentada sobre **CESIÓN, PUBLICACIÓN, TRANSFERENCIA DE DATOS PERSONALES** por la/s víctima/s **Lissette Aguirre**. Por lo tanto la denuncia implica como posible culpable al Sr. **Pedro Alvarado**. Me encuentro en la dirección **XYZ** de la ciudad de **Guayaquil** de la sr(a). **Lissette Aguirre** de nacionalidad **Ecuatoriana**, de **18** años de edad, de estado civil **Soltera**, de ocupación **Estudiante**, cédula de identidad **09xxxxxxxx**. En presencia de la denunciante con el objetivo de dar cumplimiento a la labora pericial del cual se me fue asignado, donde la víctima estaba presente en el lugar de los hechos. Para ello se realizó el peritaje respectivo de la incautación de cada elemento digital, de los elementos incautados fueron los siguientes:

Computador PC de escritorio, marca DELL, sistema operativo Windows XP.

ONSERVACIONES:

No se encontró ninguna observación

Se da por finalizado la pericia, previa e integra lectura del acta de incautación, se procede a realizar las firmas de aceptación:

DENUNCIANTE **PERITO**

Elaborado por: Autor

2. Línea previa

Como inicio a la recolección de aquellos datos principales, sobre el caso de **CESIÓN, PUBLICACIÓN, TRANSFERENCIA DE DATOS** antes mencionado, por Sra. Lissette Aguirre se detallan los siguientes aspectos de la entrevista:

Víctima:	Sra. Lissette Aguirre
Notificación de la denuncia:	8 de Diciembre del 2014
Vía de Acoso:	Red social, llamadas, mensajes
Tipo de archivo:	Imágenes de contenido sexual
Ubicación del archivo:	Computador de la víctima
Sospechoso:	Ex – Enamorado
Nombre del sospechoso:	Pedro Alvarado
Correo del sospechoso:	pedroalvara18@hotmail.com
Motivo que implica al sospechoso:	Ruptura amorosa.
Equipo incautado:	PC, marca Dell, Windows XP
Respuesta de la víctima:	Auguraba no conocer como obtuvo fotos personales.

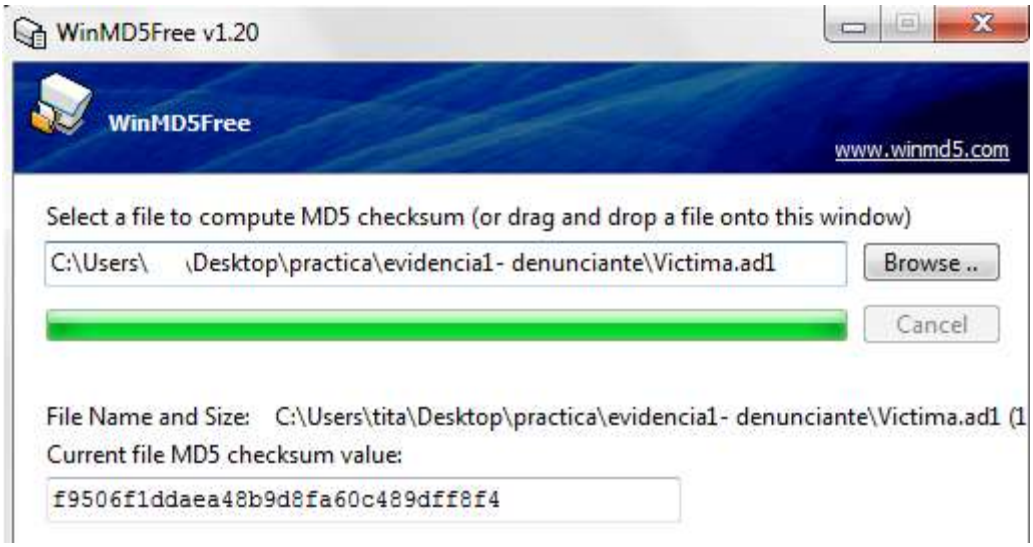
Figura 20: Línea previa denunciante

Elaborado por: Autor

Una vez aprobado, se procede a realizar la imagen forense sobre el equipo que la denunciante que utilizaba constantemente para uso personal. La cual la fiscal nos brinda la imagen forense para realizar la pericia digital correspondiente.

Primer paso: Se realizó la comprobación de la imagen forense para verificar que la evidencia digital no haya sido alterada, se utilizó la herramienta winmd5free la suma de verificación del código hash con el objetivo de encontrar si la evidencia ha sufrido algún cambio por mala manipulación.

Figura 21: Comprobación de código hash del computador de la denunciante



Fuente: Herramienta Winmd5free

Elaborado por: Autor

En el proceso de verificación de la imagen forense es auténtica, se puede dar como fe, que esta no fue alterada y su resultado es correcto.

Observación: En caso de ser asignados como peritos informáticos nos asignara una imagen forense para su investigación y su código hash no sea igual a la que tiene la fiscal, se da como resultado que la cadena de custodia ha sido alterada por lo tanto no hay una sustentación legal de la evidencia por lo que no se puede hacer el análisis.

3. Entorno de análisis

Se utilizó las siguientes herramientas para encontrar indicios sobre la evidencia digital referente a la computadora de la denunciante.

Herramientas utilizadas

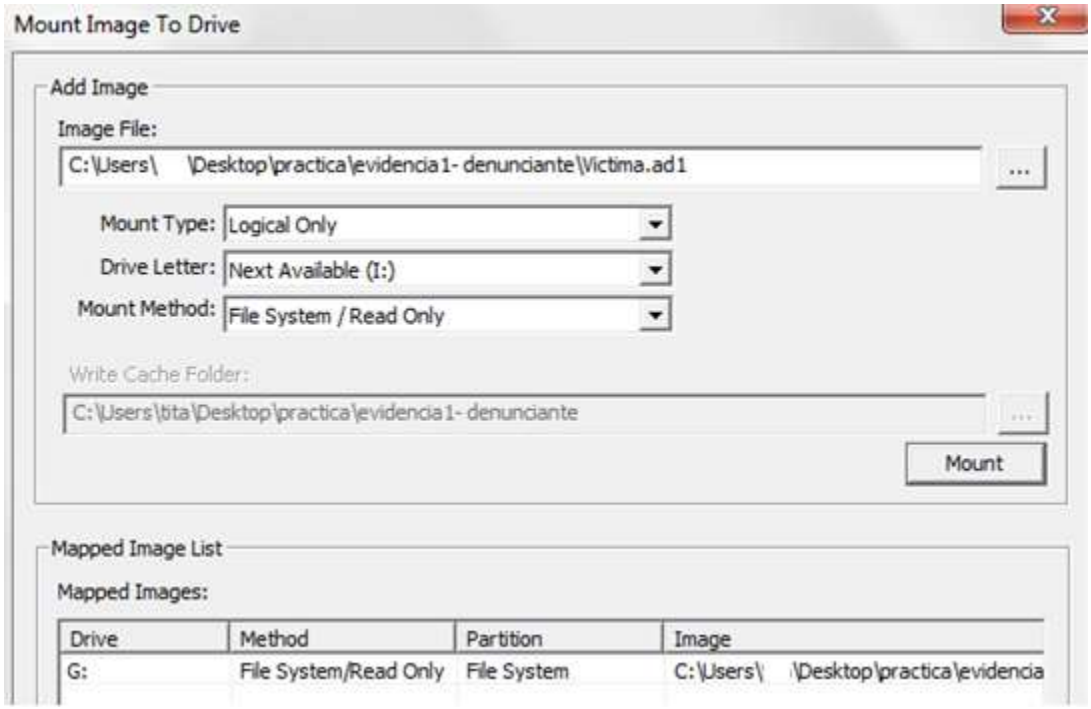
Tabla 18: Herramientas de análisis usadas en la evidencia de la denunciante

HERRAMIENTA	DESCRIPCIÓN
winmd5free	Herramienta que permite hacer la comprobación de seguridad de la imagen.
FTK Imager 3.1.1.8	Se puede realizar imágenes forenses, montajes de distintos formatos.
Windows Registery Recovery	Extrae información útiles acerca de los ajustes de configuración.

