UNIVERSIDAD AMAZÓNICA DE PANDO

DIRECCIÓN DE POSTGRADO E INVESTIGACIÓN

TESIS PARA OPTAR EL GRADO ACADEMICO DE

MAGISTER EN INGENIERIA EN INFORMATICA

"Desarrollo de una Técnica Informática
Forense para el uso en las Investigaciones de Delitos Informáticos
en la Policía Nacional Departamento – Fiscalía del Distrito de Potosí."

POSTULANTE: ROSALVA CONDORI HUANCA

TUTOR: RAMIRO VILLA

POTOSI – BOLIVIA

2011

INDICE DE CONTENIDOS

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA, OBJETIVOS Y ESTRATEGIA METODOLÓGICA

INTRODUCCIÓN…….. 1

1.1 SITUACION PROBLEMICA....4

1.2 OBJETIVOS Y ESTRATEGIA.....5

1.3 JUSTIFICACION.....6

1.4 METODOLOGÍA.....6

CAPÍTULO II

MARCO TEORICO

2.1. INFORMÁTICA FORENSE.....10

2.2. EVIDENCIA DIGITAL..... 12

2.3. DELITOS INFORMÁTICOS.....14

2.4. PRINCIPIO DE LOCARD.....16

2.5. MEDIDAS DE SEGURIDAD LEGALES..... 17

2.5.1 SECUESTRO..... 17

2.5.2 INCAUTACION..... 18

2.5.3 ALLANAMIENTO..... 18

2.6. METODOLOGÍA Y TÉCNICA..... 20

2.7. HERRAMIENTAS INFORMATICAS..... 21

2.7.1 SOFTWARE..... 21

2.7.2 HARDWARE.....24

CAPITULO III

MARCO REFERENCIAL

3.1. SITUACIÓN ACTUAL DE LA INFORMÁTICA FORENSE..... 26

3.2. REGULACIONES EXISTENTES EN LATINOAMÉRICA..... 26

a) Delitos Informáticos: Aplicación Chile..... 27

b) Delitos Informáticos: Aplicación Argentina……..…….……...…29
c) Delitos Informáticos: Aplicación Colombia……..…30
3.3. PROCESO FORENSE……...…32
3.3.1. RFC3227…..…….……... 32
3.3.2. Guía de la IOCE……..…….... 33
3.3.3. Investigación en la Escena del Crimen Electrónico (Guía DoJ 1)…….. 34
3.3.4. Examen Forense de Evidencia Digital (Guía DoJ 2)……...……... 34
3.3.5. Computación Forense - Parte 2: Mejores Prácticas (Guía Hong Kong)…….… 35
3.3.6. Guía de buenas prácticas para Evidencia basada en Computadores (Guía Reino Unido)…….…..34
3.3.7. Guía para el Manejo de Evidencia en IT (Guía Australia)…….. 36
3.4. SITUACION DE LA INFORMATICA FORENSE EN POTOSI…..…….….. 36
3.4.1. Observación……...……37
3.4.2. Entrevista y Cuestionario……...…. 37
3.4.3. Fuentes de información……...…… 37
3.4.4. Población y Muestra. ……38
3.4.4.1. Población. ……..…38
3.4.4.2. Muestra. …….……38

CAPITULO IV

APLICABILIDAD DE LA INFORMÁTICA FORENSE

4.1. IMPLEMENTACIÓN DE LABORATORIO……...……... 40
4.2. METODOLOGÍA INFORMÁTICO FORENSE……..……...… 41
4.2.1. Marco Científico…….…... 42
4.2.2. Marco Criminalística…….. 42
4.2.3. Marco Informático general……. 42
4.2.4. Marco Informático específico…… 42
4.2.5. Marco Legal……..…… .42
4.2.6. Metodología Sistémica……...…… 43
4.3.1. FASE IDENTIFICACIÓN…….…..... 44
4.3.2. FASE PRESERVACIÓN DE LA EVIDENCIA…….…… 49

4.3.2.1. Copias de la evidencia……..... 49
4.3.2.2. Cadena de custodia…….... 49
4.3.3. FASE DE ANÁLISIS……. 51
4.3.3.1. Preparación para el análisis……..... 52
4.3.3.2. Reconstrucción de la secuencia temporal del ataque……..…..…. 52
4.3.3.3. Determinación de cómo se realizó el ataque…….....…. 54
4.3.3.4. Identificación del atacante…….. 55
4.3.4. FASE DE PRESENTACIÓN DE INFORME…… 56
4.3.4.1. Evaluación del impacto causado al sistema…….…. .56
4.3.4.2. Documentación del incidente…….…... .57
4.3.4.3. Utilización de formularios de registro del incidente……...…….. .57
4.3.4.4. El Informe Técnico……...…….... 59
4.3.4.5. El Informe Ejecutivo…….…. 59
4.4. CASO DE ESTUDIO……..…. 60
CAPITULO V
INTERPRETACIÓN DE RESULTADOS…….……..……..…. 61
5.1. PRESENTACIÓN DE RESULTADOS. …….……..…. 61
5.2. VALIDACIÓN DE RESULTADOS ……..……..…. 65
CONCLUSIONES…… ..69
RECOMENDACIONES…….…….70
REFERENCIAS BIBLIOGRAFICAS…….71
BIBLIOGRAFIA…….....72
ANEXOS.

INDICE DE CUADRO Y FIGURAS:

Cuadro Nro.2.1 Comparación de herramientas forenses……...…. 22

Cuadro Nro.3.1. Resumen de las Leyes de Delitos Informáticos en Latinoamérica…… 27

Cuadro Nro.3.2. Legislación en Chile – Informática e información…….……..…… 28

Cuadro Nro.3.3. Legislación en Argentina – Informática e información……..……. 29

Cuadro Nro.3.4. Legislación en Colombia – Informática e información……..……... 30

Figura.4.1. Organización del Laboratorio…….……..……. 41

Figura 4.2. Metodología Sistémica……...……..…. 44

Figura 4.3. Diagrama de Flujo Fase Identificación……...….... 48

Figura 4.4. Diagrama de Flujo Fase Preservación……...…… 50

Figura 4.5. Diagrama de Flujo Fase Análisis……...…… 56

Figura 4.6. Diagrama de Flujo Fase Presentación De Informe….……..…. 59

Grafico 5.1. Pregunta 1-Cuestionario…….……...…61

Grafico 5.2. Pregunta 2-Cuestionario……62

Grafico 5.3. Pregunta 3-Cuestionario……62

Grafico 5.4. Pregunta 3-Cuestionario- motivos…….……...……63

Grafico 5.5. Pregunta 4-Cuestionario……63

Grafico 5.6. Pregunta 5-Cuestionario……64

Grafico 5.7. Pregunta 6-Cuestionario……64

Grafico 5.8. Fase Identificación-Cuestionario……..…65

Grafico 5.9. Fase Preservación-Cuestionario……..……..……66

Grafico 5.10. Fase Análisis-Cuestionario……...……..…….……66

Grafico 5.11. Fase Presentación-Cuestionario……..…..……..……67

Grafico 5.12. Implementación del laboratorio-Cuestionario……..……...…67

INTRODUCCION

En la actualidad las empresas o instituciones operan a través del recurso informático, por lo que necesitan dotar a los sistemas que utilizan de confiabilidad, seguridad y mejorar las infraestructuras informáticas, por lo cual se requieren profesionales del área con los conocimientos suficientes para implementar nuevas tecnologías de seguridad, controlen y gestionen eficazmente los sistemas, o en su caso para desarrollar los mismos, esto no ocurre, los profesionales que son formados en las universidades se limitan a dar soporte tanto en software como en hardware, más aun en la ciudad de Potosí donde no hay empresas que desarrollen Software de calidad o peor aún éstas empresas al servicio del público no confían en las pocas que hubieran y contratan empresas del interior, motivo por el cual los profesionales del área se ven limitados a dar solo esos servicios. Sin embargo en la ciudad de Potosí y en Bolivia los delitos informáticos van incrementándose y ya salen a luz tímidamente, sin duda más rápidamente que el desarrollo de software en la ciudad, a medida que la ciencia avanza también los delincuentes se actualizan y crean más armas, cometiendo fechorías, al igual que un crimen en la dimensión física deja evidencias, aquí también se deja evidencias del crimen, pero dichas evidencias quedan almacenadas de forma digital, en la mayoría de los casos dicha información no se puede leer o recolectar por medios comunes o mecanismos tradicionales, es así que nace el estudio de la informática forense, que provee el conocimiento y los instrumentos para estudiar y solucionar este nuevo tipo de delitos, la informática forense puede ser explotada, usando la gran cantidad de herramientas existentes en todas la empresas que usan recursos informáticos y gracias a ella se puede anticipar delitos informáticos, sin que los profesionales del área estén a la espera de desarrollar software, es posible aplicar esta ciencia utilizando lo existentes en el medio, de esa manera apoyar a las empresas a protegerse a la delincuencia informática.

Es menester anticiparse a la delincuencia informática, principalmente en la Policía Nacional del Departamento de Potosí en su departamento de LABORATORIO DE INVESTIGACIONES y otras unidades que apoyan, además de la FISCALÍA DEL

DISTRITO DE POTOSI, en las mencionadas instituciones se hacen cargo de las denuncias de delito informáticos usando una parte de la informática forense, culminando el trabajo en la ciudad de La Paz, donde un perito informático emite informes con los resultados. La situación descrita demora un tiempo excesivo o no se concluye, razones que en muchos casos impide que llegue a su fin el proceso o que se denuncie por delitos informáticos.

Por lo expuesto se propone el uso de procedimientos prácticos que servirán para poder apoyar en el manejo de investigaciones dando pautas para el tratamiento de la evidencia digital, además de identificar un marco general sobre la conceptualización básica necesaria relativo a los delitos informáticos, tipos de delitos, sus objetivos, importancia, sus principios, la evidencia digital y la informática forense.

En la actualidad se sigue procedimientos manera errónea en la División de Laboratorio de la Policía, tratan de realizar el trabajo siguiendo lineamientos basados en el Código Penal en su Art.268, donde menciona como se debe realizar un trabajo forense, de manera general omitiendo algunos pasos informáticos forenses que son necesarios, por factores que en el medio son compresibles, personal empírico trabajando en esta unidad, ya que los mismos son los uniformados preparados militarmente, sin estudios técnicos informáticos, no se cuenta con personal especializado y con conocimientos en la informática forense, por lo que se recurre al empirismo y a la práctica diaria, cometiendo errores en el tratamiento de evidencia digital. La evidencia digital es tratada de manera descuidada, siendo el trabajo realizado de forma práctica sin ningún procedimiento normado, realizado por un equipo de trabajo de áreas policiales y legales, donde la preparación del Policía a cargo es Técnico Superior en la informática. Una vez descrita la situación problemática el problema es formulado de la siguiente manera: ¿Cuál es el conjunto de procedimientos capaz de mejorar las investigaciones que realizan sobre los delitos informáticos efectuados por la Policía Nacional-Fiscalía del Distrito de Potosí?

Para apoyar al desarrollo de la técnica se recurrirá al uso de las metodologías, herramientas y técnicas que se aplican para prevenir un siniestro informático en las empresas comerciales se hacen cada vez más un objetivo primordial para evitar los siniestros dentro de una empresa. Existiendo variedad de metodologías informáticas forenses que indican el camino a seguir para realizar una investigación forense, en la presente tesis se mostrará la practicidad en detalle usando una técnica informática forense.

Debido a que en la presente tesis se estudiará la parte legal con relación a la informática es que el objeto de estudio será la Informática Forense y pudiendo trabajar en el campo de acción en el análisis de las investigaciones sobre delitos informáticos realizados en la unidad de investigaciones en la Policía.

Una vez identificado el problema, se presenta a continuación el objetivo general que es: Desarrollar una técnica informático forense para mejorar las investigaciones de delitos informáticos que se realicen en la Policía Nacional Departamento de Potosí – Fiscalía del Distrito de Potosí.

Para sustentar la validez de la tesis, se empleará la siguiente hipótesis: "La implementación de la técnica informático forense para el uso en las investigaciones de delitos informáticos mejorará el tiempo de obtención de resultados que se realicen en el laboratorio de la Policía Nacional del Departamento – Fiscalía del Distrito"

La Unidad de Observación es el Laboratorio de investigación de la Policía Nacional del Departamento – Fiscalía del Distrito, la Variable Dependiente es el Tiempo de obtención de resultados y la Variable Independiente es la Técnica informático forense para el uso en las investigaciones de delitos informáticos.

Las Metodologías que serán usadas son los Métodos teóricos: Análisis –Síntesis, Inducción-deducción y Análisis histórico-lógico. Así también se usó el Método Empírico, con el uso de las herramientas de observación, entrevista, y cuestionario; en el capítulo I será ampliamente detallado.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA, OBJETIVOS Y ESTRATEGIA METODOLÓGICA

1.1.SITUACION PROBLEMICA.

La tecnología avanza a pasos agigantados, los datos de las instituciones están en mayor porcentaje en computadoras por lo cual también los delitos informáticos avanzan a esa misma velocidad. A la oficina de la FISCALIA DE LA NACION le llegan denuncias, se procesan en compañía de la unidad de Laboratorio de la POLICIA DE LA NACION y un Juez de la CORTE SUPERIOR DE DISTRITO, mismos que proceden a la obtención del equipo usado para cometer el delito, aplicando la experiencia con la que se cuenta en caso penales, civiles y otros, pero no así en experiencia pericial informática, posteriormente lo incautado no se almacena con el debido cuidado, cometiendo errores en el tratamiento de evidencia digital, peor aún no se cuenta con en el registro de quienes manipularon lo incautado, posteriormente se envía a la ciudad de La Paz para concluir con el análisis. Todo este proceso muestra que el personal no está capacitado con el uso de procedimientos técnicos informáticos forense y hace que las pruebas estén sujetas a duda, si en el camino fue cambiado o no, si la evidencia digital no fue manipulada. Por lo que al descentralizar y realizar el trabajo completo en la ciudad de Potosí aceleraría el proceso de la aplicación de la técnica forense que se pretende implementar en esta unidad.

1.2.FORMULACION DEL PROBLEMA.

¿Cuál es el conjunto de procedimientos capaz de mejorar las investigaciones que realizan sobre los delitos informáticos efectuados por la Policía Nacional-Fiscalía del Distrito de Potosí?

1.3.OBJETIVOS Y ESTRATEGIA

Para obtener resultados favorables y desechar el uso de procedimientos empíricos con los que actualmente se realizan los estudios de los casos de delitos informáticos, la presente Tesis propone el siguiente Objetivo General es: Desarrollar una técnica informático forense para mejorar las investigaciones de delitos informáticos que se realicen en la Policía Nacional Departamento de Potosí – Fiscalía del Distrito de Potosí.

Identificar cuáles son los factores legales y tecnológicos que se presentan ante el manejo de un delito informático antes, durante y después de un proceso de pericia informática.

- Identificar cuáles son las herramientas más apropiadas para cada delito y ganar familiaridad con las mismas antes que la investigación lo requiera.
- Plantear un procedimiento para secuestrar la evidencia digital.
- Plantear un procedimiento para preservar la evidencia digital.
- Plantear un procedimiento para obtener y analizar la evidencia digital.
- Plantear un procedimiento para mostrar y dar a conocer los resultados.

Para sustentar la validez de la tesis, se empleará la siguiente hipótesis: "La implementación de la técnica informático forense para el uso en las investigaciones de delitos informáticos mejorará el tiempo de obtención de resultados que se realicen en el laboratorio de la Policía Nacional del Departamento – Fiscalía del Distrito"

La Unidad de Observación es el Laboratorio de investigación de la Policía Nacional del Departamento – Fiscalía del Distrito, la Variable Dependiente es el Tiempo de obtención de resultados y la Variable Independiente es la Técnica informático forense para el uso en las investigaciones de delitos informáticos.

1.4.JUSTIFICACION.

Es justificable la realización de la presente tesis por lo siguiente:

- ✓ La presente investigación es conveniente para la sociedad en su conjunto debido a que la técnica a desarrollar ayudará de sobremanera a que se puedan prevenir los delitos informáticos y a investigar los mismos una vez detectados.
- ✓ Al ser una ciencia poco conocida en el medio, la sociedad podrá denunciar los casos que se conozcan como delitos informáticos y no como hasta ahora lo hacen como otros tipos de delitos penales, tratando de encontrar otras alternativas para demandar y no como evidentemente es, un delito informático. Así también las denuncias que hubieren podrán obtener los resultados de forma confiable y en menor tiempo, usando la técnica desarrollada en el presente trabajo de investigación.
- ✓ Este instrumento coadyuvara a los profesionales del área de la informática siendo una guía seguir para cualquier investigación que se presente, así también a estudiantes de esta carrera, para que puedan especializarse en el área, siguiendo esta técnica podrán interiorizarse con las herramientas que existen tanto en software como en hardware, debido a que en la ciudad de Potosí no existen peritos en informática forense, por lo que se recurre a profesionales de otros departamentos.

1.5.METODOLOGÍA.

Las Metodologías que están siendo usadas son los:

Métodos Teóricos.

a. Análisis –Síntesis.

Siendo la Informática Forense una ciencia amplia se analizará los delitos informáticos que están inmersos los distintos tipos de sistemas informáticos, la información digital manejada en red, la que está en las computadores, etc., así como las distintas herramientas informáticas forenses que existen, que

posteriormente se sintetizará usando la técnica adecuada aplicando al caso requerido.

b. Inducción y deducción.

Contando con casos particulares, delitos informáticos que son pasados por alto considerándose como casos penales comunes es que con la técnica adecuada todos los delitos informáticos podrán ser tratados, investigados sin tropiezos.

c. Lógico Deductivo.

Una vez concluido el presente trabajo se podrá demostrar la hipótesis planteada, usando la nueva técnica informática forense.

d. **Análisis histórico y lógico.**

Permitió descubrir cómo se llevó a cabo el proceso de relevamiento de evidencia digital, del tratamiento de los delitos informáticos hasta ahora, de esa forma permitir que la técnica informática forense cumpla con todos los requerimientos.

Métodos Empíricos.

Permitieron revelar y explicar las características que se observaron durante el desarrollo de trabajo de investigación, obteniendo la información necesaria.

a. Observación.

La observación es fundamental para investigar cómo se trabaja actualmente. Las oficinas en las que se realizan las investigaciones y el lugar donde se mantienen los equipos secuestrados. Así también observará a detalle el laboratorio de la Policía Nacional.

b. Entrevista.

Para conocer la situación actual se entrevistó al Sargento W. Salguero encargado de la unidad LABORATORIO, siendo el usuario primario. Así también con personal de la Fiscalía de Distrito siendo los usuarios secundarios. Durante el desarrollo de la tesis se continuará con las entrevistas al personal pertinente.

c. Cuestionario.

Método auxiliar o complementario que se emplea de forma masiva para recoger información para reflejar y comprender el funcionamiento del proceso de investigación en caso de delitos informáticos, para este propósito se utilizo éste instrumento con personas involucradas, empleados de la institución, cuestionario aplicado al Jefe de la Sección (ver ANEXO A).

d. **La revisión de documentación.**

Utilizada para conocer y estudiar los documentos que son manejados con en el proceso actual, además de los reportes y tipo de informes genera.

e. Revisión y recopilación de material bibliográfico.

Proceso que se realiza durante todo el ciclo de desarrollo del sistema.

f. **Método estadístico.**

Permitió definir la **población – muestra** involucrados en el sistema, medio por el cual se obtuvo resultados de la encuesta para conocer información precisa, teniendo como población universo a 45 personas, siguiendo las formula estadística probabilística denominado **“** Tamaño de la muestra para poblaciones finitas **”**, se obtuvo una población muestral de 27 personas encuestadas, siendo los encuestados Policías y Fiscales.

CAPITULO II
MARCO TEORICO

2.1.INFORMÁTICA FORENSE.

La informática forense es el proceso de identificar, preservar, analizar y presentar evidencia digital de manera que esta sea legalmente aceptable. (HERRERA Hernán y GÓMEZ Sebastián, 2009).

Una primera revisión sugiere diferentes términos para aproximarnos a este tema, dentro de los cuales se tienen: computación forense, digital forensics (forensia digital), network forensics (forensia en redes), entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular o general temas que son de interés para las ciencias forenses aplicadas en medios informáticos. (MCKEMMISH 1999)

Computer forensics, generalmente es traducido computación forense, es interpretada de dos maneras:

- Disciplina de las ciencias forenses, que considerando las tareas asociadas con la evidencia digital, procura descubrir e interpretar la información en cualquier medio informático hallado en la escena del crimen, de esa manera es posible establecer los hechos y formular las hipótesis relacionadas con el caso.

- Como la disciplina científica y especializada con los elementos asociados a las tecnologías de los equipos de computación, mismos que ofrecen la posibilidad de realizar un análisis de la información residente en dichos equipos.

Ambas definiciones no son excluyentes, sino complementarias. Una de ellas hace énfasis en las consideraciones forenses y la otra en la especialidad técnica, pero las dos procuran el esclarecimiento e interpretación de la información en los medios informáticos como valor fundamental, uno para la justicia y otro para la informática. (CANNO Jeymi, 2008).

Network forensics, forensia en redes, estudia de manera profunda las redes, comprendiendo cómo los protocolos, configuraciones e infraestructuras de comunicaciones, donde se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.

Esta conjunción de palabras establece un profesional especializado en el área que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción criminal. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente. (CANNO Jeymi, 2008).

Digital forensics, forensia digital, trata de conjugar de manera amplia la nueva especialidad. Se podría hacer semejanza con informática forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿porqué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática. (CANNO Jeymi, 2008).

Cabe hacer notar que las definiciones que maneja el perito informático forense o especialista, debe aplicar estos conocimientos con ética y respeto de las entidades, aplicar con sabiduría y con criterio cada una de estas definiciones, ya que de lo contrario la evidencia digital podría ser maleable, sujeto a distorsión.

