# DISEÑO E IMPLEMENTACIÓN DE UN CENTRO DE INFORMÁTICA FORENSE EN LA UNIVERSIDAD AUTÓNOMA DE OCCIDENTE

**GUILLERMO UMAÑA RAMIREZ**
**ISABEL CRISTINA MOSQUERA NAVARRETE**

**UNIVERSIDAD AUTÓNOMA DE OCCIDENTE**
**FACULTAD DE INGENIERÍA**
**DEPARTAMENTO OPERACIONES Y SISTEMAS**
**PROGRAMA INGENIERÍA INFORMÁTICA**
**SANTIAGO DE CALI**
**2014**

# DISEÑO E IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE EN LA UNIVERSIDAD AUTÓNOMA DE OCCIDENTE

**GUILLERMO UMAÑA RAMIREZ**
**ISABEL CRISTINA MOSQUERA NAVARRETE**

**Director**
**MIGUEL JOSE NAVAS JAIME**
**Ingeniero de sistemas con maestria en telemática**

**UNIVERSIDAD AUTÓNOMA DE OCCIDENTE**
**FACULTAD DE INGENIERÍA**
**DEPARTAMENTO OPERACIONES Y SISTEMAS**
**PROGRAMA INGENIERÍA INFORMÁTICA**
**SANTIAGO DE CALI,**
**2014**

**Nota de aceptación:**

**Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la universidad Autónoma de Occidente para optar al título de ingeniero Informático.**

**JUAN CARLOS VALENCIA**

**Jurado**

**JHON JAIRO HERNANDEZ**

**Jurado**

**Santiago de Cali, 12 de mayo del 2014**

## CONTENIDO

## LISTA DE FIGURAS

## LISTA DE CUADROS

## GLOSARIO

**ARCHIVO CRUDO**: archivo sin formato definido, que no tiene definida una aplicación para abrirlo.

**CADENA (STRING)**: es una sucesión de caracteres (letras, números u otros signos o símbolos).

**CHECKSUM**:(llamado suma de chequeo) esquema simple de detección de errores, donde cada mensaje transmitido es acompañado con un valor numérico basado en el número de grupo de bits del mensaje.

**LIF**: simplificación de la frase “laboratorio de informática forense”.

**CLÚSTER:** unidad mínima del sistema de archivos (todos los archivos tienen un tamaño físico (cantidad de clústeres que ocupa) y un tamaño lógico (bytes que ocupa).

**DUPLICADOR FORENSE**: dispositivo que sirve para realizar la copia bit a bit a un disco sin escribir en este.

**EMBALAJE**: proceso de empaque de la evidencia.

**EVIDENCIA**: pruebas válidas para procesos legales.

**FEHACIENTE**: que atestigua o certifica que algo es cierto dentro de un proceso judicial.

**HARDWARE**: conjunto de los componentes que conforman la parte material (física) de una computadora, todo lo visible y tangible.

**HASH:** la función hash hace referencia a un tipo de algoritmo que permite resumir y posteriormente identificar de manera íntegra la información contenida en un

mensaje, texto, etc. evitando que la información pueda modificarse sin que se modifique de igual modo la función resumen (hash).

**IMAGEN FORENSE**: llamada también "espejo" la cual es una copia bit a bit de un medio electrónico de almacenamiento. En la imagen quedan grabados los espacios que ocupan los archivos, áreas borradas incluyendo particiones escondidas.

**INDEX.DAT:** el archivo index.dat es un archivo de base de datos. Es un repositorio de información, como direcciones URL de Internet, las búsquedas y archivos recientemente abiertos.

Su objetivo es permitir el acceso rápido a los datos utilizados por Internet Explorer. Por ejemplo, todas las direcciones web visitadas se almacenan en el archivo index.dat, lo que permite Internet Explorer para acceder rápidamente Autocompletar cuando el usuario escribe una dirección web. El archivo index.dat específica del usuario desde que está abierto ya que permanece todo el tiempo desde que un usuario ha iniciado sesión en Windows. Archivos separados index.dat existen para el historial de Internet Explorer, caché y las cookies. El archivo Index.dat no se cambia el tamaño o eliminados. Un archivo de index.dat grande puede perjudicar el rendimiento.

**MD5**: (algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. También es una función de cifrado tipo hash que acepta una cadena de texto como entrada, y devuelve un número de 128 bits.

**MARKETING ESTRATÉGICO**: filosofía que enfatiza la correcta identificación de las oportunidades de mercado como la base para la planeación de marketing y el crecimiento del negocio.

**MARKETING MIX O MEZCLA DE MERCADOTECNIA**: es un concepto que se utiliza para nombrar al conjunto de herramientas y variables que tiene el responsable de marketing de una organización para cumplir con los objetivos de la entidad y está compuesto por la totalidad de las estrategias de marketing que apuntan a trabajar con los cuatro elementos conocidos como las Cuatro P: Producto, Precio, Plaza y Promoción (Publicidad).

**MINERIA DE DATOS**: es el proceso de detectar la información procesable de los conjuntos grandes de datos. Utiliza el análisis matemático para deducir los patrones y tendencias que existen en los datos.

**EXPERTO FORENSE**: es un profesional idóneo dotado de conocimientos especializados y reconocidos, a través de sus estudios superiores, que suministra información u opinión fundada a los tribunales de justicia sobre los puntos litigiosos que son materia de su dictamen.

**PREFETCH:** los archivos prefetch contienen el nombre del ejecutable, una lista unicode de archivos dll utilizados por ese ejecutable, un recuento de cuántas veces el ejecutable se ha ejecutado, y una marca de tiempo (timestamp) que indica la última vez que se ejecutó el programa.

**PRIMER RESPONDIENTE:** primera persona en ver la evidencia, la embala e inicia la conservación de la evidencia.

**PUNIBLE:**adjetivo que refiere a lo susceptible o merecedor de ser castigado.

**PUTTY:** aplicación de código abierto que sirve de emulador de terminal, consola serial y para transferir archivos por internet.

**REGISTRO**: en los sistemas operativos Windows, el registro contiene información del hardware, conexiones de red, preferencias del usuario y otra información crítica.

**SAM:**"securityaccount manager" es una base de datos presente en los sistemas operativos Windows donde se almacena la información de los usuarios (nombre, contraseñas, grupos a los que pertenece, etc.

**SANITIZAR**: en manejo de información confidencial es el proceso lógico y/o físico mediante el cual se remueve información considerada sensible o confidencial de un medio ya sea físico o magnético, ya sea con el objeto de desclarificarlo, rehusar el medio o destruir el medio en el cual se encuentra.

**SHA1**: es la función hash designada por la agencia de seguridad de los Estados Unidos para encriptar información, también sirve para validar que un archivo no ha sido modificado.
**SISTEMAS MUERTOS**: equipos de cómputo que sirven de evidencia y se encontraron apagados.

**SISTEMAS VIVOS**: equipos de cómputo que sirven de evidencia y se encontraron prendidos.

**SOFTWARE:** programas e información operativa usada en una computadora.

**STARTUP**: arranque.

**WBS:** workbreakdownstructure es un término de gerencia de proyectos que significa Estructura de descomposición del trabajo y es una descomposición jerárquica de las actividades orientada al entregable del trabajo a ser ejecutado por el equipo del proyecto.

## RESUMEN

Este proyecto es la primera de dos etapas de montaje de un laboratorio de informática forense (LIF) en la Universidad Autónoma de Occidente (UAO), la cual consta en crear el modelo de implementación, es decir definir todo lo necesario para su funcionamiento a nivel de software, hardware, manejo de riesgos, recurso humano y recurso económico para su funcionamiento, la segunda etapa consiste en la implantación de este LIF, es decir su puesta en marcha, lo cual implica su promoción, construcción y operación.

El desarrollo de dicho LIF permitirá realizar análisis de evidencia digital frente a delitos informáticos que pueden presentarse en el sector público o privado, siendo estos casos manejados de manera rápida, profesional y eficaz mediante el cumplimiento de lineamientos judiciales como la conservación de la evidencia a base de la cadena de custodia, donde los hallazgos encontrados en un análisis sean válidos ante una corte judicial.

Este laboratorio inicialmente beneficiará mediante sus servicios a toda la comunidad universitaria y a la población en general en la region del valle del cauca en cuanto a atención a incidentes informaticos, permitiendo capacitar a los estudiantes de la Universidad Autónoma de Occidente en la atención a delitos informáticos y al mismo tiempo atender incidentes informáticos ya ejecutados en cualquier sector.

Con este laboratorio se pretende dar mayor reconocimiento a la UAO a nivel nacional al ser este capaz de atender incidentes que involucren medios informáticos y fortaleciendo su enfoque hacia la seguridad informática.



**Palablas clave**: Laboratorio de informática forense, Seguridad informática, Universidad Autonoma de Occidente.

# INTRODUCCIÓN

En la actualidad se ha identificado una necesidad puntual de los estamentos que se ocupan de las investigaciones de tipo forense relacionados con medios informáticos, debido a que la calidad del servicio a prestar, implica un amplio conocimiento en el manejo de herramientas forenses, técnicas de recolección y manejo de la evidencia digital, el conocimiento e identificación de sistemas de archivos, manejo de diferentes sistemas operativos y métodos de búsqueda de evidencias, entre otros, para lo cual, en nuestro medio, no se dispone del personal debidamente capacitado.

Para garantizar la transparencia en este tipo de investigaciones, es necesario contar mínimo con una persona experta en informática forense para la defensa y otro para el ente acusatorio en cada uno de los diferentes casos que puedan presentarse, pero dada la falta de personal apto se evidencia un nicho de mercado que no está siendo explotado y que por medio de la puesta en operación de este proyecto puede llegar a cubrir esta necesidad.

Debido a que hay pocos laboratorios de Computer Forensec para cubrir la demanda de este tipo de delitos informáticos, se desarrolló este proyecto que diseña e implementa un Laboratorio de Informática Forense (LIF) en la Universidad Autónoma de Occidente, mediante el uso de metodologías y estándares internacionales aplicados a través de herramientas especializadas y recolecion de evidencias digitales.

Por otro lado la legislación en Colombia ha avanzado mediante la promulgación de la ley 1273

la cual establece formalmente el concepto de delito informático y las diferentes penas por incurrir en él, sin embargo existe un vacío frente al manejo de la evidencia digital, no obstante las recomendaciones internacionales para el tratamiento de ésta, junto con la resolución 0-6394 de 2004[1] por medio de la cual se adopta el manual de procedimientos del Sistema de Cadena de Custodia[2] para el Sistema Penal Acusatorio Colombiano, sirven como referente para la solución de esta carencia.

[1] Resolución emanada por el fiscal general de la nación de Colombia el 22 de diciembre de 2004.

[2] Solo entes gubernamentales como la policia judicial pueden realizar una cadena de custodia, en el LIF se toma es la conservación de la evidencia.

Esta investigación se enfocó en establecer la metodología de trabajo que responda eficientemente a los casos requeridos por el LIF, cumpliendo la legislación colombiana de tal manera que sea ético, confiable y veraz en el momento de presentar sus análisis ante una corte jurídica.

El modelo a implementar en el LIF cuenta con la información de todos los recursos de software, hardware y estructura apropiada para la generación de nuevo conocimiento que brinde a la comunidad en general un recurso importante para la resolución de casos en los cuales se involucren medios informáticos.

Este desarrollo le permitirá a la Universidad Autónoma de Occidente reforzar el reconocimiento que tiene en el sector educativo regional y nacional con respecto al área de seguridad informática.

Nota del autor: este proyecto es el primer para afianzar el enfoque de la UAO hacia el área de informática forense, y es una gran oportunidad para la institución de fortalecer su liderazgo en cuanto a seguridad informática.

# 1. ANTECEDENTES

En la actualidad existen diversos laboratorios de informática forense, tales como:

## 1.1. LIF'S A NIVEL NACIONAL:

**1.1.1 Centro cibernetico policial de colombia.** Centro de informática forense de la policía nacional Colombiana, el cual atiende de manera gratuita a los ciudadanos, pero para poder acceder a sus servicios debe haber una ordenjudicial emitida por un juez solicitada por el fiscal asignado, también debe existir una investigación en curso por oficioo solicitud expresay por ende una demanda para proceder a realizar el proceso de investigación, la página web de este es http://www.ccp.gov.co/en la cual se describen todos sus servicios tales como:

Laboratorio Forense:

**Figura 1. Centro cibernético Policial**


CENTRO CIBERNETICO POLICIAL [En línea]. Consultado el día 05 de junio de 2013. Disponible en internet: http://www.ccp.gov.co/

Csirt-Ponal: Es un equipo de respuesta a incidentes de seguridad informática el cual garantiza las condiciones que aseguran la plataforma tecnológica de la policía nacional dando apoyo a la estrategia de ciberseguridad.

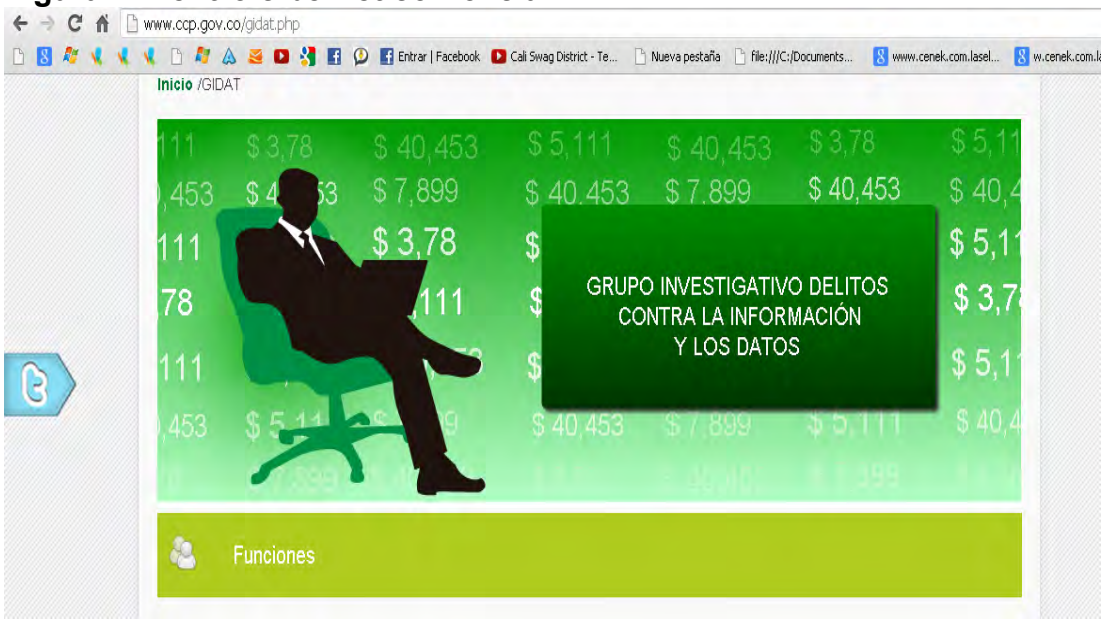
**Figura 2. Centro cibernético Policial 2**


CENTRO CIBERNETICO POLICIAL [En línea]. Consultado el día 05 de junio de 2013. Disponible en internet: http://www.ccp.gov.co/

**Figura 3. Centro cibernético Policial 3**


CENTRO CIBERNETICO POLICIAL [En línea]. Consultado el día 05 de junio de 2013. Disponible en internet: http://www.ccp.gov.co/

**Figura 4. Centro cibernético Policial 4**




CENTRO CIBERNETICO POLICIAL [En línea]. Consultado el día 05 de junio de 2013. Disponible en internet: http://www.ccp.gov.co/.

**Figura 5. Centro cibernético Policial 5**

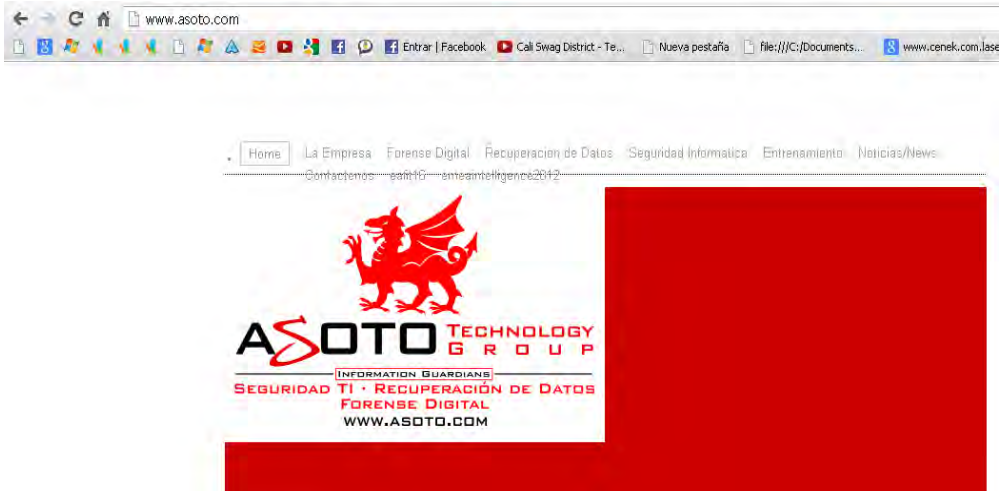

CENTRO CIBERNETICO POLICIAL [En línea]. Consultado el día 05 de junio de 2013. Disponible en internet: http://www.ccp.gov.co/.

### 1.1.2 Asoto en colombia.

**Figura 6. Asoto technology group**


Asoto [En línea]. Consultado el día 10 de junio de 2013. Disponible en internet: http://www.asoto.com/

**Figura 7. Asoto technology group 2**



Asoto [En línea]. Consultado el día 10 de junio de 2013. Disponible en internet: http://www.asoto.com/

Desde 1995 “ASOTO TechnologyGroup” ha fundamentado sus objetivos en ser un aliado estratégico para los sectores empresarial y gubernamental, especializándonos en proveer soluciones de Forense Digital, Recuperación de datos y Seguridad Informática.

Son distribuidores de tecnología exclusiva en soluciones especializadas para gobierno tales como: Paraben, Tableau, Digital Intelligence etc. Esta es usada por agencias internacionales de ley y orden como CIA, FBI, Department of Homeland Security, Interpol, entre otras así como proveedores de soluciones corporativas de alto nivel.

Esta empresa goza de reconocimiento internacional en países como USA, Rusia, Ucrania, China, Turquía, Brasil, entre otros. Cuenta con personal especializado y actualizado constantemente a nivel internacional[3].

### 1.1.3. Laboratorio de informática forense en la universidad de los andes colombia.

**Figura 8. Laboratorio de informática forense universidad de los andes**


Laboratorio de Informatica Forense Universidad de los Andes [En línea]. Consultado el día 05 de junio de 2013. Disponible en internet: http://sistemas.uniandes.edu.co/main/laboratorios/laboratorio-de-informatica-forense

[3]ASOTO TECHNOLOGY GROUP, [en línea] Bogotá D.C. [consultado en enero de 2014] Disponible en Internet http://www.asoto.com/

Este es un laboratorio móvil, el cual no es muy reconocido y permite realizar labores de adquisición, investigación y análisis de evidencias digitales con equipos de última tecnología, como duplicadores forenses de alta velocidad, dispositivos de toma de imágenes forenses, bloqueadores de dispositivos, docking para discos duros, kit para recuperación de datos, estaciones forenses portátiles y de escritorio con software especializado de captura y análisis de evidencia, sistema de almacenamiento centralizado de evidencias digitales y una infraestructura virtual que soporta todas las labores del laboratorio.
Este conjunto de elementos hacen del laboratorio el espacio ideal para que los estudiantes adquieran el conocimiento que les permita asumir el rol de investigadores forenses, sobre casos reales, en investigaciones digitales[4].

### 1.1.4. The muro group international.

**Figura 9. The muro group**


The muro group [En línea]. Consultado el día 05 de junio de 2013. Disponible en internet: http://www.themurogroup.com/analisis_forense.html

Es una empresa de consultoría que ofrece servicios de análisis forense entre otros como:

[4]LABORATORIO DE INFORMATICA FORENSE UNIVERSIDAD DE LOS ANDES, [en línea] [consultado en enero de 2014] Disponible en Internet: http://sistemas.uniandes.edu.co/main/laboratorios/laboratorio-de-informatica-forense

- Concientización de Seguridad Informática.
- Red TeamTesting.
- Servicios de Penetración Caja Negra.
- Endurecimiento de Sistemas (Hardening).
- PCI Direccionamiento & Planeación.
- Remediación PCI.
- Análisis Forense.
- Evaluación Seguridad de la Red.
- Evaluación Seguridad de Aplicaciones.
- ISO 27002 GAP.
- Servicios de Capacitación[5].

### 1.1.5. Internet solutions.

**Figura 10. Internet Solutions**

[5] THE MURO GROUP INTERNATIONAL, [en línea] Santiago de Cali [consulado en diciembre de 2013] Disponible en Internet: http://www.themurogroup.com/analisis_forense.html


Internet Solutions [En línea]. Consultado el día 29 de enero de 2014. Disponible en internet: http://www.internet-solutions.com.co/emp.php.

Internet Solutions S.A.S. es reconocida nacional e internacionalmente como líder en proveer servicios en análisis forense digital, cibernético y seguridad, servicios de certificación digital y servicios de solución tecnológica que transforma los lugares de trabajo en espacios interactivos laborales y académicos.

Las soluciones tecnológicas que ofrecen llevan a cabo investigaciones informáticas exhaustivas y eficaces de cualquier tipo, incluyendo el robo de la propiedad intelectual, respuesta a incidentes, auditoría de cumplimiento y respuesta a las solicitudes de e-discovery-a la vez que se mantiene la integridad forense de los datos.

También ofrecen servicios personalizados de respuesta a incidentes, la informática forense, la presentación de pruebas, testimonios de prueba, aseguramiento de servidores, de bases de datos, diseño, ejecución, control y calificación de la estrategia de la seguridad de la información. Otro foco de servicio son los certificados digitales que autentican y validan los documentos e información virtual de las personas naturales y jurídicas, de las empresas públicas y privadas generándoles una identidad digital.

Estos servicios ayudan a sus clientes a evaluar, implementar, respaldar y mantener soluciones de seguridad de la información.

- Consultoría.

- Servicios de gestión en seguridad.
- Servicios profesionales de respuesta a incidentes y computo forense.
- Soporte técnico.
- Capacitación y formación en seguridad informática[6].

**Figura 11. Internet Solutions 2**

Internet Solutions [En línea]. Consultado el día 29 de enero de 2014. Disponible en internet: http://www.internet-solutions.com.co/serv.php

## 1.2. LIF'S A NIVEL INTERNACIONAL:

[6]INTERNET SOLUTIONS, [en línea] Santiago de Cali:[consultado en agosto de 2013] Disponible en internet: http://www.internet-solutions.com.co/qs.php

**1.2.1 Mattica en mexico y colombia.** Es una empresa que desde 2006 se dedica a las Investigaciones Digitales y casos relacionados con el uso de tecnologías informáticas en diferentes ámbitos, donde eventualmente se pueden presentar delitos cibernéticos. Con una visión vanguardista y comprometida con el país se fundó el primer Laboratorio de Investigaciones digitales en América Latina, apegado a los estándares y procedimientos de las agencias de investigación en delitos cibernéticos líderes en Estados Unidos y Europa.