Elaborado por: Autor

Segundo Paso: Se realiza el montaje de la imagen forense de la evidencia digital de la denunciante llamada "Victima.AD1".

Figura 22: Montaje de imagen forense con ftk imager

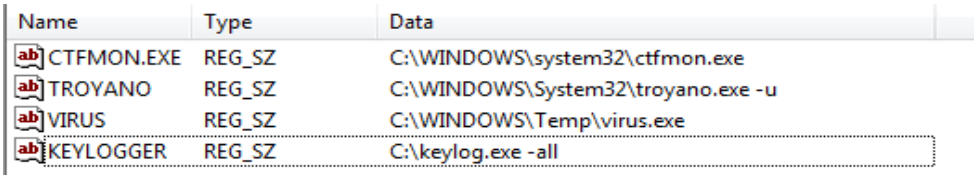


Fuente: Fiscalía del Guayas

Elaborado por: Autor

Tercer paso: Se usó la herramienta Windows Registery Recovery para analizar los perfiles de los usuarios encontrados en la evidencia digital. Se analiza el perfil del administrador donde no se encontró ningún tipo de software malicioso. En el perfil de la cuenta pirata se encontró software malicioso del cual fueron los siguientes:

Figura 23: Registros de programas instalados de la imagen Victima.ad1



Name	Type	Data
CTFMON.EXE	REG_SZ	C:\WINDOWS\system32\ctfmon.exe
TROYANO	REG_SZ	C:\WINDOWS\System32\troyano.exe -u
VIRUS	REG_SZ	C:\WINDOWS\Temp\virus.exe
KEYLOGGER	REG_SZ	C:\keylog.exe -all

Fuente: Herramienta Windows Registery Recovery

Elaborado por: Autor

4. Línea de investigación

- **¿Qué programas maliciosos se encuentra en la máquina de la denunciante?**

En la imagen forense Victima.ad1, había un usuario creado llamado **"PIRATA",** de la cual tiene instalado: un troyano, virus, keylooger.

- **¿Cuál es la ruta donde se encontraban los programas?**

Al utilizar la herramienta Windows Registery Recovery, se puede encontrar en Raw Data, software, Windows, Run, se encuentre los siguientes:

C:\WINDOWS\System32\troyano.exe –u

C:\WINDOWS\Temp\virus.exe

C:\Keylog.exe –all

INFORME TÉCNICO SOSPECHOSO

Se pudo hallar al responsable de la siguiente manera:

Al momento de analizar la computadora de la denunciante se encontró software malicioso por lo tanto para investigar al sospechoso se lo relaciono a través de redes sociales por lo que se realizó de la siguiente manera:

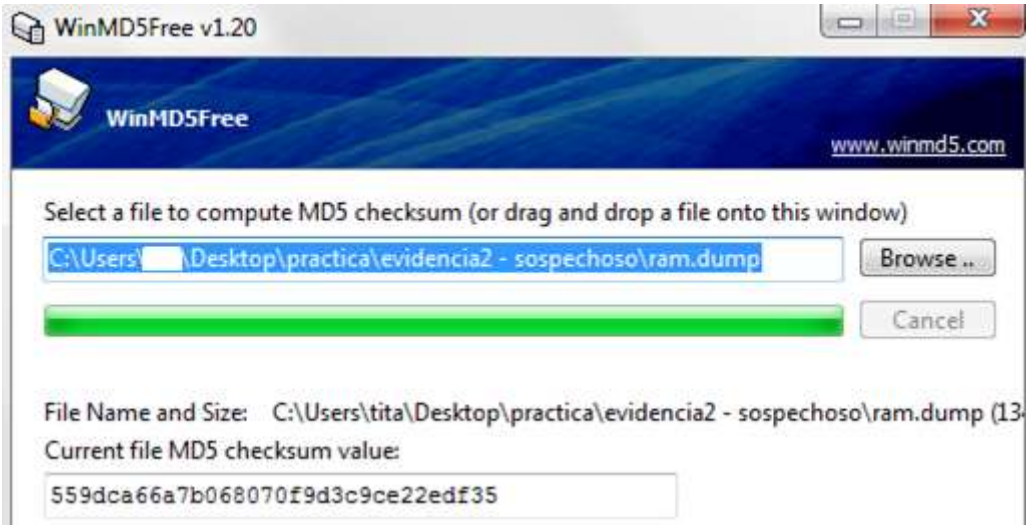
- Se creó un usuario en una red social con la finalidad de poder ser amigos con el sospechoso con el objetivo de investigarlo.
- Se agregó como amigo al presunto atacante.
- Por medio de un enlace en una dirección web se capturó la dirección ip, sistema operativo, navegador que estaba usando.
- Una vez capturada la información se entrega a la fiscal las pruebas, para que tome acción y considere emitir una orden para buscarlo a través del proveedor.
- Se comprueba a través de proveedor de servicio de internet
- Se localiza al culpable, se procede hacer la incautación de los medios tecnológicos correspondientes que se encontraba en el domicilio del presunto sospechoso.

2. Línea previa

Sospechoso:	Pedro Alvarado
Notificación de la denuncia:	8 de Diciembre del 2014
Vía de acoso:	Red social, llamadas, mensajes
Tipo de delito:	Cesión, Publicación, Transferencia de datos
Motivo que implica al sospechoso:	Ruptura amorosa.
Respuesta del sospechoso:	Confirmaba no conocer a la Sra. Lissette Aguirre

Primer paso: Se comprobó el código hash de la imagen forense.

Figura 24: Comprobación evidencia ram.dump, código hash



Fuente: Herramienta Winmd5free

Elaborado por: Autor

Observación: En caso de que la evidencia digital ha sido alterada, este no tiene fundamento legal para la investigación.

3. Entorno de análisis

Se usó las siguientes herramientas para encontrar indicios sobre la evidencia digital involucrada al sospechoso.

Herramientas utilizadas

Tabla 19: Herramientas de análisis usadas en la evidencia del sospechoso

HERRAMIENTA	DESCRIPCIÓN
Winmd5free	Herramienta que permite hacer las comprobación de seguridad de md5
Winhex	Es un editor hexadecimal capaz de abrir ficheros, discos y procesos en memoria
Forensic ToolKit 1.81.6	Permite crear y analizar imágenes forenses.
Xiao Steganography	Oculta archivos en imágenes o sonidos.
FTK Imager 3.1.1.8	Se puede realizar imágenes forenses, montajes de distintos formatos.
SQLITE MANAGER	Lectura, creación de base de datos.
SANTOKU	Distribución de Linux para análisis forenses.
Photorec	Permite recuperar archivos borrados.

Elaborado por: Autor

Para la elaboración de la primera evidencia se tomó como ejecución los siguientes pasos:

Segundo Paso: Se utilizó la herramienta Winhex para hacer el análisis forense de la memoria RAM llamada “ram.dump”.

Primera evidencia: (EXTRACCIÓN DE INFORMACIÓN DE LA MEMORIA RAM)

¿Buscar sitios web?

Durante la investigación se realizó la extracción de los datos en la memoria RAM, se utilizó la herramienta Winhex, se registró y analizo que la página principal que estaba visitando el sospechoso, era sobre una tienda de armas.

¿Tenía algo planificado?

El sospechoso tenía planificado un asalto según en la evidencia digital analizada.

Tercer Paso: Se monta la imagen utilizando la herramienta ftk Imager. Luego de realizar el montaje de la imagen forense como una unidad de disco, se utiliza la herramienta Photorec para realizar extracción de toda la información encontrada en la memoria.

¿Recuperación de archivos del volcado de memoria RAM?