El presente estudio se desenvuelve en Forensia digital, ya que los casos con los que se tropieza en el medio no exigen mayor énfasis en las otras disciplinas, se tocará un poco de Forensia en redes, de manera los especialistas deben contar con todos estos conocimientos. A medida que la tecnología avanza, los conocimientos de los profesionales también se actualizarán, ya que la delincuencia está ingresando con fuerza al campo tecnológico, más aún con el internet, que en muchos países este servicio ya es como la energía eléctrica, todos la usan.

2.2.EVIDENCIA DIGITAL.

La evidencia computacional es única, cuando se la compara con otras formas de "evidencia documental". A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario. (LÓPEZ Óscar, AMAYA Haver y LEÓN Ricardo, 2001)

La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno. La evidencia digital

posee, entre otros, los siguientes elementos que la hacen un constante desafío para aquellos que la identifican y analizan en la búsqueda de la verdad:

- Es volátil
- Es anónima
- Es duplicable
- Es alterable y modificable
- Es eliminable

Estas características advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos, como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. (CANNO Jeymi, 2008).

Los especialistas deberán mantener un conocimiento minucioso de las normas y regulaciones legales tanto en Bolivia como en Latinoamérica asociadas con el código Penal y su procedimiento, así como de una técnica y sus procedimientos que permita mantener la confiabilidad de los datos recogidos, la integridad de las pruebas, el análisis detallado de los datos y la presentación idónea de los resultados, tareas realizadas de inicio a fin por personal ético, para que el estudio realizado pueda ser útil, de otro modo no se confiaría en la informática forense ya que estaría sujeto a manipulación, otra vez por un humano.

Considerando estas características se deberá manejar con mucho cuidado los datos obtenidos, ya que cualquier mal trato que se le da la evidencia digital podría ensuciarse y dejar de ser evidencia.

Es necesario hacer notar que las evidencias son iguales sean estas físicas digitales, con la única diferencia que las evidencias digitales pueden ser recogidas de elementos físicos o digitales, de acuerdo el caso que se presente.

2.3.DELITOS INFORMÁTICOS.

Todos los humanos son testigos de que la tecnología informática no tiene límites previsibles y su avance es sorprendente, su incursión dentro de las empresas jurídicas y naturales es irremediable, dando lugar a la significativa importancia para el funcionamiento y la seguridad informática, la administración, la defensa y la sociedad, el grado que en la actualidad se da a los documentos digitales, a la información digital, que a pasos agigantados han originado la criminalidad informática, el crecimiento espectacular de la informática ha abierto puertas a muchas posibilidades de delincuencia, misma que también avanza con esta actualización, mientras se crean curas para males, existen personas que van creando nuevos crímenes digitalmente, sin que estos puedan detectarse de manera inmediata, o peor sin descubrir cómo es que ocurrió, todo esto apoyados con las herramientas tecnológicas de la actualidad.

Estando frente a la realidad donde algunos individuos o grupos sin escrúpulos buscan obtener el poder que la información puede otorgarles para satisfacer sus intereses personales, beneficiándose muchas veces económicamente, por lo cual se advierte una amenaza futura proporcional a los adelantos tecnológicos.

Se entiende por delitos informáticos "a las actitudes ilícitas en que se tienen a las computadoras como instrumento o fin o a las conductas tipificadas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin… " (TELLEZ Julio, 2008).

Las principales característica de este tipo de delito son: (TOLA Ramiro, 2010)

a. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

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

c. Provocan serias pérdidas económicas ya que casi siempre producen beneficios aquellos que las realizan.

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

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

f. Presentan grandes dificultades para su comprobación, por su mismo carácter técnico.

Esta es la realidad en la que se encuentra Bolivia, esas son las características sociales a la que cualquiera que use una computadora se enfrenta cuando se trata de delitos informáticos, es de lamentar que aún no se cuente con una clasificación en cuanto a delitos informáticos se refiere, aún se trabaja en este aspecto en la Ley de Telecomunicaciones y TICs,

Para tener una mejor idea de la definición de Delitos Informáticos en la Legislación Boliviana, a continuación se muestra artículos del código penal que fueron reformulados en el 1997 en el capítulo XI, 1que están relacionados en los siguientes artículos

ARTICULO 363 bis.- (MANIPULACIÓN INFORMÁTICA).- El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un

proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días. (Código Penal, 1997).

ARTICULO 363 ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS).- El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días. (Código Penal, 1997).

La manipulación Informática y la Alteración, acceso y uso indebido de datos informáticos son definiciones generales, donde el criminal o su abogado se pueden apoyar en estos artículos podría salir libre, ya que no existen pasos a seguir, guías, reglas sobre el manejo de las evidencias digitales, con respecto a la recolección, preservación, análisis y presentación del informe, para lo cual en el presente trabajo se basará en estos artículos y definición de delito informático para desarrollar la técnica informática forense, la cual indicará los pasos a seguir en cada fase.

2.4.PRINCIPIO DE LOCARD.

Este principio es usado para análisis forense criminalístico, que indica que cuando se comete un crimen siempre se deja huella, siempre dos objetos que entran en contactos transfieren evidencias entre el autor y la víctima, además del lugar del hecho. Los mejores investigadores se basan en este principio para resolver crímenes, el autor se lleva consigo algo de la víctima, deja su huella en el lugar del hecho o lo que fuera, también deja algo en la víctima.

Es también aplicado en términos informáticos, ya que de la misma manera el autor del crimen transfiere información a la victima que puede ser la computadora. Basados en este

principio se podrá obtener pruebas o evidencias digitales, mismo que también es aplicado digitalmente, incluso en instrucciones a las computadoras que muchas veces se piensa haber eliminado todo rastro de ingreso no autorizado en una computadora, sin embargo se deja huellas, sean estas registradas en la memoria volátil, en eventos del mismo equipo u otros. Es así que se aplicará este principio durante el desarrollo del presente trabajo.

2.5.MEDIDAS DE SEGURIDAD LEGALES.

Se debe considerar que en todo el desarrollo del presente trabajo está inmerso el proceso legal, para ello se deben considerar medidas de seguridad legales, para ello se aplicará la legislación boliviana y de esa manera este documento se enmarcará en la ley.

Cuando existe una denuncia de un caso de delito informático, se recurre a los medios legales para obtener la evidencia digital de acuerdo a las normas que están establecidas en la legislación boliviana se procede de tres maneras: el secuestro, incautación y el allanamiento.

2.5.1. SECUESTRO.

ARTICULO 184. (ENTREGA DE OBJETOS Y DOCUMENTOS, SECUESTROS). Los objetos, instrumentos y demás piezas de convicción existentes serán recogidos, asegurados y sellados por la policía o el fiscal para su retención y conservación, dejándose constancia de este hecho en acta. Si por su naturaleza es imposible mantener los objetos en su forma primitiva, el fiscal dispondrá la mejor manera de conservarlos.

- Todo aquel que tenga en su poder objetos o documentos de los señalados procedentemente estará obligado a presentarlos y entregarlos, cuando le sea requerido, a cuyo efecto podrán ser compelidos por la fuerza pública, sin perjuicio de la responsabilidad que corresponda.

- Quedan exceptuadas de este deber las personas que por ley no están obligadas a declarar como testigos.

2.5.2. INCAUTACION.

ARTICULO 254. (RESOLUCION DE INCAUTACION). El juez de la instrucción, si existen indicios suficientes acerca de la condición de bienes sujetos a decomiso o confiscación, mediante resolución fundamentada, dispondrá:

1) Su incautación e inventario en el que conste su naturaleza y estado de conservación;
2) La anotación preventiva de la resolución de incautación tratándose de bienes sujetos a registro; y,
3) Su entrega a la Dirección de Registro, Control y Administración de Bienes Incautados a efecto de su administración conforme a lo establecido en este Capítulo.

No serán objeto de incautación los bienes muebles que fueran de uso indispensable en la casa habitación del imputado ni los objetos de uso personal del imputado y su familia.

La anotación de la incautación de los registros públicos estará exenta del pago de valores judiciales y administrativos.

2.5.3. ALLANAMIENTO.

ARTICULO 180. (ALLANAMIENTO DE DOMICILIO). Cuando el registro deba realizarse en un domicilio se requerirá resolución fundad del juez y la participación obligatoria del fiscal.

Queda prohibido el allanamiento de domicilio o residencia particular en horas de la noche, este únicamente podrá efectuarse durante las horas hábiles del día, salvo el caso de delito

flagrante. Se entiende por horas de la noche el tiempo comprendido entre las diecinueve horas y las siete del día siguiente. (ORTEGA Alejandro, 2010).

ARTICULO 182. (MANDAMIENTO Y CONTENIDO). El mandamiento de allanamiento contendrá los siguientes requisitos:

1) El nombre y cargo del juez o tribunal que ordena el allanamiento y una breve identificación del proceso;
2) La indicación precisa del lugar o lugares por ser allanados;
3) La autoridad designada para el allanamiento;
4) El motivo especifico del allanamiento, su respectiva fundamentación, las diligencias por practicar y, en lo posible, la individualización de las personas u objetos buscados; y,
5) La fecha y la firma del juez.

El mandamiento tendrá una vigencia máxima de noventa y seis horas, después de las cuales caduca. El fiscal que concurra al allanamiento tendrá a su cargo la dirección de la diligencia. (ORTEGA Alejandro, 2010)

Todo este proceso está definido y viene acompañada con orden judicial.

ARTICULO 183. (PROCEDIMIENTO Y FORMALIDADES). La resolución que disponga el allanamiento será puesta en conocimiento del que habite o se encuentre en posesión o custodia del lugar, que sea mayor de catorce años de edad, para que presencie el registro entregándole una copia del mandamiento. En ausencia de estas personas se fijara copia del mandamiento en la puerta del inmueble allanado.

Practicado el registro se consignara en acta su resultado, cuidando que el lugar quede cerrado y resguardado de otras personas, si hay razones fundadas para ello. El acta será firmada por todos los intervinientes en el acto y el que presencio el registro, si este no lo hace se consignara la causa. (ORTEGA Alejandro, 2010).

Respetando la legislación boliviana y siguiendo los procedimientos para realizar la recolección de evidencia, se usarán estos artículos para la recolección y preservación de la evidencia digital cuando haya casos de delitos informáticos, en los procedimientos que se detallan en las fases de la técnica planteada.

Es importante conocer estos artículos y debe hacer caso al pie de la letra, debido a que las evidencias digitales que serán recolectadas, mas adelante podrían servir de pruebas en juicios y la forma como fueron recolectadas también podrían validar o invalidar la prueba. Es así que la técnica informática forense a plantear se apoyará en estos artículos.

2.6. METODOLOGÍA Y TÉCNICA.

"El método es un proceso de pasos a seguir para alcanzar una meta, y la técnica es el conjunto de procedimientos de los recursos de que se vale la ciencia para llegar a su fin, la técnica se puede repetir según el investigador lo considere para que su trabajo tenga validez" (CUSTODIO Angela, 2008).

En este sentido el presente trabajo desarrolla una técnica debido a que para cada fase se implementará una serie de procedimientos, debido a que ya se cuenta con el camino que es la metodología que se usa en el presente documento y la técnica mostrara como se debe recorrer el camino.

2.7.HERRAMIENTAS INFORMATICAS.

2.7.1. SOFTWARE.

Las herramientas informáticas, son la base primordial de cualquier análisis de evidencias digitales en los medios informáticos. Por lo que la definición de herramientas informático forense se describe como "que éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento del investigador que las utiliza. Estos dos elementos hacen del uso de las herramientas, una constante reflexión y cuestionamiento por parte de la comunidad científica y práctica de la informática forense en el mundo". (CANNO Jeymi, 2008).

Las herramientas más completas y frecuentemente utilizadas en procedimientos forenses en informática son las siguientes, que son aplicaciones que tratan de cubrir todo el proceso en la investigación forense en informática: ENCASE, FORENSIC TOOLKIT, WINHEX.

Si bien las herramientas detalladas anteriormente son licenciadas y sus precios oscilan entre los 600 y los 5000 dólares americanos, existen otras que no cuentan con tanto reconocimiento internacional en procesos legales, que generalmente son aplicaciones en software de código abierto (Sleuth Kit, Coroner Toolkit). (CANNO Jeymi, 2008). A continuación se muestra un cuadro comparativo de algunas características de estas herramientas:

	LICENCIA	IMAGEN	CONTROL INTEGRIDAD	ANÁLISIS	ADMON CASO
ENCASE	si	si	si	si	si
FORENSIC TOOLKIT	si	si	si	si	si
WINHEX (Forensic edition)	si	si	si	si	si

Cuadro Nro.2.1 Comparación de herramientas forenses.
Fuente: Jeymi Canno 2008.

Las herramientas arriba mencionadas solo son unas cuantas de la gran cantidad que existen, muchas veces se las usa sin saber que forman parte de la informática forense, es así que durante el análisis forense se puede usar una o varias de estas herramientas, de acuerdo al caso.

A continuación se detalla software agrupado por el tipo de trabajo que realizan (GOMEZ, 2012):

- **Para preservación y autenticación de evidencia digital.**
  FTK Imager Crea una imagen del Disco duro o de la Memoria RAM
  Forensic Acquisition Utilities (FAU) Utilitarios para preservar imágenes

- **Para técnica de carving(extracción de archivos de datos del sistema de Archivos.)**
  Winhex , *PhotoRec, Scalpel y Simple Carver* Suite

- **Para análisis de datos. Se realiza un análisis minucioso.**
  ProDiscover Basic, *The Sleuthkit and Autopsy, PTK, WinHex*, *PyFlag* y *SANS SIFT Workstation*.

- **Para análisis detallado de memoria.**
  mdd, *Volatility* y *Memoryze*.

- **Para virtualización**
  LiveView (ejecuta una imagen forense in VMWare),
  ProDiscover Basic (crea archivos de configuración para VMWare),
  VDKWin (edita archivos de configuración de VMWare),

- **Live CDs para inspección de evidencia digital**
  Helix, Caine, PlainSight, BackTrack (permite montar dispositivos y tiene herramientas forenses)

- **Para recolección de evidencia digital volátil**
  Evidence Collector.

Este Software arriba mencionado es posible encontrarlo en internet, muchos de ellos son completos, sin embargo es posible usar de acuerdo al caso el software elegido, incluso para realizar un análisis completo entre sise complementan.

2.7.2. HARDWARE.

Dentro de las herramientas informáticas forenses es necesario contar con el equipamiento necesario, usado para la investigación y muchas veces debe ser portable, también para proteger la integridad de los dispositivos a analizar, de forma que sigan siendo válidos como prueba judicial. Existen en el mercado equipos con la más avanzada tecnología en el campo del Análisis Informático Forense, copiadoras duplicadoras, creadoras de imágenes ultrarrápidas; equipos para investigación "en caliente" no intrusivos, que no dejan huella así como equipos para borrado seguro. Así como son de alta tecnología, su precio también es elevado y poco accesible. Sin embargo a continuación se muestran los equipos con algunas de sus características:

- **HARDCOPY 3.** Realiza copias de discos duros a una velocidad de hasta 7.5 Gb por minuto en la transferencia de datos, puede realizar dos copias a la vez de un mismo disco duro, además de verificar SHA256.También tiene modos de Duplicación (Clonación y creación de imágenes), diferentes métodos de Borrado, duplicación de otros Discos Duros (ATA, portátiles, etc.)

- **SHADOW 2. A**cceden al soporte magnético sin alterar su contenido, permite arrancar, en caliente, al investigador forense el sistema a analizar sin alterar su

contenido, también permite instalar herramientas propietarias en caliente sin alteración de contenidos y actualizar el Firmware del Shadow 2 con futuras actualizaciones y mejoras.

- **DRIVEWIPER.** Alta calidad de borrado a gran velocidad (5,5 GB por minuto), facilidad de uso y fácilmente ampliable, borrado de dos discos duros simultáneamente a 8 GB por minuto en conjunto, es posible que trabaje con ATA o SATA, desbloquea y borra automáticamente áreas protegidas y para manejar el equipo tiene pantalla LCD y solo tres botones.

- **DUPLICADORES FORENSES**. Touch Screen Forensic Imager Model TD3, Forensic 1:2 Duplicator Model TD2, Model TD1.

  Estas herramientas ofrecen imágenes de disco duro sin dejar huella. Además de ser rápidos, confiables y fáciles de usar, además traen consigo características útiles para el usuario avanzado.

Estas son unas cuantas herramientas que se pueden utilizar, como también existen más y van fabricándose con el avance de la tecnología, además que el costo de los mismos es elevado, sin embargo es posible contar con un Kit de herramientas sencillas que sean portables, vale decir desarmadores, cintas antiestáticas, material aislante, marcadores, polvo para detección de huellas, guantes, etc.

CAPITULO III
MARCO REFERENCIAL

3.3.SITUACIÓN ACTUAL DE LA INFORMÁTICA FORENSE.

Los delitos informáticos por lo general no se detectan, o se detectan demasiado tarde o simplemente no se quieren investigar por distintos factores.

La mayoría de investigaciones están relacionadas con:

- Pornografía infantil.
- Derechos de autor.
- Envío de información no permitida mediante el uso de la red de computadores, mediante correo electrónico.
- Acciones dañinas realizadas por empleados, ex empleados o personas externas a la institución.
- Robos por internet, etc.

Solo en aquellos casos en que vale la pena la inversión se realiza una investigación forense, porque la investigación puede no llevar a nada concluyente, las conclusiones no llevan a la captura del delincuente o sencillamente este ya no se encuentra al alcance, o peor aún, las pruebas no son suficientes para aprender al criminal o simplemente se lo procesa penalmente con un delito tipificado que se acerca al crimen cometido, por ejemplo si se malogra intencionalmente una computadora, atacando a la CPU con un café, al culpable solo se hace pagar por el costo del equipo y no paga ni un peso por el costo de la información que en muchos casos es más costosa que el equipo.

3.2. REGULACIONES EXISTENTES EN LATINOAMÉRICA.

En Latinoamérica algunos países como Chile, Argentina, Venezuela, Perú, cuentan con regulación, a nivel legislativo que tipifica los delitos informáticos, en otros países se ha procedido a la reforma o interpretación de los Códigos de Procedimiento Penal para la aplicación de las sanciones, ante las infracciones informáticas cometidas. Además de las reformas concernientes al Código de Procedimiento Penal se mantienen leyes como: Ley de Propiedad Intelectual, Ley de Comercio Electrónico, Ley de Habeas Data, Ley de Firmas Digitales, entre otras, que sancionan los delitos relacionados con la informática, en el siguiente cuadro se verá un resumen de las leyes que existen o están en proyecto de ley, o aprobado pero sin reglamento aún, como es el caso de Bolivia con la Ley de Telecomunicaciones y TICs.

Legislación de Países Latinoamericanos	**Ley de Propiedad intelectual**	**Ley del Habeas Data**	**Ley de Comercio Electrónico, Mensaje de Datos**	**Ley de Delitos informáticos**	**Ley de transparencia y acceso a la información**	**Ley de pornografía infantil**	**Ley de Uso de correo electrónico SPA**	**Ley de Telecomunicaciones y TICS**
Argentina	X	X	X	X				
Bolivia								X
Brasil		X	X					
Chile	X		X	X		X		
Colombia			X	X	X			
Costa Rica				X				
Ecuador	X	X	X		X			
Guatemala			X		X			
México				PROY.	X			
Panamá			X					
Paraguay					X			
Perú			X	X	X		X	
Repúb. Dominicana			X					
Uruguay							PROY.	
Venezuela			X	X				

Cuadro Nro.3.2. Resumen de las Leyes de Delitos Informáticos en Latinoamérica

Fuente: Actualización de Estadísticas de la OEA.

a. Delitos informáticos: Aplicación Chile

Chile es un país adelantado en Latinoamérica con relación a la tecnología, fue el primer país sancionar la ley contra delitos informáticos en donde se legislan aspectos concernientes a la información y a la informática. A continuación la tabla 2.2 lista las leyes, decretos y normas que han incorporado al contexto legal.

AÑO	LEY / DECRETO/ACUERDO	ORDENANZA
1970	Ley 17336 (Inicial)	Ley de Propiedad Intelectual (incluye programas de computadora, a través de la Ley 18957 - 1990)
1993	Ley 19223	Ley de Delitos Informáticos. Figuras penales relativas a la informática
1999	Decreto 81/99	Uso de la Firma Digital y Documentos Electrónicos en la Administración del Estado
1999 2002	Ley 19628 Ley 19812	Protección de la vida privada. Protección de datos de carácter personal.
2002	Ley 19799	Ley de Firma Electrónica. Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firma Digital
2003	NCH 2777	Código de práctica para la Gestión de la Seguridad de la Información
2004	Ley 19927	Pornografía Infantil

Legislación en Chile – Informática e Información.

Cuadro Nro.3.2. Fuente. URETA Laura, 2008

La Ley 19223 (Ley de Delitos Informáticos - Chile), esta ley habla sanciona claramente sobre los delitos informáticos en los que se incluyen los siguientes tipos de actos ilícitos de acuerdo a lo que establecen sus articulados:

- Sabotaje.
- Espionaje informático.
- Destrucción maliciosa de la información.
- Divulgación de información no autorizada.

Además este país cuenta con la Brigada Investigadora del CiberCrimen, que pertenece como Unidad departamental a la Policía de Investigaciones, dedicada específicamente a la investigación de los delitos informáticos.

b. Delitos informáticos: Aplicación Argentina

Argentina es uno de los países que a nivel de legislación ha desarrollado el tema sobre los delitos informáticos y aprobado la Ley 26388 en la que se penalizan los delitos electrónicos

y tecnológicos, pese a que este país fue uno de los primeros en plantear la ley cerca al 2000, recién el 2008 fue aprobada. La tabla 2.3 muestra las leyes y decretos que mantiene Argentina y que contemplan especificaciones de informática e información:

AÑO	LEY / DECRETO/ ACUERDO	ORDENANZA
1933	Ley 11723	Régimen Legal de Propiedad Intelectual.
1996	Ley 24766	Ley de Confidencialidad.
1998	Ley 25036	Ley de Propiedad Intelectual (Modificación de la Ley 11723)
2000	Ley 25326	Habeas Data (Modificada en el 2008)
2001	Ley 25506	Firma Digital
2002	Decreto 2628/	Reglamentación de Firma Digital
2004	Ley 25891	Servicio y Comunicaciones Móviles
2005	Ley 26032	Difusión de Información
2008	Ley 26388	Delitos Informáticos.