El primer laboratorio de investigación de delitos informáticos en América Latina, fue creado por Andrés Velázquez; éste especialista, se presentó ante los estudiantes de la Universidad Autónoma del Estado de Hidalgo (UAEH) para dictar una conferencia acerca de los alcances de esta rama del conocimiento, señaló que los alumnos de carreras como sistemas computacionales pueden elegir esta especialidad poco aplicada y muy solicitada.

Explicó que el cómputo forense es una disciplina que va de la mano con la parte legal, pero realizada por ingenieros, para presentar pruebas que sean aceptadas y validadas para consignar a los culpables de delitos como el abuso de confianza, difamación y amenazas, hasta llegar a temas mucho más complejos como pornografía infantil y lavado de dinero, indicó el investigador.

Dijo que en Matica, 33% de las investigaciones están relacionadas con robo de propiedad intelectual, es decir que si un trabajador renuncia o es despedido de la empresa para la que labora, puede extraer material secreto de la agencia y entonces incurre en robo de propiedad intelectual.

En cualquiera de estos casos, citó, son útiles las investigaciones de cómputo forense, pues es posible presentar pruebas contundentes en casos de delitos informáticos gracias al uso de la tecnología.

El laboratorio que representa, dijo, es el primero en función como tal y asesoran al gobierno federal, trabajan con la Interpol e incluso con la Organización de las Naciones Unidas (ONU).

“La informática forense es la aplicación de técnicas científicas y analíticas a dispositivos electrónicos o tecnología, para presentar pruebas en un procedimiento

legal", es como Andrés Velázquez definió su actividad principal, a quien los estudiantes observaban y escuchaban atentos por lo novedoso de su tema[7].

### 1.2.2. Suscerte en Venezuela.

**Figura 12. Suscerte**


Suscerte [En línea]. Consultado el día 26 de marzo de 2013. Disponible en internet: http://www.vencert.gob.ve/

Es la operadora de la AC Raíz del estado venezolano, primera autoridad jerárquica dentro de la Infraestructura Nacional de Certificación Electrónica, cuya función consiste en regular y certificar las condiciones necesarias para atribuir certeza jurídica a las operaciones realizadas mediante la utilización de los mecanismos ofrecidos por proveedores de servicios de certificación electrónica.

SUSCERTE tiene a su cargo el Sistema Nacional de Gestión de Incidentes Telemáticos (VenCert), iniciativa en materia de seguridad de la información que se traduce en la implementación y operación de una importante plataforma tecnológica destinada a potenciar la ciberseguridad nacional, mediante el

[7]MATTICA,[en línea] Mexico D.F.[Consultado en agosto de 2013] Disponible en internet: www.mattica.com

monitoreo en tiempo real de los sistemas de información de la infraestructura crítica de la Nación, con el fin de actuar proactivamente hacia la detección y solución temprana de incidentes informáticos.

**Figura 13. Suscerte 2**


Suscerte [En línea]. Consultado el día 26 de marzo de 2013. Disponible en internet: http://www.vencert.gob.ve/.

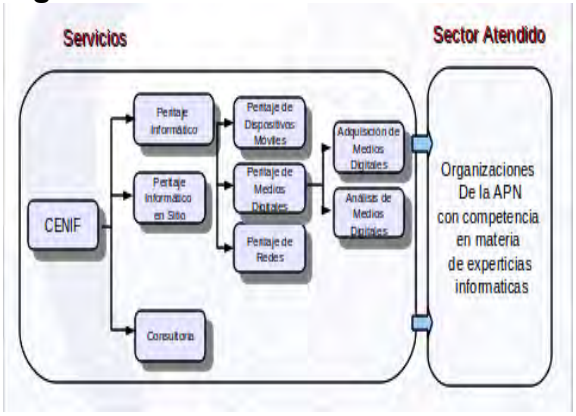
El Centro Nacional de Informática Forense (CENIF), es un laboratorio de informática forense para la adquisición, análisis, preservación y presentación de las evidencias relacionadas a las tecnologías de información y comunicación, con el objeto de prestar apoyo a los cuerpos de investigación judicial órganos y entes del Estado que así lo requieran.

También es una iniciativa de la Superintendencia de Servicios de Certificación Electrónica y producto del trabajo en conjunto de diferentes instituciones del Estado que tiene por intención conformar un modelo de servicio para el apoyo técnico de todos los cuerpos y órganos del Estado con competencia en materia de experticias digitales.

Perteneciente a la Superintendencia de Servicios de Certificación Electrónica (Suscerte), ente adscrito al Ministerio del Poder Popular para Ciencia, Tecnología e Industrias Intermedias, es un laboratorio encargado de realizar la colección, preservación, análisis y presentación de las evidencias relacionadas a las

Tecnologías de Información y Comunicación que apoya y trabaja mancomunadamente con los cuerpos de investigación judicial de nuestro país[8].

**Figura 14. Cenif**




Cenif [En línea]. Consultado el día 26 de marzo de 2013. Disponible en internet: http://www.vencert.gob.ve/

### 1.2.3. Yanapti en Bolivia.

**Figura 15. Yanapti**

[8]SUSCERTE [en linea] Caracas, Venezuela [consultado en agosto de 2013] Disponible en Internet: http://www.vencert.gob.ve/


Yanapti [En línea]. Consultado el día 26 de marzo de 2013. Disponible en internet: http://www.yanapti.com/

La idea de hacer una empresa de seguridad surgió ante la situación de no tener este campo muy desarrollado en Bolivia y estar involucrado en análisis de procesos corporativos mundiales como fue en su momento el problema Y2K. Cuando en el mundo se incursionaba en análisis, prevención y corrección de seguridad de la información, mientras que en BOLIVIA había un aletargamiento tecnológico. En ese momento para el año 1999 surgió la idea de suplir una necesidad local y una oportunidad de negocio.

Se constituye en la portada de una nueva etapa bajo el lema “asegurando su vida digital”. Convencidos que la sociedad se nutre con la diversidad de personas y no necesariamente maquinas, enfocansusservicios al lado humano de la seguridad, a ese factor humano que constantemente es considerado el débil o el culpable de la inseguridad.

### 1.2.4. Inteco en España

**Figura 16. Inteco**


Inteco [En línea]. Consultado el día 04 de junio de 2013. Disponible en internet: http://cert.inteco.es

**Figura 17.Certinteco**


Inteco [En línea]. Madrid,España [Consultado el día 04 de junio de 2013]. Disponible en internet: http://cert.inteco.es

El Instituto Nacional de Tecnologías de la Comunicación, S.A., (INTECO), sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), es la entidad de referencia para el desarrollo de la

ciberseguridad y de la confianza digital de ciudadanos y empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INTECO es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INTECO lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

INTECO-CERT, centro de respuesta a incidentes de seguridad TIC, trabaja para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad.

El Instituto Nacional de Tecnologías de la Comunicación cuenta con INTECO-CERT cuya finalidad es servir de apoyo preventivo y reactivo en materia de seguridad en tecnologías de la información y la comunicación tanto a entidades como a ciudadanos. Tiene vocación de servicio público sin ánimo de lucro y ofrece ayuda que, en todos los casos, es gratuita y de rápida gestión[9].

### 1.2.5. Fbi oficina federal de investigación en estados unidos.

**Figura 18. FBI**


FBI [En línea]. Consultado el día 04 de junio de 2013. Disponible en internet: http://www.fbi.gov

El FBI es una organización de seguridad nacional que responde a amenazas y que es regida por la recopilación e interpretación de información. Su misión es

[9]Inteco [En línea]. Madrid,España [Consultado el día 04 de junio de 2013]. Disponible en internet: http://cert.inteco.es

proteger y defender a los Estados Unidos contra amenazas terroristas y de inteligencia extranjera, defender y hacer cumplir las leyes del código penal de los Estados Unidos, y proporcionar liderazgo y servicios de justicia penal a agencias federales, estatales, municipales e internacionales, así como otros socios.

El FBI es una agencia federal de investigación e inteligencia con jurisdicción sobre una gran variedad de delitos federales, incluyendo asuntos de seguridad nacional de los Estados Unidos de Norteamérica como terrorismo y espionaje, secuestro o extravío de menores, crimen organizado, corrupción pública, y delitos cibernéticos/informáticos.

El FBI cuenta con oficinas en varias partes del mundo y puede ser contactado a cualquier hora todos los días del año. Las personas que se encuentren en peligro inminente deben llamar inmediatamente al 9-1-1 o a la policía local[10].

**1.2.6. Inif en peru.** Es un centro que brinda talleres, cursos y conferencias sobre Ethical Hacking, criptología, data recovery, ingeniera reversa, intrusiones y temas de criminología, criminalística y ciencias forenses.

El INIF tiene por funciones principales:

- Propiciar el Progreso de la especialidad en Ciencias Forenses y Criminalística.
- Promover y desarrollar la investigación científica de la criminología, la criminalística y las ciencias forenses.
- Establecer el intercambio científico, así como de las respectivas competencias laborales en el ámbito.
- Contribuir al mejor conocimiento y difusión del código de ética y deontología en el ejercicio profesional.
- Cooperar en la organización de la enseñanza y la investigación de las ciencias forenses[11].

[10]FBI [En línea]. Consultado el día 04 de junio de 2013. Disponible en internet: http://www.fbi.gov

[11] INIF [en linea] Lima, Peru [consultado en junio de 2013] Disponible en Internet: http://www.sedeforense.edu.pe/

### 1.2.7. Intrasoft en panamá.

**Figura 19. Intrasoft**


**Fuente:** Intrasoft [En línea].Consultado el día 10 de junio de 2013. Disponible en internet: http://www.intrasoftpanama.com/

Intrasoft S. A. es una empresa dedicada a la instalación y servicios de Redes e Investigación Forense de Computadoras. Recobramos información borrada, formateada y cifrados de contraseñas. Somos especialistas en soluciones que le representen al cliente un mejor retorno de su inversión en tecnología.

Esta empresa ofrece servicios de investigación forense tales como:

**Figura 20. Intrasoft 2**


Intrasoft [En línea].Consultado el día 10 de junio de 2013. Disponible en internet: http://www.intrasoftpanama.com/

- Datos 911.
- Análisis Forense.
- Peritaje.
- Soporte.

Tomando estas referencias el equipo investigador de este proyecto de grado extraerá toda la información necesaria para desarrollar su modelo para una implementación de un laboratorio de informática forense.

# 2. PROBLEMA DE INVESTIGACION

## 2.1 PLANTEAMIENTO DEL PROBLEMA

A causa del crecimiento del fenómeno de la computación han aparecido nuevas formas de delinquir, tales como la delincuencia informática, por lo cual se ve la necesidad de crear laboratorios de investigación forense que cuenten con la infraestructura y con personal capacitado para atender los incidentes que involucren medios informáticos, ya que actualmente el estado cuenta con muy pocos profesionales idóneos para estos tipo de incidentes.

Esto sumado al hecho que no existen laboratorios de entrenamiento que preparen a los investigadores de manera óptima para las situaciones que se presentan en una investigación judicial, en los cuales se recreen las posibles situaciones a experimentar.

Adicional a esto es de gran importancia garantizar el cumplimiento de procedimientos como la conservación de la evidencia digital que sea válida la evidencia, presentada ante una corte judicial, aspecto que es difícil de cumplir para la población en general si no se cuenta con el conocimiento, ni las herramientas adecuadas, ya que las evidencia se leda mal manejo se altera y se modifica.

Debido a los posibles ataques informáticos a los que se ven enfrentadas las pequeñas, medianas y grandes compañías tanto públicas como privadas, tienen la necesidad de dar respuesta a estos incidentes mediante un laboratorio de informática forense diseñado para resolver este tipo de delitos.

## 2.2 FORMULACIÓN DEL PROBLEMA

Por lo tanto, con el desarrollo de este proyecto se busca brindar respuesta a la pregunta ¿Cómo un laboratorio de Informática Forense puede responder o ayudar a esclarecer los incidentes informáticos en las organizaciones?

# 3. JUSTIFICACIÓN

En Colombia tanto la forma de hacer justicia como la forma de delinquir están evolucionando constantemente, razón por la cual es necesaria la implantación de un nuevo laboratorio de Informática forense con la capacidad de responder ante cualquier tipo de investigación en la cual se vean involucrados medios informáticos y cumpla con los requerimientos de la legislación nacional.

Por medio de este laboratorio se puede brindar a la comunidad, a las empresas y al estado el servicio forense[12] para que posteriormente sea presentada como prueba en una corte jurídica como soporte en la resolución de casos.

El desarrollo de este proyecto contribuye a un amplio reconocimiento a nivel nacional para la Universidad Autónoma de Occidente, adicional a esto, un LIF[13] desarrollado en la UAO[14] brinda el espacio para la capacitación de los estudiantes, profesores y comunidad en general, permitiendo llenar el vacío de personal idóneo para dar respuesta a los diferentes tipos de casos que se presenten, esto mejora la imparcialidad de los casos ya que permite la presencia de más de un experto forense de acuerdo con el sistema penal acusatorio el cual permite que se cuente con un experto forense para la defensa y otro para el ente acusatorio.

Con lo anterior se resalta la importancia de este proyecto, pues beneficia a la comunidad al contar con este servicio especializado y a la vez afianza el prestigio de la Universidad Autónoma de Occidente en el ámbito de la seguridad informática. Además un LIF en la Universidad Autónoma de Occidente debe verse también como un:

- Importante laboratorio de estudio y análisis de la evidencia digital, desde el punto de vista institucional.
- Sistema de servicios al sector empresarial público y privado, desde el punto de vista de la población.
- Base de conocimientos, desde el punto de vista del contenido.

[12]1 Nota de los autores: Servicio Forense se entiende como: recolección de información, análisis de esta, data carving y entrega de hallazgos.
[13]LIF: Define la sigla como Laboratorio de Informática Forense.
[14] UAO: Define la sigla como Universidad Autónoma de Occidente.

El LIF en la UAO va permitir avanzar en la respuesta a incidentes en la búsqueda de la verdad, en el análisis de la informacion residente en los dispositivos tecnológicos con los que cuenta la universidad, la poblacion estudiantil de la UAO, y la población en general.

# 4. OBJETIVOS

## 4.1 OBJETIVO GENERAL

- Diseñar e implementar un laboratorio de informática forense en la Universidad Autónoma de Occidente utilizando metodologías y estándares internacionales dentro del marco legal colombiano.

## 4.2. OBJETIVOS ESPECIFICOS

- Establecer un diseño de metodología de trabajo para un laboratorio de informática forense cumpliendo la legislación local.

- Identificar los recursos de software y hardware apropiados para la implementación.

- Implementar un modelo para el laboratorio de informática forense con amplia estructura que conlleve a la generación de nuevo conocimiento en la Universidad Autónoma de Occidente y adicionalmente por medio de este generar una formación académica idónea.

- Lograr reconocimiento en el sector educativo regional y nacional con el diseño de un laboratorio de informática forense en el cual trabaje personal capacitado para dicho fin.

# 5. MARCO REFERENCIAL

## 5.1 MARCO TEÓRICO

**5.1.1 Conceptos básicos en seguridad informática.** Para empezar con la definición de seguridad informática se debe aclarar que no es lo mismo que seguridad de la información, especialmente si se considera que el desarrollo y avance de la tecnología informática se enfoca al manejo electrónico de sistemas de información, aunque esta segunda es mucho más extensa y no se limita únicamente a medios digitales, sino al manejo los datos en cualquier entorno.
La seguridad informática se ocupa de las implementaciones técnicas y de la operación para la protección de la información, empleando el uso de antivirus, firewalls, IDS (sistemas de detección de intrusos), IPS (sistemas de prevención de intrusos), entre otros.

Esta consta de cinco pilares básicos, los cuales son:

**Confidencialidad:** la información solo puede ser accedida por las personas que tienen la autorización de hacerlo.

**Integridad:** la Información no puede ser alterada, eliminada o copiada, no solo en su trayecto, sino también en su origen.

**Disponibilidad:** la información se encuentra disponible al momento de necesitarla.

**Autenticidad:** la información y los datos son originales.

**No repudio**: asegura que el origen de una información no puede rechazar su transmisión o su contenido, y/o que el receptor de una información no puede negar su recepción o su contenido.

En la seguridad informática también se manejan los conceptos “amenaza, vulnerabilidad y riesgo”, los cuales se definen a continuación:

**Amenaza:** cualquier cosa, evento, máquina o persona que pueda causar daño al sistema a proteger.

**Vulnerabilidad**: es la falla que el sistema presenta, por donde puede ejecutarse el ataque.

**Riesgo:** es la probabilidad que el ataque sea efectivo, se presenta cuando se juntan una vulnerabilidad y una amenaza.

Un ataque se presenta cuando se materializa una amenaza, existen diferentes tipos de ataques:

**Interrupción**: Es un ataque contra la disponibilidad, busca que el sistema deje de funcionar causando un bloqueo, parada de la operación o destrucción del sistema. Ejemplo de este ataque es la destrucción de un elemento de hardware, como un disco duro, un servidor, cortar un enlace de comunicaciones o deshabilitar un sistema de bases de datos.

**Interceptación**: Es un ataque contra la confidencialidad, normalmente ocurre cuando un intruso se mete en medio de la comunicación o transmisión de la información para escuchar y tomar la información que le convenga, generalmente no causa daño a sistema.

**Generación**: Es un ataque contra la autenticidad, en este caso una entidad no autorizada inserta mensajes en el sistema o añade registros en archivos.

**Modificación**: Es un ataque contra la integridad, en este caso hay un ingreso al sistema cambiando a su gusto algunos elementos del sistema para sacar provecho de estas modificaciones.

Dichos ataques se pueden clasificar como ataques pasivos o ataques activos:

**Ataques pasivos:** En este tipo de ataques no se altera la comunicación, únicamente se escucha o controla, con el fin de obtener la información que circula por la red. Su objetivo es interceptar los datos y analizar el tráfico de la red. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos, aunque es posible evitar que se presente, haciendo uso de técnicas criptográficas, cifrando la información.

**Ataques activos:** En los ataques activos si se presenta modificación del flujo de datos transmitido, o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de Identidad**: El intruso se hace pasar por una entidad diferente, esto es posible al sustraer la contraseña de acceso a una cuenta.

- **Repetición Indeterminada**: El intruso captura uno o varios mensajes y los envía nuevamente por ejemplo ingresar dinero repetidas veces a una misma cuenta.

- **Modificación de Mensajes**: El intruso modifica una parte del mensaje o genera un reordenamiento de los mensajes, para producir un efecto no autorizado.

- **Degradación del servicio**: El intruso impide el uso normal de los recursos informáticos o de comunicaciones. El intruso puede suprimir todos los mensajes dirigidos a un determinado sitio o por el contrario puede sobresaturar de mensajes un sitio logrando con esto interrumpir el servicio[15].

## 5.2. CONCEPTOS BASICOS DE INFORMATICA FORENSE

**5.2.1 Informática forense.** Es la ciencia que se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial. Esta aplicación de técnicas y herramientas de hardware y software para determinar datos potenciales acerca de un delito ya existente.

También puede servir para informar adecuadamente al cliente acerca de las posibilidades reales de la evidencia existente o supuesta, garantizando la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información.Cualquier empresa o persona puede contratar este servicio ya que se basa en un estudio jurídico.

[15]Revista Autonoma al día [en línea] – Santiago de Cali – Octubre 2013 [consultado en noviembre 2013] disponible en internet: http://www.uao.edu.co/

Consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas.

La necesidad de este servicio se torna evidente desde el momento en que la enorme mayoría de la información generada está almacenada por medios electrónicos.

En la recuperación de información nos enfrentamos con información que no es accesible por medios convencionales, ya sea por problemas de funcionamiento del dispositivo que lo contiene, ya sea porque se borraron o corrompieron las estructuras administrativas de software del sistema de archivos. La información se perdió por un problema de fallo de la tecnología de hard y/o soft o bien por un error humano. El usuario nos indica su versión de los hechos y a menudo encontramos sobre la falla original otras que el usuario o sus prestadores técnicos agregaron en un intento de recuperación. Así es que debemos figurarnos a partir del análisis del medio qué ocurrió desde el momento en que todo funcionaba bien y la información era accesible.

En informática forense hablamos ya no sólo de recuperación de información sino de descubrimiento de información dado que no hubo necesariamente una falla del dispositivo ni un error humano sino una actividad subrepticia para borrar, adulterar u ocultar información. Es por lo tanto esperable que el mismo hecho de esta adulteración pase desapercibido.

La informática forense apela a nuestra máxima aptitud dado que enfrentamos desde casos en que el dispositivo fue borrado, golpeado y dañado físicamente hasta ligeras alteraciones de información que pueden constituir un crimen.

Este servicio es de utilidad a empresas que llevan adelante juicios laborales con sus empleados, o con sus asociados por conflictos de intereses, a estudios jurídicos que necesitan recabar información ya sea para presentarla frente a un tribunal o bien para negociar con las partes un acuerdo extrajudicial de resarcimiento, renuncia, etc. Es de utilidad a los organismos judiciales y policiales que buscan evidencias de todo tipo de crímenes. Es un componente indispensable en litigios civiles.

Las pruebas electrónicas extraídas de las computadoras fueron admitidas como prueba en un juicio desde los años 70, pero en su fase inicial las computadoras no se consideraban más que un dispositivo para almacenar y reproducir registros de papel, que constituían la evidencia real. Sus orígenes se remontan a los Estados

unidos a mediados de los años 80, los cuales respondían al incremento de crímenes relacionados con las computadoras.[16]

En el siguiente orden cronólogico se mencionan los acontecimientos más relevantes relacionados con la informática forense.

- En 1978 Florida reconoce los crímenes de sistemas informáticos en el "Computer Crimes Act", en casos de sabotaje, copyright, modificación de datos etc.
- En 1981 Nace Copy II PC de Central Point.
- En 1982 Peter Norton publica UnErase: Norton Utilities 1.0, la primera versión del conjunto de herramientas "Norton Utilities", entre las que destacan UnErase, una aplicación que permite recuperar archivos borrados accidentalmente.
- En 1984 el FBI forma el Magnetic Media Program, que más tarde, en 1991, será el Computer Analysis and Response Team (CART)
- En 1986 Clifford Stoll colabora en la detección del hacker Markus Hess.
- En 1987 se crea la High Tech Crime Investigation Association (HTCIA) y nace la compañía AccessData.
- En 1988 se crea la International Association of Computer Investigative Specialists (IACIS) una de las certificaciones más prestigiosas en el ámbito forense.
- En 1995 se funda el International Organization on Computer Evidence (IOCE).
- A partir de 1996 la Interpol organiza los International Forensic Science Symposium, como foro para debatir los avances forenses.
- En agosto de 2001 nace la Digital Forensic Research Workshop (DFRWS), un nuevo grupo de debate.[17]

[16] Tomado del documento de D. Manuel José Lucena López, del Departamento de Informática de la Universidad de Jaén.

[17] Historia de la Informatica [en linea] Santiago de Cali – Octubre 2013 [consultado en noviembre de 2013] disponible en internet http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html

De ahí en adelante han nacido nuevos estándares los cuales son aplicados a esta ciencia y se han establecido muchas firmas digitales.