Por medio de la herramienta Photorec, se recuperó las siguientes imágenes que estaba buscando el sospechoso, relacionado con el sitio web del cual fueron las siguientes:

Figura 25: Registro de imágenes encontradas en la memoria RAM

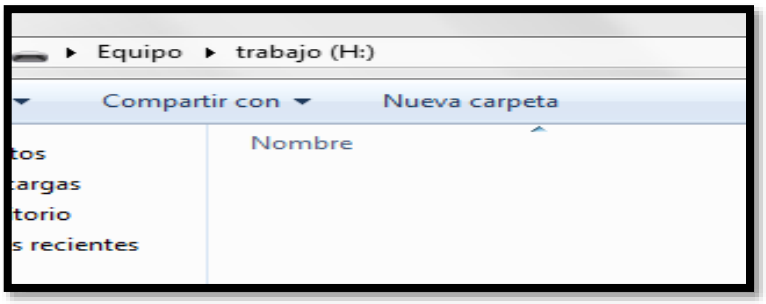
Fuente: Herramienta Photorec

Elaborado por: Autor

Segunda evidencia: FLASH MEMORY

- Al momento de incautar la memoria flash, el presunto acosador formatea la unidad extraíble.

Figura 26: USB vacío



Fuente: Fiscalía del Guayas

Elaborado por: Autor

- Inmediatamente se realiza la imagen forense del dispositivo, utilizando el software ftk Imager.

Figura 27: Comprobación evidencia USB código hash, Herramienta FTK IMAGER

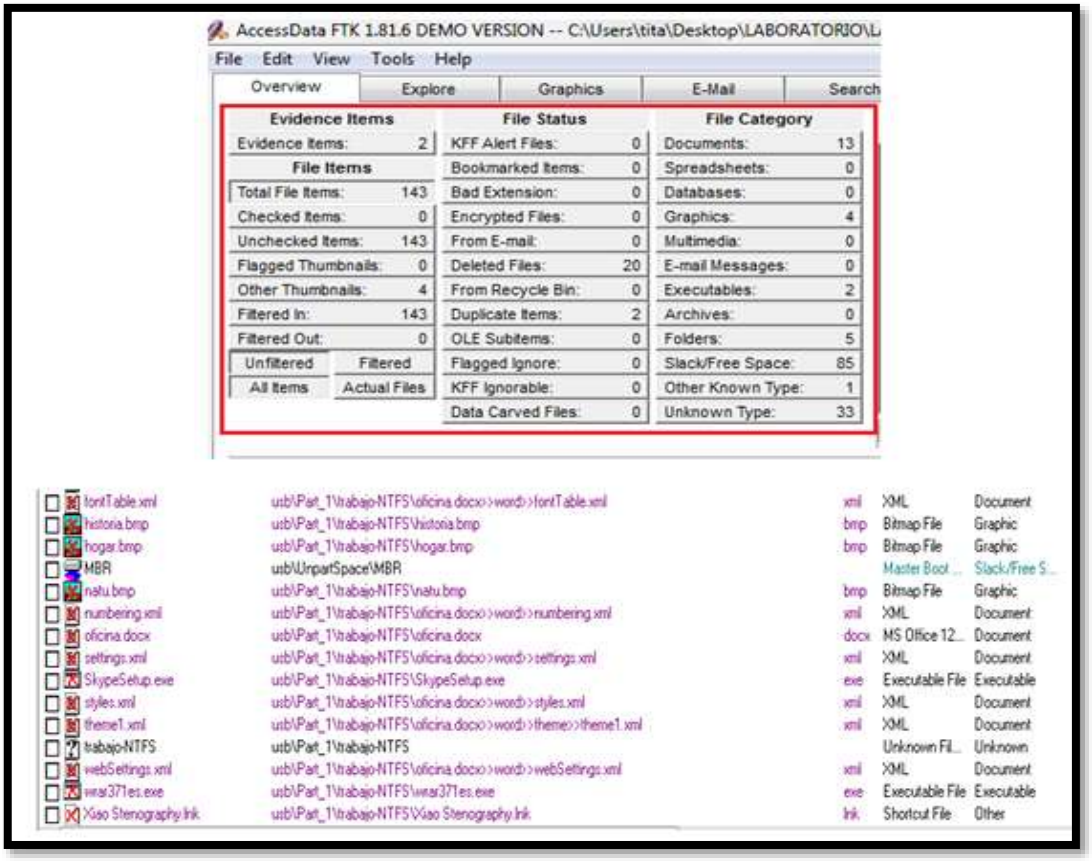
```
Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 247
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 3.973.120
[Physical Drive Information]
 Drive Model: Kingston DT 101 II USB Device
 Drive Serial Number:
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 1940 MB
 Sector count:     3973120
[Computed Hashes]
 MD5 checksum:     20c8817f117a7d84712f0f661dc83ffb
 SHA1 checksum:    63986da129e0719f8224170aac8a21a6d5381c32

Image Information:
 Acquisition started:   Mon Dec 22 22:50:08 2014
 Acquisition finished:  Mon Dec 22 22:52:47 2014
 Segment list:
  C:\Users\     \Desktop\Nueva carpeta\ .001
  C:\Users\     \Desktop\Nueva carpeta\ .002

Image Verification Results:
 Verification started:  Mon Dec 22 22:52:48 2014
 Verification finished: Mon Dec 22 22:53:02 2014
 MD5 checksum:     20c8817f117a7d84712f0f661dc83ffb : verified
 SHA1 checksum:    63986da129e0719f8224170aac8a21a6d5381c32 : verified
```

Fuente: Fiscalía del Guayas

Elaborado por: Autor

- Posterior a comprobar la imagen, se empleó la herramienta Forensic ToolKit 1.81.6, se hizo un análisis exhaustivo sobre la cantidad de archivos de diferentes extensiones que se encontraba en el dispositivo del cual fueron las siguientes:

Figura 28: Análisis forense de USB, Herramienta AccessData FTK



Fuente: Fiscalía del Guayas

Elaborado por: Autor

Tabla 20: Cantidad de archivos extraídos

Total de archivos	143
Eliminados	20
Duplicados	2
Documentos	13
Gráficos	4
Others Thumbnails	4

Elaborado por: Autor

Se encontró diferentes archivos como imágenes, programas ejecutables, documentos y archivos borrados entre otras cosas más.

Software instalado

Analizando la evidencia digital, el usuario contaba con las siguientes herramientas:

- Winrar
- Skype
- Xiao stenography

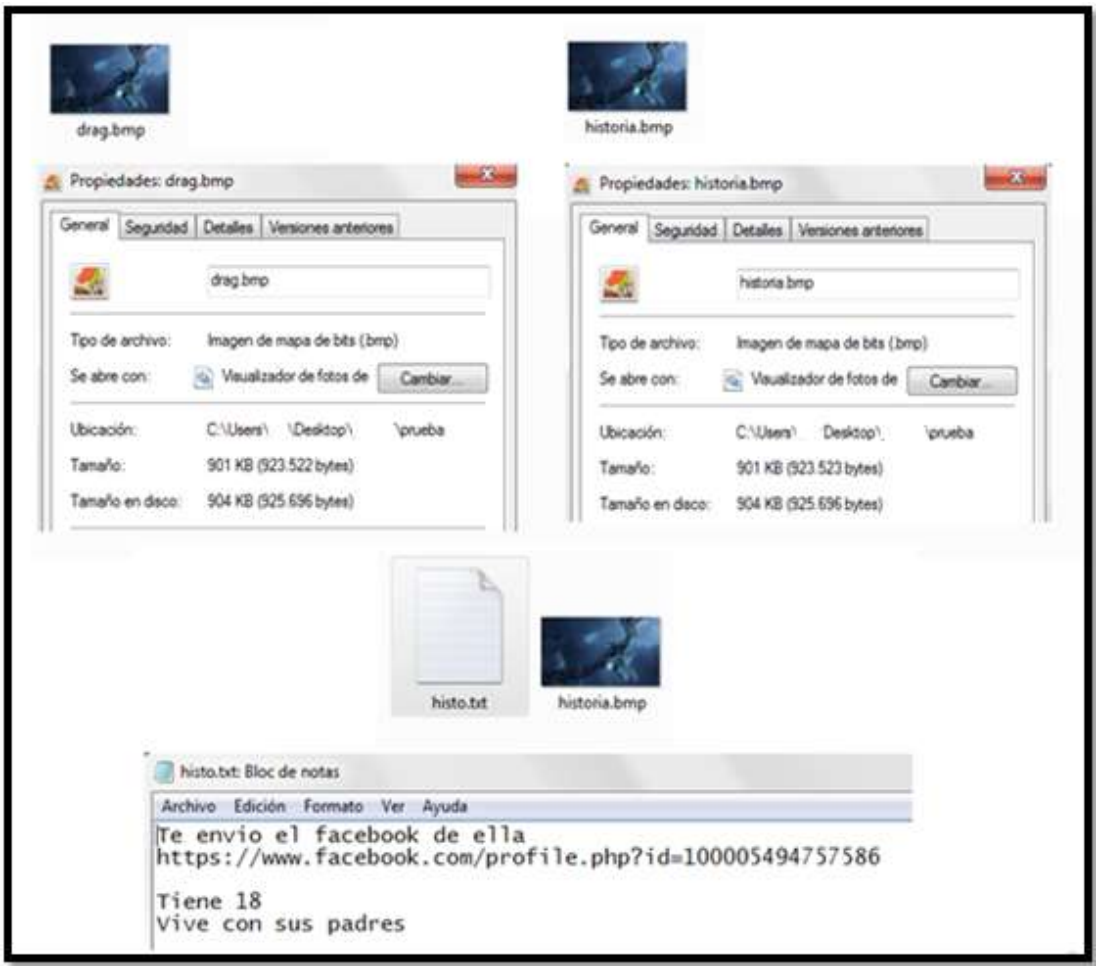
Entre las imágenes halladas entre extensiones de archivos de formato .bmp y .jpg, fueron los siguientes:

- drag.bmp
- historia.bmp
- hogar.bmp
- natu.bmp
- oficina.docx

Analizando el archivo "drag.bmp" y el archivo "historia.bmp", se puede demostrar que las imágenes son completamente iguales con el mismo peso, donde se encontró que el usuario ha hecho uso de una herramienta para ocultar la información y así poder enviar contenido a sus contactos.

En el archivo **historia.bmp**, utilizando la herramienta XIAO STHEGANOGRAPHY, hay un documento de texto, donde se encuentra que hay un enlace de dirección de facebook, sobre la denunciante **"Lissette Aguirre".**

Figura 29: Comparación de imágenes y extracción de datos drag e historia



Fuente: Evidencia USB, Fiscalía del Guayas

Elaborado por: Autor

Analizando el otro archivo **"hogar.bmp"** y el archivo **"natu.bmp"**, se puede demostrar que las imágenes son completamente iguales con el mismo peso, pero se pudo hallar que el usuario ha hecho uso de una herramienta esteganográfica, con el fin de ocultar la información.

El archivo **hogar.bmp**, utilizando la herramienta XIAO STHEGANOGRAPHY, hay un documento de Word, donde se encuentra imágenes que involucra la integridad de la denunciante **"Lissette Aguirre".**

Figura 30: Comparación de imágenes y extracción de datos hogar y natu

Fuente: Evidencia USB, Fiscalía del Guayas

Elaborado por: Autor

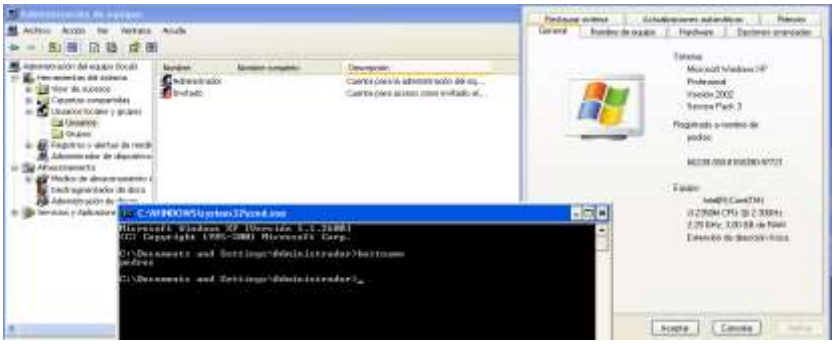
Tercera evidencia: COMPUTADOR

Se realizó una imagen instantánea de la computadora incautada. De la cual se puede mantener intacta y recuperar información de la memoria RAM, procesos, páginas web visitadas.

Características del equipo incautado:

- Sistema Operativo Windows XP
- Cuenta de usuario activo: administrador
- Nombre de la máquina: pedroc
- Zona horaria: Bogotá, Lima, Quito
- Páginas abiertas