Legislación en Argentina – Informática e información.

Cuadro Nro.3.3. Fuente. URETA Laura, 2008

La Ley 26388 (Ley de delitos informáticos - Argentina), dio paso a que se incorpore importantes cambios en el Código Penal Argentino sobre el uso de las tecnologías de la información, en la cual se sanciona:

- Pornografía infantil.
- Destrucción maliciosa y accesos no autorizados a la información y sistemas de información.
- Intercepción e interrupción de las comunicaciones electrónicas y de telecomunicaciones.
- Divulgación de información no autorizada.

A partir de la promulgación de la Ley 26388 la justicia argentina, conformó un equipo de peritos expertos en delitos informáticos, mismos que asisten a las cámaras y juzgados del país, en los casos en los que se encuentran computadoras u otro tipo de dispositivos informáticos, sin embargo, también existen otro tipo de peritos, entre los que se encuentran los peritos oficiales, de oficio y de parte, que pasan por un proceso de acreditación

establecido de acuerdo a la jurisdicción por ser un país federal y poseer poderes judiciales descentralizados por provincias.

Es preciso destacar que a pesar de que Argentina, implantó la Ley de Delitos Informáticos recientemente, se han dado una serie de casos que han sido sancionados de acuerdo a las disposiciones del Código Penal, bajo el ámbito de haber cometido infracciones en otro tipos de delitos como la propiedad intelectual y la pornografía infantil.

c. Delitos informáticos: Aplicación Colombia

Colombia ha implementado iniciativas que le permiten controlar los delitos relacionados con las tecnologías en el campo jurídico, Colombia mantiene las siguientes leyes decretos y acuerdos, relacionados con la informática y la información, resumidas en la tabla Nro. 2.4:

AÑO	LEY / DECRETO/ ACUERDO	ORDENANZA
1985	Ley 57	Transparencia y Acceso a la Información Gubernamental
1999	Ley 527	Información en forma de mensaje de datos
2000	Decreto 1747	Entidades de Certificación, los Certificados y las Firmas Digitales
2000	Resolución 26930	Estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.
2001	Ley 679	Explotación, la Pornografía y el Turismo Sexual con Menores de Edad
2003	Decreto 2170	Certificación y Firmas Digitales
2004	Proyecto de Ley 154	Reglamento del Derecho a la Información
2006	Acuerdo PSAA06-3334	Reglamentación de medios electrónicos e informáticos en la justicia.
2009	Ley 1273	Ley de la protección de la información y de los datos

Legislación en Colombia – Informática e información.

Cuadro Nro.3.4. Fuente. URETA Laura, 2008

Colombia ha tenido un desarrollo particular con respecto a la investigación de delitos de índole informático, factores como el narcotráfico, lavado de dinero, falsificación y terrorismo, ha incentivado que este país implemente unidades de investigación que les colabore en los procesos de indagación de actos ilícitos en los que se utilizan medios tecnológicos o que afectan sistemas de tecnología o de información.

La Ley1273 (Ley de delitos informáticos - Colombia), es denominada "protección de la información y de los datos", en la sociedad colombiana, en la que se penalizan y sancionan los siguientes actos:

- Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicaciones.
- Interceptación de datos informáticos
- Daño informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.

En la Ley muestra que las sanciones establecidas se orientan específicamente a preservar aspectos que se delinean con la seguridad de la información, donde se trata de salvaguardar la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos.

Colombia ha sido uno de los países que ha recibido la ayuda de los Estado Unidos para la persecución de actos criminales y la rama de investigación de naturaleza informática se originó a partir del año 1984 cuando los laboratorios del FBI y otras agencias que pertenecen a los Estados Unidos promovieron el desarrollo de programas para examinar evidencias computacionales.

Colombia mantiene el Grupo Investigativo de Delitos Informáticos (GRIDI) como parte de la Dirección de Investigación Criminal de Colombia, que investiga las conductas delictivas que se derivan del uso de la tecnología y las telecomunicaciones, éste organismo se sustenta con el apoyo de equipos de informática forense y personal profesional capacitado que atienden incidentes informáticos presentes durante una investigación judicial.

Los grupos de investigación de delitos informáticos se encuentran equipados con laboratorios de Cómputo Forense, en las ciudades de Bogotá, Medellín, Bucaramanga, Cali y Barranquilla, otros más que son laboratorios particulares, los cuales permiten el análisis de la evidencia digital.

3.3. PROCESO FORENSE

Una investigación forense tiene valor si cumple algunas normas y leyes, ya sea a nivel legal o corporativo. Por lo cual la ciencia forense provee metodologías básicas que contemplan el correcto manejo de la investigación y de la información.

A continuación se enuncian siete guías existentes a nivel mundial de mejores prácticas en computación forense.

3.3.1. RFC3227

El "RFC 3227: Guía Para Recolectar y Archivar Evidencia" (Guidelines for Evidence Collection and Archiving), escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Muestra las mejores

prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos relacionados a la parte legal. Su estructura es:

a. Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.
b. El proceso de recolección: transparencia y pasos de recolección.
c. El proceso de archivo: la cadena de custodia y donde y como archivar.

3.3.2. Guía de la IOCE

La IOCE, publicó "Guía para las mejores prácticas en el examen forense de tecnología digital" (Guidelines for the best practices in the forensic examination of digital technology). El documento provee una serie de estándares, principios de calidad y aproximaciones para la detección prevención, recuperación, exanimación y uso de la evidencia digital para fines forenses. Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte.

Su estructura es:

a. Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de las mismas y espacio de trabajo).
b. Determinación de los requisitos de examen del caso.
c. Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).
d. Prácticas aplicables al examen de la evidencia de digital.
e. Localización y recuperación de la evidencia de digital en la escena: precauciones, búsqueda en la escena, recolección de la evidencia y empaquetado, etiquetando y documentación.
f. Priorización de la evidencia.

g. Examinar la evidencia: protocolos de análisis y expedientes de caso.
h. Evaluación e interpretación de la evidencia
i. Presentación de resultados (informe escrito).
j. Revisión del archivo del caso: Revisión técnica y revisión administrativa.
k. Presentación oral de la evidencia.
l. Procedimientos de seguridad y quejas.

De toda esta estructura se puede rescatar en general 4 fases principales:

1. Recolección de la evidencia sin alterarla o dañarla.
2. Autenticación de la evidencia recolectada para asegurar que es idéntica a la original.
3. Análisis de los datos sin modificarlos.
4. Reporte final.

3.3.3. Investigación en la Escena del Crimen Electrónico (Guía DoJ 1)

El Departamento de Justicia de los Estados Unidos de América (DoJ EEUU), publico "Investigación En La Escena Del Crimen Electrónico" (Electronic Crime Scene Investigation: A Guide for First Responders) [ElCr01]. Esta guía se enfoca más que todo en identificación y recolección de evidencia. Su estructura es:

a. Dispositivos electrónicos (tipos de dispositivos se pueden encontrar y cual puede ser la posible evidencia).
b. Herramientas para investigar y equipo.
c. Asegurar y evaluar la escena.
d. Documentar la escena.
e. Recolección de evidencia.
f. Empaque, transporte y almacenamiento de la evidencia.
g. Examen forense y clasificación de delitos.
h. Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento).

3.3.4. Examen Forense de Evidencia Digital (Guía DoJ 2)

Otra guía del DoJ EEUU, es "Examen Forense de Evidencia Digital" (Forensic Examination of Digital Evidence: A Guide for Law Enforcement) [FoEx04]. Esta guía está pensada para ser usada en el momento de examinar la evidencia digital. Su estructura es:

a. Desarrollar políticas y procedimientos con el fin de darle un buen trato a la evidencia.
b. Determinar el curso de la evidencia a partir del alcance del caso.
c. Adquirir la evidencia.
d. Examinar la evidencia.
e. Documentación y reportes.
f. Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos de entrenamiento).

3.3.5. Computación Forense - Parte 2: Mejores Prácticas (Guía Hong Kong)

El ISFS, Information Security and Forensic Society (Sociedad de Seguridad Informática y Forense) creada en Hong Kong, publicó "Computación Forense - Parte 2: Mejores Prácticas" (Computer Forensics – Part 2: Best Practices). Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del crimen hasta la presentación de los reportes en la corte. Su estructura es:

a. Introducción a la computación forense.
b. Calidad en la computación forense.
c. Evidencia digital.
d. Recolección de Evidencia.
e. Consideraciones legales (orientado a la legislación de Hong Kong).
f. Anexos.

3.3.6. Guía de buenas prácticas para Evidencia basada en Computadores (Guía Reino Unido)

La ACPO, Association of Chief Police Officers (Asociación de Jefes de Policía), del Reino Unido, mediante su departamento de crimen por computador, publicó "Guía de Buenas Prácticas para Evidencia basada en Computadores" (Good Practice Guide For Computer Based Evidence). La policía creó este documento con el fin de ser usado por sus miembros, como una guía de buenas prácticas para ocuparse de computadores y de otros dispositivos electrónicos que puedan ser evidencia. Su estructura es:

a. Los principios de la evidencia basada en computadores.
b. Oficiales atendiendo a la escena.
c. Oficiales investigadores.
d. Personal para la recuperación de evidencia basada en computadores.
e. Testigos de consulta externos.
f. Anexos (legislación relevante, glosario y formatos)

3.3.7. Guía para el Manejo de Evidencia en IT (Guía Australia)

Estándares de Australia (Standards Australia) publico en agosto de 2003 "Guía Para El Manejo De Evidencia En IT" (HB171:2003 Handbook Guidelines for the management of IT evidence). Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico. Establece puntos de referencia para la preservación y recolección de la evidencia digital.

Detalla el ciclo de administración de evidencia de la siguiente forma:

a. Diseño de la evidencia.

b. Producción de la evidencia.
c. Recolección de la evidencia.
d. Análisis de la evidencia.
e. Reporte y presentación.
f. Determinación de la relevancia de la evidencia.

3.4. SITUACION DE LA INFORMATICA FORENSE EN POTOSI.

Para describir la situación actual de la Informática Forense en Potosí se usó la metodología descriptiva y la metodología empírica, donde se uso las siguientes herramientas:

3.4.1. Observación.

Las dos oficinas con las que cuenta el laboratorio de la Policía Nacional del departamento de Potosí, cumplen de sala de recepción, laboratorio y la misma oficina es usada también de depósito de equipos que están en custodia.

3.4.2. Entrevista y Cuestionario.

Se realizaron cuestionarios, al personal de la Policía en la unidad de Laboratorio de criminalística, respuestas que confirman la falta de una técnica informática forense, laboratorio equipado y de personal capacitado en informática forense.

3.4.3. Fuentes de información

i. Primarias

Las fuentes de información primarias que se determinan para la realización de este proyecto son: Fiscalía General de la República, Policía Nacional, ya que estas instituciones son las que están directamente involucradas en:

- Recolección de evidencia cuando se ha cometido un delito.

- Esclarecimiento de cómo fueron los hechos y Resolución de juicios en casos de delitos informáticos.

i. Secundarias

Las fuentes de información que se establecieron como secundarias es la información que se obtuvo de documentos consultados por internet, libros, revistas, periódicos pero sobre todo la información brindada por personas que vieron los casos de cerca.

3.4.4. Población y Muestra.

Debido a que las Instituciones que trabajan en forma conjunta Fiscalía del Distrito de Potosí y la Policía Nacional del Departamento de Potosí cuando se trata de investigaciones relacionados con la informática forense, intervienen en el mismo un gran porcentaje del personal de ambas instituciones, en el caso de la Fiscalía todo el personal está involucrado, siendo un total de 20, sin embargo en la Policía no interviene todo el personal sino más bien un área, internamente los mismos rotan, por lo tanto suman 45 personeros que se relacionan con de alguna manera con el departamento de investigaciones.

3.4.4.1. Población.

El grupo o colectivo de personas en que se concentra nuestro interés de conocimientos, se llama Universo o Población estadística. El universo o población es definido por el interés de conocimiento del investigador. (BIJARRO, 2007).

3.4.4.2. Muestra.

Por muestra se entiende a una parte seleccionada o fracción de la población que se estudia. (BIJARRO, 2007).

Para determinar el tamaño de la muestra se utilizo la formula estadística denominada **"Tamaño de la muestra para poblaciones finitas ".** El tamaño de la muestra depende de la variabilidad de las unidades de población con respecto a las características que se está investigando, el tamaño de la muestra está en función de la confiabilidad que se quiera y del error de muestreo que se espere.

La muestra es obtenida a través de una estimación de la Proporción siguiendo la siguiente fórmula del tamaño de la muestra en la estimación de la proporción:

$$n_o = \frac{Z_o^2 \quad (I)}{4 * e^2}$$

Donde:

n_o = Muestra Inicial

Zo= Punto Critico

e= Margen de Error

Se aplica el factor de corrección para población finita para obtener el tamaño final de la muestra.

$$n = \frac{n_o * N \quad (II)}{n_o + (N-1)}$$

Desarrollo:

Zo = 1, 645

1-α =90% Nivel de confianza

e= 10%

N= 45 Personas

Aplicando a la Formula se tiene:

1) Obtener el valor de **n_o**

$$n_o = \frac{(1{,}645 * 1{,}645)}{4 * (0.10 * 0.10)} = 67.6 \rightarrow \mathbf{68}$$

2) Reemplazar el valor de n en (I)

$$n = \frac{(68 * 45)}{68 + 44} = \mathbf{27}$$

Por lo tanto el tamaño de la muestra es de 27 personas.

CAPITULO IV

APLICABILIDAD DE LA INFORMÁTICA FORENSE

4.1. IMPLEMENTACIÓN DE LABORATORIO.

Para la implementación se debe considerar varios aspectos, seguridad, infraestructura, equipos de computación y otros, que son los siguientes:

- Infraestructura:
  - Un ambiente de recepción.
  - Un ambiente de depósito.
  - Un ambiente para el análisis de la evidencia
- Seguridad.
  - Circuito cerrado CCTV.
  - Personal de seguridad.
  - Alarmas, sensores de movimiento, timbres de pánico y otros.
  - Extinguidor.
  - Rejas en puertas y ventanas.
  - Ingreso solo de personal autorizado
- Equipos.
  - Dos equipos de computación de escritorio.
  - Un equipo portátil.

- Dos discos duros.
- Una impresora
- Un Scanner.
- Una cámara fotográfica
- Material antiestático.
- Precintos de seguridad
- Guantes antiestáticos.
- Lector de CD.
- Herramientas informática forense

- Software con Herramientas Informático forense.
  - CD/DVDs con un kit completo de Software de herramientas para crear imágenes de discos duros, flash y de memorias RAM

Existen recomendaciones de cómo tratar con la evidencia digital, sin embargo se debe considerar que gran parte del éxito en el análisis está en la preservación de la evidencia, para ello se debe contar con un laboratorio especializado que cumpla con los requerimientos de seguridad adecuados, así mismo en la figura 2.1 se observa un flujo de trabajo que servirá de guía, entre el personal que trabaje en ésta área.

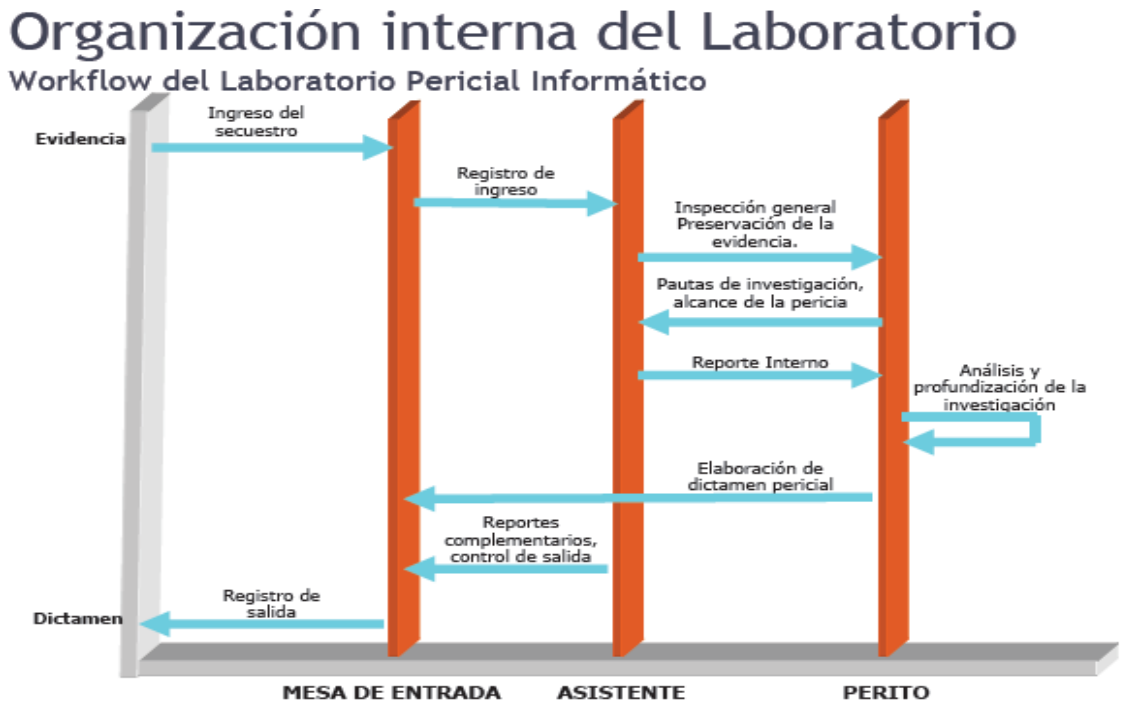


Figura.4.1. Organización del Laboratorio. **Fuente:** Herrera-Gomez 2009

4.2. METODOLOGÍA INFORMÁTICO FORENSE.

Para realizar un análisis forense se requiere de una metodología científica probada, y del uso de la tecnología informática de acorde con el avance del tiempo, así como de una cuidadosa cautela y de tener buenos conocimientos.

Los componentes principales que debe cumplir una metodología para un análisis forense es:

4.2.1. **Marco Científico:** Investigaciones y experiencias apoyadas estrictamente en el método científico. Más allá de la fluidez argumentativa propia de cada profesional se debe aportar estructura lógicas necesarias para justificar las fundamentaciones de manera estricta e irrebatible.

4.2.2. **Marco Criminalístico**: Aplicar el concepto de iter criminis" el delito no surge a la realidad de la vida, como Minerva, de repente y totalmente completo, sino que

recorre un camino, una vía, el Iter Criminis, que empieza desde que surge la idea criminal en la mente del autor y llega hasta el momento en que se agotan los efectos del delito"[GALVEZ José, 2007].

Además de interrelacionarse con especialistas del área, trabajar en forma mancomunada para obtener una idea de cómo se inició y concluyó el delito, de tal manera que se podrá obtener conclusiones desde el punto de vista del crimen.

4.2.3. **Marco Informático general:** Las ciencia informática comprende conceptos, teorías herramientas de uso general se pueden adaptar a las actividades periciales informáticas. Las etapas de relevamiento de información y desarrollo de un modelo coherente de análisis, se evidencian como instrumentos adecuados para brindar soporte metodológico a la actividad del experto en informática Forense.

4.2.4. **Marco Informático específico:** Con las herramientas propias del análisis forense informático, deben ser abordadas desde las características más adecuadas en cada caso que son en muchos casos delitos distintos, un cúmulo de herramientas que se usaron para cometer el delito, que vayan con la realidad de la sociedad en la que vivimos, ya sean ambientes de software libre o software propietario.

4.2.5. **Marco Legal:** Implica la inserción legal siguiendo pasos legales en el accionar pericial al concurrir al lugar del hecho, utilizando las herramientas legales, cumplimientos de plazos legales, la condición de testigo experto, etc., así mismo los artículos de las leyes vigentes en Bolivia.

Al cumplir con los componentes metodológicos nombrados el Informe Pericial será:

- Científicamente fundamentado
- Criminalísticamente interrelacionado
- Modelado mediante la ciencia informática.
- Investigado con las mejores herramientas disponibles.

- Inserto en el marco legal correspondiente.

4.2.6. Metodología Sistémica

La investigación es una serie actividades tendientes a resolver un problema específico y acotado, la metodología sistémica es una de las más apropiadas y actualizadas para enfrentar dicha tarea, esta metodología está basada en los métodos científicos, métodos de inducción-deducción.

Los aspectos que se consideraron dentro de las metodologías de la Informática forense son: Considerar a un grupo multidisciplinario como grupo de trabajo, el cual estará compuesto por personal de la Fiscalía de la Nación, personal asignado de la Policía del Departamento de Potosí, Peritos informáticos forenses, quienes en caso de denuncia irán al lugar del hecho a allanar o incautar los equipos del lugar denunciado, siguiendo la metodología y las técnicas aplicadas al caso.

La metodología Sistémica es la más básica, que contiene las fases: Identificar, Preservar, Analizar y Presentar, que posteriormente se presenta la técnica para cada fase.