El principio de intercambio de Locard se suele expresar así: "siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto". El principio ha permitido obtener indicios relevantes en numerosos lugares, desde huellas en el barro o sus restos en neumáticos y calzado, hasta huellas dactilares o restos en las uñas.

Expertos criminalistas han señalado recientemente que el llamado "Principio de intercambio de Locard", referido como tal en gran parte de la literatura criminalística y reconocido como uno de los más importantes de esta ciencia, no había sido formulado como tal por el propio Locard en su monumental obra. Locard hizo la observación "es imposible que un criminal actúe, especialmente en la tensión de la acción criminal, sin dejar rastros de su presencia"[18].

El Principio de Locard tiene plena validez en el ámbito informático y las evidencias electrónicas, hay que determinar el cómo y el dónde se pueden encontrar las evidencias, por ejemplo: determinar que quien escribió un ".doc", o quién envió un e-mail, es quien está acusado de ello.

[18] WIKIPEDIA Edmond Locard [en línea] Santiago de Cali [Consultado en enero de 2014] Disponible en internet: http://es.wikipedia.org/wiki/Edmond_Locard.

**Figura 21**. **Principio de intercambio de Locard**


**Fuente**: Principio de intercambio de Locard [En línea]. Consultado el día 08 de enero de 2014.Disponible en internet: http://www.slideshare.net/dianaprincess1/computacion-forense-17228027

A continuación se muestran dos artículos, uno del diario EL ESPECTADOR de agosto de 2013 y otro de LA FM de marzo de 2014 donde se habla del tema.
Articulo 1:

"La seguridad informática ha sido un tema que ha cobrado importancia recientemente, entre otras cosas, gracias a escándalos internacionales sobre ciberespionaje, o violaciones en la web a multinacionales. Edward Snowden, el hombre que reveló el espionaje que se llevaba a cabo en Estados Unidos a miles de sus ciudadanos, incluso fue ejemplo del uso de correos encriptados y varias maniobras para poder mantener privada cierta información.

Pese a la sonoridad de estos casos es poca la importancia que los colombianos le dan a la seguridad en la web, es por ello que varias compañías especializadas en seguridad informática han intentado divulgar cifras que alerten sobre las tácticas utilizadas para la extorsión y el robo en la web.

Las empresas colombianas están perdiendo cerca de 40 millones de dólares por estos delitos 2.0, una realidad que seguirá creciendo dado que en el último año esta modalidad aumentó del 36% al 56%, debido a que las empresas no toman las

medidas necesarias para blindarse frente a los delincuentes que ahora navegan en internet para saquear las empresas.

Según datos de la compañía Andina Digital Security en el último año cerca de 10 millones de colombianos han sido víctimas de algún delito informático. Pero la problemática va más allá, el 99.9% de las víctimas de estas modalidades delictivas no las denuncian, entendiendo así que las denuncias por esta causa no superan la cifra de 23.000, según el Colegio Colombiano de Juristas.

Estudios recientes revelan que el 77% de los colombianos (36 millones de personas) en algún momento de sus vidas han sido víctimas de delincuentes informáticos. Así laspérdidas financieras por ciberataques en los últimos doce meses ascienden a un monto de 79.180 millones de pesos.

Ante la problemática Miguel Angel Díaz, experto en seguridad y gerente de Andina Digital Security, asegura que para esta forma de delinquir, que ha aumentado de 36% a 56%, es necesario, entre otras cosas, tomar las siguientes medidas:

- No reenviar cadenas de correos electrónicos.

- Al hacer una transacción por internet asegurarse de digitar correctamente la página.

- Verificar que en las páginas de internet dónde se realicen transacciones, tengan al inicio de la dirección url, las siglas https y no solamente http, ya que estas últimas no poseen el certificado de seguridad que garantice una transacción.

- Con los teléfonos inteligentes no usar redes wi-fi para manejar datos confidenciales con los cuales el delincuente pueda suplantarnos o acceder a información confidencial.

- Las empresas deben revisar periódicamente todos sus computadores en busca de programas espía o virus que afecten el correcto funcionamiento en especial de los correos electrónicos.

- Revisar las condiciones de privacidad en todas las redes sociales y no publicar o revelar información con los que los “ciberdelincuentes” puedan identificar

datos como nuestro lugar de residencia, si salen de vacaciones o no, así como la cantidad de adquisiciones de alto valor"[19].

Articulo 2:
**"**Fiscalía inspeccionaría computador de Santos por 'chuzadas' a su correo

Fuentes de la Fiscalía General de la Nación dieron a conocer que investigadores expertos en informática evalúan realizar una inspección al computador del presidente Juan Manuel Santos en los próximos días.

Frente a la denuncia que motivó la investigación referente a una supuesta interceptación ilegal al correo del mandatario de los colombianos.

Acción que se daría para revisar ese elemento electrónico con el objetivo de establecer el origen de ese caso de denominada chuzada informática.

Cabe recordar que una delegación especial del ente acusador viajara en a México para tomar la declaración del ex ministro de defensa Fernando Botero Zea.

El objetivo de los investigadores es corroborar y establecer la autenticidad de los correos electrónicos que de dieron a conocer entre el Presidente de la República Juan Manuel Santos y Botero Zea.

En el que se habla del precio de unas obras de arte en especial sobre una negociación para obtener por parte de Santos un descuento del 20 por ciento de tres cuadros del padre del exministro el reconocido pintor Fernando Botero."[20]

Para dar solucion a este tipo de incidentes, la computación forense tiene aplicación en un amplio rango de crímenes incluido pero no limitado a:

---

[19] El Espectador, diez millones de colombianos, víctimas de delitos informáticos en el último año [En línea]. Bogotá D.C. [Consultado el día 14 de Marzo de 2014]. Disponible en internet: http://www.elespectador.com/tecnologia/diez-millones-de-colombianos-victimas-de-delitos-inform-articulo-442538.

[20] La FM, Fiscalía inspeccionaría computador de Santos por 'chuzadas' a su correo [En línea]. Bogotá D.C. [Consultado el día 14 de Marzo de 2014]. Disponible en internet: http://www.lafm.com.co/noticias/fiscalia-inspeccionaria-156288.

- Mal uso de la computadora que conlleve a pérdida de productividad de empleados (uso personal de correo electrónico, uso de internet para actividades personales o entretenimiento).

- Robo de secretos comerciales e industriales.

- Robo o destrucción de propiedad intelectual.

- Destrucción de archivos judiciales, de auditoría, etc.

La evidencia informática es frágil por definición y puede fácilmente ser alterada o modificada y así perder autenticidad frente a una corte. Se deben por lo tanto establecer rígidas normas de preservación y cadena de custodia de la misma.

Esta ciencia lo que busca es perseguir objetivos preventivos, anticipándose al posible problema u objetivos correctivos, para una solución favorable una vez que la vulneración y las infracciones ya se han producido.

Las diferentes metodologías forenses incluyen la toma segura de datos de diferentes medios digitales y evidencias digitales, sin alterar los datos de origen. Cada fuente de información se cataloga preparándola para su posterior análisis y se documenta cada prueba aportada. Las evidencias digitales recolectadas permiten elaborar un dictamen claro, conciso, fundamentado y con justificación de las hipótesis que en él se barajan a partir de las pruebas encontradas.

Para proceder ante todo el procedimiento debe hacerse tenido en cuenta los requerimientos legales para no vulnerar en ningún momento los derechos de terceros que puedan verse afectados. Ello para que, llegado el caso, las evidencias sean aceptadas por los tribunales y puedan constituir un elemento de prueba fundamental, si se plantea un litigio, para alcanzar un resultado favorable.

OBJETIVOS DE LA INFORMATICA FORENSE:

- Recolectar evidencia digital presente en toda clase de infracciones en delitos informáticos actuando en primer término como medida preventivasirviendo a la empresa para auditar mediante las diversas pruebas técnicas, esto a pesar que la función principal de la informática forense es correctiva por requerirse a posteriori de los hechos, o sea cuando se ha identificado una incidencia o

eventoque atente contra la integridad de la información y gestando un hecho punible.

- Detectar vulnerabilidades de seguridad con el fin de corregirlas.
- Detectar evidencia de la realización de los distintos delitos informáticos.
- Compensar los daños causados por los criminales o intrusos.
- Perseguir y procesar judicialmente a los criminales informáticos.
- Aplicar medidas como enfoque preventivo ante los diferentes delitos.

Cuestiones técnicas y legales de la informática forense: Para realizar un adecuado análisis de Informática forense se requiere un equipo multidisciplinar que incluya profesionales expertos en derecho de las TI y expertos técnicos en metodología forense. Todo estopara garantizar el cumplimiento tanto de los requerimientos jurídicos como los requerimientos técnicos derivados de la metodología forense.

Los usos de la informatica forense son:

- Persecución criminal.
- Litigación Civil.
- Investigación de seguros.
- Temas corporativos.
- Mantenimiento de la ley.

Comunidades que utlizan informatica forense:

- Entidades que aplican la ley.
- Fuerzas militares.
- Empresas privadas y públicas.
- Industrias y bancos.

Actividades de la computacion forense: recolección segura de los datos de un computador sin contaminar la evidencia.

Identificación de datos sospechosos y lo que se enmarca en el medio.
Toma de fotos para corroborar la evidencia.

El examen de datos sospechosos para determinar los detalles tales como origen y su contenido.

Presentación de información con base a lo encontrado en una computadora.

**Figura 22. Informática Forense**

Informatica Forense [En línea]. Consultado el día 04 de Diciembre de 2013.Disponible en internet: http://www.eltiempo.com/colombia/llano/ARTICULO-WEB-NEW_NOTA_INTERIOR-8201241.html

## 5.3. CONSERVACION DE LA EVIDENCIA DIGITAL

En el interior de un LIF se debe contar con una adecuada conservación de la evidencia digital que haga complemento con la cadena de custodia que aseguran las autoridades competentes.

**Importancia**: los delincuentes hoy están utilizando la tecnología para facilitar el cometimiento de infracciones y eludir a las autoridades. Este hecho ha creado la necesidad de que tanto la policía judicial, la fiscalía general del estado y la función judicial deba especializarse y capacitarse en estas nuevas áreas en donde las TIC

se convierten en herramientas necesarias en auxilio de la justicia y la persecución de delito y el delincuente.

La obtención de Información (elementos de convicción) se constituye en una de las facetas útiles dentro del éxito de en una investigación criminal, aspecto que demanda de los investigadores encargados de la recolección preservación, análisis y presentación de las evidencias digitales una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal Penal.

**5.3.1 Principios del análisis. Objetividad:** El experto debe ser objetivo, debe observar los códigos de ética profesional.

**Autenticidad Y Conservación**: Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios.

**Legalidad:** El experto debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de sus actividad pericial y cumplir con los requisitos establecidos por ella.

**Idoneidad:** Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso.

**Inalterabilidad:** En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados durante la pericia.

**Documentación:** Deberá establecerse por escrito los pasos dados en el procedimiento pericial.

Estos principios deben cumplirse en todas las pericias y por todos los expertos involucrados.

**5.3.2 Reconocimiento de la evidencia digital.** Es importante aclarar los conceptos y describir la terminología adecuada que señale el rol que tiene un

sistema informático dentro del *iter criminis*[21]. Con el fin de encaminar correctamente el tipo de investigación, la obtención de indicios y posteriormente los elementos probatorios necesarios para sostener un caso.

Es así que por ejemplo, el procedimiento de una investigación por homicidio que tenga relación con evidencia digital será totalmente distinto al que, se utilice en un fraude informático, por tanto el rol que cumpla el sistema informático determinara "donde debe ser ubicada" y "como debe ser usada" la evidencia.

Ahora bien, para ese propósito se han creado categorías a fin de hacer una necesaria distinción entre el elemento material de un sistema informático o hardware (evidencia electrónica) y la información contenida en este (evidencia digital). Esta distinción es útil al momento de diseñar los procedimientos adecuados para tratar cada tipo de evidencia y crear un paralelo entre una escena física del crimen y una digital. En ese contexto el hardware se refiere a todos los componentes físicos de un sistema informático, mientras que la información, se refiere a todos los datos, programas almacenados y mensajes de datos trasmitidos usando el sistema informático.

**5.3.3 Clases de equipos informáticos y electrónicos.** Algunas personas tienden a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo es necesario distinguir entre aparatos electrónicos como los celulares y PDA´s[22] y la información digital que estos contengan. Esto es indispensable ya que el foco de la investigación siempre será la evidencia digital aunque en algunos casos también serán los aparatos electrónicos.

A fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuando para su posterior recolección y preservación.

Las fuentes de evidencia digital pueden ser clasificadas en tres grande grupos:

[21] Iter Criminis: locución latina, que significa «camino del delito», utilizada en Derecho penal para referirse al proceso de desarrollo del delito.

[22] PDA: del inglés "personal digital assistant (asistente digital personal)".

- Sistemas de computación abiertos: son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles, y los servidores. Actualmente estos computadores tiene la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.

- Sistemas de comunicación: estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.

- Sistemas convergentes de computación: son los que están formados por los teléfonos celulares llamados inteligentes o Smartphones[23], los asistentes personales digitales PDA´s, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

Dada la ubicuidad[24] de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.

Ejemplos de aparatos electrónicos e informáticos:

- Computador de escritorio.

- Computador Portátil.

- Estación de Trabajo.

- Hardware de Red.

- Servidor – aparato que almacena o transfiere datos electrónico por el Internet.

- Teléfono celular.

- Teléfono inalámbrico.

[23] Smartphone: es un teléfono móvil construido sobre una plataforma informática móvil.

[24] Ubicuo: significa que esta en todas partes.

- Aparato para identificar llamadas.
- “GPS” – aparato que utiliza tecnología satélite capaz de ubicar geográficamente al persona o vehículo que lo opera.

- Video cámaras.

- Memorias flash.

- Juegos electrónicos – en su unidad de datos se puede guardar, incluso, una memoria de otro aparato.

- Sistemas en vehículos – computadoras obvias y computadoras del sistema operativo del vehículo que registra cambios en el ambiente y el mismo vehículo.

- Impresoras.

- Duplicadora de discos.

- Discos, disquetes, cintas magnéticas.

- Aparatos ilícitos – tales como los aparatos que capturan el número celular de teléfonos cercanos para después copiarlo en otros teléfonos, o los llamados sniffers, decodificadores, etc.

**5.3.4. Incautación de equipos informáticos o electrónicos.** Si el investigador presume que existe algún tipo evidencia digital en algún aparato electrónico o en algún otro soporte material relacionado con el cometimiento de una infracción, debe pedir la correspondiente autorización judicial para incautar dichos elementos, de igual forma debe tener la autorización judicial para acceder al contenido guardado, almacenado y generado por dichos aparatos.

En el momento en que la policía judicial va a realizar un allanamiento e incautación de equipos informáticos o electrónicos, esta debe tomar en cuenta lo siguiente:

- ¿En qué momento debe realizarse?, con el fin de:
    - Minimizar destrucción de equipos, datos.

- El sospechoso puede estar en línea.

- Proporcionar seguridad a los investigadores.

- Entrar sin previo aviso
    - Utilizar seguridad.
    - Evitar destrucción y alteración de los equipos, o la evidencia contenida en esta.
- Materiales previamente preparados (Conservacion de la evidencia).
    - Embalajes de papel.
    - Etiquetas.
    - Discos y disquetes vacíos.
    - Herramienta.
    - Cámara fotográfica.

- Realizar simultáneamente la obtención de la evidencia digital en diferentes sitios.
    - Los datos pueden estar en más de un lugar, sistemas de red, conexiones remotas.
- Examen de equipos.
- Aparatos no especificados por el cliente.
- Creación de Respaldos en el lugar, creación de imágenes de datos.
    - Autorización para duplicar, reproducir datos encontrados (por ejemplo, un aparato contestador).
- Fijar/grabar la escena.
    - Cámaras, videos, etiquetas.

- Códigos/claves de acceso/contraseñas.

- Buscar documentos que contienen información de acceso, conexiones en redes, etc.

- Cualquier otro tipo de consideración especial (consideraciones de la persona involucrada: médicos, abogados, información privilegiada, etc.).

**5.3.5. Qué hacer al encontrar un dispositivo informático o electrónico.** No tome los objetos sin guantes de latex, podría alterar, encubrir o hacer desaparecer las huellas dactilares o adeníticas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.

- Asegure el lugar.

- Asegure los equipos de cualquier tipo de intervención física o electrónica hecha por extraños.

- Si no está encendido, no lo encienda (para evitar el inicio de cualquier tipo de programa de autoprotección).

- Si usted cree razonablemente que el equipo informático o electrónico está destruyendo la evidencia, debe desconectarlo inmediatamente.

- Si está encendido, no lo apague inmediatamente *(para evitar la pérdida de información "volátil").*

- No use el equipo informático que está siendo investigado, ni intente buscar evidencias sin el entrenamiento adecuado.

- Si tiene un "Mouse", muévalo cada minuto para no permitir que la pantalla se cierre o se bloquee.

- Si una computadora portátil (Laptop) no se apaga cuando es removido el cable de alimentación, localice y remueva la batería, esta generalmente se encuentra debajo del equipo, y tiene un botón para liberarla, Una vez que está es removida debe guardarse en un lugar seguro y no dentro de la misma máquina, a fin de prevenir un encendido accidental.

- Si el aparato está conectado a una red, anote las direcciones de conexión, (direcciones IP).

- Fotografíe la pantalla, las conexiones y cables.

- Usar bolsas especiales antiestática para almacenar diskettes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.

- Coloque etiquetas en los cables para facilitar reconexión posteriormente.

- Tome nota de la información de los menús y los archivos activos (sin utilizar el teclado), cualquier movimiento del teclado puede borrar información importante.

- Si hay un disco, un disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retírelo, protéjalo y guárdelo en un contenedor de papel y lejos de cualquier imán o campo magnetico.

- Bloquee toda unidad de grabación con una cinta, un disco o un disquete vacío aportado por el investigador (NO DEL LUGAR DE LOS HECHOS). Al utilizar algún elemento del lugar de los hechos donde se obtiene la evidencia digital, se contamina un elemento materia de prueba con otro.

- Selle cada entrada o puerto de información con cinta de evidencia.

- De igual manera deben selle los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.

- Desconecte la fuente de poder.

- Al llevar los aparatos, tome nota de todo número de identificación que estos tengan, por medio de un formato de conservación de la evidencia.[25]

- De ser posible se debe contar con todo tipo de cable, accesorio y conexión, asi como con manuales, documentación y anotaciones.

- Se debe tener en cuenta la posibilidad de que existan otros datos importantes en sistemas periféricos, si el aparato fue conectado a una red, es necesario desconectar el cable de poder de todo hardware de Red (Router, modem, Swich, Hub).

[25] Ver anexo 6 Formatos página 66 del archivo “anexos.docx”.

- Si el equipo es una estación de trabajo o un Servidor (conectado en red) o está en un negocio, el desconectarla puede traer consecuencias negativas como:
    - Daño permanente al equipo.
    - Interrupción ilegal del giro del negocio.[26]

## 5.4 DEFINICIÓN DE CADENA DE CUSTODIA

La cadena de custodia se define como una secuencia de actos llevados a cabo por la persona experta, implicando pruebas de seguimiento que surgen en un caso desde el momento de su toma hasta que se presenta, siendo fundamental en el desarrollo de la investigación y probatorio para el control de los elementos físicos encontrados en el lugar de los hechos, tiene el propósito de garantizar la integridad, conservación e inalterabilidad de los elementos materiales de prueba, siendo un procedimiento establecido por la normatividad jurídica.

Cabe aclarar que la policía judicial y los abogados responsables son los encargados de iniciar y mantener la cadena de custodia y el LIF lo que hace es una "conservación de la evidencia".

Para asegurar un éxito en las investigaciones forenses la policía judicial debe seguir al pie de la letra el procedimiento reglamentario de la cadena de custodia de la Resolución no. 0-6394 del 22 de diciembre de 2004 que se encuentra a continuación, el cual el experto forense complementa por medio del formato de conservación de la evidencia:

**5.4.1 Marco normativo de la cadena de custodia.** Para la ejecución del proceso y los procedimientos contenidos en este manual, debe observarse la siguiente normatividad:

[26] Acurio Del Pino, marco normativo [en linea], Ecuador, 2013 [consultado en agosto de 2013]. Disponible en internet: http://www.oas.org/juridico/english/cyb_pan_manual.pdf

- Constitución Política de Colombia Artículos: 15, 29, 209, 228, 249, 250,251 y 253. (con las modificaciones introducidas por el Acto Legislativo 03de diciembre de 2002).

- Ley 30 de 1986, Por la cual se adopta el Estatuto Nacional de estupefacientes y se dictan otras disposiciones.

- Ley 99 de 1993, Por la cual se crea el Ministerio del Medio Ambiente, sereordena el Sector Público encargado de la Gestión y conservación delmedio ambiente y los recursos naturales renovables, se organiza el sistema Nacional Ambiental, SINA, y se dictan otras disposiciones.

- Ley 270 de 1996, Estatutaria de la administración de justicia, título I;artículo 153 (deberes de los funcionarios y empleados).

- Ley 397 de 1997, Por la cual se desarrollan los artículos 70, 71 y 72 ydemás artículos concordantes de la Constitución Política y se dictannormas sobre patrimonio cultural, fomentos y estímulos a la cultura, secrea el Ministerio de la Cultura y se trasladan algunas dependencias.

- Ley 418 de 1997, Por la cual se consagran unos instrumentos para labúsqueda de la convivencia, la eficacia de la justicia y se dictan otrasdisposiciones.

- Ley 600 de 2000 (Código de Procedimiento Penal), artículos 27, 232, 233, 241, 244, 245, 249, 251, 254, 255, 256, 257, 288, 289, 290, 314, 315,317, 318, 319, 320, 321, 329, 345 y demás concordantes.

- Ley 906 de 2004 (Código de Procedimiento Penal), artículos 67, 114, 208,213, 214, 215, 216, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263,264, 265, 266, 268, 276, 277, 278, 279, 280, 281, 484, 485.

- Ley 489 de 1998, por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden lasdisposiciones, principios y reglas generales para el ejercicio de lasatribuciones previstas en los numerales 15 y 16 del artículo 189 de laConstitución Política y se dictan otras disposiciones.

- Ley 678 de 2001, por medio de la cual se reglamenta la determinación deresponsabilidad patrimonial de los agentes del Estado a través delejercicio de la acción de repetición o de llamamiento en garantía con finesde repetición.

- Decreto 2811 de 1974, por el cual se adopta el Código Nacional de Recursos Naturales Renovables.

- Decreto 786 de 1990, por el cual se reglamenta la práctica de autopsiasen el territorio nacional.

- Decreto 300 de 1993, Por el cual se establecen unas obligaciones paralos Distribuidores Mayoristas, Distribuidores Minoristas y Transportadoresde Combustibles Blancos derivados del Petróleo.

- Decreto 2113 de 1993, Por el cual se modifica y adiciona algunosartículos del Decreto 300 de 1993.

- Decreto 1503 de 2002, por el cual se reglamenta la marcación de loscombustibles líquidos derivados del petróleo en los procesos dealmacenamiento, manejo, transporte y distribución".

- Decreto 1521 de 1998, por la cual se consagran unos instrumentos parala búsqueda de la convivencia, la eficacia de la justicia y se dictan otrasdisposiciones.