Figura 31: Usuario y nombre de la computadora



Fuente: Evidencia Computador, Fiscalía del Guayas

Elaborado por: Autor

Zona Horaria

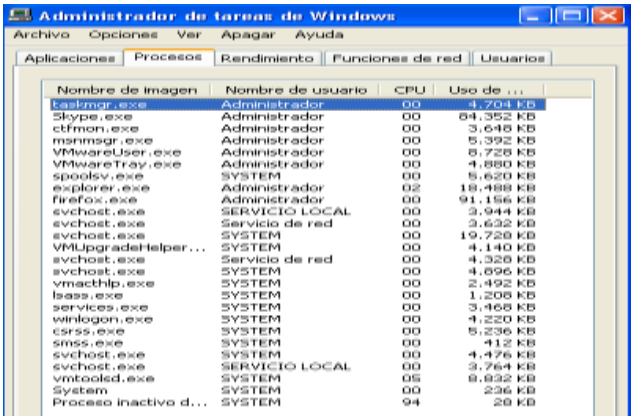
Figura 32: Zona horaria

Fuente: Evidencia Computador, Fiscalía del Guayas

Elaborado por: Autor

Procesos de windows

Figura 33: Procesos del equipo incautado



Fuente: Evidencia Computador, Fiscalía del Guayas

Elaborado por: Autor

Conexión de red

Figura 34: Conexión de red a través de netstat

```
Conexiones activas

  Proto  Direcci4n local        Direcci4n remota       Estado
  TCP    pedroc:1435            localhost:1436         ESTABLISHED
  TCP    pedroc:1436            localhost:1435         ESTABLISHED
  TCP    pedroc:1438            localhost:1439         ESTABLISHED
  TCP    pedroc:1439            localhost:1438         ESTABLISHED
  TCP    pedroc:1440            host-181-198-58-28.telconet.net:http  ESTABLISHED
  TCP    pedroc:1442            startpage-zlb.vips.scl3.mozilla.com:https  TIME_WAIT
  TCP    pedroc:1445            startpage-zlb.vips.scl3.mozilla.com:https  TIME_WAIT
  TCP    pedroc:1446            72.21.91.8:https       ESTABLISHED
  TCP    pedroc:1447            mia07s24-in-f30.1e100.net:https  ESTABLISHED
  TCP    pedroc:1452            a23-35-171-27.deploy.static.akamaitechnologies.com:http  ESTABLISHED
  TCP    pedroc:1454            a23-57-175-148.deploy.static.akamaitechnologies.com:http  ESTABLISHED
  TCP    pedroc:1455            134.170.189.4:http     ESTABLISHED
  TCP    pedroc:1456            191.238.42.36:http     ESTABLISHED
  TCP    pedroc:1458            host-181-198-58-36.telconet.net:http  ESTABLISHED
  TCP    pedroc:1460            host-181-198-58-36.telconet.net:http  ESTABLISHED
  TCP    pedroc:1461            137.116.81.24:http     ESTABLISHED
  TCP    pedroc:1464            edge-star-shv-15-mia1.facebook.com:http  ESTABLISHED
  TCP    pedroc:1466            edge-star-shv-15-mia1.facebook.com:https  ESTABLISHED
  TCP    pedroc:1469            ec2-107-20-245-242.compute-1.amazonaws.com:http  CLOSE_WAIT
  TCP    pedroc:1470            host-181-198-58-28.telconet.net:http  ESTABLISHED
  TCP    pedroc:1471            host-181-198-58-28.telconet.net:http  ESTABLISHED
  TCP    pedroc:1473            host-181-198-58-30.telconet.net:http  ESTABLISHED
  TCP    pedroc:1474            edge-star-shv-15-mia1.facebook.com:http  ESTABLISHED
  TCP    pedroc:1481            edge-star-shv-15-mia1.facebook.com:https  ESTABLISHED
  TCP    pedroc:1482            199.16.158.17:https    ESTABLISHED
  TCP    pedroc:1483            host-181-198-58-36.telconet.net:https  ESTABLISHED
  TCP    pedroc:1484            host-181-198-58-36.telconet.net:https  ESTABLISHED
  TCP    pedroc:1485            a23-57-187-83.deploy.static.akamaitechnologies.com:http  ESTABLISHED
  TCP    pedroc:1486            edge-star-shv-13-mia1.facebook.com:https  ESTABLISHED
  TCP    pedroc:1489            a23-35-165-163.deploy.static.akamaitechnologies.com:http  ESTABLISHED
  TCP    pedroc:1491            131.253.61.66:https    FIN_WAIT_2
  TCP    pedroc:1493            a23-57-187-83.deploy.static.akamaitechnologies.com:http  ESTABLISHED
  TCP    pedroc:1497            a23-35-168-70.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    pedroc:1498            a23-35-168-70.deploy.static.akamaitechnologies.com:https  ESTABLISHED

  TCP    pedroc:1499            a23-35-168-70.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    pedroc:1501            a23-57-169-28.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    pedroc:1504            a23-57-169-28.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    pedroc:1505            a23-57-169-28.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    pedroc:1506            a23-57-169-28.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    pedroc:1507            173.192.220.67-static.reverse.softlayer.com:https  TIME_WAIT
  TCP    pedroc:1510            ec2-177-71-184-37.sa-east-1.compute.amazonaws.com:https  CLOSE_WAIT
  TCP    pedroc:wins            66.235.155.62:https    TIME_WAIT
  TCP    pedroc:1513            host-181-198-58-36.telconet.net:http  ESTABLISHED
  TCP    pedroc:1514            a23-57-171-145.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    pedroc:1515            173.192.220.67-static.reverse.softlayer.com:https  TIME_WAIT
  TCP    pedroc:1516            66.235.155.62:https    CLOSE_WAIT
  TCP    pedroc:1517            s.imp.microsoft.com:https  FIN_WAIT_2
```

Fuente: Evidencia Computador, Fiscalía del Guayas

Elaborado por: Autor

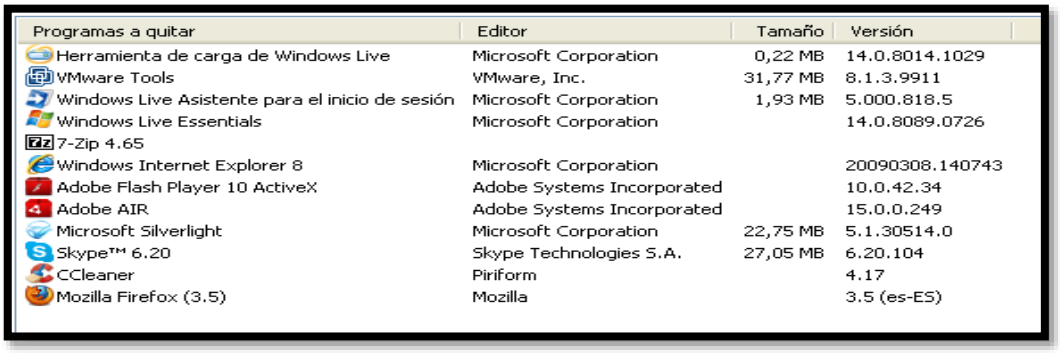
- Para poder visualizar las conexiones activas, fue mediante el uso del comando: netstat–an se utilizó comodines para copiar aquella información en un documento de texto.

Software instalado

Se registró los programas principales instalados, para ello se dio en; Inicio, Panel de Control, Programas y Características:

- Windows Live
- 7zip
- Skype 6.20
- CCleaner
- Iexplorer 8
- Mozilla Firefox 3.5

Figura 35: Software instalado en el equipo incautado



Programas a quitar	Editor	Tamaño	Versión
Herramienta de carga de Windows Live	Microsoft Corporation	0,22 MB	14.0.8014.1029
VMware Tools	VMware, Inc.	31,77 MB	8.1.3.9911
Windows Live Asistente para el inicio de sesión	Microsoft Corporation	1,93 MB	5.000.818.5
Windows Live Essentials	Microsoft Corporation		14.0.8089.0726
7-Zip 4.65			
Windows Internet Explorer 8	Microsoft Corporation		20090308.140743
Adobe Flash Player 10 ActiveX	Adobe Systems Incorporated		10.0.42.34
Adobe AIR	Adobe Systems Incorporated		15.0.0.249
Microsoft Silverlight	Microsoft Corporation	22,75 MB	5.1.30514.0
Skype™ 6.20	Skype Technologies S.A.	27,05 MB	6.20.104
CCleaner	Piriform		4.17
Mozilla Firefox (3.5)	Mozilla		3.5 (es-ES)

Fuente: Evidencia Computador, Fiscalía del Guayas

Elaborado por: Autor

Carpetas

- En el escritorio del computador del sospechoso, se encuentra una carpeta llamada **"IMÁGENES BEBE",** donde se encuentran imágenes de la denunciante.

Figura 36: Carpeta de imágenes hallado en el equipo incautado

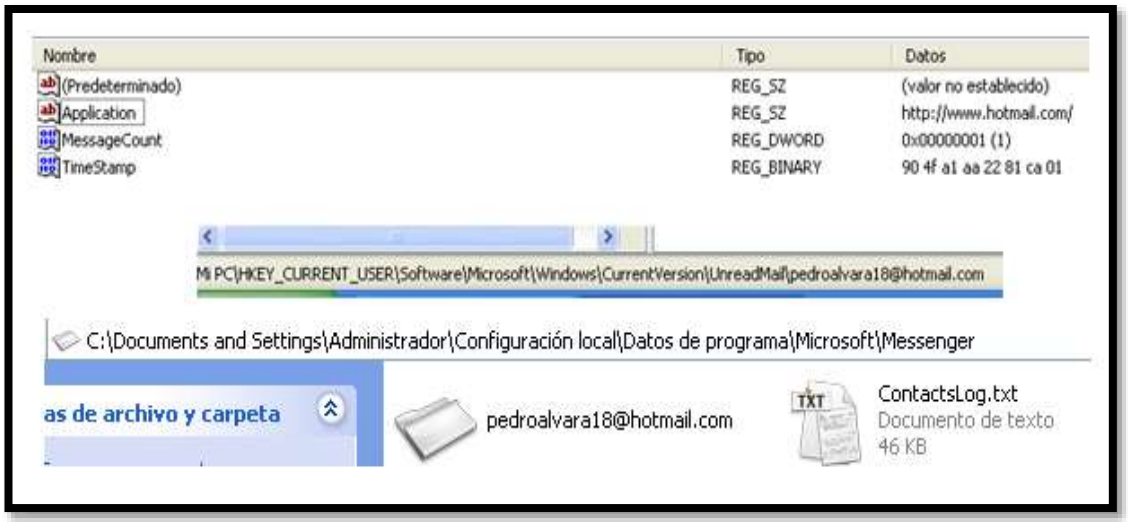
Fuente: Evidencia Computador, Fiscalía del Guayas

Elaborado por: Autor

Análisis de mensajería Windows Live

- Se comenzó a realizar la investigación desde REGEDIT, esperando que se encuentre registrado el correo que adjunta la denunciante, al verificar se encuentra con una entrada de dicho correo, pero no se pudo extraer la mensajes, solo el correo.