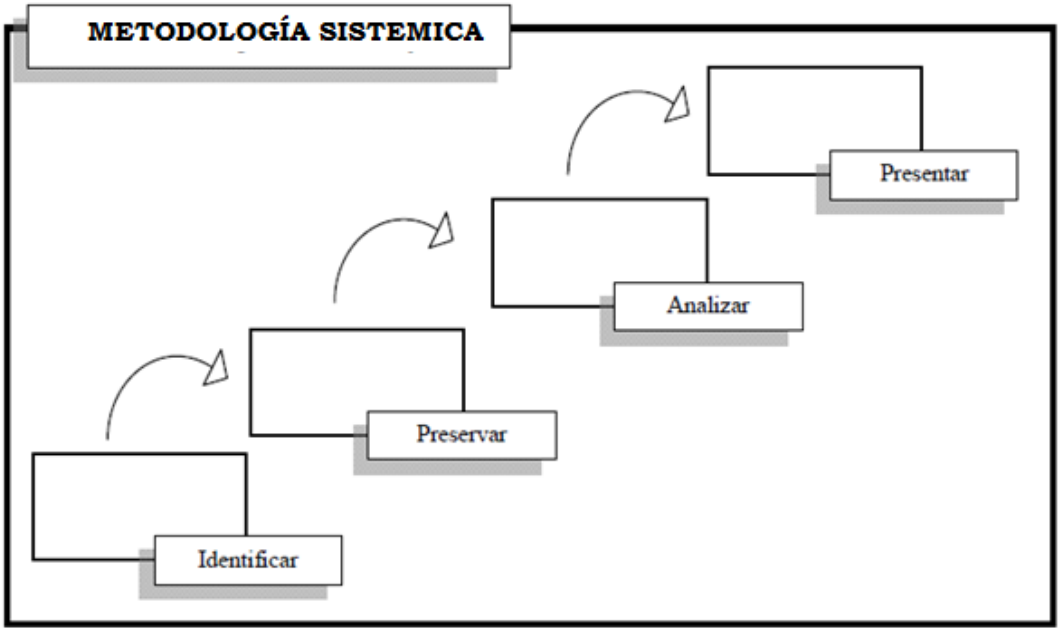


Figura 4.2. Metodología Sistémica

La técnica que se detalla para cada fase está basada en metodología sistémica y orientada específicamente a la Policía Nacional Departamento de Potosí – Fiscalía del Distrito de Potosí según los delitos informáticos y las leyes vigentes en Bolivia. La técnica para cada fase es seguir un orden adecuado para intervenir ante un delito y análisis del mismo en base al tipo de evidencia digital encontrada, además se cuenta con las guías RFC3227 y la guía IOCE, que recomienda como se debe trabajar, es así que a continuación se presenta las técnicas para cada Fase.

4.3.1. FASE IDENTIFICACIÓN.

Esta fase también es conocida como búsqueda y recopilación de evidencias, durante la identificación se debe realizar una inspección somera, para conocer con qué tipo de pruebas se contará, una vez que se ingresa al allanamiento del domicilio y se encuentre las computadoras apagadas o encendidas, esto para conservar la evidencia, utilizando herramientas que no cambien los sellos de tiempo de acceso (timestamp), o provoquen modificaciones en los archivos y que no borren nada, considerar que existen varios

sistemas operativos, preparado en un maletín de herramientas de hardware, así también se usaran formularios que se deben llenar para que la recopilación de información y cadena de custodia sea un éxito, dichos formularios están en anexo B, para lo cual se harán las siguientes tareas:

- Asegurar que ninguna persona tenga acceso a la computadora y a sus alrededores. Si es una empresa y se trabaja en red se debe identificar al personal informático interno y a los usuarios de aplicaciones específicas que deben someterse a peritaje.
- Fotografiar una toma completa del lugar donde se encuentran los equipos, a las conexiones de todos los equipos y luego diagramarlas. En algunos casos si es conveniente se puede realizar una filmación.
- Si está encendida, tomar una fotografía de la pantalla y realizar cuidadosamente una verificación de integridad de los ficheros del sistema y realizar verificaciones sobre del equipo.
- Investigar el área en busca de información relacionada o de contraseñas.
- Verificar que procesos se están ejecutando actualmente en el equipo, buscando uno extraño, especialmente aquellos que consuman recursos en exceso, con ubicaciones poco frecuentes en el sistema de archivos, que mantengan conexiones de red en puertos TCP o UDP no habituales, etc.
- Realizar otra comprobación listando todos los puertos TCP y UDP abiertos además de los procesos (PID), usuarios y aplicaciones que los utilizan
- Rotular todas las conexiones de los equipos para poder restaurar la configuración original.
- Buscar indicios en máquinas próximas si hubiera tales como escaneado de puertos o tráfico inusual en cortafuegos y routers de la red.
- Anotar la fecha y hora de inicio y fin de cada uno de los pasos a seguir.
- Registrar características de los equipos: números de serie, de sus componentes, escáner, cámaras fotográficas, routers, swicht, Sistema Operativo.
- Secuestrar libros, notas, manuales, software, discos, sistemas de almacenamiento y todo lo relacionado al sistema; y realizar un inventario de lo secuestrado.
- Debe estar presente una autoridad competente (Notario, Fiscal, Policía etc.) por

guardar las garantías procesales.

- Tratar de obtener pruebas ocultas con diferentes niveles de volatilidad, como los registros del procesador, estructuras de datos en la memoria RAM o memoria de tipo caché, conexiones de red activas, usuarios y procesos actuales, sistema de archivos, etc. Ya que se perderá si decide apagar el equipo de la forma habitual, ya que en este proceso se realizan una serie de pasos programados para cerrar el sistema de forma limpia. Bien podría tener instalado las herramientas adecuadas éste podría eliminar, modificar y sustituir ficheros durante el apagado, y se "limpiarán" también del equipo las huellas de su atacante.
- También se corre el riesgo de que el intruso siga en línea y actuar con una acción evasiva o, peor aún, destructiva eliminando todo tipo de información. Dependiendo a la forma del ataque o por la importancia de los datos comprometidos se debe apagar el equipo, desconectando la energía eléctrica y se conservará bastante información sobre el ataque.
- Para tocar el material informático se lo debe hacer con guantes descartables ya que el objeto de la investigación puede ser el mouse, teclado, CDs, DVDs, etc. y puede servir para el análisis de huellas dactilares, ADN, etc.
- Poner los discos en sobres de material que no conduzca la estática
- Fotografiar el área después de que el gabinete ha sido removido.
- Interrogar a todos los sospechosos
- Transportar la evidencia, no colocar elementos cerca de fuentes electromagnéticas (radios policiales)

El proceso de **recopilar evidencia** con un equipo encendido, se describe en la guía RFC 3227, se establece el siguiente orden de volatilidad y por tanto de recopilación de evidencias:

- Registros y contenidos de la caché.
- Contenidos de la memoria.
- Estado de las conexiones de red, tablas de rutas.
- Estado de los procesos en ejecución.

— Contenido del sistema de archivos y de los discos duros.
— Contenido de otros dispositivos de almacenamiento.

Dentro de las evidencias volátiles será de interés recuperar los siguientes datos del sistema en tiempo real:

— Fecha y hora.
— Procesos activos.
— Conexiones de red.
— Puertos TCP/UDP abiertos y aplicaciones asociadas “a la escucha”.
— Usuarios conectados remota y localmente.

Realizar una **imagen del disco**, que es una copia bit-a-bit del disco original preservando toda la información, incluyendo los bloques de los ficheros eliminados, espacio libre tras cada bloque, nodos (metadatos), etc.

Cada paso del procedimiento de la Fase de Identificación se debe seguir, ya que el pasar por alto alguno de ellos podría ocasionar alguna pérdida o ensuciar la evidencia, a continuación se muestra un diagrama de flujo que ayudará al Laboratorio de informática forense a trabajar de forma garantizada.

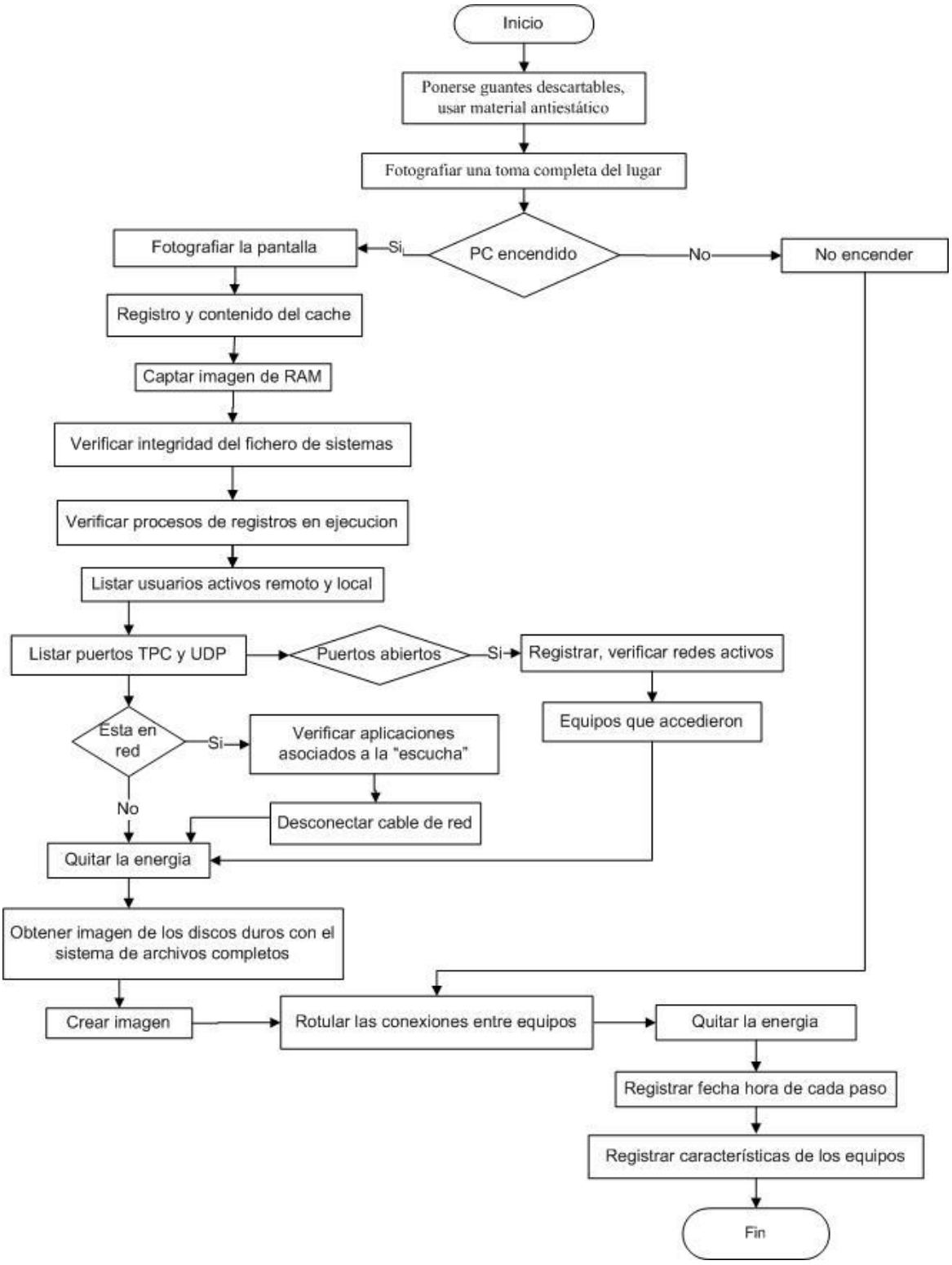


Figura 4.3. Diagrama de Flujo Fase Identificación

4.3.2. FASE PRESERVACIÓN DE LA EVIDENCIA.

En esta fase es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias. Una vez que se cuenta con todas las evidencias del incidente es necesario conservarlas intactas ya que son las "huellas del crimen", se deben asegurar estas evidencias a toda costa. Para ello se sigue el siguiente proceso.

4.3.2.1. Copias de la evidencia

Se debe realizar dos copias de las evidencias obtenidas, generar también una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5 o SHA1. Incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio medio de almacenamiento como CD o DVD etiquetando la fecha y hora de creación de la copia.

Si se extrae los discos duros de la CPU para utilizarlos como evidencia, se debe pegar la etiqueta "EVIDENCIA ORIGINAL", incluir las correspondientes sumas hash, fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó.

Se debe tener en cuenta que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Por lo cual velar a la seguridad de la evidencia.

4.3.2.2. Cadena de custodia.

Se deben establecer las responsabilidades y controles de cada una de las personas que manipulen la evidencia.

Se debe elaborar documentación en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento. Estos documentos deben contener la siguiente información:

- Lugar, fecha y encargado del día que se examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc.
- Personal que custodia la evidencia, durante cuánto tiempo y dónde se almacenó.
- Cuando se cambie la custodia de la evidencia también se deberá documentar cuándo y cómo se produjo la transferencia y quién la transportó.

Todas estas medidas harán que el acceso a la evidencia sea muy restrictivo quedando claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas, intentos de acceso no autorizados o que algún otro dispositivo electromagnético se use dentro de un determinado radio.



Figura 4.4. Diagrama de Flujo Fase Preservación

4.3.3. FASE DE ANÁLISIS.

En esta fase se deben preparar las herramientas, técnicas, autorizaciones de monitoreo y soporte administrativo para iniciar el análisis forense sobre las evidencias obtenidas o presentadas. Una vez que se dispone de las evidencias digitales recopiladas y almacenadas de forma adecuada, en esta fase se debe reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc. En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

4.3.3.1. Preparación para el análisis

En el laboratorio forense se debe realizar lo siguiente:

- Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar.

- Trabajar con las imágenes que se recopiló como evidencias.

- Preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.

- Instalar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias. En esta misma estación de trabajo y sobre un segundo disco duro, instalar las imágenes manteniendo la estructura de particiones y del sistema de archivos En otro equipo instalar un sistema

operativo configurado exactamente igual que el equipo atacado, este segundo equipo servirá para realizar pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

4.3.3.2. Reconstrucción de la secuencia temporal del ataque

Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos:

1. Crear una línea temporal de sucesos, información que servirá de punto de partida para el análisis, para ello se debe recopilar la siguiente información sobre los archivos:

    - Nodos asociados
    - Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
    - Ruta completa.
    - Tamaño en bytes y tipo de archivo.
    - Usuarios y grupos a quien pertenece.
    - Permisos de acceso.
    - Si fue borrado o no.

2. Ordenar los archivos por sus fechas MAC. En busca de archivos y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Buscar los archivos de sistema modificados tras la instalación del sistema operativo, averiguar después la ubicación de los archivos ocultos, de qué

tipo son, identificar también los archivos borrados o fragmentos de éstos, pues pueden ser restos de logs y registros borrados por los atacante, usar la metodología que va de lo general a lo particular, por ejemplo partir de los archivos borrados, intentar recuperar su contenido, anotar su fecha de borrado y compararla con la actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.

3. Comenzar a examinar con más detalle los archivos logs y registros que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una similitud temporal entre eventos. Quizá los archivos log y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que se tendrá que buscar entradas extrañas y compararlas con la actividad de los archivos. Editar también el archivo de contraseñas y buscar la creación de usuarios y cuentas extrañas sobre la hora que se considere como inicio del ataque en el sistema.

4. Examinar los fragmentos del archivo, que es donde se detectan y registran los accesos FTP, esto permitirá descubrir si sobre esa fecha y hora se crearon varios archivos en la máquina comprometida, además se debe tener presente que este directorio puede ser borrado por el atacante y deberá ser recuperado.

4.3.3.3. Determinación de cómo se realizó el ataque

En esta etapa se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha.

La información se deberá obtener de forma metódica, empleando una combinación de consultas a archivos de logs, registros, claves, cuentas de usuarios, etc. El siguiente proceso permitirá conocer que acciones realizó el atacante:

- Revisar los servicios y procesos abiertos que se recopilaron como evidencia volátil, así como los puertos TCP/UDP y conexiones que estaban abiertas cuando el sistema estaba aún funcionando. Examinar con más detalle aquellas circunstancias que resultan sospechosas cuando se buscó indicios sobre el ataque, y realizar una búsqueda de vulnerabilidades a través de Internet.

- Si ya se tiene claro cuál fue la vulnerabilidad que dejó el sistema desprotegido, es necesario ir un paso más allá y buscar en Internet algún exploit anterior a la fecha del incidente, que utilice esa vulnerabilidad.

- Reforzar cada una de las hipótesis empleando una formulación causa-efecto, también es el momento de arrancar y comenzar a utilizar la máquina preparada

4.3.3.4. Identificación del atacante

Consultar las evidencias volátiles que se recopiló en las primeras fases, revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

Si el ataque fue en red se debe intentar averiguar la dirección IP del atacante, para ello revisar con detenimiento los registros de conexiones de red y los procesos y servicios que se encontraban a la escucha. También se podría encontrar esta información en fragmentos

de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de correo electrónico, conexiones fallidas, etc.

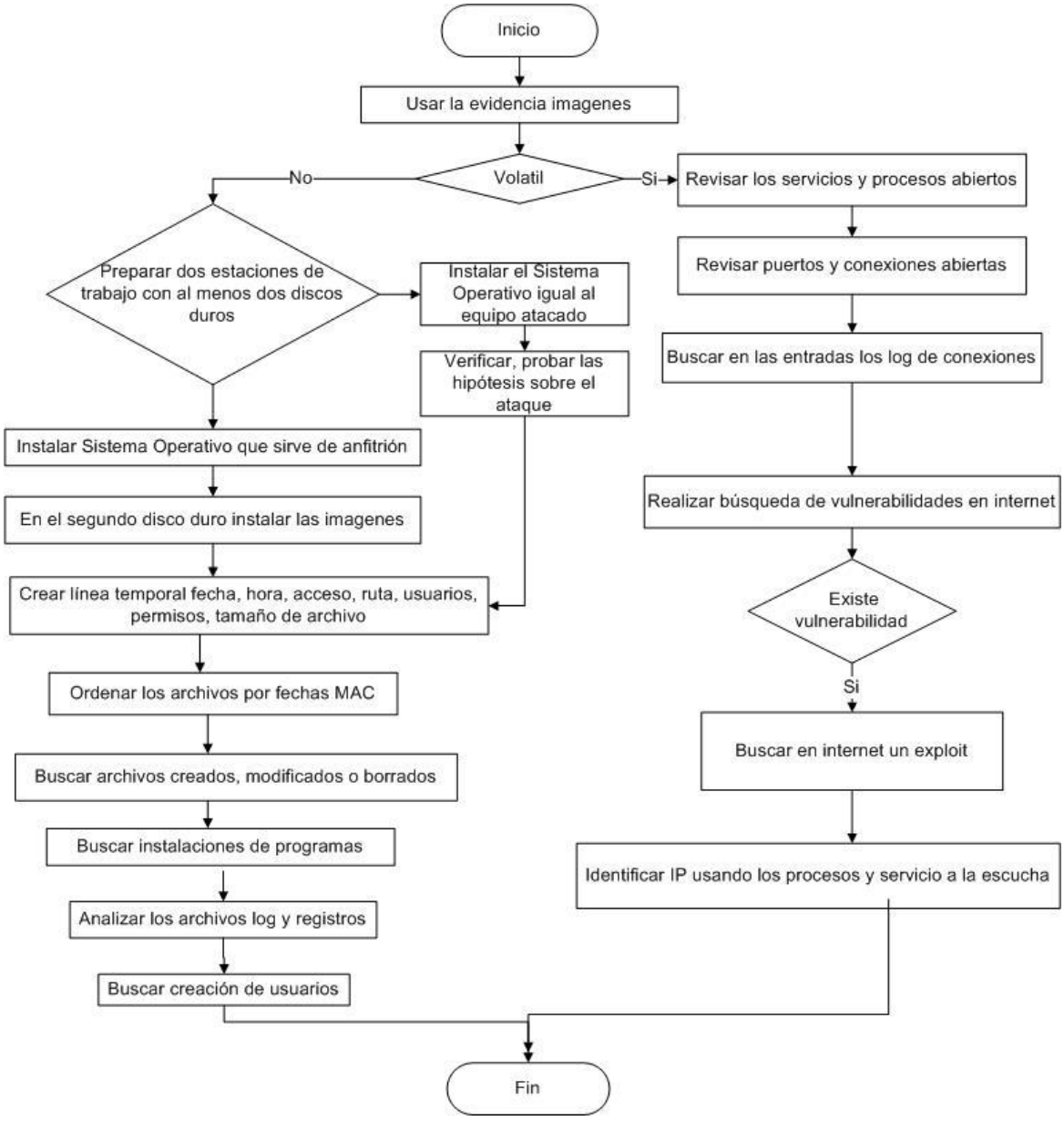


Figura 4.5. Diagrama de Flujo Fase Análisis

4.3.4. FASE DE PRESENTACIÓN DE INFORME.

4.3.4.1. Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema. Esto permitirá evaluar el compromiso de los equipos y realizar una estimación del impacto causado.

Generalmente se pueden dar dos tipos de ataques:

- **Ataques pasivos.-** En los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.

- **Ataques activos**.- En los que se altera y en ocasiones seriamente, tanto la información como la capacidad de operación del sistema.

Se deberá tener en cuenta, además otros aspectos del ataque como los efectos negativos de tipo técnico que ha causado el incidente, tanto inmediatos como potenciales además de lo crítico que eran los sistemas atacados. Por ejemplo ataques a los cortafuegos, el router de conexión a Internet o Intranet, el servidor Web, los servidores de bases de datos, tendrán diferente repercusión según el tipo de servicio que presta la empresa o institución y las relaciones de dependencia entre los usuarios.

4.3.4.2. Documentación del incidente

Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finalice el proceso de análisis forense, esto le hará ser más eficiente y efectivo al tiempo que reducirá las posibilidades de error. Finalmente se presenta la resolución del incidente al menos dos tipos de informes uno Técnico y otro Ejecutivo.

4.3.4.3. Utilización de formularios de registro del incidente

Se deberá emplear formularios estrictamente. Éstos deberán ser rellenados por los departamentos afectados por el compromiso o por el propio equipo que gestionará el incidente. Alguno de los formularios que debería preparar serán:

- Documento de custodia de la evidencia.
- Formulario de identificación del equipo y componentes.
- Formulario de incidencias tipificadas.
- Formulario de publicación del incidente.
- Formulario de recogida de evidencias.
- Formulario de discos duros.