- Decreto 261 de 2000, por el cual se modifica la estructura de la Fiscalía General de la Nación y se dictan otras disposiciones.

- Decreto 2535 de 1993, por el cual se expiden normas sobre armas, municiones y explosivos.

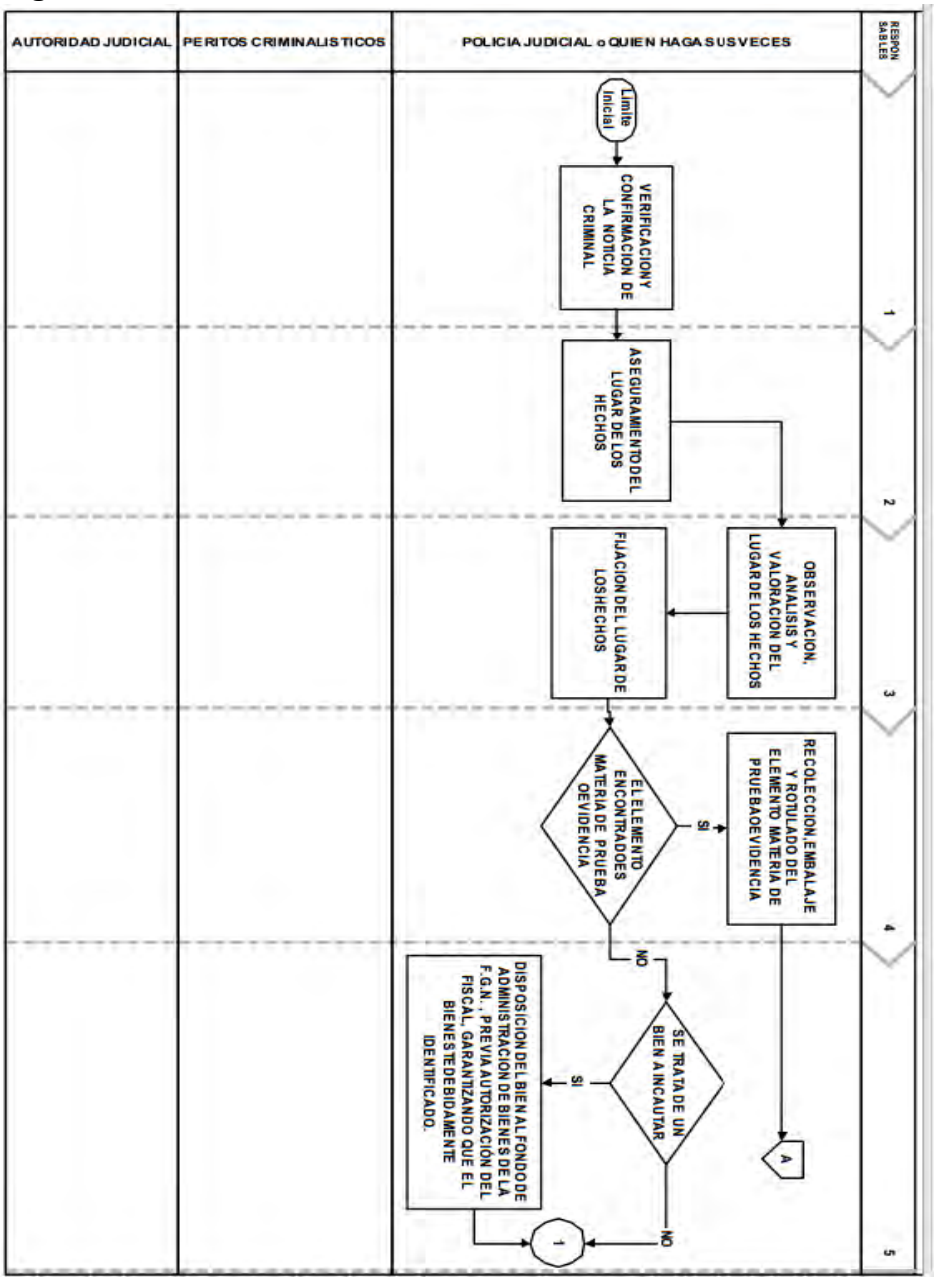
- Acuerdo 002 de 1999 del Consejo Nacional de Policía Judicial, mediante el cual se adopta el manual de procedimientos para la prueba de identificación homologada de sustancias sometidas a fiscalización.

- Resolución 0-0646, del 31 de mayo de 2001, de la Fiscalía General de la Nación, por medio de la cual se fijan las directrices para la ejecución de programas de mejoramiento institucional, oficialización de manuales de procesos y procedimientos administrativos, operativos y de funciones y en general sobre todo lo relacionado con el desarrollo organizacional de la Fiscalía General de la Nación.

- Resolución 1890, de noviembre 5 de 2002, de la Fiscalía General de la Nación, por medio de la cual se reglamenta el artículo 288 de la Ley 600 de 2001. - Resolución 0-2869 de diciembre 29 de 2003, de la Fiscalía General de la Nación, por medio de la cual se adoptó el manual de procedimientos de cadena de custodia.

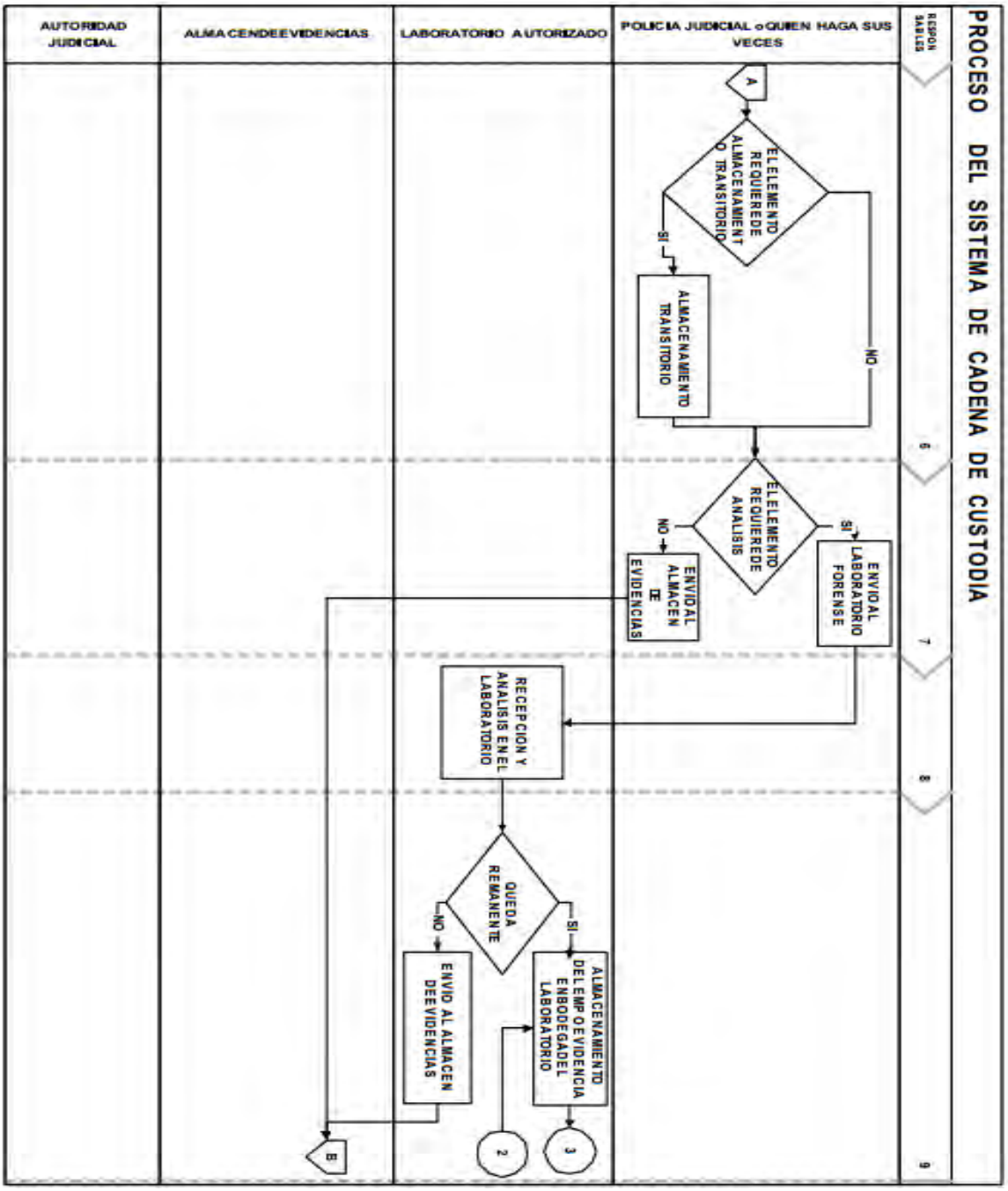
### 5.4.1.1 Diagrama del proceso del sistema de conservacion de la evidencia del laboratorio uao (alineado a la cadena de custodia).

**Figura 23. Conservacion de la evidencia 1**



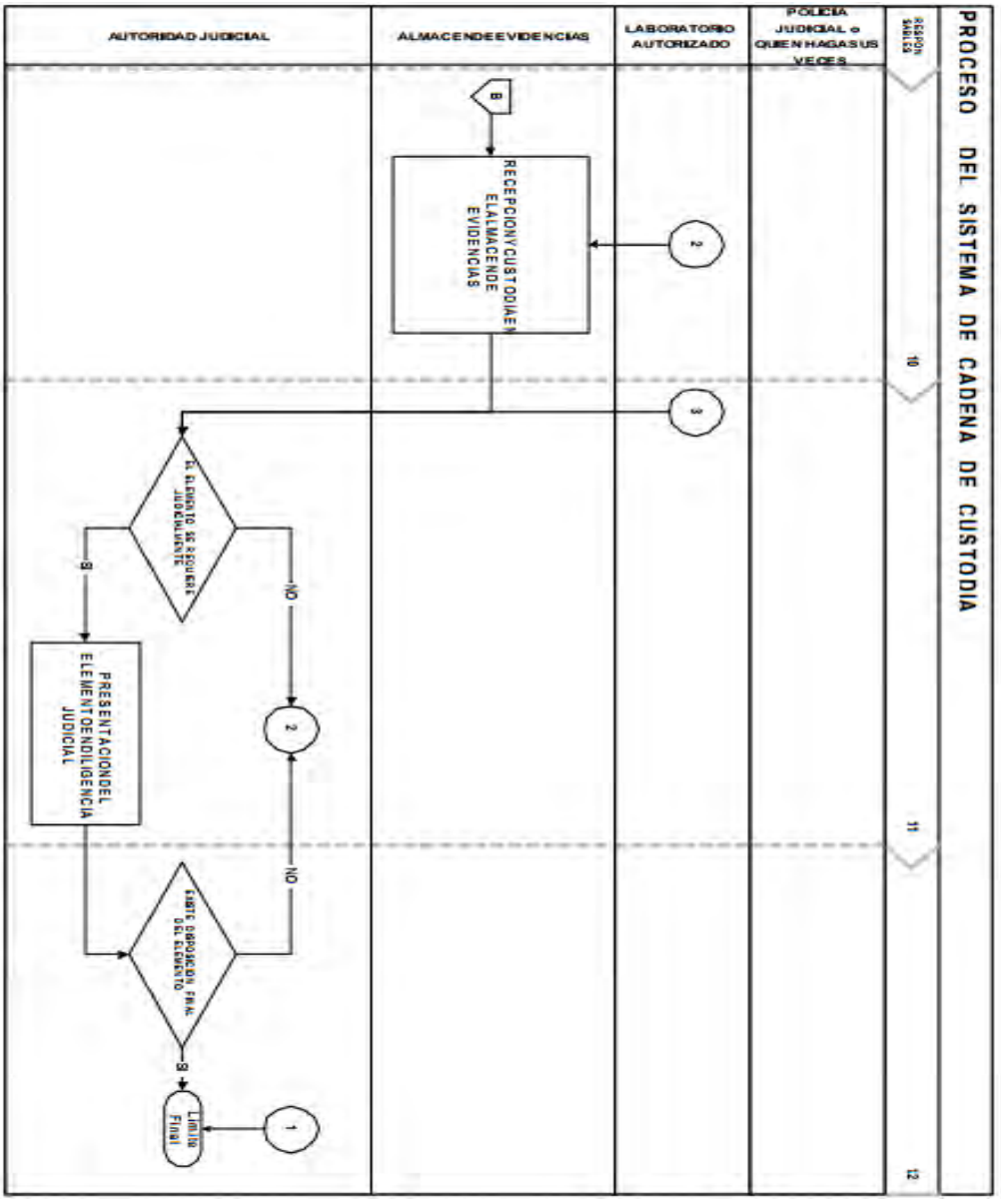

Marco normativo [En línea]. Consultado el día 22 de Septiembre de 2013. Disponible en internet: http://www.usergioarboleda.edu.co/derecho_penal/pdf/2004-MANUAL%20CADENA%20DE%20CUSTODIA.pdf PAG.19

**Figura 24. Conservacion de la evidencia 2**



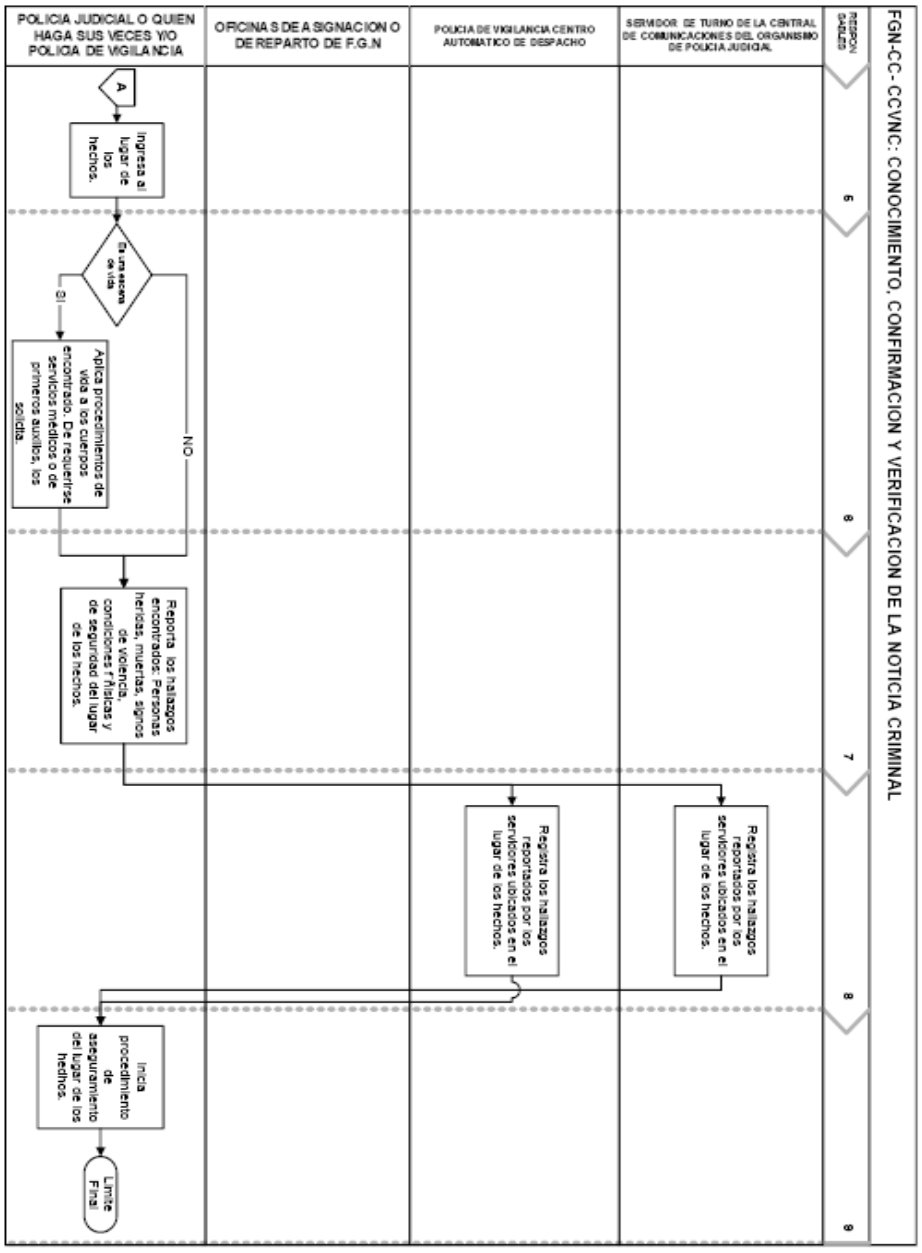

Marco normativo [En línea]. Consultado el día 22 de Septiembre de 2013. Disponible en internet: http://www.usergioarboleda.edu.co/derecho_penal/pdf/2004-MANUAL%20CADENA%20DE%20CUSTODIA.pdfPAG.19

**Figura 25. Conservacion de la evidencia 3**




Marco normativo [En línea]. Consultado el día 22 de Septiembre de 2013. Disponible en internet: http://www.usergioarboleda.edu.co/derecho_penal/pdf/2004-MANUAL%20CADENA%20DE%20CUSTODIA.pdfPAG.21

**Figura 26. Conocimiento, confirmación y verificación del Incidente UAO**




Marco normativo [En línea]. Consultado el día 22 de Septiembre de 2013. Disponible en internet: http://www.usergioarboleda.edu.co/derecho_penal/pdf/2004-MANUAL%20CADENA%20DE%20CUSTODIA.pdfPAG.29

## 5.5 SISTEMAS DE ARCHIVOS

Un sistema de archivos es el componente del sistema operativo por medio del cual este administra el uso de memorias periféricas como discos duros, memorysticks, entre otros. Sus funciones son:

- Asignación de espacio de archivos.
- Administración del espacio libre.
- Administración del acceso a los datos resguardados.

Un sistema de archivos estructura la información guardada en un medio de almacenamiento para permitir que el gestor de archivos la muestre de manera gráfica.

Por lo general cada sistema operativo cuenta con su propio sistema de archivos, por ejemplo los sistemas operativos Windows tienen los sistemas de archivos NTFS FAT y EXFAT, los sistemas operativos LINUX cuentan con los sistemas de archivos EXT2, EXT3, EXT4, JFS entre otros, el sistema operativo SOLARIS cuenta con el sistema de archivos ZFS y UFS y así dependiendo de cada sistema operativo[27].

Conocer los diferentes tipos de archivos es importante dado que la estructura de estos permite recuperar información aparentemente borrada pero que en realidad se encuentra todavía en sectores del disco duro[28], de esta manera se puede hallar evidencia importante, además, en algunos sistemas de archivos también se permite "ocultar archivos" dentro de otros[29], y el experto debe estar en capacidad de poder analizar la información independientemente de que tipo de sistema de archivos se esté utilizando.

[27] Wikipedia, Sistemas de archivos [em linea] Santiago de Cali: 2014 [consultado el 12 de marzo de 2014] Disponible en internet: http://es.wikipedia.org/wiki/Sistema_de_archivos.

[28] A esto se le denomina "borrado lógico".

[29] A esta propiedad se le llama "Esteganografia".

**Figura 27. Sistemas de archivos**

Sistema de archivos [En línea]. Consultado el día 15 de noviembre de 2013. Disponible en internet: http://es.wikipedia.org/wiki/Sistema_de_archivos.

Para el análisis de estos sistemas de archivos existen herramientas de software como ENCASE y FTK, las cuales se utilizan a nivel mundial para el analisis forense a equipos informaticos, dichas herramientas permiten la visualizacion de todos los archivos que se encuentran en el elemento de material probatorio, facilitan la elaboración de reportes, permiten clasificar los hallazgos y cumplen con los parámetros internacionales en cuanto a metodos y guias para el tratamiento de la información, dichas herramientas se mencionan con mas detalle en el capitulo “7.2 Adquisiciones” de este documento.

# 6. METODOLOGÍA

Para el desarrollo de este proyecto se utilizó el método de investigación de análisis, este es un proceso mediante el cual se relacionan cada una de las partes aparentemente aisladas que caracterizan una realidad y se formula una teoría que unifica los diversos elementos.

Esto conlleva a establecer la relación de estos diferentes elementos dispersos en una nueva totalidad la cual para este caso es el laboratorio de informática forense.
Los diferentes elementos que se tomaron para este caso son:

- Herramientas de software.
- Herramientas de Hardware.
- Marco legal colombiano.
- Antecedentes nacionales e internacionales de laboratorios creados.
- Riesgos posibles de un LIF.
- Habilidades necesarias para el personal que labore en el LIF.
- Entrevistas a diferentes personas encargadas de laboratorios existentes.
- Aspectos sociales, operativos, financieros y de mercado.

Se escogió este método debido a que el equipo investigador no tiene control sobre variables como la legislación, el manejo de la evidencia, pero en cambio existen puntos que son intrínsecamente manipulables, tales como las herramientas de software a utilizar, razón por la cual fue necesario realizar una relación causa efecto entre diferentes situaciones para de esa manera empezar a darle forma al LIF.

# 7. DESARROLLO

La implementación de un LIF en la Universidad Autónoma de Occidente debe garantizar que los datos que entrega el usuario serán protegidos siempre llevando un adecuado manejo y conservación de la evidencia digital.

En la adquisición de recursos de hardware y software, se debe tener un solo proveedor que suministre tales equipos para de esta forma tener unanimidad en cuanto a garantías, suministro, instalación, capacitación y mantenimiento.

En la adquisición de software se debe tener en cuenta que para este proyecto se estudia la posibilidad de comprar la herramienta ENCASE[30]o la herramienta FTK[31] además de la herramienta UFED 4PC o XRY[32] (para el análisis a equipos móviles) debido al gran reconocimiento de ambas en el medio y respaldo por sus respectivas casas desarrolladoras de software, aunque cabe aclarar que también existen muchas otras herramientas que se pueden encontrar en internet de manera gratuitalas cuales se verán más a fondo en los subcapítulos siguientes y forman parte del toolbox[33] del investigador forense,con los cuales se obtiene la garantía en cuanto a la veracidad y fácil interpretación de la evidencia hallada ante una corte judicial.

Este laboratorio puede emplear tres formas para la recolección de la evidencia: una forma es de manera remota enviando la imagen de la evidencia por internet a un servidor localizado físicamente en el laboratorio para posteriormente ser trabajada, la segunda forma es tomar el material probatorio y trasportarlo al laboratorio para su posterior tratamiento, siguiendo los pasos del formato de conservación de la evidencia digital, la tercera es realizar la copia bit a bit de la evidencia in situ y llevar esta copia al laboratorio para su respectivo análisis.

[30]ENCASE, software desarrollado por la firma Guidance software, altamente reconocido en el mercado.

[31] FTK, software desarrollado por la firma AccessData, es una herramienta de fácil manejo y muy completa para llevar a cabo las investigaciones de tipo forense.

[32] UFED 4PC o XRY, herramientas de software desarrolladas para el analiis a dispositivos móviles.

[33]Toolbox (caja de herramientas): conjunto de herramientas del perito forense

Es de suma importancia tener en cuenta que un proceso de obtención de la imagen mal elaborada causa una violación del debido proceso[34] atentando contra la integridad de cadena de custodia y convirtiendo en no fehaciente al material probatorio en un proceso judicial.