Figura 37: Mensajería Windows Live



Fuente: Evidencia Computador, Fiscalía del Guayas

Elaborado por: Autor

Análisis forense en SKYPE del sospechoso

- Al registrar el equipo tenía instalado skype, se inicia la busqueda para obtener información relevante dentro de la investigación. Vemos que existe un archivo llamado **SHARED.XML,** realizando el análisis correspondiente obtenemos lo siguientes datos:
- Inicio de sesión del usuario: Wed, 03 Dec 2014 01:18:19 GMT
- Versión: 6:20
- Idioma: Español

Figura 38: Análisis forense archivo shared.xml

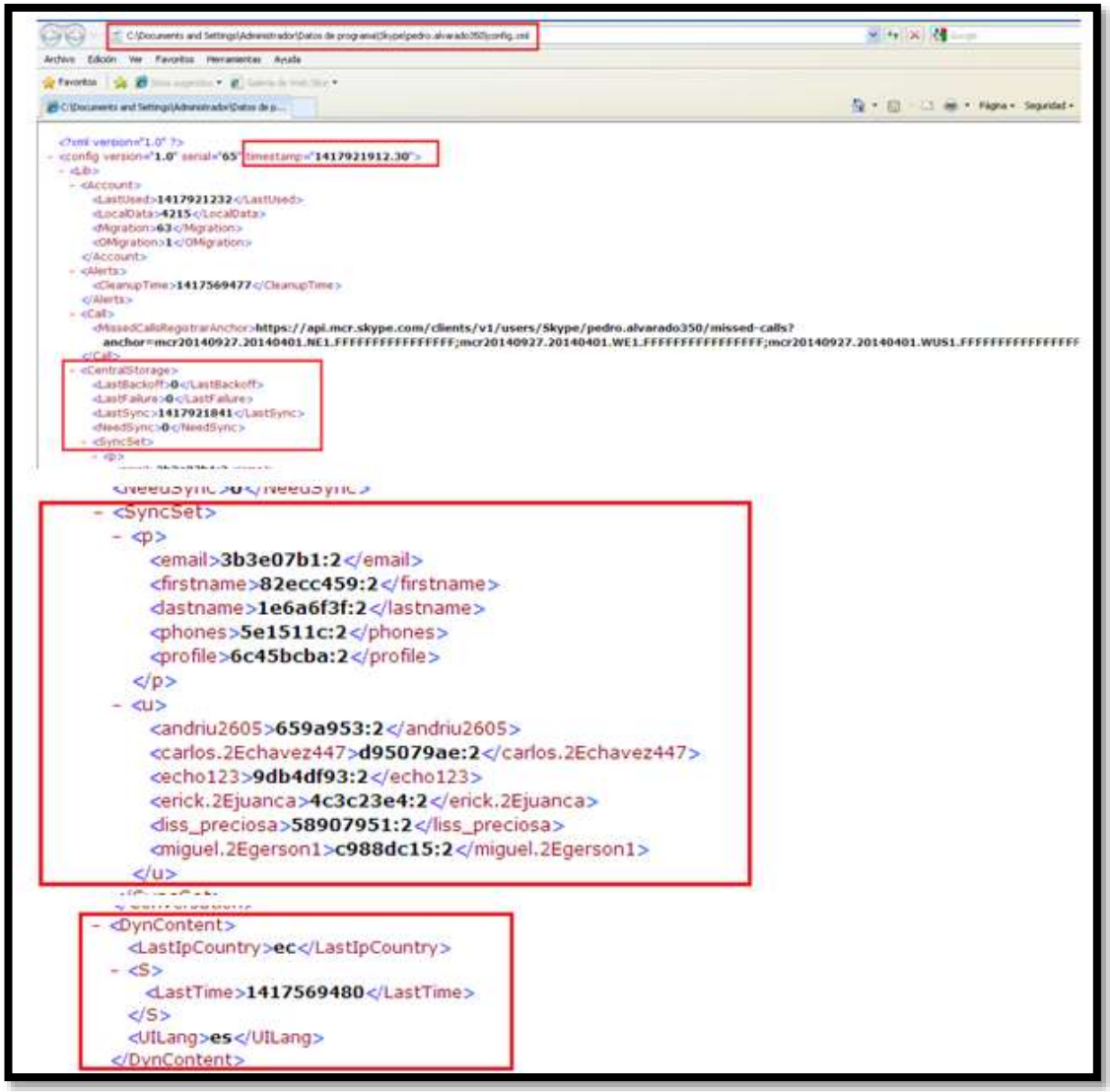
Fuente: Evidencia Skype, Fiscalía del Guayas

Elaborado por: Autor

Analizando la carpeta **pedro.alvardo350,** se realiza el análisis forense respectivo del archivo **config.xml**

- Último fecha de inicio de sesión del usuario: Sábado, 07-Dec-14 03:11:52
- Creación del archivo
- Contactos: andriu2605, carlos.chavez447, erick.juanca, miguel.gerson1, **liss_preciosa(denunciante).**
- País: Ecuador
- Idioma: Español
- Versión del software.