4.3.4.4. El Informe Técnico

Este informe consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. El contenido del informe deberá contener al menos estos puntos:

- Antecedentes del incidente.
- Recolección de datos
- Descripción de dispositivos encontrados e implicancia.
- Entorno del análisis
- Información del sistema analizado.
- Cronología.
- Conclusiones.

4.3.4.5. El Informe Ejecutivo

Este informe consiste en un resumen del análisis efectuado pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido a personal no especializado.

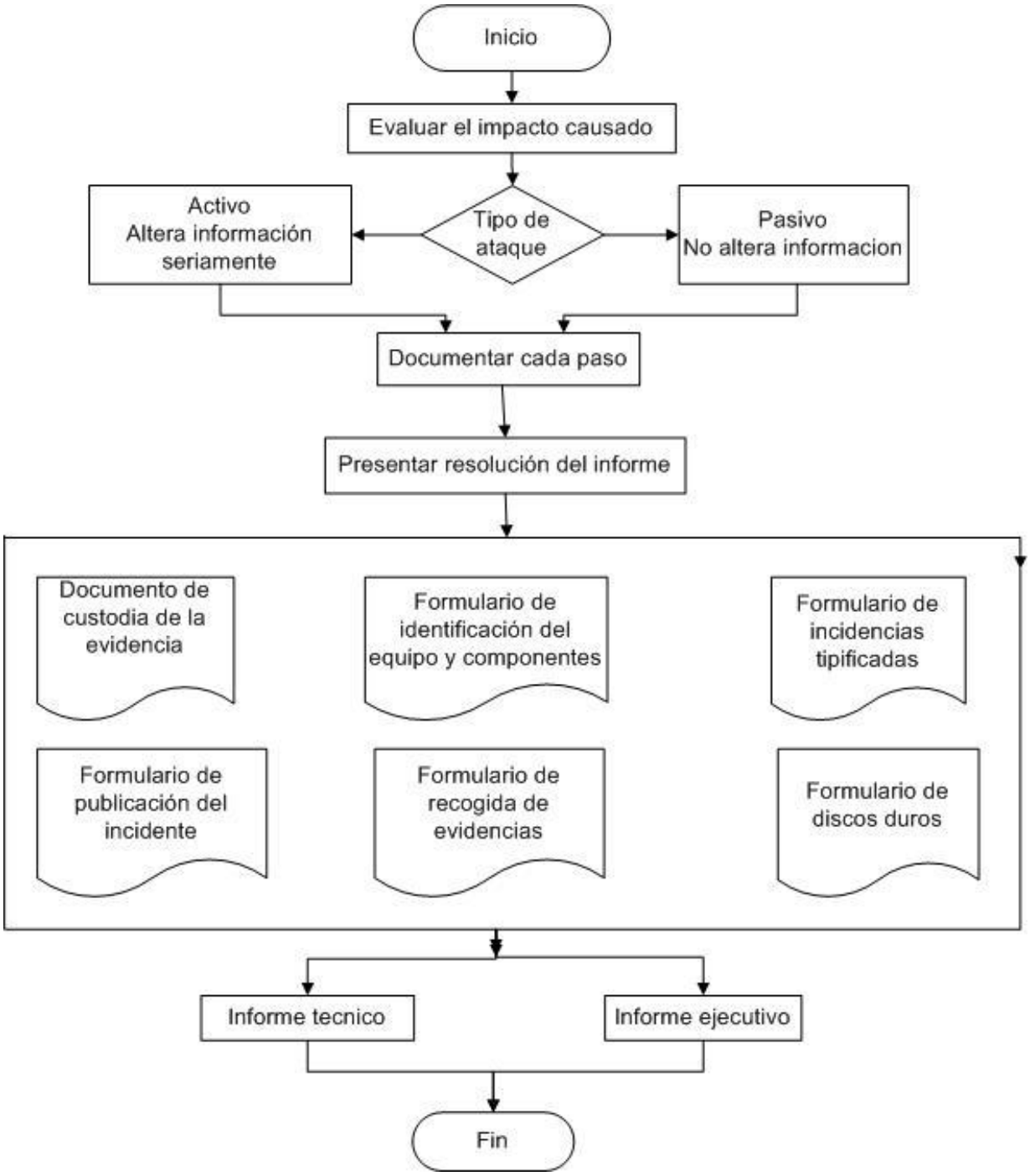


Figura 4.6. Diagrama de Flujo Fase Presentación De Informe

4.4. CASO DE ESTUDIO.

La delicadez de los casos denunciados a la Fiscalía por delitos informáticos no hace posible que se puede aplicar en el laboratorio de la Policía Nacional de Potosí la presente técnica, sin embargo se pudo conseguir un caso de Pornografía Infantil, la imagen del disco duro y de acuerdo a las entrevistas informales que se consiguió, se pudo averiguar más con relación al caso, además por tratarse de este trabajo con fines enteramente académicos no fue posible conseguir mayor documentación, sin embargo se aplicó en la medida de lo posible las fases de la técnica informática forense, y finalmente se presenta el informe que fue analizado conjuntamente la documentación y la técnica informática forense, para su revisión en anexo C esta la descripción de los hechos.

CAPITULO V

INTERPRETACIÓN DE RESULTADOS

5.1. PRESENTACIÓN DE RESULTADOS.

Concluida la etapa de relevamiento de información, siguiendo la metodología empírica, se usó cuestionarios y entrevistas, los resultados arrojados son los siguientes:

1. ¿Conoce o aplica la informática forense en las investigaciones que se realizan**?**

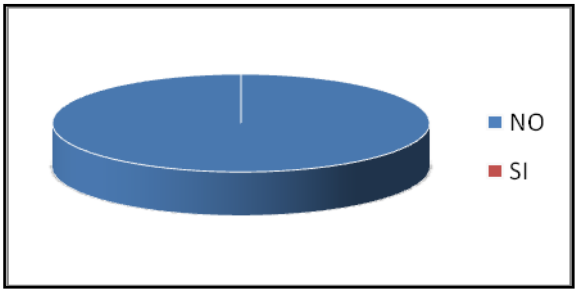


Gráfico 5.1

Fuente. Elaboración propia en base a encuesta.

Todas las personas a las que se aplico el cuestionario y la entrevista respondieron que desconocen de alguna técnica informatica forense, las investigaciones que se realizan son basadas solo en el procedimiento de la Ley Penal.

2. **¿**Cree que la forma de investigar los casos de delitos informáticos por la Policía es incompleta, sin pasos que seguir, sin procedimientos, por lo que la investigación es tratada como un caso común**?**

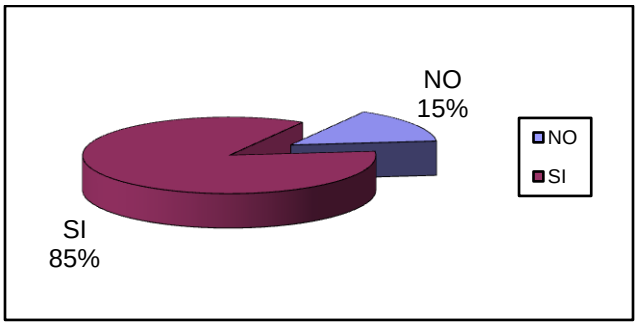


Gráfico 5.2

Fuente. Elaboración propia en base a encuesta.

Cuando se realizan las investigaciones en casos de delitos informáticos cuando existen las denuncias, el personal que trabaja en el área respondió que no siguen ninguna técnica, si son incompletas.

3. ¿Cree que la gente que no denuncia por delitos informáticos, prefiere denunciar usando otras leyes?

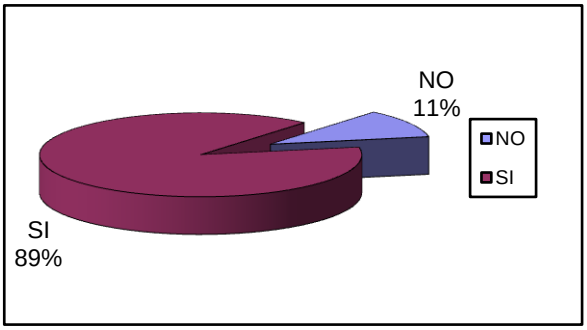


Gráfico 5.3

Fuente. Elaboración propia en base a encuesta.

Un 89% de los encuestados cree que las personas que tienen que ver con problemas de delitos informáticos prefieren usar otras leyes, antes que acudir al delito informático, sin embargo también existen personas que prefieren ir por la vía del delito informático.

Si respondió SI ¿Cuáles son los motivos?

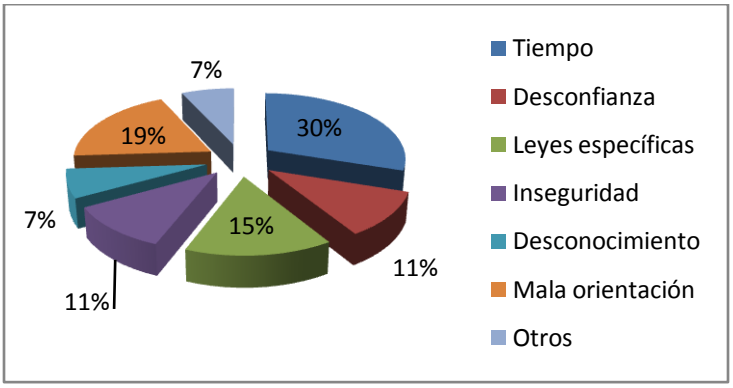


Gráfico 5.4

Fuente. Elaboración propia en base a encuesta.

Los motivos por los que la gente prefiere hacerlo usando otras leyes con un 30% es el factor tiempo, con un 19% se tiene mala orientación que reciben tanto en las Fiscalía como en la Policía, ya que la gente que trabaja allí desconoce sobre la informática forense y prefieren desviar hacia otro tipo de delitos, orientándolos a otras vías. Un 15% de la muestra indica que no se realizan este tipo de denuncias debido a la falta de leyes específicas en Bolivia. Existe un 11% de desconfianza por el trabajo que se realiza y otro 11% por la inseguridad en el manejo de las evidencias, pueden llegar a ensuciarse o contaminarse. Un 7% que los encuestados indicaros que fueron otros los motivos.

4. **¿**Sobre los delitos informáticos, cuáles fueron los más denunciados**?**

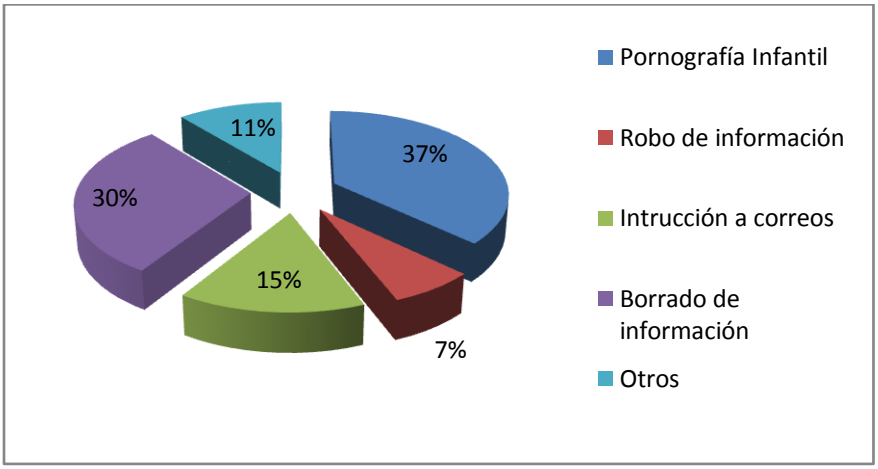


Gráfico 5.5. Fuente. Elaboración propia en base a encuesta.

5. **¿Las investigaciones con casos de denuncias de delitos informáticos los realizan en la ciudad de Potosí**?

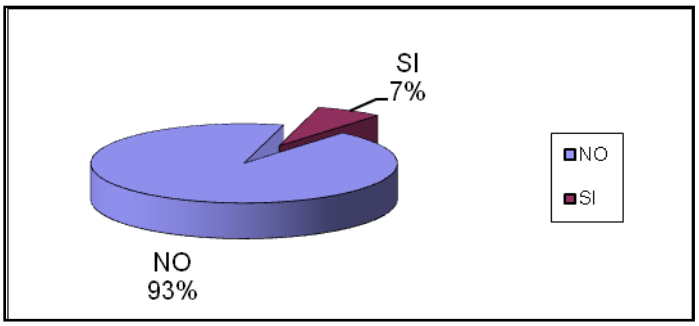


Gráfico 5.6

Fuente. Elaboración propia en base a encuesta.

De acuerdo a los encuestados, los mismos indican que el 7% de las investigaciones son realizadas en la ciudad de Potosí y el 93%ces realizado fuera del departamento.

6. **¿Cree que con la implementación de un laboratorio equipado y una técnica informática forense los tiempos de resolución de casos mejorarían**?

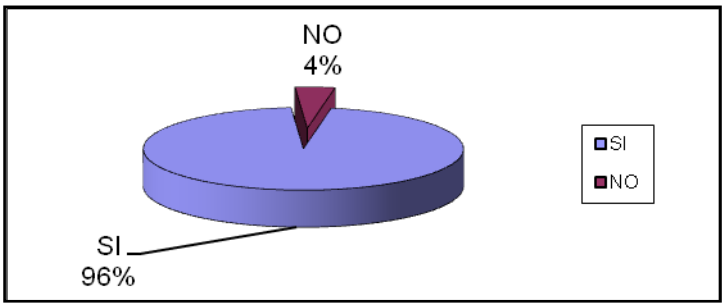


Gráfico 5.7

Fuente. Elaboración propia en base a encuesta.

El 96% de los encuestados están seguros que las investigaciones mejorarían enormemente, ya que contando con el laboratorio y la técnica informática forense.

Con la entrevista realizada al Sargento W. Martinez que está a la cabeza del Laboratorio de investigaciones, se obtuvo bastante información para determinar que existe una necesidad

en dicha área, la ausencia de una técnica informática forense es notable. A partir de los comentarios se pudo deducir que hay necesidad de implementar el laboratorio de investigaciones, el tiempo que se demora para obtener los resultados de la ciudad de La Paz, así como también se debe pagar los costos la persona denunciante.

5.2. VALIDACION DE RESULTADOS.

El personal inmerso en este tipo de investigaciones que pertenece a la Fiscalía conoce el movimiento que existe y la forma de trabajar, sin embargo son los que están a la cabeza de las áreas involucradas, son dos Fiscales a cargo, así también en la Policía en el Departamento de Investigaciones Forenses, el Sargento W. Martinez está al frente de dicho departamento, mismos que son los adecuados para validar el trabajo realizado, es en tal sentido que el cuestionario dirigido a dichas autoridades esta en Anexo D, en el cual se realizan preguntas puntuales con el fin de mejorar el trabajo de investigación, de contar con más herramientas y de esa manera vean que con la implementación de la Técnica Informática Forense mejorarían los tiempos de atención a la resolución de los delitos informáticos denunciados. En tal virtud a continuación se muestra los resultados de los cuestionarios realizados:

- Fase de Identificación.

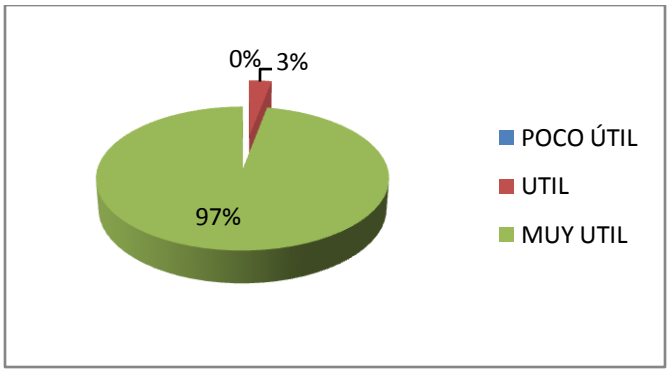


Gráfico 5.8

Fuente. Elaboración propia en base a encuesta.

Donde los encuestados indicaron que la técnica usado para este hecho es útil en un 3%, el mayor porcentaje de los mismos aseguran que es muy útil la técnica usada.

- Fase de Preservación.

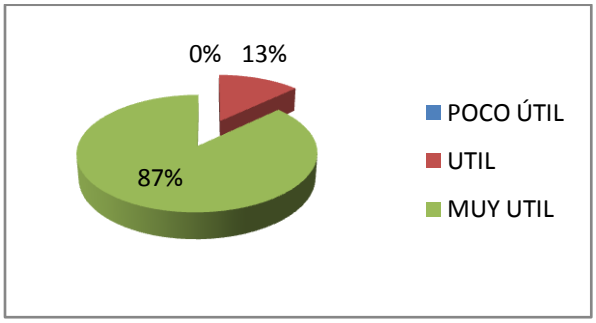


Gráfico 5.9

Fuente. Elaboración propia en base a encuesta.

Ninguna persona de los entrevistados indican que la técnica fuera poco útil, más al contrario vieron que la técnica en su fase de Preservación es muy útil en un 87% y otro 3% asegura que es útil.

- Fase Análisis.

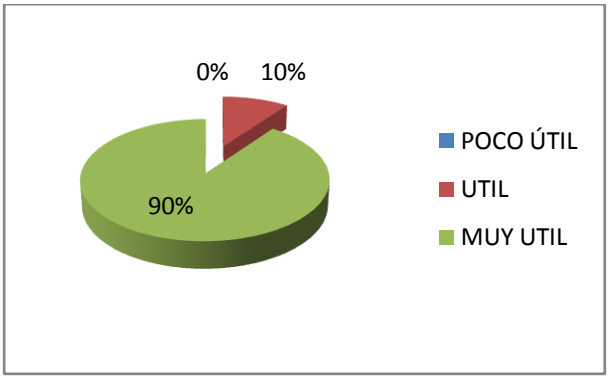


Gráfico 5.10

Fuente. Elaboración propia en base a encuesta.

Al igual que las anteriores fases, un gran porcentaje de los encuestados es de acuerdo con que es muy útil la técnica en esta fase, un 10 en que es útil y ninguno cree que es poco útil.

- Fase Presentación.

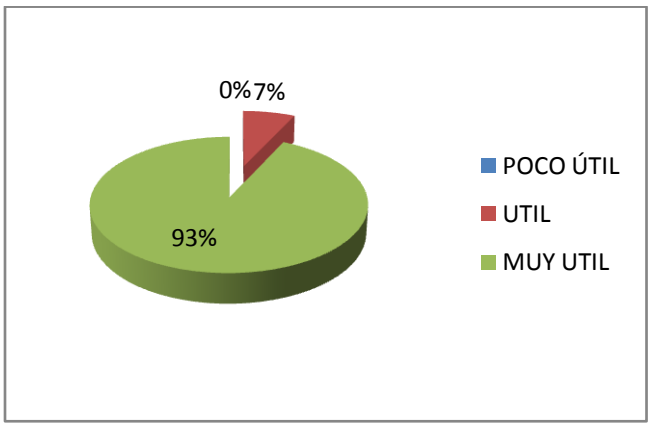


Gráfico 5.11

Fuente. Elaboración propia en base a encuesta.

Un 93 % de los encuestados creen que ésta herramienta es muy útil para su desempeño laboral, un 7% asegura que le será útil en cuanto a la presentación de informes durante las investigaciones de delitos informáticos.

- Implementación del laboratorio de Investigaciones Forenses: Hardware-Software.

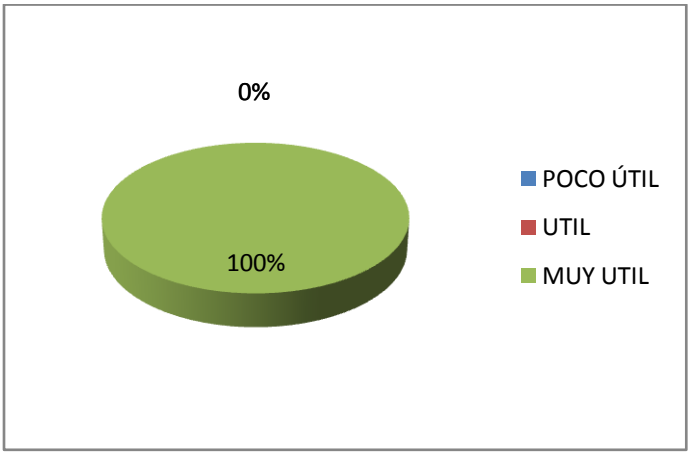


Gráfico 5.12. Fuente. **Elaboración propia en base a encuesta.**

El total del 100% asegura que la implementación del laboratorio de informática forense es muy útil en la investigación de delitos informáticos, ninguno asegura lo contrario.

En tal virtud se puede concluir que la herramienta desarrollada durante esta investigación apoya en la mejora de tiempos de resolución de los casos, al seguir los fases de la técnica se podrá prevenir de errores que se comete cuando se está realizando el trabajo, mismos que en lo futuro ya no será de utilidad, si es aún se continua trabajando de esa manera. Sin embargo cumpliendo con las fases de la Técnica Forense se podrá garantizar el tiempo de resolución de los casos

CONCLUSIONES

En Latinoamérica la informática forense se está haciendo presente poco a poco, las denuncia contar delitos informáticos se hacen presentes en mayor cantidad, en la ciudad de Potosí ya se tiene denuncias, para lo cual se cuenta con una técnica que servirá de guía para futuras denuncias además de una propuesta de un laboratorio apropiado para realizar el seguimiento, es así que con la presente tesis la institución se apoyará enormemente del documento.

Se realizó un análisis de los artículos legales del Código Penal y Procedimiento Penal, que actualmente se usa en el proceso de recolección de evidencia digital.

La técnica informática forense cuenta con cuatro etapas y en cada una se planteó un procedimiento, para la Fase de Recolección, Preservación, Análisis y Presentación de informe, estos mismos procedimientos fueron usados de forma académica en un caso real.