Para conocer el costo de un análisis forense se deben considerar los siguientes parámetros:

- Qué tipo de equipo se va a analizar.
- Capacidad del disco.
- Desplazamiento de los expertos forenses.
- Sistema operativo que usa el equipo a analizar.
- Tipo de entidad a la que se prestara el servicio (privada o estatal) por los diferentes lineamientos a seguir.
- Tipo de delito a investigar.
- Tiempo que transcurre entre el delito y el inicio de la investigación.
- Tiempo que requiere la investigación.
- Recursos que implica realizar la investigación.
- Objetivos forenses a lograr.
- Cantidad de equipos a tomar como elementos de material probatorio.

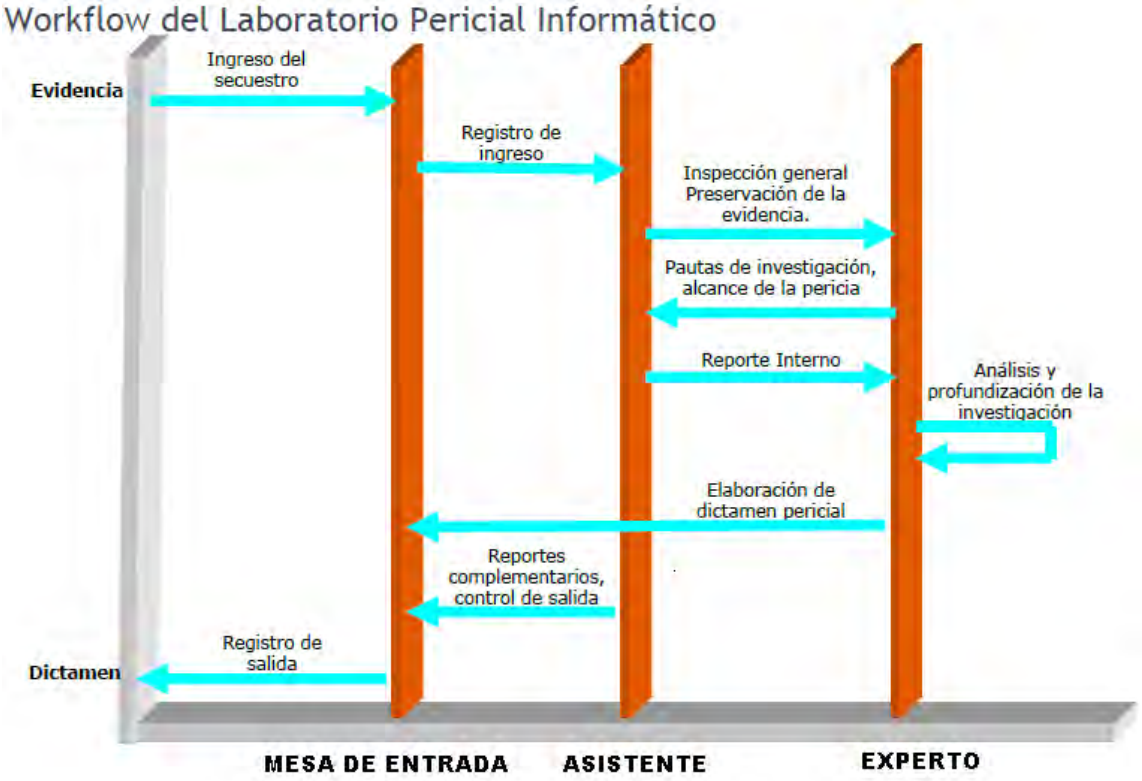
Se debe tener en cuenta que según datos obtenidos de otros LIF's, la frecuencia de casos es de tres por mes, de las cuales en su mayoría son para estaciones de trabajo en vez de servidores y/o equipos móviles.

## 7.1. ORGANIZACIÓN INTERNA DEL LABORATORIO

[34] Se entiende por debido proceso a lo requerido para la adecuada conservación de la evidencia.

A continuacion se muestra una grafica de como es el flujo de trabajo en un laboratorio de informatica forense:

**Figura 28. Workflow de un LIF**




Workflow de un laboratorio forense [En línea].Consultado el día 15 de Noviembre de 2013. Disponible en internet: http://www.neuquen.gov.ar/seguridadinformatica/pdf/Informatica%20Forense%20-%20Hernan%20Herrera.pdf

El laboratorio de informática forense debe estar diseñado de tal manera que facilite cada uno de los pasos de la conservación de la evidencia, para lo cual se analiza paso a paso lo que habla la Ley 600 de 2000, artículo 288, reglamentado a través de la resolución 1890 de 2002 y la Ley 906 de 2004 en su Capítulo V (legislación colombiana), dichos pasos son los que se nombran a continuación junto a los implementos necesarios para poderlos llevar a cabo:

**Figura 29. Diagrama de proceso para investigación forense**


**7.1.1. Recepción del material probatorio.** Se debe asegurar que los elementos de material probatorio no tengan medios de almacenamiento de ningun tipo en su interior, ademas todas las unidades se deben cubrir con cinta y revisar minuciosamente, si la evidencia es recolectada y embalada por otra persona ajena al LIF, se debe validar que se lleva a cabo el debido proceso, en caso contrario no se puede recibir el elemento de material probatorio, además es necesario contar con una guia para la recoleccion de evidencias, la cual se debe socializar a toda la comunidad de la UAO para de esa manera preparar a todo el personal (tanto de planta como estudiantes) para el manejo de la evidencia, ya que este puede variar por aspectos tales como “si el equipo está encendido” o “apagado”, por otro lado si el personal del LIF va a recolectar la evidencia debe contar con herramientas para embalaje del material probatorio, tales como:

Formatos de registro (los cuales se pueden ver en los anexos de este documento).

**Guantes de látex:** para no contaminar la escena del crimen.

**Figura 30. Guantes de látex**


Guantes de Látex [En línea].Consultado el día 12 de Diciembre de 2013. Disponible en internet: http://www.elitienda.com/es/guantes-latex-vinilo/77-guantes-de-latex.html

**Bata de laboratorio**: protección biológica del personal.

**Cinta de señalización de la evidencia**.

**Figura 31. Cinta**


Cinta [En línea].Consultado el día 12 de Diciembre de 2013. Disponible en internet: http://liristatiana.blogspot.com/

**Regla:** necesaria para medir la evidencia, cuando se va a tomar este registro el experto debe hacer uso de manilla antiestatica y guantes para protegerse a si mismo y a la evidencia.

**Placas para enumeración de la evidencia:** necesarias para clasificar y organizar los elementos de material probatorio.

**Figura 32. Numeración de cada evidencia.**


**7.1.2. Registro del ingreso.** Equipo de oficina, papel (para los formatos que se deben diligenciar, anexos a este documento).

**7.1.3. Inspección general, preservación de la evidencia.** Contenedores de evidencia: para este fin el LIF requiere un inventario de bolsas antiestáticas y de espuma.

También se debe tener en cuenta el uso de manillas antiestática para no afectar la evidencia dañándola por medio de la estatica.

**Figura 33. Preservación de la evidencia**

Bolsa anti estática [En línea].Consultado el día 05 de Enero de 2014. Disponible en internet: http://www.corma.com.mx/600181-bolsa-anti-estatica-scc1000-con-cierre-tipo-zip-lock

**7.1.4. Análisis y profundización de la investigación.** Para esta labor se requiere 1 estación forense, 1 estación de trabajo forense portátil, 1 kit de bloqueadores, software para la adquisición y criptoanálisis, medios de almacenamiento de evidencias, 1 unidad duplicadora especializada para duplicar y clonar discos, los cuales se verán a más detalle en los próximos capítulos.

## 7.2. ADQUISICIONES

A continuación se da una lista de todos los productos disponibles en el mercado tanto software como hardware necesarios para la implementación de un laboratorio de informática forense:

- 1 equipo portable forense.
- 1 equipo fijo forense.

- Por cada computador licencia de cada uno de los programas instalados para el análisis forense para este caso (ENCASE O FTK).

- Dispositivos de almacenamiento.

- 1 equipo de campo (portátil).

- Bloqueadores de disco para diferentes conexiones porque no se saben los discos que resulten en el análisis. (hay que tener en cuenta las clases de conectores).

**7.2.1 Adquisiciones de software.** A continuación se muestran las descripciones de las diferentes herramientas de software que hay en el mercado (tanto gratuitas como licenciadas), Lo que se recomienda tener para la implementación de este proyecto es el software FTK o ENCASE, ya que al ser licenciados proporcionan una mayor confianza ante una corte.

**FTK** (Forensic toolkit) es una plataforma de investigaciones digitales aprobada por tribunales, que está diseñada para ser veloz, analítica y contar con escalabilidad de clase empresarial. Conocida por su interfaz intuitiva, el análisis de correo electrónico, las vistas personalizadas de datos y su estabilidad, FTK establece el marco para una expansión sin problemas, por lo que su solución de informática forense puede crecer de acuerdo a las necesidades de su organización.

Adicionalmente, AccessData ofrece nuevos módulos de expansión, entregando el primer software de esta industria con capacidad de análisis y con visualización de última generación. Estos módulos se integran con FTK para crear la plataforma de informática forense más completa en el mercado.

Dentro el desarrollo de este proyecto se logró realizar una práctica de laboratorio en las instalaciones de la UAO para un curso de especialización de seguridad informática del módulo de Informática forense de forma real con la herramienta FTK donde hay capturas de pantalla de noviembre de 2013[35].

[35]Ver anexo 1 página 4 del archivo “anexos.docx”.

**ENCASE** (EncaseForensic) es una herramienta usada investigación digital por los profesionales forenses que necesitan llevar a cabo la recolección eficiente de datos y las investigaciones mediante un proceso repetible y defendible.

Según la pagina web http://www.encase.com/products/Pages/encase-forensic/overview.aspx se describe la herramienta de la siguiente manera:

Objetivo del software: Proporcionar a los examinadores la mayor eficiencia, potencia y resultados. Este software es aceptado por las cortes y permite:

- Adquirir datos de la más amplia variedad de dispositivos.
- Mostrar las posibles pruebas con el análisis forense a nivel de disco.
- Producir informes detallados sobre lod hallazgos realizados.
- Mantener la integridad de la evidencia en un formato de confianza ante los tribunales.

Los beneficios que tiene la herramienta es buscar, analizar e informar sobre las posibles pruebas de manera rápida además de adquirir y analizar los datos en una amplia variedad de ordenadores, teléfonos inteligentes y tabletas, descubre las pruebas potencialespormediode búsqueda avanzadas, aumenta la productividad mediante la pre visualización de los resultados a medida que se adquiere datos, una vez que se crean los archivos de imagen, se puede buscar y analizar varias unidades o los medios de comunicación de forma simultánea.

Adicional a eso permite preservar la integridad de la evidencia con la creación de imágenes de discos en los formatos L01 y E01.

**SECURE VIEW 3** herramienta desarrollada por la firma Susteen, la cual permite realizarle análisis forense a dispositivos móviles como Iphone, Android, Blackberry, entre otros.

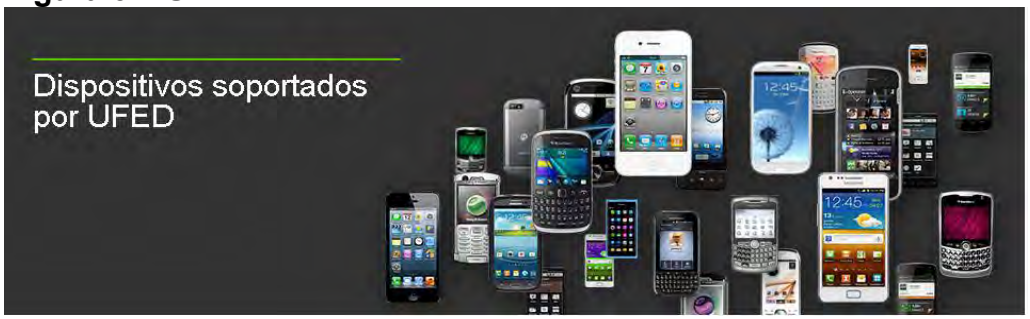
Las siguientes son otras herramientas de software existentes, que para este proyecto solo sirvieron como referente, ya que las más viables son las dos primeras ya mencionadas.

**CERBERUS** es una tecnología de clasificación de malware que está disponible como accesorio para FTK 4. El primer pasó hacia la ingeniería inversa automatizada. Cerberus califica las amenazas y hace un análisis de desmontaje para determinar tanto el comportamiento como la intención de binarios sospechosos.

Visualización**:** Vista de datos en varios formatos, incluyendo líneas de tiempo, gráficas de clúster, gráficas circulares y más. Permite determinar rápidamente las relaciones en los datos, encontrar piezas claves de información y generar informes de fácil comprensión por los abogados, los Oficiales de Información (CIOs) u otros investigadores.

**Adquisición para equipos móviles:** Las 2 herramientas más utilizadas y robustas los cuales cubren a totalidad las gamas de equipos moviles son (UFED 4PC Y XRY):

**Figura 34. UFED 4PC**




UFED 4PC [En línea]. Consultado el día 08 de abril de 2014. Disponible en internet: http://www.tynmagazine.com/373638-Cellebrite-amplia-su-linea-de-soluciones-forenses-moviles-con-UFED.note.aspx

**UFED 4PC** es la solución de software de análisis forense de dispositivos móviles de Cellebrite, el cual está diseñado para entidades que requieren extracción lógica, económica rápida y simplificada para analizar datos probatorios de una amplia variedad de dispositivos móviles como (teléfonos antiguos, comunes, inteligentes tablets entre otros). La ventaja es que puede instalarse en cualquier PC basada en Windows, también brinda las herramientas necesarias para extraer rápidamente los datos de una memoria SIM y de la memoria del teléfono en forma adecuada[36].

[36] CELLEBRITE [en linea], Petah Tikva, Israel, [consultado en agosto de 2013] Disponible en internet: http://www.cellebrite.com/es/mobile-forensics/products/pc-based/ufed-4pc-logicall

Están disponibles en dos versiones:

- UFED 4PC Logical (el cual se utiliza para datos lógicos y extracciones de contraseñas).

- UFED 4PC Ultimate (el cual se utiliza para sistema de archivos tanto lógico como físico y permite la extracción de datos clave en profundidad).

**Figura 35. XRY**

XRY [En línea]. Consultado el día 08 de abril de 2014. Disponible en internet: http://www.msab.com/xry/xry-complete

**XRY** COMPLETE es el sistema integral de análisis forenses de móviles de Micro Systemation; una combinación de nuestras dos soluciones lógicas y físicas en un solo paquete. XRY completa permite a los investigadores el acceso completo a todos los métodos posibles para recuperar los datos desde un dispositivo móvil.

XRY es un software que se diseño especialmente para análisis forense móvil basado en Windows, que incluye todo el hardware necesario para la recuperación de datos de los dispositivos móviles, de una manera segura en el ámbito forense. Con XRY Complete puede lograr más y profundizar en un dispositivo móvil al detalle para recuperar datos vitales. Con una combinación de herramientas de análisis lógicos y físicos disponibles para los dispositivos compatibles; XRY complete puede crear informes combinados los cuales pueden contener datos actuales y eliminados de que proceden de la misma terminal[37].

[37]Tomado de http://www.msab.com/xry/xry-complete

Especificaciones:

- Requisitos del pc.
- Procesador Intel - Atom 1.33 GHz, 1 GB de RAM, 2 puertos USB como minimo.
- Requisitos del sistema operativo.
- Microsoft Windows 7, vista, XP SP3 (solo sistemas de 32 bits).
- Requisitos de potencia.
- AC 100 – 240 V | 50 – 60 Hz.

**FTK IMAGER** Permite montar: Prácticamente todo tipo de formatos de imagen forenses habituales, como Encase, SnapBack, Safeback, ExpertWitness, Linux DD, ICS, Ghost, SMART, AccessDataLogicalImage y AdvancedForensicsFormat (AFF), con un soporte muy extenso para sistemas de ficheros de unidades ópticas, discos duros cifrados y sistemas de fichero de disco.
Ventajas: Sin coste, es una *suite* forense completa que permite realizar diversas operaciones de análisis, incluyendo la captura en vivo de la memoria del sistema en ejecución.

Desventajas: Ninguna digna de reseña

**PRODISCOVER BASIC** Costo: Existe una versión de pago (1495 USD en adelante) y una versión básica gratuita.

Permite montar: No es una herramienta de montaje de imágenes.

Ventajas: Aunque no permite el montaje directo de imágenes, permite abrir los ficheros forenses habituales para trabajar con ellos. Adicionalmente, tiene incorporadas herramientas para la conversión de imágenes que permite, entre otras, lanzar imágenes DD en VMware. Es una *suite* forense completa que posibilita operaciones de análisis.

Desventajas: No permite el montaje de imágenes en unidades lógicas

URL: http://www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14

**P2 EXPLORER PRO** Costo: Existe una versión de pago (199 USD) y una versión gratuita.

Permite montar: Paraben's Forensic Replicator, Paraben's Forensic storage containers, Encase 4-5-6, Safeback, RAW, DD, FTK Encase, FTK DD y FTK SMART.

Ventajas: Es tremendamente versátil en cuanto a imágenes que pueden ser montadas, soportando prácticamente todos los formatos usuales. La versión de pago tiene un coste asumible.

Desventajas: La versión gratuita no soporta integración con VMware
URL: http://www.paraben.com/p2-explorer-pro.html

**MOUNT IMAGE PRO** Costo: 300 USD, versión de prueba disponible este software permite montar: EnCase .E01, .L01, Access Data FTK .E01, .AD1, Unix/Linux DD, RAW, Forensic File Format .AFF, SMART, ISO, VMWare, ProDiscover, Microsoft VHD, Apple DMG.

Ventajas: Es un producto forense profesional, sencillo de utilizar, y soporta una enorme variedad de formatos de imagen, incluido VMware, y permite generar una unidad lógica en sólo lectura para acceder cómodamente a los contenidos de la imagen.

**DAEMONTOOLS** Costo: Existen distintas versiones de pago y una gratuita, el software permite montar: Prácticamente todo tipo de formatos de imagen de medios ópticos (ISO, NRG, B5T, B6T, BWT, CCD, CDI, CUE, ISZ).

Ventajas: Sencilla de utilizar, soporta una enorme variedad de formatos de imagen para medios ópticos. Los costes de las licencias no gratuitas son pequeños y asumibles.

Desventajas: La funcionalidad de la versión de pago supera a la gratuita en dos aspectos fundamentales: ni permite montar medios en el sistema de archivos, ni

se permite la conversión de imágenes.URL: http://www.daemon-tools.cc/eng/downloads

GIZMO DRIVE Costo: Gratuita.Permite montar: ISO, VHD, IMG, BIN, CUE, CCD, NRG, MDS, MDF, GDRIVE.

Ventajas: Es gratuita y forma parte de una *suite* con otros productos interesantes
Desventajas: No es una herramienta forense, con lo que no soporta RAW ni DD, así como otros formatos forenses habituales. Otros productos tienen más compatibilidad y soportan más formatos, incluso en su área de especialidad URL: http://arainia.com/software/gizmo/overview.php?nID=4.

Debido a que la mayoría de este software es pago licenciado, con algunas demos disponibles o trial, se esta evaluando la opción de usar la herramienta gratuita "Backtrack". En caso de no aprobarse un presupuesto alto para esta inversión, con la desventaja de no contar con soporte técnico del fabricante, esta decisión depende del sponsor del proyecto.

BACKTRACK: Backtrack[38] es una herramienta de software gratuita, la cual cuenta con las siguientes características:

- Levantamiento de información (Data carving).
- Análisis forense.
- Adquisición de la imagen.

[38]Backtrack [en linea]: Santiago de Cali, [consultado en agosto de 2013] Disponible en internet:http://www.backtrack-linux.org/

**Figura 36. Backtrack**


Backtrack [En línea].Consultado el día 20 de mayo de 2013.Disponible en internet: http://www.backtrack-linux.org/

Debido a que es software libre no es tan sencillo de operar y requiere cierta experiencia del analista forense.

**7.2.2. Adquisiciones de hardware.** FRED (FORENSIC RECOVERY OF EVIDENCE DEVICE) - ESTACION FORENSE Este equipo es de vital importancia para el desarrollo de este proyecto, ya que esta es la herramienta para hacer todos los procedimientos del análisis forense, tales como duplicados de discos, cargar imágenes, analizar evidencia y generar informes.

**Figura 37. FRED-SR**


FRED SR [En línea].Consultado el día 10 de junio de 2013. Disponible en internet: http://www.digitalintelligence.com/products/fredsr/

**Valor:** US$14.999

**Procesador:** Dual QuadCoreXeon

**Memoria RAM:** desde 32GB hasta 64GB

**Base de datos (Para imágenes, índice, etc.):** cuenta con 160GB dedicados a PostgresSQL.

**Sistema operativo:** Windows 7-64bits

- FRED L – ESTACION FORENSE PORTATIL Este equipo es importante al momento de llevar a cabo un análisis de tipo forense que requiera desplazamiento de toda la herramienta de trabajo al lugar del crimen.

**Figura 38.FRED L**

FRED L [En línea].Consultado el día 10 de junio de 2013. Disponible en internet: http://www.digitalintelligence.com/products/fredl/

**Procesador:** Intel Core i7-4800MQ QuadCore, 2.7 GHz, 6MB L3 Cache

**Memoria RAM:** 8GB.

**Disco duro:** 256GB, disco de estado solido.

**Sistema operativo:** Windows 7-64bits.

Incluye el kit de bloqueadores de escritura.

- ULTRAKIT III

**Figura 39. ULTRAKIT**


Ultrakit [En línea].Consultado el día 10 de junio de 2013. Disponible en internet: http://www.digitalintelligence.com/products/ultrakit/

**7.2.2.1 Medios de almacenamiento.** Se debe contar una capacidad de almacenamiento entre 20Gb para PC´s y 50 Tb para servidores, ese espacio siempre debe estar disponible para los casos, estos pueden estar en arreglos de discos duros, o en servidores.