Figura 39: Análisis forense archivo config.xml

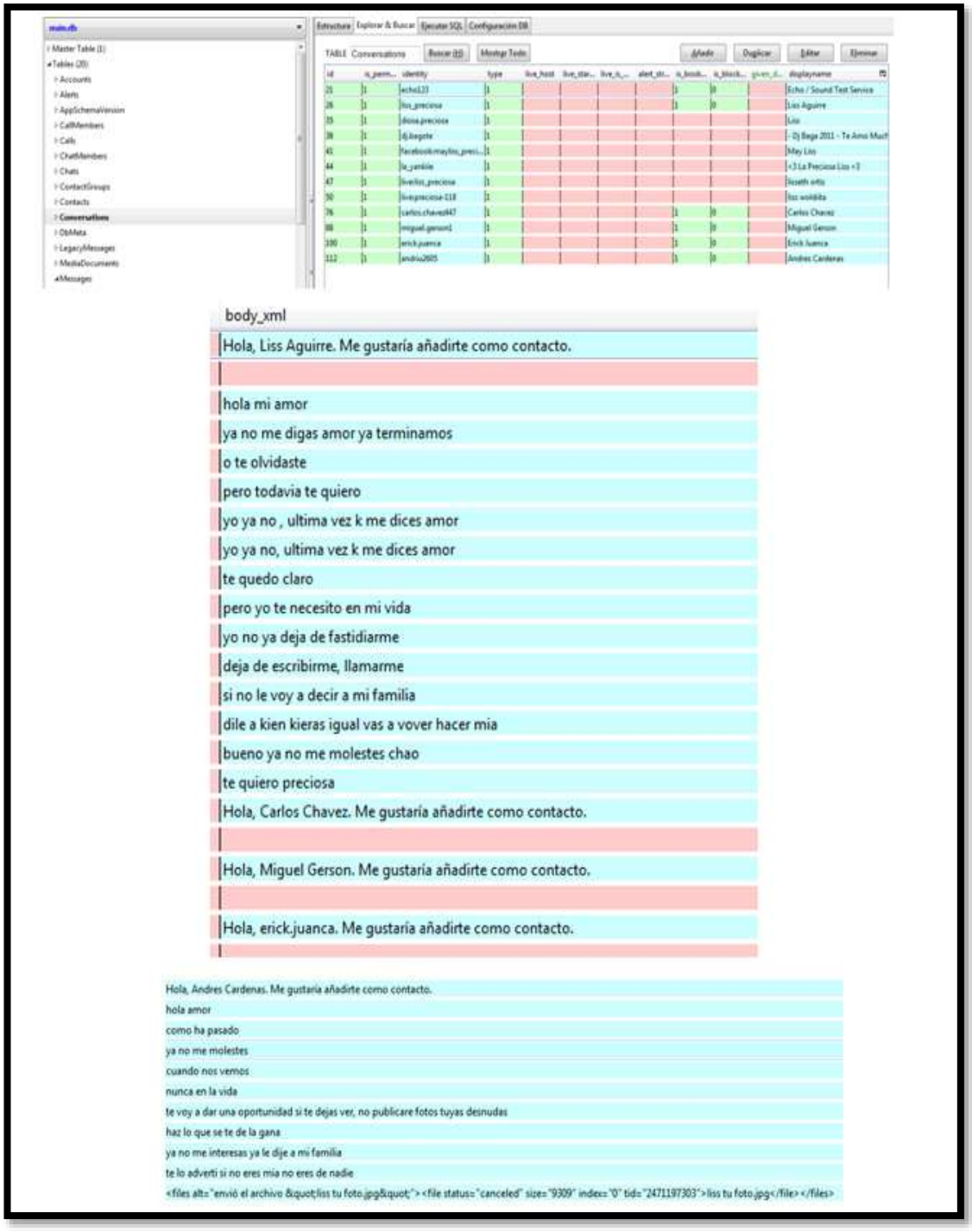


Fuente: Evidencia Skype, Fiscalía del Guayas

Elaborado por: Autor

En la carpeta **pedro.alvardo350,** se encuentra un archivo de base de datos de nombre, **"main.db",** del cual se realiza el análisis forense respectivo, encontrando algunas conversaciones que tenía con la denunciante.

Figura 40: Análisis forense archivo main.db



Fuente: Evidencia Skype, Fiscalía del Guayas

Elaborado por: Autor

Al analizar el archivo “main.db”, se verifica la conversación que mantuvo con la Sra. Aguirre del cual ella adjunta en la denuncia en su fase inicial.

INFORME EJECUTIVO

Conclusión:

El objetivo de esta investigación era comprobar si el presunto sospechoso era la persona responsable que estaba enviando mensajes a la Sra. Lissette Aguirre, a través de la denuncia presentada sobre **“Cesión, Publicación, Transferencia de datos”**. Después de haber realizado el proceso de adquisición, evaluación y análisis de la evidencia, se determina el señor Pedro Alvarado, tuvo el tiempo necesario desde diciembre, para acosar a la denunciante. Del cual se describe las actividades que tuvo el denunciado:

- En el mes de diciembre el sospechoso comienza a intimidar a la denunciante con mensajes que involucran su dignidad personal.
- A las 18:00, tenía planeado el sospechoso asaltar una empresa.
- El Sr. Alvarado utilizaba una herramienta para ocultar archivos en fotos para poder enviar a sus contactos, donde aquellos archivos ocultos se encuentra información, como fotos y un enlace de red social de la denunciante.
- En su computador, se encuentra fotos de la Sra. Aguirre, mediante el análisis respectivo en el programa Skype, se observa por medio de los registros que se mantuvieron dos conversaciones el 3 y 7 de Diciembre del 2014, donde el contenido de aquellos mensajes era de acoso para que regresara con él.
- Se comprueba la conversación de acoso que mantuvo con la Sra. Aguirre

<u>Víctimas del sospechoso</u>

Durante todo el proceso analítico de la investigación, la única víctima del sospechoso fue la Sra. **Lissette Aguirre.**

Los contactos que tenía relación con el sospechoso son: andriu2605, carlos.chavez447, erick.juanca, miguel.gerson1.

Recomendaciones de seguridad de la información

Es necesario crear las medidas preventivas para aquellas personas que enfrenten algún tipo de amenazas:

WIFI:

- No conectarse a una red inalámbrica sin clave.
- No realizar transacciones bancarias en una red abierta.
- No escribir información confidencial por esta vía de comunicación.
- Tener activado nuestro firewall.
- Utilizar navegación a través de https.

HOGARES:

- No guardar las claves en papeles.
- No utilizar la computadora de nadie, sin previa revisión, pueda que el dueño del equipo tenga instalado un Keylogger (herramienta que permite capturar toda su información digitada).
- No prestar sus cuentas bancarias para que le depositen o retiren dinero.
- Utilizar software licenciado.
- Utilizar antivirus.
- No descargar programas con fuentes desconocidas.
- No dar clic en enlaces bancarios desconocidos, ofertas y publicidades, que llegan al email, pueden ser víctima de Phishing.
- No dar información de sus cuentas por teléfono, tampoco por correo electrónico.

EMPRESARIAL:

- Utilizar software licenciado.
- Manejar políticas de seguridad de información
- Establecer credenciales de usuario administrador y otra estándar.
- Bloquear los puertos de computadoras que no sean necesarios.
- Utilización de antivirus.
- Todo medio extraíble que ingrese o salga de la empresa debe pasar por sistemas.

REDES SOCIALES

- No publicar información personal más de la necesaria, puede ser víctima de ingeniería social.
- No publicar fotos de dineros, cheques, tarjetas de crédito. Puede ser víctima de un secuestro.
- No agregar extraños, no establecer ninguna conversa.
- No publicar fotos de contenido sexual.
- Deshabilitar ubicaciones.
- Mantener la privacidad de los datos.

CELULAR:

- No utilizar el dispositivo para tomar fotos eróticas, grabar escenas sexuales y sobre todo no compartirlas por ningún motivo.
- No prestar el celular a cualquier persona.
- No conectar el celular en ninguna computadora, deshabilitar la conexión mediante USB.
- Proteger a través de patrones y claves el inicio del celular.
- Borrar registros de navegación
- Desactivar el GPS cuando se toma alguna foto o video.

BIBLIOGRAFÍA

Brezinski, D., & Killalea, T. (2002). *Guidelines for Evidence Collection and Archiving*. Obtenido de RFC 3227: http://www.ietf.org/rfc/rfc3227.txt

Balestrini. (1997). *Técnica de la Investigación.* Mc. Graw Hill.

CASEY, E. (2011). *Digital Evidence and Computer Crimen, 3era. Edición.* Elsevier.

COIP. (1 de 2 de 2014). *www.registrofical.gob.ec*. Obtenido de Código Orgánico Integral Penal: http://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

DAVARA, Miguel. (1990). Análisis de la Ley de Fraude Informático. *Revista de Derecho de UNAM* , 30.

Evidencias Informáticas. (s.f.). Obtenido de Peritaje Informático: http://www.evidenciasinformaticas.com/index.asp?IdContenido=3

HUERTA, M., y LÍBANO, C. (1996). *Delitos informáticos.* Chile: ConoSur.

IOCE. (2002). *Guidelines for Best Practice in the Forensic Examination of Digital Technology*. Obtenido de http://archive.today/rct16

KLEIMAN, D. (2007). *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators, 1era. Edition.* Syngress.

López Delgado, M. (2007). *Análisis Forense Digital, 2da. Edición*. Obtenido de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

López Oscar, Amaya Haver & León Ricardo. (2001). *Informática forense: generalidades, aspectos técnicos y herramientas.*

REZA, F. (1997). *Ciencia metodología e investigación.* México: Pearson .

ANEXOS

Anexo 1: Formato de encuesta

Las encuestas fueron realizadas a personas que estaban realizando denuncias en la fiscalía con el objetivo de conocer la realidad si tienen algún tipo de conocimiento con el tema de los delitos informáticos. Los nombres de los encuestados son de total confidencialidad, en función de realizar un análisis estadístico. Por lo tanto las respuestas están orientadas a la verdad.