RECOMENDACIONES.

La presente tesis ayudará a prevenir que no ocurran los delitos informáticos, a tener mayor cuidado con la información, a tratar de evitar siniestros y a elaborar políticas de seguridad.

Así también se recomienda que se implemente la técnica mostrada en la presente tesis, así como se debe implementar el laboratorio de informática forense, para que la evidencia digital no se vea como dudosa por ser enviada a otras ciudades, además de generar un costo enorme por el traslado y por el uso del laboratorio.

En la actual ley de telecomunicaciones y TICs Ley 164 se deberá incluir los delitos informáticos y además de las tipificaciones en el Código Penal.

REFERENCIAS BIBLIOGRAFICAS.

1. HERRERA Hernán y GÓMEZ Sebastián, 2009 '' Informática Forense'', Jornadas de Seguridad Informática.
2. NTI, 2008 "The World Leader in computer Forensics". http://www.forensics-intl.com/def3.html
3. Ley nro 1768, 11 de marzo de 1997 Código Penal Legislación Boliviana.
4. CUSTODIO Ruiz Angela, 2008. "Métodos y Técnicas"
5. TELLEZ Julio, 2008. Código Penal Mexicano.
6. ORTEGA Soto Alejandro, 2010. Código de Procedimiento Penal Boliviano.

BIBLIOGRAFIA.

1. ARIAS Chavez Michael, Mayo 2007 ''Panorama general de la Informática Forense y de los delitos informáticos en Costa Rica''. Revista Inter Sedes Costa Rica.
2. BIJARRO Hernandez Francisco, 2007,"Desarrollo Estratégico para la Investigación Científica"
3. CANO Jeimy J., Ph.D, CFE, 2009. "Introducción a la Informática Forense"
4. HERRERA Hernán y GÓMEZ Sebastián, 2009 '' Informática Forense'', Jornadas de Seguridad Informática.
5. Ley Nro 1768, 11 de marzo de 1997 Código Penal. Legislación Boliviana.
6. ORTEGA Soto Alejandro, 2010. Código de Procedimiento Penal Boliviano.
7. SABINO Carlos, 1994. Como hacer una tesis.
8. SILVERHACK, 2007. "Introducción a la informática forense en entornos Windows".
9. TELLEZ Julio, 2008. Código Penal Mexicano.
10. VILLA Juan Ramiro, "Presentación de Perfil de un trabajo de Tesis".
11. GOMEZ Leopoldo Sebastián, 2012, Delitos, prueba y evidencia digital,
12. Access Data, visitado por última vez 22-08-2011 http://www.accessdata.com/products/utk/

13. Computer Forensic Analysis, visitado por última vez 21-10-2012, http://www.porcupine.org/forensics
14. EnCase Forensic, visitado por última vez 20-07-2012 http://www.encase.com/products/ef_index.asp
15. Forensic Acquisition Utilities, visitado por última vez 12-08-2012, http://gmgsystemsinc.com/fau/
16. Mandiant Solutions, visitado por última vez 12-08-2012, http://www.mandiant.com/software/memoryze.htm
17. PhotoRec Digital Picture Recovery, visitado por última vez 12-08-2012, http://www.cgsecurity.org/wiki/PhotoRec
18. SANS SIFT Workstation, visitado por última vez 12-08-2012, http://forensics.sans.org/community/downloads/
19. Scalpel: A Frugal, High Performance File Carver, visitado por última vez 12-08-2012, http://www.digitalforensicssolutions.com/Scalpel/
20. Simple Carver Suite, visitado por última vez 12-08-2012, http://www.simplecarver.com/

    PTK forensics is a computer forensic framework , visitado por última vez 12-08-2012, http://ptk.dflabs.com/.
21. Sleuthkit.org is the official website for The Sleuth Kit, Autopsy Forensic Browser, visitado por última vez 21-10-2012, http://www.sleuthkit.org/
22. Source Forge mdd, visitado por última vez 12-08-2012, http://sourceforge.net/project/showfiles.php?group_id=228865
23. Volatile System, visitado por última vez 12-08-2012, https://www.volatilesystems.com/default/volatility
24. Winhex:Software para Informática forense y recuperación de archivos, visitado por última vez 12-08-2012, http://www.x-ways.net/winhex/
25. X-Ways Forensics: Integrated Computer Forensics Software, visitado por última vez 21-10-2012, http://www.x-ways.net/forensics/index-m.html

ANEXO A

CUESTIONARIO

Contando con su atención le solicito por favor responda a las preguntas del presente cuestionario cuyo objetivo es:

> "Desarrollar una técnica informático forense para el uso en las investigaciones de delitos informáticos que se realicen en la Policía Nacional Departamento de Potosí – Fiscalía del Distrito de Potosí."

Para lo cual se le solicita marcar con una **"X"**, en los recuadros correspondientes, o en su caso llenar con el texto apropiado en la línea punteada.

1. **¿**Conoce o aplica la informática forense en las investigaciones que se realizan**?**

   SI ☐ NO ☐

7. **¿**Cree que la forma de investigar los casos de delitos informáticos por la Policía es incompleta, sin pasos que seguir, sin procedimientos, por lo que la investigación es tratada con un caso común**?**

   SI ☐ NO ☐

8. **¿**Cree que la gente que no denuncia por delitos informáticos, prefiere denunciar usando otras leyes**?**

   SI ☐ NO ☐

Si respondió SI ¿Cuáles son los motivos?

.....

4. **¿**Sobre los delitos informáticos, cuáles fueron los más denunciados**?**

   SI ☐ NO ☐

5. ¿Las investigaciones con casos de denuncias de delitos informáticos los realizan en la ciudad de Potosí?

   SI ☐ NO ☐

Si respondió NO ¿Donde se realizan los estudios?

…….....

6. ¿Cree que con la implementación de un laboratorio equipado y una técnica informática forense los tiempos de resolución de casos mejorarían?

   SI ☐ NO ☐

GRACIAS POR SU COLABORACION

ENTREVISTA

Contando con su atención le solicito por favor responda a las preguntas del presente cuestionario cuyo objetivo es:

> "Desarrollar una técnica informático forense para el uso en las investigaciones de delitos informáticos que se realicen en la Policía Nacional Departamento de Potosí – Fiscalía del Distrito de Potosí."

¿Cuántos casos de delito Informático existen en curso?

……
……

¿Cuánto tiempo tarda en analizar el caso?

……

¿El costo de la revisión lo paga el que solicito el estudio, la institución, el gobierno?

……

¿Se cuenta, con un perito calificado? Si la respuesta es SI ¿Dónde se especializo?

……¿El personal de la Fiscalía acude en estos casos? Si la respuesta es SI ¿Cuántos acuden y que tareas realizan?

……
……
……

¿Se cuenta con una técnica informática forense para recabar datos?¿Cómo se procede?

……
……
……

¿Se cuenta con laboratorio para la cadena de custodia, análisis de la evidencia digital?

……
……

¿Los resultados obtenidos en el laboratorio son enviados por el área de revisión de pruebas digitales de forma inmediata?

……
……

Gracias por su Atención

CUESTIONARIO DIRIGIDO AL ENCARGADO DEL LABORATORIO DE INVESTIGACIONES FORENSES.

1. **¿Cuántos casos de delito Informático existen en curso?**

R. Tenemos actualmente un caso de pornografía infantil, se hizo el allanamiento y se secuestraron los equipos usados. Se los embaló y se procederá la envío correspondiente a la ciudad de La Paz, para su investigación

2. **¿Cuánto tiempo tarda en analizar el caso?**

R. Dependiendo el caso, con normalidad tarda unos seis meses

3. **¿El costo de la revisión lo paga el que solicito el estudio, la institución, el gobierno?**

R. Lo gastos corren por la persona denunciante, el gobierno no puede pagar todos esos gastos, o en su caso el gastos se divide por las partes afectadas.

4. **¿Se cuenta, con un perito calificado? Si la respuesta es SI ¿Dónde se especializo?**

R. Si, mi persona es la que se encarga de realizar las investigaciones y soy el perito a cargo. Mis estudios son de técnico de informática. Sin embargó sé que debería especializarme más, ya que de las denuncias que se hicieron tengo un conocimiento leve, sin embargo contando con un manual, una guía o una técnica donde acudir, que nos indique que pasos debemos seguir o como hacerlo nos ayudaría de sobre manera.

5. **¿El personal de la Fiscalía acude en estos casos? Si la respuesta es SI ¿Cuántos acuden y que tareas realizan?**

R. Claro que sí, de acuerdo a la ley de procedimiento penal es que un grupo multidisciplinario de fiscales, policías a cargo y un Juez acudimos a estos, para levantar los objetos a secuestras y otros.

6. **¿Se cuenta con una técnica informática forense para recabar datos? ¿Cómo se procede?**

R. No, nos basamos en la Ley de Procedimiento penal en sus artículos dice cómo proceder, más no nos indica cómo realizar el proceso para delitos informáticos específicamente, por lo que se procede de manera general como si se tratara de un objeto cualquiera pero teniendo cuidado de no dejar huellas.

7. **¿Se cuenta con laboratorio para la cadena de custodia, análisis de la evidencia digital?**

R. Tenemos un laboratorio, en realidad 2 oficinas, en la primera trabajo yo, en la segunda oficina están ubicados los equipos que han sido secuestrados, es el almacén, muchos de estos equipos ya no vinieron a recoger, pero si se encuentran inventariados. Seria interesante tener un laboratorio equipado para realizar las investigaciones y con las normas de seguridad correspondientes.

8. **¿Los resultados obtenidos en el laboratorio son enviados por el área de revisión de pruebas digitales de forma inmediata?**

   Todo lo que enviamos a la ciudad de La Paz tarda en regresar, como es la única que se encarga de realizar estos estudios, demora bastante, además de que se trata de envío y recepción de correspondencia eso implica de hecho un retraso.

ANEXO B

FORMULARIO CADENA DE CUSTODIA

Articulo	**Código**	**Fecha/Hora**	**Entregado por:**	**Recibido por:**	**Propósito y ubicación**
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	

Disposición Final de la evidencia	
Acción Final: Registrar los datos de quienes mantengan la cadena de custodia	Personal receptor de la evidencia digital **Nombre** **Firma** **Fecha y Hora** 1) 2) 3) 4)

FORMULARIO DE ADQUISICION DE EVIDENCIA DIGITAL

Caso N°				Expediente Judicial N°……..		
Fiscal a cargo:						
Investigador Asignado:						
Perito Informático Forense:						
Tipo de caso:						
Localización donde se obtuvo la evidencia:						
Articulo	Código	Descripción de la evidencia		Serial	Fabricante	Modelo
Evidencia recuperada por:	☐ Recolección de elementos Inf.	☐ Volcado de bits	☐ Extracción de unidades de almacenamiento internas		☐ Recolección del equipo de computación	Fecha/Hora
Herramienta Forense utilizada:						
Si realizo volcado de bits:		Valor Hash:				
Evidencia entregada a:			Recibe conforme:		Entrego conforme:	Fecha/Hora
Departamento:		Provincia:		Localidad:		

FORMULARIO PARA EVIDENCIA COMPUTACIONAL

Nombre del caso: Examinadores:

Numero de caso: Fecha:

Informacion del ordenador:

Marca:..... Modelo:.....

Numero de serie:.....

Motivo de analisis:.....

Tipo de compuatdor: Desktop ☐ Lactop ☐ Otra:.....

Condicion: Buena ☐ Mala ☐

Numero de discos duros:..... 3.5° Floppy Drive ☐ Lector Multitarjetas ☐

Modem ☐ Tarjeta de red ☐ Tarjeta de Video ☐ Otra:.....

Memoria Ram..... DVDRW ☐ CD Rom ☐ CD RW ☐

DVD ☐ Other:.....

Informacion- Bios | No disponible ☐

Pasword: Si ☐ No ☐ Pasword = ...

Hora Actual:..... AM ☐ PM ☐ Fecha actual: ..../..../....

Hora del Bios:..... AM ☐ PM ☐ Fecha actual: ..../..../....

Informacion del BIOS sobre el Disco Duro

Capacidad: ..... Cilindro: Heads:..... Sectors:.....

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

Disco Duro 2

Capacidad: ..... Cilindro: Heads:..... Sectors:.....

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

Disco Duro 3

Capacidad: ..... Cilindro: Heads:..... Sectors:.....

Mode: LBA ☐ Normal ☐ Auto ☐ Legacy CHS ☐

Firmas de constancia:

_____ Atte.

_____ Atte.

DETALLE DE INVENTARIO DE EQUIPOS COMPUTACIONALES

Nombre del Caso:..... **Nro. Caso**

Nombre Perito Informático Forense:.....

Lugar y Fecha:

Nro.	DESCRIPCION	NRO. SERIE	MARCA	MODELO	UBICACIÓN	USUARIOS

Firman

Perito Informatico **Tecnico Asignado**

Almacenero

FORMULARIO TRABAJO EN DISCO DURO

Nombre de caso: …….. Examinadores: ……..……..

Numero de caso: …… Fecha: ……...……..……

Disco Duro 1 -2 -3 Etiqueta de Información (No Disponibles)

Manufacturado:……...…
Modelo:……...……...……..
Numero Serial:……...……
Capacidad:……...…… Cilindros:……
Heads:……...……. Sectores:……

Control Rev:

IDE: Pin SCSI SATA: Otro:……

Jumper: Master Slave Clave Select No determiando

Parámetros de información del Disco

Software utilizado:

Capacidad:…… Cilindros:…….. Heads:…….. Sectores: ……..
LBA: ……. Capacidad de Disco formateado: ……..……...

Nombre de volumen:…….
Particiones:

Nombre	Boteadle	Inicio	Finalización	Tipo

Información de la imagen de disco

Software utilizado: ……

Método utilizado: Raw SMART E01 otro:……

Información de la Plataforma de Análisis

Sistema Operativo utilizado: …… Versión: ……
Software de análisis utilizado: …… Versión: ……

Después del trabajo se mantuvo la integridad de la imagen SI NO

LISTA DE SOFTWARE UTILIZADO

Nombre de caso: ……..

Numero de caso: ……

Tipo de dispositivo: ……

Modelo: ……..

Examinadores:
……..

Fecha:
……

Numero de serie:
……

Marca:
……..

Nro.	Software/Comandos	Version	Trabajo Realizado

Responsables:

Atte.

Atte.

ANEXO C

CASO DE ESTUDIO

DELITO INFORMATICO PORNOGRAFÍA INFANTIL.

1. Motivos.

Un ciudadano extranjero de nombre X dueño de un café internet que trabajaba con el personal que atendía el Café Internet abierto al público, que para conseguir réditos sustanciosos se dedicaba a la pornografía infantil, el cual tenía contactos en el extranjero, este lugar era apropiado para capturar las imágenes de inocentes adolescentes que posaban creyendo que no era nada malo, además de contar con una cámara escondida, este personaje que se hacía pasar como un buen amigo de las victimas para convencerlas y luego comercializar lo obtenido, son algunos de los atributos de este delito de pornografía infantil. Por lo tanto el motivo principal para realizar esta tarea fue el conseguir ingresos económicos mediante páginas web con pornografía infantil.

2. Desarrollo.

Para cometer este delito fueron necesarios unos adolecentes que trabajaban atendiendo el lugar, niños inocentes, contactos que pagaban por las imágenes.

– *Entrada en el sistema.*

El extranjero vino a instalar este negocio en nuestra ciudad con la experiencia necesaria y conocimientos para implementar y producir las páginas web con pornografía infantil, este español ya había venta realizado este mismo trabajo en España, al verse acorralado escapo a nuestra ciudad. Un 14 de febrero apertura este Café internet para los vecinos de la Zona San Pedro ubicada en la Plaza Minero, sin embargo este lugar lo usa de pantalla aparentando un negocio de internet normal, en dicho centro se administra y produce el verdadero negocio, utilizando como pantalla un portal, donde bajo la apariencia de comercializar prendas de vestir, los

interesados debían registrarse y abonar una suma mensual, tras lo cual les remitía vía e-mail el nombre de usuario y contraseña para acceder a los contenidos.

- *Obtención de datos e información.*

  El uso de Scanner, cámaras fotográfica, computadoras fueron las herramientas usadas para cometer el delito. Las víctimas eran convencidas de mirar a una cámara mostrando ciertas partes de su cuerpo, otras víctimas desconocían de la existencia de la cámara que se encontraba encima de la puerta por donde ingresaban al lugar.

  Este personaje conocía de programación usaba el software especializado para diseñar y editar páginas web, editar imágenes, subir al servidor y otros.

  Para capturar las imágenes usaba una cámara fotográfica convenciendo a las víctimas de posar, como si fuera algo muy normal. Así también se valía de una cámara escondida detrás la puerta principal para tomar imágenes donde las víctimas mostraban ciertas partes de su cuerpo.

  El español recolectaba, editaba las imágenes y actualizaba la página web, revisaba su cuenta, enviaba los correos electrónicos con la cuenta y clave periódicamente.

3. Resultados del análisis.

Este café internet era usado como pantalla mostrado a los vecinos y para los cibernautas comunes un portal de venta de ropa, eso es lo que aparentaba, siendo la realidad otra, se trataba de pornografía infantil. Para ello se usaron herramientas informáticas, tales como editores de páginas web, editores de imágenes, la computadora donde se administraba el lugar servía de servidor, también era el repositorio de las miles de imágenes pornográficas, cuentas, correos electrónicos de los contactos y otros, todo apuntaba a un delito informático.

4. Recomendaciones.

- Incluir en el Código Penal las tipificaciones de Delitos Informáticos y sus penalizaciones, principalmente el de pornografía infantil.
- Realizar controles sorpresivos a los cafés internet por parte de la institución que autoriza la apertura de estos negocios para que no se desvíen en el negocio.
- Hacer seguimientos del crecimiento exponencial de ingresos económicos de personas que implementan cafés internet.
- Realizar batidas periódicas a los cafés internet de personal de la Fiscalía y Policía para velar la seguridad de los menores que ingresen a estos lugares.

INFORME TECNICO

1. ANTECEDENTES DEL INCIDENTE.

La corrupción de menores está tipificada y penalizada en el Código Penal Boliviano, sin embargo en la sociedad potosina aun costumbrista, no se ven casos de que gente con conocimientos en el diseño de programas lo mal use para realizar trabajos pornográficos de menores con el afán de conseguir dinero.

Es así que un ciudadano extranjero pudo cometer el delito de pornografía infantil en España durante mucho tiempo, al verse acorralado huyó de dicho país, llegando a la ciudad Potosí, donde procedió a instalar nuevamente el mismo negocio en la Zona San Pedro Plaza Minero, contando ya con herramientas necesarias y con varios contactos también extranjeros, utilizó de pantalla un café internet y un portal de venta de ropa, ocultando el verdadero negocio ilícito. Dicho español era técnico programador que usando ese portal de pantalla a sus clientes indicaba depositar un monto mensual y enviaba vía correo los usuarios y claves para ingresar a otras páginas con pornografía infantil. El equipo donde administraba y editaba lo obtenido sirvió de servidor de las páginas pornográficas.

Siendo un café internet poco llamativo donde asistían personas de toda edad, principalmente niños y adolescentes que llevados por la inocencia y curiosidad eran convencidos de posar. Así también se obtenía fotos a través de una cámara oculta donde capturaba partes del cuerpo de las víctimas.

La policía española estuvo buscando a este criminal durante meses sin éxito, hasta que fue denunciado por uno de sus clientes insatisfechos, que por venganza indico desde donde operaba, el policía asignado al caso pudo reconocer el mismo trabajo por el cual estaba siendo buscado, fue denunciado a la justicia boliviana y solicitado para su extradición y

castigo en España; en Bolivia se hizo el seguimiento respectivo y mediante la Fiscalía de la Nación se lo detuvo por corrupción de menores.

2. RECOLECCIÓN DE LOS DATOS

La Fiscalía del Distrito de Potosí se hizo cargo del hecho gestionando que se atrape al sospechoso, conjuntamente con la Policía Nacional del Departamento, se reunió a un grupo multidisciplinario, conformado por: Un Fiscal asignado al caso, un Perito informático, un Policía asignado al caso y varios Policías para apoyo.

Para la recolección de datos se realizó un allanamiento, además de la incautación, se obro de la siguiente manera:

1. Allanamiento del café internet a hrs 16:30 sin previo aviso.
2. El personal de apoyo de la Policía separó a los presentes, a un lado a los que parecían clientes y a otro lado al dueño del lugar.
3. Se tomaron fotografías de cómo se encontraban los equipos de manera general, una toma completa.
4. Otras tomas de todas las computadoras encendidas de la pantalla en la que encontraba el cada equipo, siendo en su totalidad cinco en el lado cliente y dos en el lado administración.
5. Se incautaron las dos CPUs.
6. Se suspendió el sistema de las dos computadoras y se quito la energía eléctrica. Previo a ello se realizaron las siguientes actividades:
   6.1. Se realizo una copia de la memoria volátil, realizando un copiado de las memorias de ambos equipos.
7. Desconectar el router.
8. Desconectar la fuente de la impresora
9. Se rotuló todas la conexiones de los equipos para poder restaurar la configuración original
10. Se registró el área en busca de información relacionada al caso o de contraseñas, se revisaron los libros, notas, manuales, CDs, DVDS y otros.
11. Se registró detalladamente los elementos a secuestrar en el acta de allanamiento: USB y un scanner, una cámara fotográfica.

12. Se realizó un inventario de los objetos secuestrado.
13. Se llenaron formularios donde se detalla cuantos equipos fueron secuestrados, firmado por el equipo multidisciplinario.
14. Se rotuló con cinta de seguridad.
15. Finalmente se Fotografió el área después de que el gabinete ha sido removido

Estos fueron los formularios usados:

ACTA DE ALLANAMIENTO

Nombre del Caso:..... Nro. Caso

Nombre Fiscal Asignado: .....