## Cuadro 1. Comparativo entre estaciones de trabajo

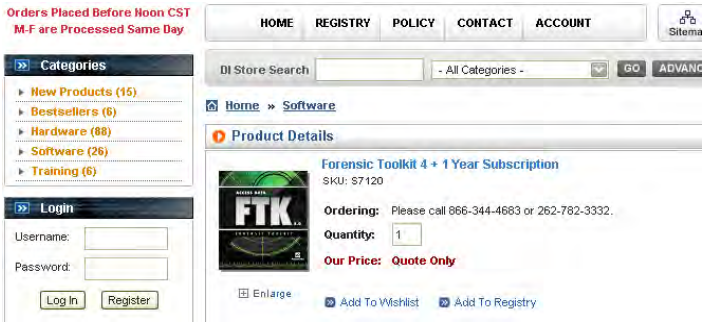
| HARDWARE | FRED L | FRED SR |
|---|---|---|
| SISTEMA OPERATIVO | Microsoft Windows 7 Ultimate 64 Bit | Windows7 64-bit |
| PROCESADOR | Intel Core i7-4800MQ Quad Core, 2.7 GHz, 6 MB de caché L3 | Dual(2) Intel Xeon E5-2609 CPU, (QuadCore) 2.4 GHz, 10MB Cache, 6.4 GT/s Intel QPI |
| MEMORIA | 8 GB | 16 GB PC3-12800 DDR3 1600 MHz ECC Memory |
| DISCO DURO | 256 GB de estado sólido SATA interno Drive | CUENTA CON DOS DISCOS:1 x 300 GB 10,000 RPM SATA III – SISTEMA OPERATIVO, 1 x 2.0 TB 7200 RPM SATA III Hard Drive – DISCO PARA DATOS. |
| PUERTOS HDMI | 1 | 0 |
| PUERTOS DISPLAYPORT 1.2 | 1 | 0 |
| MIN PUERTOS DISPLAYPORT 1.2 | 1 | 0 |
| TARJETA DE VIDEO | NvidiaGeForce GTX 770M con 3 GB GDDR5 VRAM | Nvidia GT 630 4GB 128 bit DDR3 PCI-Express Video Card |
| PUERTOS RJ45 | 1 | 2 |
| PUERTOS USB 2.0 | 1 | 8 |
| PUERTOS USB 3.0 | 3 | 6 |
| PUERTOS IEEE 1394A | 1 | 2 |
| PUERTO COMBO USB 3.0 - E SATA | 1 | 0 |
| CONECTOR DE SEGURIDAD KENSINGTON | 1 | 0 |
| PUERTOS INTEL 6.0 GB/ S SERIAL ATA (SATA) | 0 | 2 |
| PUERTOS INTEL 3.0 GB/ S SERIAL ATA (SATA) | 0 | 8 |
| PUERTOS MARVELL 6.0 GB / S SERIAL ATA (SATA) | 0 | 4 |
| PUERTOS USB BLOQUEADOS CONTRA ESCRITURA | 0 | 1 |
| BAHIAS DE DISCOS EXTRAIBLES | 0 | 3 |
| COSTO | $ 85.000.000,00 | $ 122.000.000,00 |

## 7.3. COSTOS

**7.3.1. Licencias de software.** En esta sección se tuvo en cuenta varias opciones de software, las cuales se verán a continuación, de las cuales las dos opciones que se ajustan a los requerimientos del LIF son ENCASE y FTK:

- **FTK**

**Figura 40. FTK**




FTK [En línea].Consultado el 12 de Diciembre de 2013. Disponible en internet: http://www.digitalintelligence.com/software/accessdata/forensictoolkit4/`

Valor licencia en dólares = $5.200

- **ENCASE**

**Figura 41. ENCASE**


ENCASE [En línea].Consultado el día 12 de Diciembre de 2013. Disponible en internet: http://www.digitalintelligence.com/cart/ComputerForensicsProducts/EnCase-Forensic-v7.html

Valor licencia en dólares = $2.995

**Cuadro 2. Comparativo de herramientas de software**

| CUADRO COMPARATIVO DE HERRAMIENTAS DE SOFTWARE | | |
|---|---|---|
| **HERRAMIENTA** | **FTK** | **ENCASE 7** |
| VALOR US$ | $5.200,00 | $2.995,00 |
| VALOR EN PESOS COLOMBIANOS (PARA TRES EQUIPOS)* | $ 31.989.017,97 | $ 18.427.250,01 |
| **REQUERIMIENTOS MINIMOS** | | |
| PROCESADOR REQUERIDO | QuadCore | QuadCore |
| MEMORIA RAM | 32 GB | 16 GB |
| DRIVE PARA EL SISTEMA OPERATIVO | SATA 7200 RPM | SATA 7200 RPM |
| CONFIGURACION DE LA RED | GIGABIT ETHERNET (GbE) | GIGABIT ETHERNET (GbE) |
| CONTROLADOR DE RAID DE DISCOS | ALTAMENTE RECOMENDADO SI SE CUENTA CON BASE DE DATOS POSTGRESSQL | OPCIONAL |
| CAPACIDAD DE DISCO DURO (SOLO SOFTWARE) | 1 GB DE ESPACIO LIBRE | 300 MB DE ESPACIO LIBRE |
| *VALORES SEGUN UNA TRM = $2050,58 | | |

**UFED 4PC** Valor licencia en dólares = $3999, este kit de software incluye los cables necesarios para realizar análisis forense en el 95% de los celulares que existen actualmente en el mercado, incluye dispositivo de hardware.

**XRY** Valor licencia en dólares = $9490, recupera toda la información almacenada en un telefono celular, este kit de software incluye los cables necesarios para realizar análisis forense en diversos tipos de teléfono celular, incluye dispositivo de hardware.[39]

[39] Cotizaciones, [en linea] Santiago de Cali, [consultados en enero de 2014] Disponible en internet http://www.search.org/files/pdf/CellDeviceInvestToolkit-0908.pdf

**SECURE VIEW 3 MOBILE KIT** Valor licencia en dólares = $ 6490[40].

Este kit de software incluye los cables necesarios para realizar análisis forense en diversos tipos de teléfono celular.

**7.3.2. Hardware.** A continuación se encuentra el listado de los implementos que como mínimo debe tener el LIF, estas cotizaciones fueron hechas en dólares (US$) según sitio web http://www.digitalintelligence.com y posteriormente convertidas a pesos colombianos (COP) con una TRM[41]= $2050.58.

- 1 Estación de trabajo forense "FRED SR": Valor = US$14.999 ( equivalente a $30.735.655,74 COP) según lo visto en la página previamente mencionada, pero en la cotización de la licitación de la firma Internet Solutions[42] para un LIF se aprecia el valor $121.464.000, razón por la cual se plantea un presupuesto de $122.000.000 para la compra de este elemento.

- 1 Estación forense portátil FRED L: Valor = US$4.999 ( equivalente a $10.250.849,42 COP) según lo visto en la página previamente mencionada, pero en la cotización de la licitación de la firma Internet Solutions para un LIF se aprecia el valor $84.210.000, razón por la cual se plantea un presupuesto de $85.000.000 para la compra de este elemento.

- ULTRAKIT III: US$1.649 ( equivalente a $ 3.381.406,42 COP) según lo visto en la página previamente mencionada, pero en la cotización de la licitación de la firma Internet Solutions para un LIF se aprecia el valor $13.431.600, razón por la cual se plantea un presupuesto de $14.000.000 para la compra de este elemento[43].

- 1 DUPLICADOR FORENSE: US$2.248 (equivalente a $ 4.609.703,84 COP) según lo visto en la página previamente mencionada, pero en la cotización de la licitación de la firma Internet Solutions para un LIF se aprecia el valor

[40] Cotizaciones, [en linea] Santiago de Cali, [consultados en enero de 2014] Disponible en internet http://www.digitalintelligence.com/cart/ComputerForensicsProducts/Secure-View-3.html

[41] La Tasa de Cambio Representativa del Mercado (TRM): es la equivalencia de pesos colombianos por un dólar de los Estados Unidos.

[42]Distribuidor autorizado en Colombia para los productos de Digital Intelligence.

[43] Ver anexo 3 página 53 del archivo "anexos.docx".

$20.000.000, razón por la cual se plantea un presupuesto de $20.000.000 para la compra de este elemento[44].

- ELEMENTOS PARA LABORES DE CAMPO (guantes, lentes, vestuario apropiado, números para marcación de evidencia). = se plantea un presupuesto de $2.000.000 para estos implementos de dotación.

- CÁMARA FOTOGRÁFICA: $499.000 (COP) cotizado en la página http://store.sony.com.co/.

En el siguiente cuadro comparativo se muestra las dos opciones de inversión dependiendo si se decide usar software FTK o ENCASE, donde el sponsor (universidad autónoma de Occidente) elije que opción tomar.

[44] Ver anexo 3 página 53 del archivo “anexos.docx”.

## Cuadro 3. Comparativo de costos

| PAQUETE | COSTO | VENTAJAS | DESVENTAJAS | COSTO TOTAL |
|---|---|---|---|---|
| SOFTWARE FTK PARA TRES EQUIPOS | $ 31.989.018 | Respaldo por parte de la casa desarrolladora del software de análisis forense . | El costo de esta opción es más elevado. | $ 402.448.022 |
| 1 ESTACION FORENSE FRED SR | $ 122.000.000 | | | |
| 1 ESTACION FORENSE FRED L | $ 85.000.000 | La operación del software licenciado es más sencilla. | | |
| 1 ULTRAKIT III (KIT DE BLOQUEADORES) | $ 14.000.000 | | | |
| MEDIOS DE ALMACENAMIENTO PARA EVIDENCIAS | $ 27.000.000 | | | |
| 1 CÁMARA FOTOGRÁFICAS SONY CYBERSHOT | $ 499.000 | | | |
| HERRAMIENTA XRY (DISPOSITIVOS MOVILES) | $ 19.460.004 | | | |
| DUPLICADOR DE DISCOS FORENSE | $ 20.000.000 | | | |
| CAPACITACION EN CADA UNO DE LOS MODULOS DE LA APLICACION (PARA TRES FUNCIONARIOS | $ 82.500.000 | El uso de este software tiene una trazabilidad a nivel mundial. | | |
| SOFTWARE ENCASE PARA TRES EQUIPOS | $ 18.427.250 | Se reducen los costos del proyecto. | Su operación es más compleja y requiere más experticia del analista. | $ 377.626.519 |
| 1 ESTACION FORENSE FRED SR | $ 122.000.000 | | | |
| 1 ESTACION FORENSE FRED L | $ 85.000.000 | Cuenta con múltiples herramientas de análisis forense. | | |
| 1 ULTRAKIT III (KIT DE BLOQUEADORES) | $ 14.000.000 | | | |
| MEDIOS DE ALMACENAMIENTO PARA EVIDENCIAS | $ 27.000.000 | | | |
| HERRAMIENTA UFED 4PC (DISPOSITIVOS MOVILES) | $ 8.200.269 | | | |
| 1 CÁMARA FOTOGRÁFICAS SONY CYBERSHOT | $ 499.000 | Su adquisición es fácil. | | |
| DUPLICADOR DE DISCOS FORENSE | $ 20.000.000 | | | |
| CAPACITACION EN CADA UNO DE LOS MODULOS DE LA APLICACION (PARA TRES FUNCIONARIOS | $ 82.500.000 | | | |

Del cuadro anterior se deduce que la opción más económica es utilizando el software ENCASE, con un valor de $ 377.626.519, y la opción más costosa es utilizando el software FTK con un valor de $ 402.448.022, cabe resaltar que la

gran ventaja de esta última opción es su facilidad de utilización, eso sin demeritar la herramienta ENCASE aunque implica un mayor tiempo de capacitación para el personal y el entrenamiento[45].

## 7.4 INVESTIGACION DE MERCADO

Para el desarrollo de este proyecto se realizó una investigación de mercado en la cual se consultaron los criterios que tienen diferentes LIF's para realizar el cobro de los servicios ofrecidos por estos, así como también la tarifa actual del mercado.

**Cuadro 4. Comparativo de tarifas y criterios de diferentes LIF's**

| CIF | CRITERIO QUE TIENEN EN CUENTA PARA EL COBRO DEL SERVICIO | | | | TARIFA MINIMA (COP) | |
|---|---|---|---|---|---|---|
| | RECUPERACION DE INFORMACION BORRADA | COMPLEJIDAD DE LA INVESTIGACION | UMBRAL DE TIEMPO/ TAMAÑO DE DISCO | CAPACIDAD DEL DISCO DURO | | |
| MATTICA | X | | | | $ 6.151.740,00 | |
| INTERNET SOLUTIONS | | | | X | $ 5.000.000,00 | |
| OTRAS ENTIDADES | | | X | | $ 5.000.000,00 | \ |
| INTRASOFT PANAMA | X | | | | $ 4.101.160,00 | |
| ASOTO | | X | | | $ 200.000,00 | * |
| * Valor de la valoracion y el analisis mas economico. | | | | | | |
| \ Analisis a 1TB de informacion y un umbral de tiempo de 1 mes o 2 meses. | | | | | | |

- Mattica

Por ejemplo para la recuperación de información con un umbral de 10 días en un servidor con sistema operativo windows server en un disco de 8TB[46]cobran entre $ 3,000 a $3,500 USD (entre $6.151.740COP y $7.177.030COP[47]), eso dependiendo si se requiere el desplazamiento hacia el lugar donde se encuentra la evidencia para hacer el análisis o llevando directamente a el laboratorio conservando una adecuada conservación de la evidencia, estos valores no varían si el cliente es una entidad pública o privada.

Otro factor que influye en el cobro es si el discoestá distribuido o en RAID[48]lo cual hace variar el cobro por ser necesaria la reconstrucción del sistema de

[45] Ver anexo 3 página 53 del archivo "anexos.docx".

[46] TB: Terabytes.

[47] TRM: $2050.58

[48]En informática, el acrónimo RAID (del inglés RedundantArray of Independent Disks, originalmente RedundantArrayInexpensive Disks), traducido como «conjunto redundante de discos independientes»

archivos para tratar de recuperar la información, siendo este procedimiento más complejo y no garantiza una recuperación exitosa.
Otro factor importante para el cobro es el tiempo necesario para el análisis del material probatorio, la distribución del servidor, la referencia del servidor, en caso de ser necesario el desplazamiento de equipos y personal del laboratorio hasta donde se encuentra el cliente el costo se incrementa a$4500 USD ($9.227.610 COP).

- Internet solutions.

El cobro del servicio depende de la capacidad o tamaño del disco a analizar, si es un disco pequeño (por ejemplo 500 GB) el análisis tiene un valor de$ 5.000.0000[49] COP + IVA y si es un servidor el costo mínimo es de $8.000.000[50]COP[51]+ IVA[52] en ambos casos garantizando la integridad de los datos y el cumplimiento de la cadena de custodia, cabe resaltar que esta firma es una de las mas completas y mejor preparadas para atender los incidentes.

- Intrasoft.

El cobro mínimo que se hace por el análisis de información $ 2,000 USD (equivalente a $4.101.160 COP) sin incluir el desplazamiento. (No proporcionaron más información).

- Asoto.

Este LIF tiene como política hacer primero un diagnóstico de lo que se va analizar, llevando la adquisición de la imagen hasta el laboratorio cobran de la siguiente manera:

  - Por entrega de resultados en 15 días (nivel económico) = $ 90,000 COP+ IVA.
  - Entrega de resultados en 8 días (nivel prioritario) = $190,000 COP+ IVA.
  - Entrega de resultados entre 24 y 72 horas (nivel de emergencia) = $ 390,000 COP+ IVA.

[49]Cobro mínimo por análisis a computadoras de escritorio parte de este LIF.

[50]Cobro mínimo por análisis a servidores por parte de este LIF.

[51] COP: Pesos colombianos.

[52] IVA, corresponde al 16% del valor referenciado.

Finalizando el diagnostico proceden a cobrar el valor restante del análisis del material probatorio, esto depende de la complejidad de la investigación y del nivel de dificultad con que se deban recuperar los datos, el costo total puede estar entre $200.000 y $100.000.000 COP, ya que si el caso es muy complejo y requiere la asistencia de un abogadoincluirian los honorarios de este en el cobro del análisis.

- Otras entidades.
  Para una estación de trabajo se cobra según el umbral de tiempo y el tamaño del disco, teniendo encuenta que no es el tiempo que se demora realizando el análisis, sino el análisis a la información que fue generada en un espacio de tiempo establecido por el cliente, para tener mayor veracidad en la evidencia y correlación de esta con el delito.

  Es necesario tener en cuenta que no se procesa toda la información, solamente los objetivos forenses basándose en técnicas y parámetros específicos.

  Para un TB búsqueda y un umbral de tiempo que manejan básicamente entre 1 o 2 meses cobran aproximadamente $ 5.000.000 COP.

De lo anterior se puede deducir que la tarifa más económica es la de Asoto con un costo de $ 200.000. Pero si se requiere una cadena de custodia por la complejidad de la investigación, el costo total tendría un incremento en cada nivel de servicio, el resto de laboratorios cobran en promedio $5.000.000 en su tarifa mínima.

Otro aspecto que hay que mencionar es que el tiempo que tarda cada caso puede variar dependiendo de la complejidad del mismo, por ejemplo un caso puede demorar entre 1, 6 meses o mas tiempo.

## 7.5 ESTRUCTURA DEL PROYECTO - INTEGRACION

## Cuadro 5. Estructura del proyecto Integración- Project Charter

| | |
|---|---|
| **PROJECT CHARTER** | |
| **LOCALIZACION** | INSTALACIONES DE LA UNIVERSIDAD AUTONOMA DE OCCIDENTE |
| **CLIENTE** | UNIVERSIDAD AUTONOMA DE OCCIDENTE |
| **RESPONSABLE DEL PROYECTO** | GUILLERMO UMAÑA RAMIREZ<br>ISABEL CRISTINA MOSQUERA N. |
| **OBJETIVO ESTRATEGICO** | DESARROLLO DE UN MODELO DE IMPLEMENTACIÓNPARAUN CENTRO DE INFORMÁTICA FORENSE |
| **COMPLEJIDAD**(I Para proyectos de USD50.000 o menos, II Para proyectos de entre USD 50.000 y USD 500.000 Y III Para proyectos de más de USD 500.000, Escala establecida bajo el criterio de los desarrolladores de este proyecto basados en la metodología **PMBOK**) | COMPLEJIDAD II, YA QUE SU COSTO SE EN EL ESTA ENTRE US$50.000 Y US$500.000 ($94,650,000 y $946,500,000.00) |
| **STAKEHOLDERS (INVOLUCRADOS)** | |
| **PROVEEDORES** | CASAS DE SOFTWARE |
| **SOCIOS DE NEGOCIO** | JUNTA DIRECTIVA DE LA UNIVERSIDAD AUTONOMA DE OCCIDENTE |
| **EMPRESARIOS** | PERSONAS QUE REQUIERAN DE UNA INVESTIGACION FORENSE EN UN MEDIO INFORMATICO |
| **GERENTES FUNCIONALES** | DESIGNADO POR LA UNIVERSIDAD |
| **GERENTES OPERATIVOS** | DESIGNADO POR LA UNIVERSIDAD |
| **GERENTES DE PORTAFOLIO** | DESIGNADO POR LA UNIVERSIDAD |
| **GERENTES DE PROGRAMA** | DIRECTIVOS DE LA UNIVERSIDAD |
| **PATROCINADOR** | UNIVERSIDAD AUTONOMA DE OCCIDENTE |
| **PATROCINADOR FUNCIONAL** | UNIVERSIDAD AUTONOMA DE OCCIDENTE |
| **ANALISIS DEL ALCANCE** | |
| **DENTRO DEL ALCANCE** | CREAR UN MODELO DE IMPLEMENTACION PARA UN CENTRO DE INFORMATICA FORENSE |
| **FUERA DEL ALCANCE** | LA IMPLANTACION DEL CENTRO DE INFORMATICA FORENSE |
| **AREAS INDEFINIDAS** | EL PRESUPUESTO MAXIMO ES DE $296.873.674 BASADOS EN EL ANALISIS COMPARATIVO DE COSTOS. |
| **ESTIMACION DE COSTOS** | |
| **PRESUPUESTO** | POR DEFINIR (DEPENDE DE LO QUE AUTORICE EL SPONSOR) |
| **ANALISIS DE BENEFICIOS** | |
| **DESCRIPCION CUALITATIVA** | PRESTIGIO A LA UNIVERSIDAD EN CUANTO A SU ENFOQUE DE SEGURIDAD INFORMATICA E INFORMATICA FORENSE.<br>INGRESOS ADICIONALES POR CONCEPTO DE INVESTIGACIONES EN INFORMATICA FORENSE.<br>POSIBILIDAD DE CAPACITAR A LOS ESTUDIANTES EN UN CENTRO DE INFORMATICA FORENSE REAL, SIN LAS DIFICULTADES QUE PRESENTA APRENDER EN UN LUGAR DONDE LOS ESPACIOS NO ESTAN DISEÑADOS PARA FINES PEDAGOGICOS.<br>CREACION DE PROGRAMAS ESPECIALIZADOS EN INFORMATICA FORENSE. |
| **DESCRIPCION CUANTITATIVA** | GENERAR INGRESOS A LA UNIVERSIDAD POR CONCEPTO DE INVESTIGACIONES ADEMAS DE AHORRO EN CENTROS DE CAPACITACION, ESTO SUMADO AL PRESTIGIO OBTENIDO POR EL DESARROLLO DEL CENTRO DE INFORMATICA FORENSE |

## 7.6 ALCANCE DE ESTE PROYECTO

Este proyecto culmina en el diseño de un modelo de implementación, en el cual muestran las condiciones mínimas para que un LIF funcione en la UAO, la segunda etapa de la implantación se desarrollará solo con el aval del sponsor o sea la universidad.

Para definir el alcance de este proyecto se tuvieron en cuenta los siguientes requerimientos:

- Se observa la necesidad del Mercado de las empresas del sector informático con personal capacitado para poder hacer un análisis forense adecuado en medios informáticos.
- Actualmente en el mercado hay una gran necesidad de un laboratorio especializado en análisis forenses en medios informáticos.
- El laboratorio debe tener un adecuado sistema de gestión de seguridad de la información.
- Se debe contar con espacios físicos que propicien la protección de la información que se va a manejar y se asegure la integridad de la conservación de la evidencia.
- Es necesario contar con el software de apoyo para las investigaciones forenses a desarrollar.
- Es necesario también contar con la asesoría de un abogado en cuanto a legislación.

REGISTRO DE STAKEHOLDERS

- Clientes.
- Estudiantes.
- Gobierno.
- Implicados en delitos.
- Universidad Autónoma de Occidente

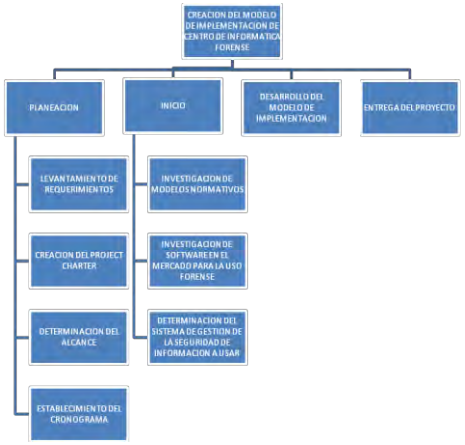
A partir de esa información se estableció que este proyecto termina con el diseño de un Modelo de Implementación para un Laboratorio de Informática Forense, donde se especifican los recursos necesarios para el montaje de este, para proteger el cumplimiento de la conservación de la evidencia y para garantizar la seguridad del espacio físico y virtual.