UNIVERSIDAD POLITÉCNICA SALESIANA	ANEXO 1
Herramienta: Encuesta	**Fecha:** 17 – 18/Septiembre/2014
Desarrollado por: Autor	**Tutor:** Msig. Nelson Mora
Dirigido a: Personas alrededor de la fiscalía	**Duración:** 4 horas

1. **Sexo**
   - Masculino
   - Femenino

2. **Datos Personales**

   - **Nombre:** **……**
   - **Cédula:** **……**
   - **Área Ocupacional:** **……**

1. **¿Ha escuchado sobre los ataques informáticos en nuestro País?**
   - Si
   - No

2. **¿Cuál es el tipo de delito informático que usted conoce?**
   - Pornografía Online
   - Fraude online
   - Violación de los Derechos de Autor
   - Robo o copia de información confidencial
   - Destrucción de Programas

3. **¿Con qué frecuencia cambia las contraseñas de sus cuentas electrónicas?**
    - Quincenal
    - Mensual
    - Cada 6 meses
    - Mayor a un año
    - Nunca

4. **¿Ha sido víctima de un ataque informático?**
    - Si
    - No

5. **¿Conoce sobre los perjuicios que ocasionan estos ataques informáticos?**
    - No ingresar a cuentas
    - Publicaciones falsas
    - Mensajes Obscenos
    - Robo de dinero electrónico
    - Ninguno

6. **¿Ha escuchado hablar sobre los peritos informáticos?**
    - Si, completamente
    - No del todo
    - No

7. **¿Conoce si en la fiscalía existe un departamento que investiga éstos tipos de delitos?**
    - Si
    - No

8. **¿Conoce cuáles son los procedimientos para realizar este tipo de denuncia?**
    - Si
    - No

9. **¿Cree usted que deberían existir campañas de prevención ante éste tipo de delitos?**
    - Completamente de acuerdo
    - No, es necesario

FIRMA

Anexo 2: Entrevista 1

UNIVERSIDAD POLITÉCNICA SALESIANA	ANEXO 3
Herramienta: Certificado de Entrevista	**Fecha:** 12/Septiembre/2014
Desarrollado por: Autor	**Tutor:** Msig. Nelson Mora
Dirigido: Ing. Roberto Olaya	**Duración:** 1: 30 hora

Guayaquil, 12 de Septiembre del 2014

CEO
Ing. Roberto Olaya B.
Director de la Empresa Hack Security S.A
Guayaquil

De mi consideración:

Por medio de la presente, dejo en constancia, que el señor José Rosero Quiroz me ha realizado una entrevista en mi oficina, dedicada en fundamentar su investigación con respecto a su tema de tesis, enfocado en los procesos de los delitos informáticos en el Ecuador, fundamentando temas como son: peritaje informático, situación actual, herramientas, mecanismos, informes, entre diversos temas más.

Para que conste, se expide el presente certificado, para que el Señor pueda presentar en su tesis como un anexo de su investigación.

Atentamente,

Ing. Roberto Olaya B.
C.C. # 0911237600

asesores de seguridad lógica
HCK-S
HACKsecurity

Anexo 3: Entrevista 2

UNIVERSIDAD POLITÉCNICA SALESIANA	ANEXO 4
Herramienta: Certificado de Entrevista	**Fecha:** 30/Septiembre/2014
Desarrollado por: Autor	**Tutor:** Msig. Nelson Mora
Dirigido a: Abogada Patricia Morán	**Duración:** 1 hora

Guayaquil, 30 de Septiembre del 2014

Fiscal
Abogada Patricia Morán Espinoza
Experta en delitos informáticos
Guayaquil

CERTIFICO

A través del presente dejo en constancia, que el señor José Rosero Quiroz ha procedido a realizarme en mi oficina una entrevista, en la cual está basado, sobre los aspectos de los delitos informáticos en el Ecuador, donde se trato sus inquietudes sobre las leyes del Ecuador, cadena de custodia, investigación forense, evidencia digital, peritaje informático.

Autorizo, para que el señor pueda adjuntar este certificado en su tesis, como parte de su investigación.
Me despido con toda mi consideración

Muy Atentamente,

Abogada Patricia Morán Espinoza

C.C. # 0703609628

Anexo 4: Entrevista 3

UNIVERSIDAD POLITÉCNICA SALESIANA	ANEXO 5
Herramienta: Certificado de Entrevista	**Fecha:** 29/Noviembre/2014
Desarrollado por: Autor	**Tutor:** Msig. Nelson Mora
Dirigido a: Lcda. Yelena Casanova Gilces	**Duración:** 1 hora

Guayaquil, 29 de Noviembre del 2014

Lcda.
Yelena Casanova Gilces
EXPERTA EN DELITOS INFORMÁTICOS

De mi consideración,

A través del presente dejo en constancia, que el señor José Rosero Quiroz ha procedido a realizarme una entrevista, sobre la cual está basada y fundamentada, sobre los aspectos que involucra un peritaje informático, basado en el delito de CESIÓN Y PUBLICACIÓN de redes sociales, donde se trato sus inquietudes sobre cadena de custodia, investigación forense, evidencia digital.

Me despido.

Muy Atentamente,

Lcda. Yelena Casanova Gilces
C.I. 0920476892

Anexo 5: Entrevista 4

UNIVERSIDAD POLITÉCNICA SALESIANA	ANEXO 6
Herramienta: Certificado de Entrevista	**Fecha:** 16/Diciembre/2014
Desarrollado por: Autor	**Tutor:** Msig. Nelson Mora
Dirigido a: Dr. Santiago Acurio del Pino	**Duración:** 1 hora

CONSEJO DE LA JUDICATURA

Quito, 16 de Diciembre del 2014

Dr.
Santiago Acurio del Pino
Juez de la Corte Provincial de Pichincha
Experto en Derecho Informático
Quito

CERTIFICO

A través del presente dejo en constancia, que el señor José Rosero Quiroz portador de la cédula 0921973541, me ha realizado una entrevista enfocada, sobre los aspectos de los delitos informáticos en el Ecuador, donde se trató temas relacionados sobre COIP, cadena de custodia, evidencia digital, área de criminalística informática.

Me despido con toda mi consideración

Muy Atentamente,

Dr. Santiago Acurio
C.I. 1713627071

Hacemos de la justicia una práctica diaria

Anexo 6: Modelo de acta de incautación

Propuesta por autor, sobre un modelo de acta de incautación para peritos externos.

En la ciudad de _____, Ecuador, a los _____días del mes de _____ del año _____, siendo las_____ horas y _____ minutos, como perito actualmente acreditado me suscribo, _____ cédula de ciudadanía_____, por disposición del SR(A). FISCAL. De la unidad_____ a cargo Del Departamento Judicial, gestionar la investigación de la denuncia presenta sobre _____ por la/s víctima/s _____.Por lo tanto denuncia como posible culpable al Sr. _____. Me encuentro en la dirección _____de la ciudad de_____. De la sr(a)_____ de nacionalidad _____, de _____ años de edad, de estado civil_____, de ocupación_____, Cédula de identidad_____, En presencia de la denunciante, con el objetivo de dar cumplimiento a la labor Pericial, donde la víctima estaba presente en el lugar de los Hechos. Para ello se realizo el peritaje respectivo de incautación de cada elemento digital, del cual fueron incautadas los siguientes: _____

_____

OBSERVACIONES:

_____

_____

_____

Se da por finalizado el acto, previa e íntegra lectura del acta de incautación, se procede a realizar las firmas de aceptación:

_____ DENUNCIANTE

_____ PERITO

ÍNDICE DE ABREVIATURAS

I.D.F	Investigador digital forense
CAINE	Computer Aided Investigative Environment
DEFT	Digital Evidence & Forensics Toolkit
CPC	Código de Procedimiento Civil
CPP	Código de Procedimiento Penal
COIP	Código Orgánico Integral Penal
SOP	Procedimiento Operativo Estándar
RFC	Request for Comments
IOCE	Organización Internacional de Prueba Informática
SBS	Superintendencia de Banco y Seguros
HTTPS	Protocolo de transferencia de hipertexto seguro
NDD	Número de Denuncias