Nombre Perito Informático Forense:.....

Nombre Policía Asignado:.....

Lugar y Fecha:

Local:

Tipo de Negocio: ..... **Nombre de Negocio.....**

Dueño: ..... **Direccion:.....**

Gente ocupante:

Nro.	Descripcion	Cantidad

Equipos Computacionales

Nro.	Descripcion	Cantidad

Firman

Perito Informatico **Fiscal Asignado**

Policia Asignado

DETALLE DE INVENTARIO DE EQUIPOS COMPUTACIONALES

Nombre del Caso:..... **Nro. Caso**

Nombre Perito Informático Forense:.....

Lugar y Fecha:

Nro.	DESCRIPCION	NRO. SERIE	MARCA	MODELO	UBICACIÓN	USUARIOS

Firman

Perito Informatico **Tecnico Asignado**

Almacenero

En el lugar se encontraron los siguientes dispositivos donde estaban los datos o material del crimen (corrupción de menores)



Fuente. Fotografía obtenida en allanamiento

Memoria USB, discos compactos, DVD

3. DESCRIPCIÓN DE LOS DISPOSITIVOS ENCONTRADOS Y IMPLICANCIA

Los dispositivos encontrados son los siguientes.

Laptop

La portátil encontrada es Compaq y tiene las siguientes características:

Procesador: Intel Pentium Dual Core T2310, Adaptador Gráfico: Intel Graphics Media Accelerator (GMA) X3100, Pantalla: 15.4 pulgadas, Ram 3 Gb, Peso: 3.1k

Computadora de escritorio

El computador tiene las siguientes características:

Procesador Intel Pentium Dual-Core E2220 o AMD Athlon64 X2 6000+, Disco duro de 120 GB, Memoria RAM de 2 GB, Monitor de panel plano matriz activa TFT LCD de 17 pulgadas, Quemador de CD / DVD (Unidad DVD+/-RW), Sistema de sonido con parlantes y micrófono de sobremesa incluidos, conector frontal para parlantes y micrófono, Módem 56K, Tarjeta de red 10/100, Puertos USB 6 con dos frontales, Teclado estándar, Mouse óptico de dos botones, sistema operativo Windows xp

Disco Duro

Disco duro SATA: marca Maxtor, 320 GB, 7200 RPM*.

Impresora

La impresora e HP PhotoSmart A52, que imprime fotos de alta calidad

Filmadora

La filmadora encontrada es Sony 990 Digital: Sus principales características son: Luz incorporada y pantalla táctil, detector de rostro, grabación directa a PC, grabación en cinta digital y memorias SD.

Cámara de seguridad

El lugar estaba vigilado con cámaras Sony 1/3 "CCD520/600TVL que tiene un asistencia de infrarrojos en entornos bajo luz. Encerrado en un recinto IP66, esta cámara estaba

encubierto con una mascarilla tipo foco y con revestimiento de vidrio, las grabaciones se hallan en el equipo de computación de escritorio.

Cámara fotográfica.

Cámara fotográfica marca Sonny, de formato digital, con 7.2 mega pixeles y un alcance de 10 x Zoom con baterías, además tiene la función de Sweep Panorama. Tiene visor de pantalla lcd de 3 x 2,5 cm

Memoria USB, discos compactos y DVD

Los dispositivos de almacenamiento que encontró son: 20 discos compactos marca sony de 700Mb de capacidad de almacenamiento, 40 DVD nuevos marca princo de 4.7 Gb de capacidad de almacenamiento, memorias de usb marca hp de 4 Gb de capacidad de almacenamiento.

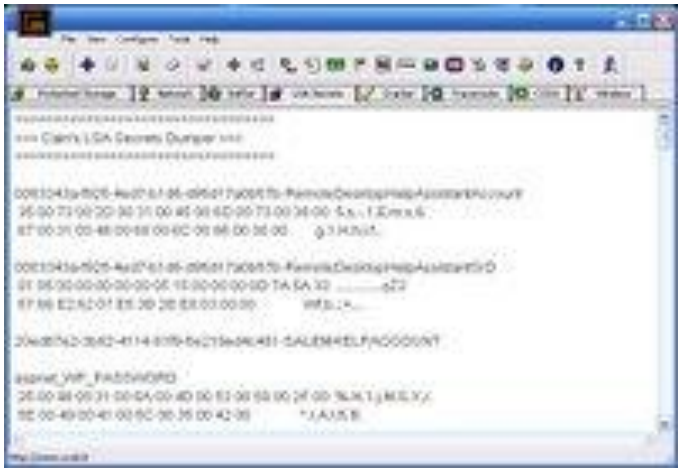
4. ENTORNO DEL ANÁLISIS.

4.1.DESCRIPCIÓN DE LAS HERRAMIENTAS.

Para trabajar con la información de ambos equipos se realizaron imágenes de los discos duros, por lo cual se trabajó sobre la imagen de los discos duros

Cain y Abel.

Herramienta de recuperación de contraseñas para los sistemas operativos de Microsoft que se suele utilizar para hackear redes. Este Software fue utilizado para descubrir la clave para el ingreso al Sistema Operativo Windows XP.



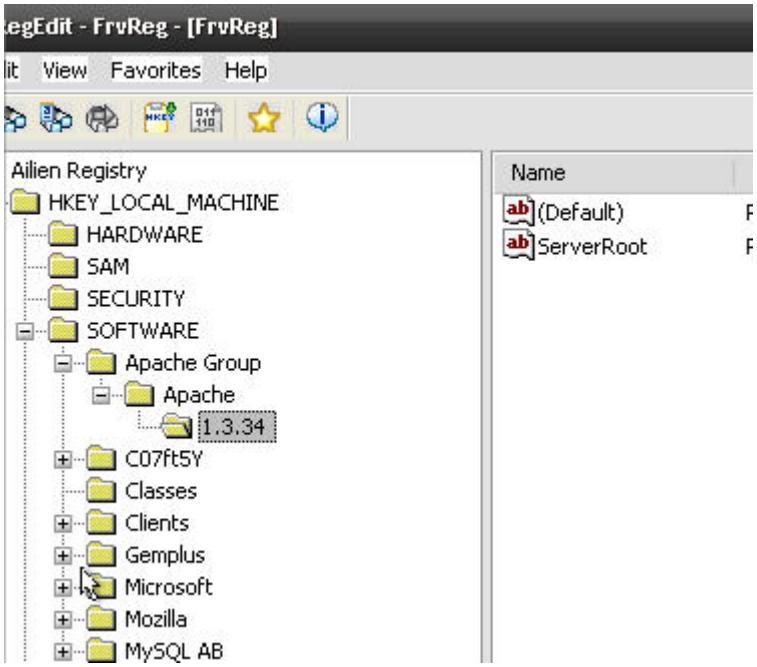
Advanced Outlook Password Recovery 1.34

Advanced Outlook Password Recovery es un programa creado para recuperar contraseñas perdidas u olvidadas de ficheros del sistema de Almacenamiento Personal Protegido. El programa recuperará rápidamente las contraseñas, sin importar su tamaño o complejidad. Una vez ingresado al disco con ayuda de este programa se obtuvo la clave del correo Outlook, de esa manera se ingreso y se listaron los correos tanto de entrada como salida.

WINHEX

Es un conjunto de utilidades para informática forense, mediante el mismo se encontró todas aquellos archivos o carpetas y otros. Con esta herramienta pudimos encontrar la variedad de fotografías que tenia ocultos en carpetas, así también en la papelera de reciclaje, de esa manera se confirmó que ambos equipos contenían archivos con imágenes que incriminaban al sospechoso.

Alien Registry Viewer



Alien Registry Viewer 1.01 es una aplicación muy parecida al RegEdit de Windows. A diferencia de RegEdit, el cual sólo trabaja con los ficheros del registro de standalone, Alien Registry Viewer 1.01 muestra absolutamente todos los contenidos incluidos en el sistema de registros, pertenecientes a Windows o no, por tanto trabaja con posibles ficheros de registro incluidos por otros programas.

Revisar Sucesos del sistema

El Visor de Sucesos es una pequeña herramienta que incorporan todos los Sistemas Operativos Windows desde Windows NT, que nos permite visualizar cualquier cosa que ocurra en nuestro ordenador, ya sean errores, advertencias o simplemente notificaciones.

Cada vez que algo ocurre en el sistema el Visor de Sucesos lo registra, sobre todo en el arranque o en el apagado. Que cuando tengamos algún problema se debe revisarlo ahí y poder comprobar que es lo que está fallando. Además se puede exportar los datos incluso a un archivo de texto, lo que sirve para consultarlo en otro momento o incluso imprimirlo para revisarlo en papel.

Visor de "Cookies" de Internet Explorer (IECookiesView) 1.70

Esta utilidad muestra los detalles de todas las "cookies" que Internet Explorer almacena en su computadora. Además, permite cambiar el contenido de las "cookies", borrar archivos "cookie" no requeridos, guardar las "cookies" a un archivo tipo texto modo lectura, encontrar "cookies" por un nombre de dominio específico, ver las "cookies" de otros usuarios y en otras computadoras.

5. INFORMACIÓN DEL SISTEMA ANALIZADO.

Computadora 1

Software.-

Sistema Operativo: Windows XP SP3

Aplicaciones: Microsoft Office 2007, Adobe Premiere Pro CS 5.5, Macromedia Flash Player, DirectX 11

Computadora 2

Software.-

Sistema Operativo: Windows XP SP3

Aplicaciones: Microsoft Office 2007, Nero Express. Macromedia Flash Player.

6. DESCRIPCIÓN DE HALLAZGOS.

En el caso de la computadora 1, se encontró que tenía la función de grabar los videos con el programa Adobe Premiere Pro CS 5.5, después del grabado de videos, se procedía a enviar a la computadora 2 para su producción.

La computadora 2, se encontró con software común, pero al aplicar las herramientas, se encontraron logs de programas como: Global Scape, Cute FTP, Adobe Dreamweaver CS5.5 útiles para la edición y administración de páginas Web, también se encontraron desinstalados Adobe Illustrator CS5.5, Adobe Photoshop CS5.5, los cuales muestran que el usuario que lo manejaba utilizaba herramientas específicas para editar y producir imágenes.

También se recuperó la cuenta de correo electrónico del implicado que utilizó para obtener los mensajes de sus clientes y proveerles las contraseñas de la página para ver las imágenes.

Se pudo acceder a los cookies del internet Explorer, se encontró que el usuario tuvo un constante acceso a la página donde realizaba sus delitos www.xxx.com

Así también se encontró diferentes archivos borrados, entre las imágenes de las menores, archivos comprimidos, videos en una cantidad de 10000 archivos comprometedores.

7. CRONOLOGÍA

El 14 de Febrero empezó a trabajar en un CyberCafé, luego de dos meses el 14 de Abril fue denunciado por un cliente de España. Para el 20 de mayo, el juez ordeno la incautación de los equipos y a partir de esa fecha se le transfirió la evidencia al perito correspondiente. 3 semanas después, el perito informó el trabajo que realizó a hacia la fiscalía.

8. CONCLUSIONES

Se descubrieron diversos programas especializados que permiten la confección, diseño y administración de páginas web e imágenes, estos fueron considerados por los peritos

como de “considerable complejidad y no resulta habitual para el usuario común el manejo de herramientas específicas como las señaladas, debiendo, por tal motivo ser ponderado como un elemento de cargo”.

Además de los programas que permiten suponer que el imputado era el administrador de este sitio web, también fueron detectados más de 10.000 archivos gráficos y de video imágenes entre los que se encontraban menores de edad realizando actividades sexuales explícitas. Así mismo se encontraron varios contactos y correos con envío de códigos en el correo electrónico.

9. RECOMENDACIONES.

- Incluir en el Código Penal las tipificaciones de Delitos Informáticos y sus penalizaciones, principalmente el de pornografía infantil.
- Realizar controles sorpresivos a los cafés internet por parte de la institución que autoriza la apertura de estos negocios para que no se desvíen en el negocio.
- Hacer seguimientos del crecimiento exponencial de ingresos económicos de personas que implementan cafés internet.
- Realizar batidas periódicas a los cafés internet de personal de la Fiscalía y Policía para velar la seguridad de los menores que ingresen a estos lugares.

ANEXO D

CUESTIONARIO

VALIDACION DE PROPUESTA

Contando con su atención le solicito por favor responda a las preguntas del presente cuestionario cuya hipótesis es:

> "La implementación de la técnica informático forense para el uso en las investigaciones de delitos informáticos mejorará el tiempo de obtención de resultados que se realicen en el laboratorio de la Policía Nacional del Departamento – Fiscalía del Distrito"

Una vez desarrollada la Técnica Informático Forense que será usada para las futuras investigaciones de delitos informáticos, es que se pide por favor que su persona llene este cuestionario que será de utilidad para la investigadora. Para lo cual se le solicita marcar con una **"X"**, en los recuadros correspondientes, de acuerdo a su criterio.

Durante las fases que se detallaran a continuación, considerar que esta herramienta mejorará los tiempos de atención en sus distintas fases, por lo cual usted nos indicará cuan útil, muy útil o en su defecto poco útil es.

2. Fase IDENTIFICACION.

   POCO ÚTIL ☐ ÚTIL ☐ MUY ÚTIL ☐

3. Fase de PRESERVACIÓN.

   POCO ÚTIL ☐ ÚTIL ☐ MUY ÚTIL ☐

4. Fase de ANÁLISIS.

   POCO ÚTIL ☐ ÚTIL ☐ MUY ÚTIL ☐

5. Fase de PRESENTACIÓN.

   POCO ÚTIL ☐ ÚTIL ☐ MUY ÚTIL ☐

6. Implementación del Laboratorio DE INVESTIGACIÓN FORENSE, software y Hardware

   POCO ÚTIL ☐ ÚTIL ☐ MUY ÚTIL ☐

GRACIAS POR SU COLABORACION

ANEXO E

MANUAL DE APLICACIÓN
DE LA TÉCNICA INFORMÁTICA FORENSE

1. Metodología Sistémica

La metodología Sistémica es la más básica, que contiene las fases: Identificar, Preservar, Analizar y Presentar, que posteriormente se detallará la técnica para cada fase, siguiendo un orden adecuado para intervenir ante un delito y análisis del mismo en base al tipo de evidencia digital encontrada, así también se describirá las posibles herramientas a ser usadas, pese al avance de la tecnología, se enumeraran las actuales, es así que a continuación se presentalas técnicas para cada Fase.

1.1. FASE IDENTIFICACIÓN.

Esta fase también es conocida como búsqueda y recopilación de evidencias, durante la identificación se debe realizar una inspección somera, para conocer con qué tipo de pruebas se contará, una vez que se ingresa al allanamiento del domicilio y se encuentre las computadoras apagadas o encendidas, esto para conservar la evidencia, utilizando herramientas que no cambien los sellos de tiempo de acceso (timestamp), o provoquen modificaciones en los archivos y que no borren nada, considerar que existen varios sistemas operativos, preparado en un maletín de herramientas de hardware, así también se usaran formularios que se deben llenar para que la recopilación de información y cadena de custodia sea un éxito, dichos formularios están en anexo B, para lo cual se harán las siguientes tareas:

1.1.1. Llenar los formularios de acuerdo a los pasos y al caso a seguir.

1.1.2. Asegurar que ninguna persona tenga acceso a la computadora y a sus alrededores. Si es una empresa y se trabaja en red se debe identificar al personal informático interno y a los usuarios de aplicaciones específicas que deben someterse a peritaje.

1.1.3. Fotografiar una toma completa del lugar donde se encuentran los equipos, a las conexiones de todos los equipos y luego diagramarlas. En algunos casos si es conveniente se puede realizar una filmación.

1.1.4. Si está encendida, tomar una fotografía de la pantalla y realizar cuidadosamente una verificación de integridad de los ficheros del sistema y realizar verificaciones sobre del equipo.

1.1.5. Investigar el área en busca de información relacionada o de contraseñas.

1.1.6. Verificar que procesos se están ejecutando actualmente en el equipo, buscando uno extraño, especialmente aquellos que consuman recursos en exceso, con ubicaciones poco frecuentes en el sistema de archivos, que mantengan conexiones de red en puertos TCP o UDP no habituales, etc.

1.1.7. Realizar otra comprobación listando todos los puertos TCP y UDP abiertos además de los procesos (PID), usuarios y aplicaciones que los utilizan

1.1.8. Rotular todas las conexiones de los equipos para poder restaurar la configuración original.

1.1.9. Buscar indicios en máquinas próximas si hubiera tales como escaneado de puertos o tráfico inusual en cortafuegos y routers de la red.

1.1.10. Anotar la fecha y hora de inicio y fin de cada uno de los pasos a seguir.

1.1.11. Registrar características de los equipos: números de serie, de sus componentes, escáner, cámaras fotográficas, routers, swicht, Sistema Operativo.

1.1.12. Secuestrar libros, notas, manuales, software, discos, sistemas de almacenamiento y todo lo relacionado al sistema; y realizar un inventario de lo secuestrado.

1.1.13. Debe estar presente una autoridad competente (Notario, Fiscal, Policía etc.) por guardar las garantías procesales.

1.1.14. Tratar de obtener pruebas ocultas con diferentes niveles de volatilidad, como

los registros del procesador, estructuras de datos en la memoria RAM o memoria de tipo caché, conexiones de red activas, usuarios y procesos actuales, sistema de archivos, etc. Ya que se perderá si decide apagar el equipo de la forma habitual, ya que en este proceso se realizan una serie de pasos programados para cerrar el sistema de forma limpia. Bien podría tener instalado las herramientas adecuadas éste podría eliminar, modificar y sustituir ficheros durante el apagado, y se "limpiarán" también del equipo las huellas de su atacante.

Para hallar información de un equipo activo se usara las siguientes herramientas en cuanto a hardware se refiere, que bien podrían ser otras más:

- **HARDCOPY 3.** Realiza copias de discos duros a una velocidad de hasta 7.5 Gb por minuto en la transferencia de datos, puede realizar dos copias a la vez de un mismo disco duro, además de verificar SHA256.También tiene modos de Duplicación (Clonación y creación de imágenes), diferentes métodos de Borrado, duplicación de otros Discos Duros (ATA, portátiles, etc.)

- **SHADOW 2. A**cceden al soporte magnético sin alterar su contenido, permite arrancar, en caliente, al investigador forense el sistema a analizar sin alterar su contenido, también permite instalar herramientas propietarias en caliente sin alteración de contenidos y actualizar el Firmware del Shadow 2 con futuras actualizaciones y mejoras.

- **DRIVEWIPER.** Alta calidad de borrado a gran velocidad (5,5 GB por minuto), facilidad de uso y fácilmente ampliable, borrado de dos discos duros simultáneamente a 8 GB por minuto en conjunto, es posible que trabaje con ATA o SATA, desbloquea y borra automáticamente áreas protegidas y para manejar el equipo tiene pantalla LCD y solo tres botones.

- **DUPLICADORES FORENSES**. Touch Screen Forensic ImagerModel TD3, Forensic 1:2 DuplicatorModel TD2, Model TD1.

  Estas herramientas ofrecenimágenes dedisco durosin dejar huella.Además de serrápidos, confiables y fácilesde usar, además traen consigo característicasútiles parael usuario avanzado.

1.1.15. También se corre el riesgo de que el intruso siga en línea y actuar con una acción evasiva o, peor aún, destructiva eliminando todo tipo de información. Dependiendo a la forma del ataque o por la importancia de los datos comprometidos se debe apagar el equipo, desconectando la energía eléctrica y se conservará bastante información sobre el ataque.
Previamente ejecutando algunos comandos para verificar que puertos están a la escucha, por ejemplo estos:

1.1.16. Para tocar el material informático se lo debe hacer con guantes descartables ya que el objeto de la investigación puede ser el mouse, teclado, CDs, DVDs, etc. y puede servir para el análisis de huellas dactilares, ADN, etc.

1.1.17. Poner los discos en sobres de material que no conduzca la estática.

1.1.18. Fotografiar el área después de que el gabinete ha sido removido.

1.1.19. Interrogar a todos los sospechosos.

1.1.20. Transportar la evidencia, no colocar elementos cerca de fuentes electromagnéticas (radios policiales)

El proceso de **recopilar evidencia** con un equipo encendido, se describe en la guía RFC 3227, se establece el siguiente orden de volatilidad y por tanto de recopilación de evidencias:

- Registros y contenidos de la caché.
- Contenidos de la memoria.
- Estado de las conexiones de red, tablas de rutas.
- Estado de los procesos en ejecución.

— Contenido del sistema de archivos y de los discos duros.
— Contenido de otros dispositivos de almacenamiento.

Dentro de las evidencias volátiles será de interés recuperar los siguientes datos del sistema en tiempo real:

— Fecha y hora.
— Procesos activos.
— Conexiones de red.
— Puertos TCP/UDP abiertos y aplicaciones asociadas “a la escucha”.
— Usuarios conectados remota y localmente.

Realizar una **imagen del disco**, que es una copia bit-a-bit del disco original preservando toda la información, incluyendo los bloques de los ficheros eliminados, espacio libre tras cada bloque, nodos (metadatos), etc.

Cada paso del procedimiento de la Fase de Identificación se debe seguir, ya que el pasar por alto alguno de ellos podría ocasionar alguna pérdida o ensuciar la evidencia, a continuación se muestra un diagrama de flujo que ayudará al Laboratorio de informática forense a trabajar de forma garantizada.