## Cuadro 6. Tipos de Requerimientos

| REQUERIMIENTO | TIPO DE REQUERIMIENTO | | | | | | | | SUPUESTOS Y RESTRICCIONES | IMPACTOS |
|---|---|---|---|---|---|---|---|---|---|---|
| | NECESIDAD DE NEGOCIO | OBJETIVO DE NEGOCIO | FUNCIONAL | NO FUNCIONAL | PROCESO DE NEGOCIO | DE CALIDAD | CRITERIO DE ACEPTACION | DOCUMENTACION | | |
| SE NECESITA UN MODELO DE IMPLEMENTACION DE UN CENTRO DE INFORATICA FORENSE | X | X | | X | X | | | X | NO EXISTE UN CENTRO DE INFORMATICA FORENSE | GENERACION DE EMPLEO, INGRESOS ECONOMICOS Y PRESTIGIOS DE LA UNIVERSIDAD |
| SE NECESITA SABER CUANTAS PERSONAS VANA ESTAR INVOLUCRADAS | X | | | X | X | X | | X | QUE LAS PERSONAS QUE TRABEJEN DENTRO DE ELLA ESTEN CAPACITADAS | HALLAZGOS ACERTADOS EN LAS INVESTIGACIONES CON ALTA CALIDAD |
| SE NECESITA UN SOFTWARE PARA EL ANALISIS FORENSE DE LOS HALLAZGOS ENCONTRADOS | X | | X | | | X | | X | SE CUENTA CON EL CAPITAL PARA ADQUIRIR TECNOLOGIA DEL CENTRO DE INFORMATICA FORENSE | CONFIABILIDAD, BUEN NOMBRE Y PRFERENCIA POR LOS CLIENTES |
| SE NECESITA CAPACITACION PARA LA CADENA DE CUSTODIA | X | X | | X | X | | X | X | NO SE CUENTA CON PERSONAL CAPACITADO CON RESPECTO A LA APLICACIÓN DELA CADENA DE CUSTODIA | CREA CERTEZA DE QUE LA EVIDENCIA TENDRA UN MANEJO ADECUADO |

**WORK BREAKDOWN STRUCTURE**

**Figura 42. Mapa conceptual wbs**




## 7.7 RIESGOS DEL PROYECTO

Entre los riesgos que pueden encontrar en el desarrollo de este proyecto es el de la filtración, fuga de información o modificación de esta a causa de accesos no autorizados, de no encriptación de la información, suplantación de identidad, violación de acuerdos de confidencialidad, violación de correo electrónico o infiltración de código malicioso, entre otro tipo de riesgos causados por diferentes tipos de vulnerabilidades[53].

Para este proyecto se tuvo en cuenta la norma ISO 27001 en cuanto a la identificación y control de riesgos, a continuación se encuentra la matriz de riesgos, en la cual se puede apreciar el activo de información[54], la amenaza, el riesgo según la norma ISO 27001[55] y los controles según la norma ISO 27002[56].

[53] Se entiende como Vulnerabilidad al acto consciente o inconsciente que da pie a que se materialice una situación desfavorable.

[54] Se entiende como activo de información como “cualquier cosa que tenga valor para el LIF”, que en este caso es el propio LIF.

### 7.7.1 Matriz de Riesgos.

## Cuadro 7. Matriz de Riesgos

| MATRIZ DE RIESGOS | | | | |
|---|---|---|---|---|
| **ACTIVO** | **AMENAZA** | **VULNERABILIDAD** | **NORMA ISO 27001** | **CONTROLES ISO 27002-2005** |
| **CENTRO DE INFORMATICA FORENSE** | **CAIDA DE LA CADENA DE CUSTODIA** | Acceso no autorizado | Los sistemas deben estar con un nivel de seguridad maximo y asi evidenciar el aceeso no autorizado (ISO 27002 NUMERAL 11,1,1). | 11.1.1 Politica de control de acceso. |
| | | Falsificación de documento electrónico digital | Los datos de prueba deberían seleccionarse cuidadosamente, así como protegerse y controlarse (ISO 27002 NUMERAL 12,4,2). | 12.4.2 Protección de los datos de prueba del sistema. |
| | | Fraudes por medio de Phishing a travez de medios digitales | En cualquier acuerdo sobre los servicios de la red se deberían identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente. (ISO 27002 NUMERAL 10,6,2) | 10.6.2 Seguridad de los servicios de red. |
| | | No encriptacion de Informacion | responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por ejemplo a través de difamación, acoso, suplantación de identidad, envío de cartas de cadena, adquisición no autorizada, etc.(ISO 27002 NUMERAL 10,8,1) | 10.8.1 Políticas y procedimientos de intercambio de información |
| | | Suplantacion de identidad | responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por ejemplo a través de difamación, acoso, suplantación de identidad, envío de cartas de cadena, adquisición no autorizada, etc.(ISO 27002 NUMERAL 10,8,1) | 10.8.1 Políticas y procedimientos de intercambio de información. |
| | | Apropiacion de informacion como BD | Todos los activos deberían estar claramente identificados y se debería elaborar y mantener un inventario de todos los activos importantes (ISO 27002 NUMERAL 7,1,1). | 7.1.1 Inventario de activos. |
| | | Violación de acuerdos de confidencialidad | que todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a información sensible deberían firmar un acuerdo de confidencialidad o no-divulgación antes de tener acceso a los servicios de procesamiento de información (ISO 27002 NUMERAL 8,1,3). | 8.1.3 Términos y condiciones de contratación. |
| | | Infracción a la ley de propiedad intelectual | Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados (ISO 27002 NUMERAL 15,1,2). | 15.1.2 Derechos de propiedad intelectual (DPI). |
| | | Violación de correo electrónico | Se deberían establecer acuerdos para el intercambio de la información y del software entre la organización y las partes externas.(ISO 27002 NUMERAL 10,8,2). | 10.8.2 Acuerdos de intercambio. |
| | | Fuga de Informacion | Se deberían evitar las oportunidades para que se produzca fuga de información. (ISO 27002 NUMERAL 12,5,4). | 12.5.4 Fugas de información. |
| | | Infiltracion de virus y codigo malicioso | Activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusión. (ISO 27002 NUMERAL 10,10,1). | 10.10.1 Registros de auditoría. |

[55]ISO 27001: Es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI), [en linea] [consultado en junio de 2013] Disponible en internet: http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/.

[56]ISO 27002: Es una guía de buenas prácticas de seguridad de la información que presenta una extensa serie de controles de seguridad, [en linea] [consultado en junio de 2013] Disponible en internet: http://blog.altosec.com.ar/tag/iso-27002/

A continuación se puede observar una relación causa – efecto entre las posibles situaciones que un LIF (laboratorio de informática forense) puede analizar.

### 7.7.2. Diagrama causa efecto.

**Cuadro 8. Diagrama Causa y Efecto**

| CAUSA | EFECTO |
|---|---|
| Mal uso de las redes internas y falta de control a estas. | Análisis forense y entrega de recomendaciones frente a los controles a implantar. |
| Acceso no autorizado. | Implantación de políticas de manejo y auditoria a los Logs de autenticación. |
| Falsificación de documento electrónico digital. | Verificación de Hash de documentos importantes así como las firmas digitales de los correos. |
| Fraudes por medio de Phishing a través de medios digitales. | Restricción de ingreso a páginas electrónicas de poca confiabilidad. |
| No encriptación de Información. | Crear lineamientos para la encriptación de la información core de negocio. |
| Suplantación de identidad. | Control de contraseñas y firmas digitales. |
| Apropiación de información como BD. | Medidas legales ante la perdida de información, análisis a las vulnerabilidades del sistema y control al área física de los recursos informáticos. |
| Violación de acuerdos de confidencialidad. | Medidas legales ante la divulgación de información. |
| Infracción a la ley de propiedad intelectual. | Medidas Legales. |
| Violación de correo electrónico. | Control de manejo de contraseñas con periodicidad y repudio a usuarios desconocidos. |
| Infiltración de virus y código malicioso. | Control de acceso a páginas web sospechosas y restricción de dispositivos de almacenamiento extraíble. |
| Ataques de denegación de servicio por falta de un parche al software de firewall. | Recuperación de información y estudio de la misma. |

## 7.8 ESPECIFICACIONES DE SEGURIDAD DEL LIF, MODELO DE DEFENSA EN PROFUNDIDAD

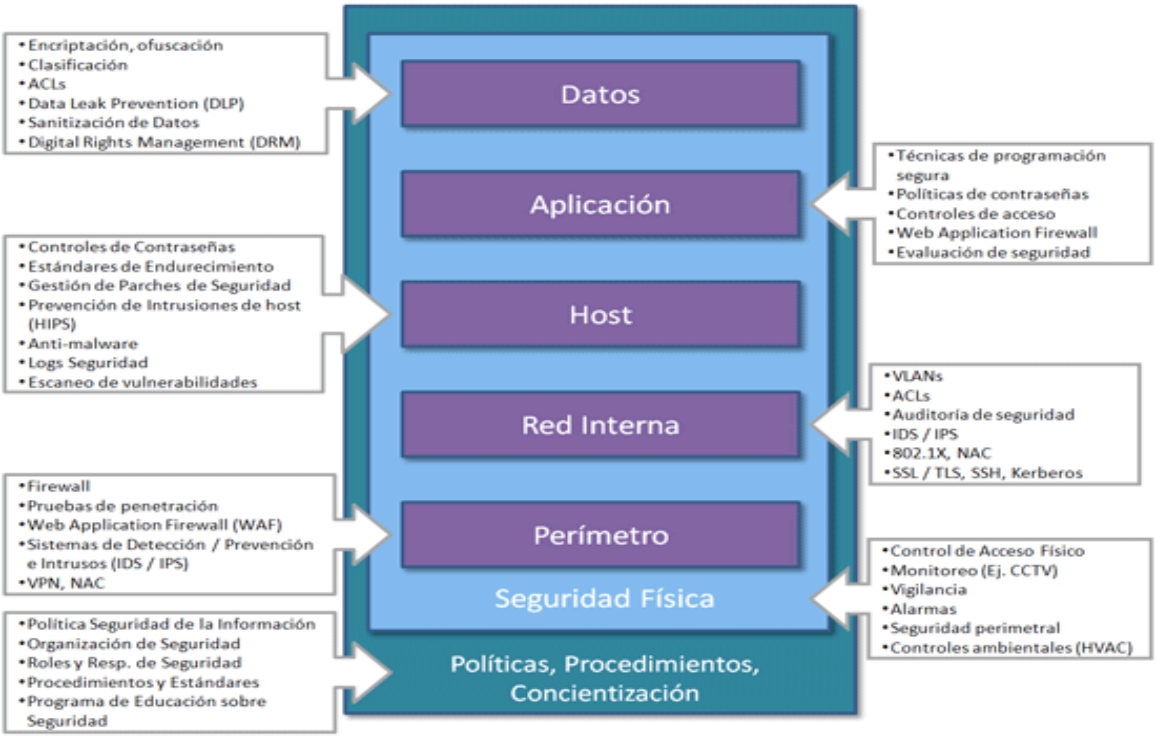
El término defensa en profundidad (en ocasiones denominada seguridad en profundidad o seguridad multicapa) se refiere a una estrategia militar que tiene por objetivo hacer que el atacante pierda el empuje inicial y se vea detenido en sus intentos al requerirle superar varias barreras en lugar de solo una.

Las infraestructuras de tecnología son una compleja formación de elementos que en conjunto albergan uno de los activos más valiosos del LIF: los datos. Podemos visualizar esta infraestructura como una serie de capas donde los datos ocupan el último nivel, precedidos de contenedores como lo son las localidades físicas, el perímetro, la red, los servidores y las aplicaciones.

La seguridad en capas aumenta de manera extraordinaria el costo y dificultad de penetración de un atacante, por lo cual se disminuye la posibilidad que los atacantes se tomen el trabajo de acceder de manera no autorizada al laboratorio.

De esta forma, cada capa de la infraestructura representa una barrera para el atacante en su camino hacia el objetivo final de acceder a los datos confidenciales, de manera que si falla cualquiera de los controles en una capa haya defensas adicionales que contengan la amenaza y minimicen las probabilidades de una brecha, para este caso observar la imagen que se encuentra a continuación.

**Figura 43. Estrategias Básicas de Seguridad Informática: Defensa en Profundidad**



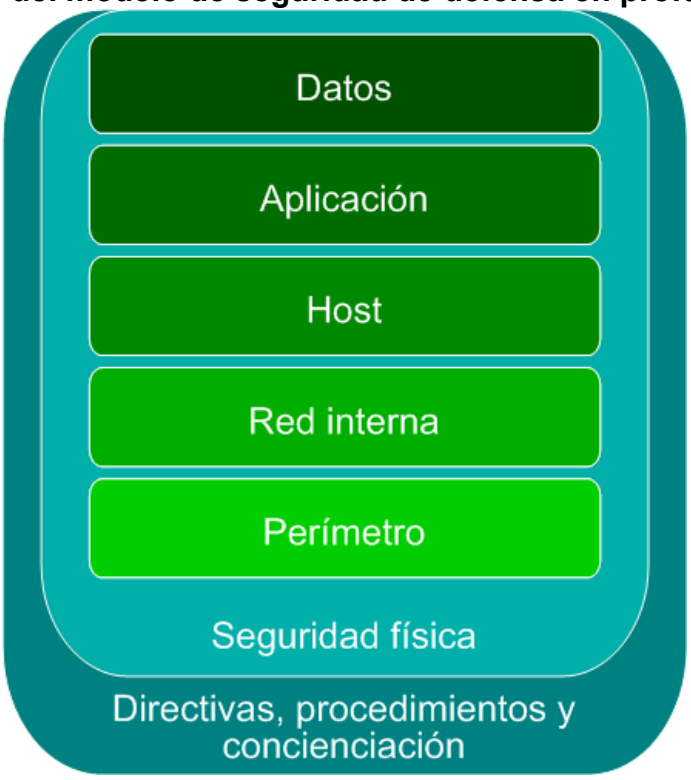

Estratégias de seguridad Informática [En línea].Consultado el día 02 de febrero de 2014.Disponible en internet: http://www.sentineldr.com/post/estrategias-basicas-de-seguridad-informatica-defensa-en-profundidad

Las capas múltiples de seguridad le permiten aplicar adecuadamente la estrategia de seguridad del LIF. Este enfoque multicapa, conocido también como “Defensa en Profundidad”, combina técnicas interactivas porque, aun cuando ninguna medida preventiva sea 100% efectiva, en la práctica la correcta combinación de capas de seguridad puede aproximarse al 100% de efectividad.

Una vez haya conocido y documentado los riesgos a los que el laboratorio hace frente, el siguiente paso consiste en examinar y organizar la defensa que utilizará para la solución. El modelo de seguridad de defensa en profundidad[57] constituye un punto de partida excelente para ello, ya que identifica siete niveles de defensas de seguridad diseñados para bloquear cualquier intento de comprometer la seguridad del laboratorio. Cada conjunto de defensa es capaz de desviar ataques en muchas y distintas escalas.

[57] MDP: Se define como modelo de defensa en profundidad.

**Figura 44.Capas del modelo de seguridad de defensa en profundidad**




Capas del modelo de seguridad de defensa en profundidad [En línea].Consultado el día 02 de febrero de 2014.Disponible en internet: http://technet.microsoft.com/es-es/library/cc162791.aspx

- **DATOS:** En el LIF esta capa aplica para determinar los datos almacenados que han sido vulnerados.

  Los datos almacenados localmente son especialmente vulnerables. Si se presenta el robo de un equipo, es posible realizar copias de seguridad, restaurar y leer los datos en otro equipo, aunque el delincuente no pueda conectarse al sistema.

  Los datos se pueden proteger de varias formas, incluido el cifrado de estos mediante EFS[58] (Encrypting File Service) o sistemas de cifrado de otros fabricantes y la modificación de las listas de control de acceso discrecional en los archivos.

[58]EFS : Es la herramienta de cifrado de archivos integrado para sistema de archivos de Windows.

- **APLICACIÓN:** En el LIF esta capa enmarca los riesgos que un atacante podría aprovechar para obtener acceso a las aplicaciones en ejecución. Las principales preocupaciones del personal del laboratorio en esta capa son el acceso a los archivos binarios que componen las aplicaciones, el acceso al host a través de las vulnerabilidades en los servicios de escucha de la aplicación o la recopilación ilícita de datos concretos del sistema para transferirlos a alguien que pueda utilizarlos en beneficio propio y la modificación de información.

- **HOST:** En el LIF esta capa aplica para determinar al laboratorio el impedir el acceso a los archivos binarios que componen el sistema operativo, así como el acceso al host a través de vulnerabilidades en los servicios de escucha, programas espías, spam, y el ingreso de virus.

  Para esto el laboratorio debe evaluar cada host del entorno y crear directivas que limiten cada servidor sólo a las tareas que tenga que realizar. De este modo, se crea otra barrera de seguridad que un atacante deberá superar antes de poder provocar algún daño. Un modo de hacerlo consiste en crear directivas individuales en función de la clasificación y el tipo de datos que contiene cada servidor.

- **RED INTERNA:** Los riesgos para las redes internas del laboratorio están relacionados con los datos confidenciales que se transmiten a través ellas. Los requisitos de conectividad para las estaciones de trabajo dentro del laboratorio en estas redes internas también suponen algunos riesgos asociados.
  Si dispone de una serie de redes en el LIF, las cuales deben ser evaluadas individualmente para asegurarse de que se ha establecido una seguridad apropiada.

  Debe examinar el tráfico admisible en sus redes y bloquear el que no sea necesario. De tal manera supervisar la existencia de detectores de paquetes en la red, que sólo deben usarse bajo controles estrictos.

- **RED PERIMETRAL:** En el LIF la protecciónde del perímetro de la red es el aspecto más importante para detener los ataques externos. Si su perímetro permanece seguro, la red interna estará protegida de ataques externos. El laboratorio debe disponer de algún tipo de dispositivo de seguridad para proteger cada punto de acceso a la red como firewalls o pruebas de penetración.

También se debe recordar que, para las redes que permiten el acceso remoto, el perímetro puede incluir los equipos portátiles del personal e incluso los equipos domésticos, cabe aclarar que el manejo de la evidencia debe ser dentro de las instalaciones del laboratorio.

- **SEGURIDAD FÍSICA:** En el LIF se debe tener control del acceso a personal no autorizado para poder asegurar la integridad de la información allí manejada la seguridad física es un elemento fundamental para la estrategia de seguridad global dentro del LIF para así prevenir ataques como:

  - La ejecución de código malicioso (por ejemplo, activar un gusano desde el interior del laboratorio).

  - El robo de información de seguridad crítica (por ejemplo, material probatorio, segundos originales, cintas de copia de seguridad y diagramas de red).

Como parte de la estrategia de administración de riesgos, debe determinar el nivel de seguridad física apropiado para su entorno, A continuación se enumeran las medidas mínimas de seguridad física a tomar:

- Establecer seguridad física para todas las áreas del edificio (esto puede incluir tarjetas de acceso, dispositivos biométricos y guardias de seguridad).

- Requerir a los visitantes que vayan acompañados en todo momento.

- Requerir a los visitantes que firmen un registro de entrada de todos los dispositivos informáticos.

- Requerir a todos los integrantes del LIF que registren cualquier dispositivo portátil de su propiedad.

- Fijar físicamente todos los equipos de sobremesa y portátiles a las mesas.

- Requerir que se registren todos los dispositivos de almacenamiento de datos antes de sacarlos del laboratorio.

- Ubicar los servidores en salas separadas a las que sólo tengan acceso los administradores.

- Conexiones a Internet, alimentación, sistemas anti incendios, etc.

- Protección contra desastres naturales y ataques terroristas.

- Establecer seguridad para las áreas en las que se puede dar un ataque por denegación de servicio (por ejemplo, las áreas en las que el cableado sale del LIF).

➢ **DIRECTIVAS, PROCEDIMIENTOS Y CONCIENCIACIÓN:** Este capa enmarca todas las capas del modelo de seguridad, por lo cual se encuentran las directivas y procedimientos que el laboratorio necesita establecer a fin de cumplir y admitir los requisitos de cada nivel. Por último, resulta importante que se estimule la concienciación en el LIF de todas las partes interesadas. En muchos casos, el desconocimiento de un riesgo puede llevar consigo infracciones en la seguridad, por lo que el aprendizaje también debe formar parte integrante de cualquier modelo de seguridad.

El uso de las capas de seguridad del modelo como base del método de defensa en profundidad le permitirá replantearse la perspectiva y optimizarlas en grupos para aplicar las defensas antivirus en el laboratorio.

### 7.8.1 Recomendaciones para cada una de las capas.

- Datos: Para el laboratorio se recomienda tener contraseñas difíciles de descifrar[59], ACL[60] y estrategias de respaldo para asegurar daños al laboratorio.

- Aplicación: Para el laboratorio se recomienda quitar o deshabilitar todas las aplicaciones o servicios innecesarios para reducir los ataques al sistema de forma malintencionada.

- Host: Para el laboratorio se recomienda tener los programas en constante auditoria para llevar a cabo una administración de actualizaciones habilitando un servidor de seguridad basado en host.

---

59 Contraseñas que incluyan números, caracteres especiales, letras mayúsculas y minúsculas.

60 ACL: Se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en un terminal u otro dispositivo de capa de red

- Red Interna: Para el laboratorio se recomienda instalar un IPS[61] y tener ACL.

- Red Perimetral: Para el laboratorio se recomienda tener firewalls[62], VPN[63], sistemas de detección como IPS y constantes pruebas de penetración[64].

- Seguridad física: Para el laboratorio se recomienda tener cámaras de seguridad, alarmas, personal de vigilancia para controlar el acceso físico al laboratorio garantizando un monitoreo constante y el correcto trabajo dentro del LIF.

## 7.9 COMUNICACIONES

Para establecer las comunicaciones se propone contar con celulares Avantel, además de los equipos de cómputo.

Se utilizarían 4 celulares Avantel's para ingenieros, abogado y expertos en seguridad informática.

## 7.10 RECURSO HUMANO

Para el manejo del recurso humano se estiman desarrollar procesos de selecciónentre los estudiantes de la universidad acompañados por un experto.

En la labor de reclutamiento del personal que laborará en el centro de cómputo, sugerimos aplicar los procesos actuales que tiene la universidad, pero es

61 IPS: Es un sistema de prevención de intrusos, monitorea la red y/o las actividades del sistema en busca de posibles intrusos.

62 Firewalls: es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado por medio de los puertos de red.

63 VPN o Red privada virtual: Es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet

64 Pruebas de penetración: son pruebas controladas de acceso no autorizado a un sistema para conocer el impacto real de un ataque informático.

recomendable además de este proceso, contar con el aval de un experto en seguridad informática.

El talento humano que participará en el proyecto debe cumplir con los siguientes requisitos básicos:

- Contar con conocimiento avanzado de telemática, herramientas de hacking ético, conocimiento de la cadena de custodia (aspectos legales) y conocimientos de sistemas de gestión de la información (Norma ISO 27001).
- Solida fundamentación técnica en el área de la seguridad informática y metodología que conduzca a la aplicación de buenas prácticas.
- Estar en capacidad de diseñar y gestionar estrategias que permitan garantizar la seguridad de la información.
- Experiencia en áreas afines a la seguridad informática.
- Liderazgo.
- Ética profesional.
- Conocimientos en lo referente a la legislación que regula el uso de herramientas informáticas[65].

  Asociación de tareas y cargos en WBS, para esto debe cumplir:

  - Aspectos de conocimiento.
  - Experiencia: Estudiantes activos o Egresados.

De acuerdo a la descomposición de las actividades o tareas de un proyecto y su asociación a las funciones que desempeñan el personal que esté involucrado en el proyecto.

**7.10.1 Roles Según Wbs.** Roles específico a cumplir dentro de cada una de las tareas del proyecto:

[65]Este punto se incluye debido a que el LIF requiere de la presencia de un abogado asesor.