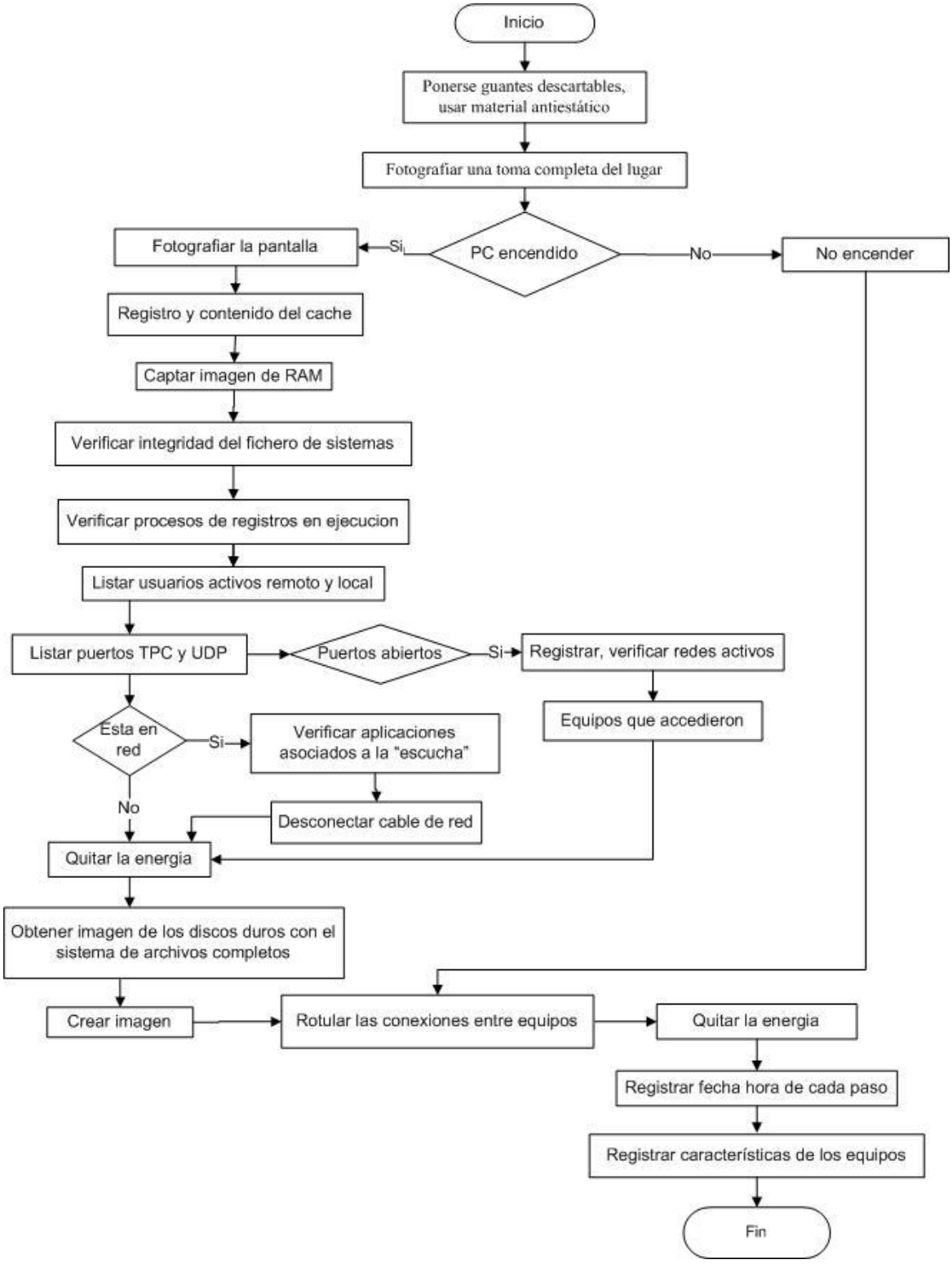


Figura 1.1.1 Diagrama de Flujo Fase Identificación

Fuente: Elaboración propia.

1.2. FASE PRESERVACIÓN DE LA EVIDENCIA.

En esta fase es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias. Una vez que se cuenta con todas las evidencias del incidente es necesario conservarlas intactas ya que son las “huellas del crimen”, se deben asegurar estas evidencias a toda costa. Para ello se sigue el siguiente proceso.

1.2.1. Copias de la evidencia

Se debe realizar dos copias de las evidencias obtenidas, generar también una suma de comprobación de la integridad de cada copia mediante el empleo de funciones hash tales como MD5 o SHA1. Incluir estas firmas en la etiqueta de cada copia de la evidencia sobre el propio medio de almacenamiento como CD o DVD etiquetando la fecha y hora de creación de la copia.

Si se extrae los discos duros de la CPU para utilizarlos como evidencia, se debe pegar la etiqueta “EVIDENCIA ORIGINAL”, incluir las correspondientes sumas hash, fecha y hora de la extracción del equipo, datos de la persona que realizó la operación, fecha, hora y lugar donde se almacenó.

Se debe tener en cuenta que existen factores externos como cambios bruscos de temperatura o campos electromagnéticos que pueden alterar la evidencia. Por lo cual velar a la seguridad de la evidencia.

1.2.2. Cadena de custodia.

Se deben establecer las responsabilidades y controles de cada una de las personas que manipulen la evidencia.

Se debe elaborar documentación en el que se registren los datos personales de todos los implicados en el proceso de manipulación de las copias, desde que se tomaron hasta su almacenamiento. Estos documentos deben contener la siguiente información:

- Lugar, fecha y encargado del día que se examinó la evidencia, incluyendo su nombre, su cargo, un número identificativo, fechas y horas, etc.
- Personal que custodia la evidencia, durante cuánto tiempo y dónde se almacenó.
- Cuando se cambie la custodia de la evidencia también se deberá documentar cuándo y cómo se produjo la transferencia y quién la transportó.

Todas estas medidas harán que el acceso a la evidencia sea muy restrictivo quedando claramente documentado, posibilitando detectar y pedir responsabilidades ante manipulaciones incorrectas, intentos de acceso no autorizados o que algún otro dispositivo electromagnético se use dentro de un determinado radio.



Figura 1.2.2 Diagrama de Flujo Fase Preservación.

Fuente: Elaboración propia.

1.3. FASE DE ANÁLISIS.

En esta fase se deben preparar las herramientas, técnicas, autorizaciones de monitoreo y soporte administrativo para iniciar el análisis forense sobre las evidencias obtenidas o presentadas. Una vez que se dispone de las evidencias digitales recopiladas y almacenadas de forma adecuada, en esta fase se debe reconstruir con todos los datos disponibles la línea temporal del ataque, determinando la cadena de acontecimientos que tuvieron lugar desde el inicio del ataque, hasta el momento de su descubrimiento.

Este análisis se dará por concluido cuando se descubra cómo se produjo el ataque, quién o quienes lo llevaron a cabo, bajo qué circunstancias se produjo, cuál era el objetivo del ataque, qué daños causaron, etc. En el proceso de análisis se emplean las herramientas propias del sistema operativo (anfitrión) y las que se prepararon en la fase de extracción y preparación.

1.3.1. Preparación para el análisis

En el laboratorio forense se debe realizar lo siguiente:

1.3.1.1. Acondicionar un entorno de trabajo adecuado al estudio que se desea realizar.

1.3.1.2. Trabajar con las imágenes que se recopiló como evidencias.

1.3.1.3. Preparar dos estaciones de trabajo, una de ellas contendrá al menos dos discos duros.

1.3.1.4. Instalar un sistema operativo que actuará de anfitrión y que servirá para realizar el estudio de las evidencias. En esta misma estación de trabajo y sobre un segundo disco duro, instalar las imágenes manteniendo la estructura de particiones y del sistema de archivos En otro equipo instalar un sistema operativo configurado exactamente igual que el equipo atacado, este segundo equipo servirá para realizar pruebas y verificaciones conforme vayan surgiendo hipótesis sobre el ataque.

1.3.2. Reconstrucción de la secuencia temporal del ataque

Si ya se tienen montadas las imágenes del sistema atacado en una estación de trabajo independiente y con un sistema operativo anfitrión de confianza, se procede con la ejecución de los siguientes pasos:

1.3.2.1. Crear una línea temporal de sucesos, información que servirá de punto de partida para el análisis, para ello se debe recopilar la siguiente información sobre los archivos:

- Nodos asociados
- Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado).
- Ruta completa.
- Tamaño en bytes y tipo de archivo.
- Usuarios y grupos a quien pertenece.
- Permisos de acceso.
- Si fue borrado o no.

1.3.2.2. Ordenar los archivos por sus fechas MAC. En busca de archivos y directorios que han sido creados, modificados o borrados recientemente, o instalaciones de programas posteriores a la del sistema operativo y que además se encuentren en rutas poco comunes. Buscar los archivos de sistema modificados tras la instalación del sistema operativo, averiguar después la ubicación de los archivos ocultos, de qué tipo son, identificar también los archivos borrados o fragmentos de éstos, pues pueden ser restos de logs y registros borrados por los atacante, usar la metodología que va de lo general a lo particular, por ejemplo partir de los archivos borrados, intentar recuperar su contenido, anotar su fecha de borrado y compararla con la

actividad del resto de los archivos, puede que en esos momentos se estuviesen dando los primeros pasos del ataque.

1.3.2.3. Comenzar a examinar con más detalle los archivos logs y registros que se examinaron durante la búsqueda de indicios del ataque, intentar buscar una similitud temporal entre eventos. Quizá los archivos log y de registro son generados de forma automática por el propio sistema operativo o por aplicaciones específicas, conteniendo datos sobre accesos al equipo, errores de inicialización, creación o modificación de usuarios, estado del sistema, etc. Por lo que se tendrá que buscar entradas extrañas y compararlas con la actividad de los archivos. Editar también el archivo de contraseñas y buscar la creación de usuarios y cuentas extrañas sobre la hora que se considere como inicio del ataque en el sistema.

1.3.2.4. Examinar los fragmentos del archivo, que es donde se detectan y registran los accesos FTP, esto permitirá descubrir si sobre esa fecha y hora se crearon varios archivos en la máquina comprometida, además se debe tener presente que este directorio puede ser borrado por el atacante y deberá ser recuperado.

1.3.3. Determinación de cómo se realizó el ataque

En esta etapa se deberá determinar cuál fue la vía de entrada al sistema, averiguando qué vulnerabilidad o fallo de administración causó el agujero de seguridad y que herramientas utilizó el atacante para aprovecharse de tal brecha.

La información se deberá obtener de forma metódica, empleando una combinación de consultas a archivos de logs, registros, claves, cuentas de usuarios, etc. El siguiente proceso permitirá conocer que acciones realizó el atacante:

1.3.3.1. Revisar los servicios y procesos abiertos que se recopilaron como evidencia volátil, así como los puertos TCP/UDP y conexiones que estaban abiertas cuando el sistema

estaba aún funcionando. Examinar con más detalle aquellas circunstancias que resultan sospechosas cuando se buscó indicios sobre el ataque, y realizar una búsqueda de vulnerabilidades a través de Internet.

1.3.3.2. Si ya se tiene claro cuál fue la vulnerabilidad que dejó el sistema desprotegido, es necesario ir un paso más allá y buscar en Internet algún exploit anterior a la fecha del incidente, que utilice esa vulnerabilidad.

1.3.3.3. Reforzar cada una de las hipótesis empleando una formulación causa-efecto, también es el momento de arrancar y comenzar a utilizar la máquina preparada

1.3.4. Identificación del atacante

Consultar las evidencias volátiles que se recopiló en las primeras fases, revisar las conexiones que estaban abiertas, en qué puertos y qué direcciones IP las solicitaron, además buscar entre las entradas a los logs de conexiones. También se puede indagar entre los archivos borrados que se recuperó por si el atacante eliminó alguna huella que quedaba en ellos.

Si el ataque fue en red se debe intentar averiguar la dirección IP del atacante, para ello revisar con detenimiento los registros de conexiones de red y los procesos y servicios que se encontraban a la escucha. También se podría encontrar esta información en fragmentos de las evidencias volátiles, la memoria virtual o archivos temporales y borrados, como restos de correo electrónico, conexiones fallidas, etc.

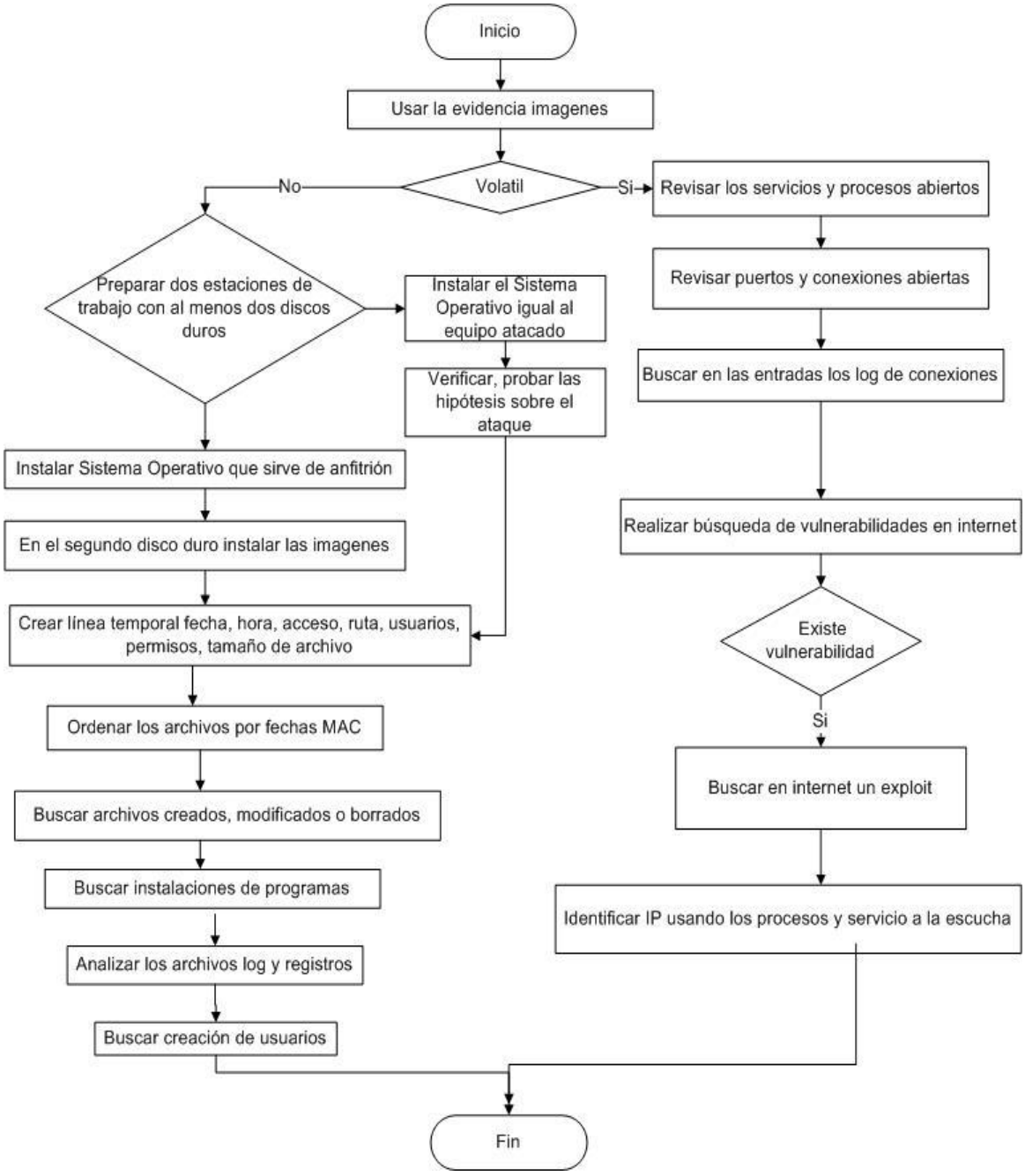


Figura 1.3.3. Diagrama de Flujo Fase Análisis

Fuente: Elaboración propia.

1.4. FASE DE PRESENTACIÓN DE INFORME.

1.4.1. Evaluación del impacto causado al sistema

Para poder evaluar el impacto causado al sistema, el análisis forense ofrece la posibilidad de investigar qué es lo que han hecho los atacantes una vez que accedieron al sistema. Esto permitirá evaluar el compromiso de los equipos y realizar una estimación del impacto causado.

Generalmente se pueden dar dos tipos de ataques:

- **Ataques pasivos.-** En los que no se altera la información ni la operación normal de los sistemas, limitándose el atacante a fisgonear por ellos.

- **Ataques activos**.- En los que se altera y en ocasiones seriamente, tanto la información como la capacidad de operación del sistema.

Se deberá tener en cuenta, además otros aspectos del ataque como los efectos negativos de tipo técnico que ha causado el incidente, tanto inmediatos como potenciales además de lo crítico que eran los sistemas atacados. Por ejemplo ataques a los cortafuegos, el router de conexión a Internet o Intranet, el servidor Web, los servidores de bases de datos, tendrán diferente repercusión según el tipo de servicio que presta la empresa o institución y las relaciones de dependencia entre los usuarios.

1.4.2. Documentación del incidente

Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finalice el proceso de análisis forense, esto le hará ser más eficiente y efectivo al tiempo que reducirá las posibilidades de error. Finalmente se presenta la resolución del incidente al menos dos tipos de informes uno Técnico y otro Ejecutivo.

1.4.3. Utilización de formularios de registro del incidente

Se deberá emplear formularios estrictamente. Éstos deberán ser rellenados por los departamentos afectados por el compromiso o por el propio equipo que gestionará el incidente. Alguno de los formularios que debería preparar serán:

- Documento de custodia de la evidencia.
- Formulario de identificación del equipo y componentes.
- Formulario de incidencias tipificadas.
- Formulario de publicación del incidente.
- Formulario de recogida de evidencias.
- Formulario de discos duros.

1.4.4. El Informe Técnico

Este informe consiste en una exposición detallada del análisis efectuado. Deberá describir en profundidad la metodología, técnicas y hallazgos del equipo forense. El contenido del informe deberá contener al menos estos puntos:

- Antecedentes del incidente.
- Recolección de datos
- Descripción de dispositivos encontrados e implicancia.
- Entorno del análisis
- Información del sistema analizado.
- Cronología.
- Conclusiones.

1.4.5. El Informe Ejecutivo

Este informe consiste en un resumen del análisis efectuado pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y

cinco, y será de especial interés para exponer lo sucedido a personal no especializado.

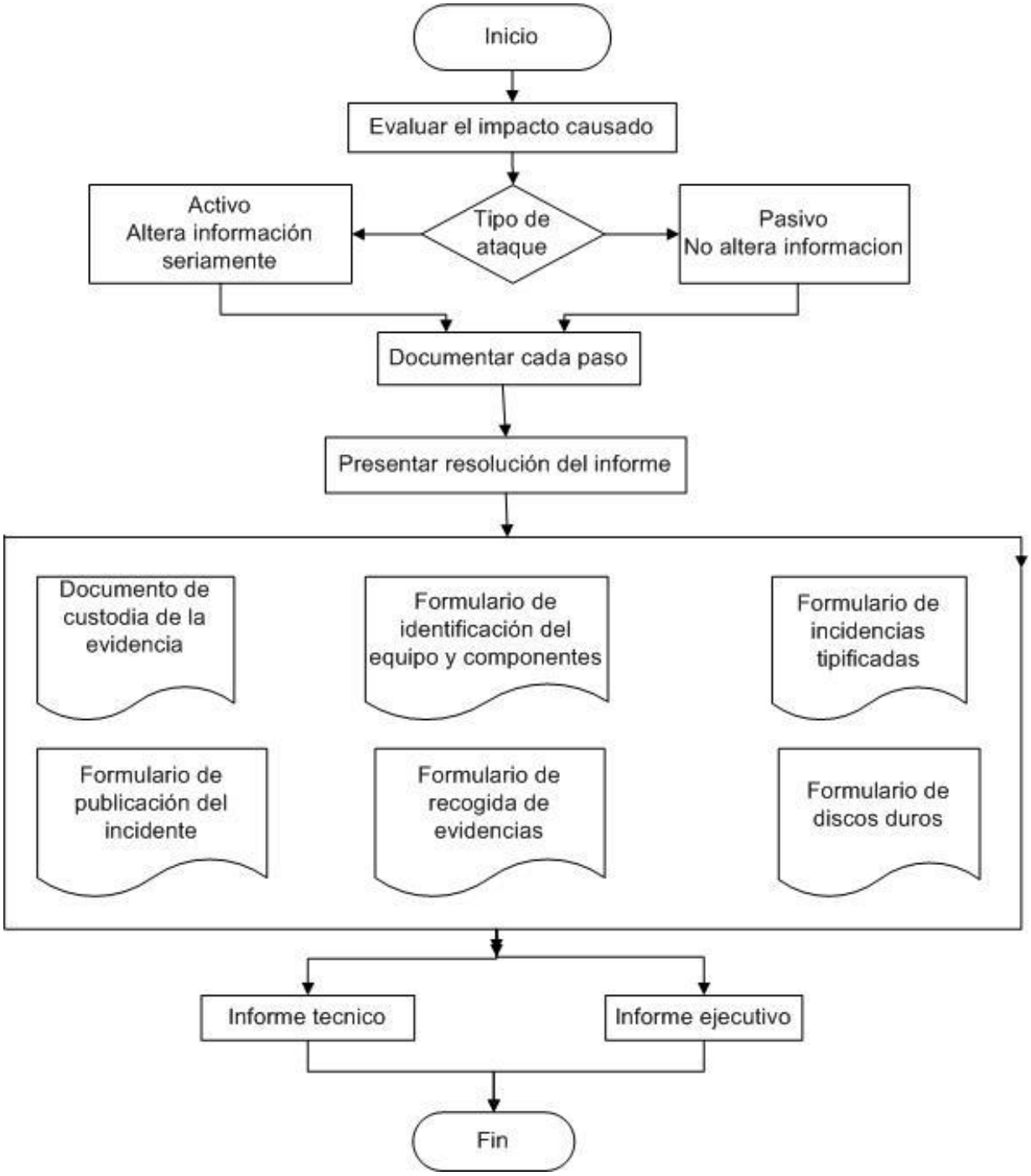


Figura 1.4.4 Diagrama de Flujo Fase Presentación De Informe

Fuente: Elaboración propia.