- Supervisa
- Controla
- Registro
- Informa
- Recibe información
- Ejecución

## 7.11 ASPECTOS RELEVANTES

### Lo básico del registro de conservación de la evidencia.

Al suceder un incidente cometido a través de un medio informático dentro de una organización, las personas encargadas de averiguar qué fue lo que sucedió, muchas veces su primer paso es tomar nota de toda las actividades que sucedieron a fin de hacer seguimiento a un posible hecho punible e iniciar la clasificación de información que sirva para despejar lo ocurrido. Eso está muy bien, pero también por desconocimiento dejan de lado información o evidencia importante, que se debía tomar en el momento que sucedieron los hechos. Esta información debe ser protegida de una manera segura, confiable y que se le pueda hacer seguimiento desde el momento que fue recolectada hasta su análisis o destino final.

Una vez ocurrido el hecho, las personas encargadas de recolectar la evidencia digital, deben asegurarse de seguir una serie de pasos sencillos pero que a futuro son importantes dentro de una auditoria o seguimiento de una conducta punible, dichos pasos, a tener en cuenta es siempre, siempre utilizar herramientas adecuadas (ver en parte II) para proteger la evidencia, garantizar que es auténtica, mantener su identidad e integridad, preservarla en lugares adecuados al tipo de evidencia, brindarle seguridad, y sobre todo saber quién ha tenido contacto con dicho elemento (continuidad y registro), todo lo anterior se llama llevar una adecuada conservación de la evidencia desde que inicia hasta que se le da destino final a elemento material de prueba (EMP), es decir que una persona que recolecte una evidencia será responsable del contenedor (embalaje o empaque) y de la evidencia. Siempre que sea posible, registre fotográficamente los EMP antes

de su embalaje, durante el embalaje y al finalizar su embalaje y rotulado (descripción del elemento).

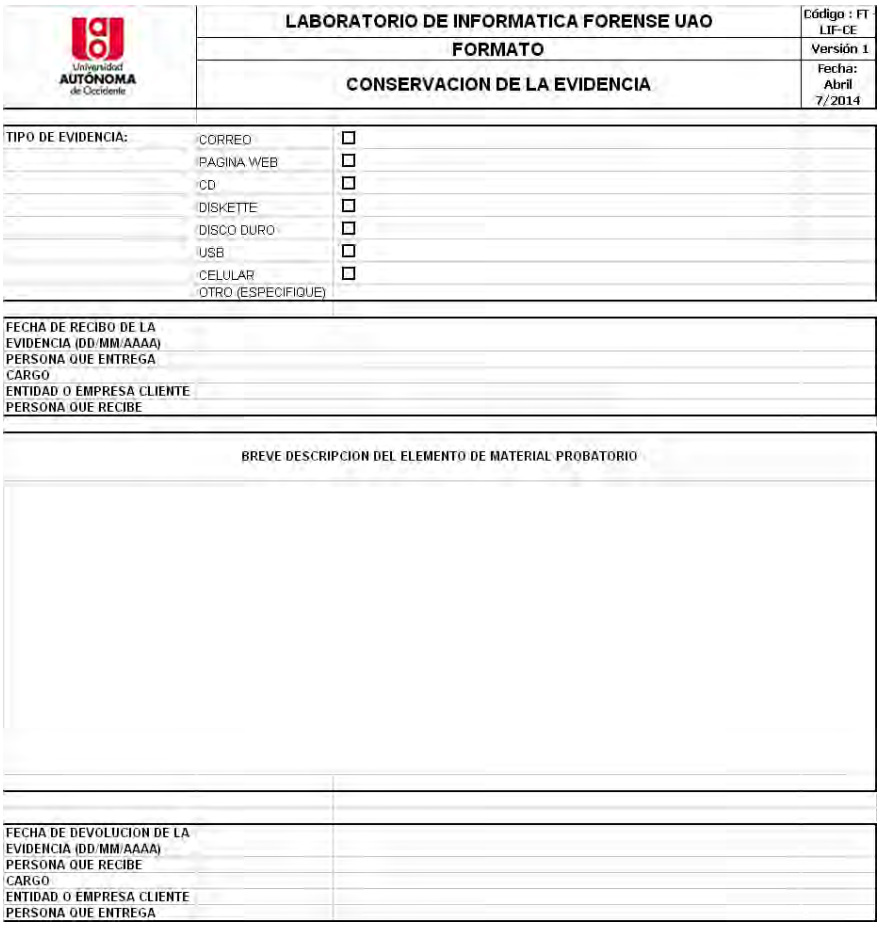
De acuerdo con lo anterior se deben diligenciar dos documentos uno se llamara rotulo, donde va la descripción del elemento y otro donde se llevara el registro y allí se plasme lo anterior y que cada vez que cambia de responsable, se diligencia su ubicación, estado y fecha de cambio, por lo que se siguiere se tengan en cuenta los siguientes campos donde la información debe ser completa y precisa:

**Figura 45. Rotulo**


- Identificación del caso.
- Fecha y hora de recolección o toma de evidencia.
- Lugar de recolección.
- Descripción del elemento (aquí se debe hacer una descripción completa del tipo de elemento, marca, serial, modelo, capacidad de almacenamiento).

Conservacion de la evidencia: Este es el formato que por medio del cual se registra la conservación de la evidencia[66].

[66] Este formato se adjunta a los anexos del proyecto.



| | LABORATORIO DE INFORMATICA FORENSE UAO | Código : FT LIF-CE |
|---|---|---|
| Universidad AUTÓNOMA de Occidente | FORMATO | Versión 1 |
| | CONSERVACION DE LA EVIDENCIA | Fecha: Abril 7/2014 |

| | | |
|---|---|---|
| TIPO DE EVIDENCIA: | CORREO | ☐ |
| | PAGINA WEB | ☐ |
| | CD | ☐ |
| | DISKETTE | ☐ |
| | DISCO DURO | ☐ |
| | USB | ☐ |
| | CELULAR | ☐ |
| | OTRO (ESPECIFIQUE) | |

| | |
|---|---|
| FECHA DE RECIBO DE LA EVIDENCIA (DD/MM/AAAA) | |
| PERSONA QUE ENTREGA | |
| CARGO | |
| ENTIDAD O EMPRESA CLIENTE | |
| PERSONA QUE RECIBE | |

| BREVE DESCRIPCION DEL ELEMENTO DE MATERIAL PROBATORIO |
|---|
| |

| | |
|---|---|
| FECHA DE DEVOLUCION DE LA EVIDENCIA (DD/MM/AAAA) | |
| PERSONA QUE RECIBE | |
| CARGO | |
| ENTIDAD O EMPRESA CLIENTE | |
| PERSONA QUE ENTREGA | |

- Identificación del caso.
- Fecha y hora de recolección.
- Quien encontró o halló, quien recolecto, embalo (persona que encontró la evidencia).
- Fecha y hora de entrega de la evidencia a otra persona.
- Nombre e identificación de la persona que recibe el elemento.
- Calidad en la que actúa (experto, custodio, analista, etc).
- Descripción de como recibe el elemento.
- Objetivo de la entrega (análisis, custodio).

- Firma.

Así pues, llevando muy sigilosamente los dos registros, durante la investigación de los hechos siempre se garantizará su integridad y que los elementos recolectados producto de una investigación de carácter digital se les ha hecho un excelente seguimiento de sus traslados y traspasos.[67].

## 7.12 MERCADEO

A pesar de que la UAO es una entidad sin ánimo de lucro, la puesta en marcha del LIF implicaría ingresos para la institución fruto de las investigaciones realizadas, pero para que se dé a conocer este laboratorio, es necesario llevar a cabo una labor previa de mercadeo.

En el desarrollo de este proyecto se determinó que es fundamental que el análisis forense se ofrezca a entidades gubernamentales y no gubernamentales, así como también ofrecer capacitación a manera de especialización para profesionales en el campo de informática.

El Marketing consta delas siguientes fases:

- Marketing Estratégico: esta parte la ejecuta directamente el representante del LIF[68], donde se analizan las oportunidades que tiene en el mercado, el estudio de la competencia, los ingresos, los costos, los beneficios y la prestación de los servicios.

- Marketing mix: Para el LIF esta fase es muy importante ya que se determinan las características de lo ofrecido vs entrega final, de acuerdo a estos 4 aspectos:

[67] LUIS CAMILO OSORIO ISAZA, manual de procedimiento de cadena de custodia [en linea] Bogota D.C [consultado en julio de 2014] Disponible en internet: http://richardgorky.com/normatividad/resolucion06394.pdf

[68] Ver descripción de este cargo en el capítulo 7.12

- Producto: Esta parte se enmarca en el LIFel servicio de análisis forense con su respectivo desarrollo, análisis y ejecución.

- Precio: Para el LIF el precio se ha de fijar en función de los beneficios que se desean obtener conforme a los competidores con el fin de ofrecer un buen servicio de análisis frente a delitos informáticos.

- Plaza: El LIF será atendido desde la región del valle del cauca dando servicio a nivel nacional.

- Promoción: La promoción del LIF se dará con charlas de presentación a estudiantes, vía web y visitas a potenciales clientes.

- Ejecución del programa de marketing: En esta parte es esencial para el LIF ya que se coloca en operación la segunda fase del proyecto, para que este obtenga así un reconocimiento a nivel educativo y social.

- Control: se ejecuta cuando el LIF ya esté en funcionamiento y se determinen realizar cambios en el marketing.

  Los siguientes son algunos de los mecanismos de control usados por las empresas:

- control de plan anual.

- control de rentabilidad.

- control de eficiencia.

- control estratégico.

## 7.13 MODELO OPERATIVO DEL LIF

A continuación se muestran los diferentes roles y procesos que se presentan dentro de un LIF, desde el punto de vista de los roles, se tiene en cuenta tres cargos[69]:

[69] Ver figura 28 “workflow de un LIF” en este documento.

- Representante del LIF: actúa en la mesa de entradas y salidas, es la cara del laboratorio ante las autoridades y clientes en general.

- Asistente: se encarga de los registros y los reportes de control, es el puente entre el representante y el experto.

- Experto: es el encargado de analizar la evidencia encontrada clasificando el material probatorio encontrado.

**7.13.1 Actividades para el representante del LIF.**Entradas:

- **Ingreso del secuestro:** es cuando se inicia oficialmente la cadena de custodia.

Salidas:

- **Registro de salida:** fin de la cadena de custodia y entrega del informe al cliente.

**7.13.2 Actividades para el asistente.**Entradas:

- **Registro de ingreso:** registra el ingreso de los elementos de material probatorio para su respectivo análisis.

Salidas:

- **Reportes complementarios, Control de salida:** documentación de todo lo hecho con la evidencia hasta su entrega al cliente.

**7.13.3 Actividades para el experto.** Este actor realiza la función del Análisis y profundización de la investigación.
Entradas:

- **Inspección general, Preservación de la evidencia:** asegurar que los elementos de material probatorio no se deterioren ni se pierdan.

- **Reporte Interno:** reporte de avances en la investigación y procedimientos realizados.

Salidas:

- **Pautas de la investigación, alcance de la pericia:** informe detallado sobre el desarrollo de la investigación y su alcance.

- **Elaboración del dictamen pericial:** Informe final resultado del análisis forense.

A continuación se muestran los procesos del LIF:

**Figura 46. Procesos de un LIF**


Procesos de un lif [En línea]. Consultado el día 28 de enero de 2014. Disponible en internet:http://www.slideshare.net/mmujica/informatica-forense-9598622

## 7.14 ASPECTO SOCIAL DEL LIF

Debido a la evolución de la informática se ha generado una revolución en la vida personal y profesional de la comunidad en general ya que la tecnología se encuentra presente en todos los aspectos de la sociedad, dando pie también a la aparición de los delitos informáticos.

El avance de la tecnología, facilita la portabilidad, la evolución de las comunicaciones y el mundo digital se ha convertido en un testigo continuo de todas las actividades de los usuarios, muchos de los cuales desconocen su funcionamiento y los riesgos que implican ciertas interacciones en redes como la internet.La mayoría de los usuarios, incluso muchos de los profesionales relacionados con el sector TI[70], desconocen la magnitud de los delitos informáticosque se cometen muchas veces por esta falta de conocimiento conllevando a conductas delictivas.

[70] TI: tecnologías de la información.

Por esta razón y cada vez con más frecuencia, se está evidenciando la necesidad de acudir a profesionales especialistas en Informática Forense.

Así mismo, la falta de conocimiento de la legislación que regula el uso de la tecnología por parte de los usuarios les limita la capacidad de valoración y verificación de la calidad y consistencia del trabajo realizado por profesionales informáticos que hacen los análisis forenses, razón por la cual es de suma importancia que se documente todo el procedimiento de manera tal que sea fácil de comprender para todo tipo de personas y de esa manera ganar confiabilidad y demostrar transparencia en los procedimientos realizados[71].

## 7.15 ASPECTO FINANCIERO DEL LIF

Inicialmente se debe contar con un presupuesto mínimo de $371.426.250, pero adicional a esto se debe tener en cuenta el sueldo del personal de planta del laboratorio, para poner en marcha el LIF es necesario contar con mínimo cuatro personas:

- 1 Abogado especializado en derecho informático.
- 1 Representante del LIF.
- 1 Asistente.
- 1 Experto Forense.

**Cuadro 9. Tabla de costos de personal**

| CARGO | INGRESO | SALUD (8,5 % | ENSION (12% | SENA (2%) | ICBF (3%) | A DE COMPENSACION | TOTAL MENSUAL |
|---|---|---|---|---|---|---|---|
| ABOGADO | $ 1.500.000,00 | $ 127.500,00 | $ 180.000,00 | $ 30.000,00 | $ 45.000,00 | $ 60.000,00 | $ 1.942.500,00 |
| REPRESENTANTE | $ 3.000.000,00 | $ 255.000,00 | $ 360.000,00 | $ 60.000,00 | $ 90.000,00 | $ 120.000,00 | $ 3.885.000,00 |
| EXPERTO FORENSE | $ 2.000.000,00 | $ 170.000,00 | $ 240.000,00 | $ 40.000,00 | $ 60.000,00 | $ 80.000,00 | $ 2.590.000,00 |
| | | | | | | SUBTOTAL MENSUAL | $ 8.417.500,00 |
| | | | | | | COSTO ANUAL PARCIAL | $ 101.010.000,00 |
| | | | | | | VACACIONES | $ 3.250.000,00 |
| | | | | | | PRIMAS | $ 6.500.000,00 |
| | | | | | | COSTO ANUAL TOTAL | $ 110.760.000,00 |

[71] LAZARUS TECHNOLOGY, xxviii congreso latinoamericano de seguridad bancaria [en línea] Madrid España [consultado en noviembre de 2013], Disponible en internet: http://www.felaban.com/archivos_actividades_congresos/SESION_04_Manuel_Huerta.pdf

Del cuadro anterior es obtiene un costo de personal anual de $110.760.000. Sumando estos valores se debe adicionar al presupuesto de $402.448.022[72]el valor de $110.760.000 equivalente al costo del personal por un año, lo cual nos da como resultado $513.208.022.

## 7.16 EQUIPO DE RESPUESTA DE INCIDENTES

El LIF debe contar con un equipo de respuestas de incidentes que puede estar conformado por estudiantes, egresados, profesores y funcionarios uao, los cuales deben estar debidamente capacitados, para lo cual se diseñó la guía para recolección de evidencias.

Pero adicional a lo mencionado anteriormente se deben diseñar instructivos para que este equipo tenga claro que hacer en caso de presentarse una situación especifica, para lo cual también deben desarrollarse manuales o guias las cuales se deben ajustar a los procesos internos de la UAO, estas se deben realizar en la segunda etapa de este proyecto en conjunto con los encargados del sistema de gestión de la calidad de la universidad.

Este equipo debe estar preparado para responder ante ataques en la plataforma tecnologica de la UAO como:

- Fuga de información.
- Ataques a servidores.
- Al tráfico de la red wifi.

## 7.17 GUIAS E INSTRUCTIVOS

En la segunda etapa de este proyecto se deben desarrollar instructivos tanto para personas expertas como para las que no lo son en cuanto a atención de

[72] Este valor se obtiene con la opción de comprar el software FTK.

incidentes, estos deben estar alineadas con los procesos internos de la UAO y también deben estar acorde a los estándares internacionales del manejo de la evidencia que se encuentre para que esta no se altere y sea valida ante una corte judicial.

Uno de los estándares que se puede tomar es el HB171:2003[73], en el cual se habla que el ciclo de vida de la evidencia digital consta de seis pasos fundamentales:

- Diseño de la evidencia.
- Producción de la evidencia.
- Análisis de la evidencia.
- Reporte y presentación.
- Determinación de la relevancia de la evidencia.

Una de las buenas prácticas que propone es la de clasificar la información de la organización para de esa manera establecer cual de ellas es critica para la parte misional y ejercer los controles necesarios.

También se debe contar con mecanismos que permitan validar la autenticidad e integridad de los registros electrónicos, tales como certificados digitales, criptografía, entre otros y es necesario identificar el autor de los registros almacenados, la fecha y hora de creación, se debe verificar que la aplicación esta operando correctamente en el momento de la generación de los registros.

Cuando se maneje evidencia digital, deben ser aplicados todos los principios procedimentales y forenses generales, como el principio de identidad de copias: del original, ya que cuando se duplica un archivo informático, la copia no es igual a la original, sino idéntica (un bit no difiere de otro bit y entre sí son inidentificables unívocamente).

Al obtener evidencia digital, las acciones que se hayan tomado, no pueden modificar esta evidencia.

[73] Handbook guidelines for the manager of I.T. evidence: Guia para la administracion de la evidencia de tecnologias de la información.

Cuando sea necesario que una persona acceda a evidencia digital original, esa persona debe estar entrenada y calificada para este propósito.

Todas las actividades relacionadas con obtención, acceso, conservación y transferencia de evidencia digital, deben estar completamente documentadas, preservadas y disponibles para revisión.

El individuo es responsable por todas las acciones que realice con respecto al manejo de evidencia digital mientras ésta esté bajo su cuidado.

Cualquier agencia gubernamental que sea responsable de obtener, acceder, conservar y transferir evidencia digital, es responsable de cumplir con estos principios.[74].

## 7.18 REPORTES, PRESENTACION Y FORMATOS

**7.18.1 Informe de recolección de la evidencia.** Es el primer formato que se diligencia, en el cual se especifica quien halla, recolecta, embala la evidencia y como la embala, este formato en su respaldo contiene la bitácora de trazabilidad de la evidencia.

Una recomendación importante en el momento de recolectar la evidencia es tomar las métricas de estas y enumerarlas.

**7.18.2 Albúm fotográfico.** Corresponde al registro fotográfico detallado de cada elemento de material probatorio hallado, antes de cada foto se escribe el número de la evidencia y debajo de esta se escribe la marca del equipo y una breve descripción de este.

Ademas de cada registro individual tambien se debe hacer un registro fotografico grupal de todas las evidencias el cual se denomina “sabana” este se anexa al album fotografico.

[74] Principios de la organización internacional de cómputo forense IOCE.

**7.18.3 Conservación de la evidencia.** Se diligencia el formato de conservación de la evidencia, en el cual se describe esta y se especifica de quien se recibe, quien la recibe, a quien se entrega al final y quien es el que la entrega.

**7.18.4 Registro imágenes forenses.** Se debe hacer un registro de cada imagen forense que se realice para de esa manera poderle hacer una trazabilidad al proceso de investigación.

**7.18.5 Informe final.** Para la elaboración del informe final se deben presentar todos los registros de lo que se hizo con el elemento de material probatorio, desde el momento de su recolección hasta su entrega.

Todos los formatos mencionados anteriormente se incluyen en los anexos de este documento.

## 7.19 INSTALACIONES

**Cuadro 10. Condiciones ambientales**

| Condición | Recomendación |
|---|---|
| Interferencia electromagnética | Protegerla con una Jaula de Faraday |
| Suministro energía eléctrica | Adquirir UPS, generador eléctrico |
| Ruido y vibración | Usar materiales aislantes del ruido |
| Sistema de refrigeración | Mantener el LIF a Temperatura 22ºC |
| | Humedad de 65% máximo |
| Sistema de extinción de incendios | Adquirir extintores de polvo químico seco, bióxido de carbono, espuma, INERGEN |

Las instalaciones deben contar con seguridad física para restringir el ingreso de personal no autorizado como se menciona en capítulos anteriores, también se debe contar con un sistema para bloquear la señal de celular y así realizar un análisis adecuado a los dispositivos móviles, en la siguiente imagen se muestra el equipo que se propone para manejar este aspecto.

**Figura 47. Bloqueador Celular 12 Watt de 4 antenas (ALBJ008)**

Bloqueador celular [En línea]. Consultado el día 01 de abril de 2014. Disponible en internet: http://www.alartel.8m.com/blank_161.html

El Bloqueador Celular 12 Watt Full Band (ALBJ008) posee gran efectividad y está especialmente diseñado para uso en interiores. Es ideal para ser instalado en aquellos lugares donde las comunicaciones celulares deben ser restringidas, ofreciendo un alcance efectivo de bloqueo que puede cubrir hasta 25-30 metros, dependiendo de las condiciones del ambiente y tiene un costo de $5900 pesos Mexicanos, equivalentes a $866.782,26 pesos Colombianos pero su compra es opcional y solo el sponsor decide si se adquiere este artefacto.

Aunque también se puede aislar la estática y restringir el uso de celular dentro del laboratorio, por medio de una malla de alambre que crea una "jaula de Faraday" la cual aisla el laboratorio. Esta se da creando una cubierta conductora que impide la entrada o escape de cualquier campo electromagnético. Las jaulas de Faraday se utilizan en laboratorios electrónicos para evitar que el electromagnetismo interfiera con las pruebas electrónicas. Un laboratorio con este recubrimiento prohíbe que los teléfonos celulares envíen o reciban alguna señal.[75]

[75] DAN BOONE, Materiales que afectan a las señales de los celulares [en linea] Bogotá D.C. Colombia [consultado en noviembre de 2013] Disponible en internet: http://www.ehowenespanol.com/materiales-afectan-senales-celulares-info_468322/

**Cuadro 11. Infraestructura interna**

| Área control de acceso | Área de almacenamiento | Área de análisis | Área mecánica |
|---|---|---|---|
| Ingreso de visitantes | Área de control de acceso y entrada | Zona con acceso a internet | Desmontaje de equipos |
| Ingreso de personal autorizado(Acceso de forma biométrica, con tarjetas de proximidad entre otros) | Estanterías | Zona sin acceso a internet | Ensamblaje de equipos |
| | Puertas con cerradura | Hardware forense | Uso de herramientas |
| | Persona responsable | Software forense | |

## 7.20 SANITIZACION DE LOS DISCOS DUROS

Se define como sanitizacion al borrado completo de los discos duros en los cuales se van a almacenar las imágenes de la evidencia del caso. Si este procedimiento no se realiza se corre el riesgo de alterar los hallazgos realizados durante la investigación, para ello se usa la herramienta de softare WIPE, la cual aplica una cierta cantidad de borrados a los discos para asegurar que estos queden completamente vacios.

También se puede utilizar el dispositivo de hadware T4 puente forense SCSI, el cual es un bloqueador de escritura para utilizar con discos duros SCSI (Small Computer Systems Interface, interfaz para sistemas de equipos pequeños). Maneja un rendimiento de 80MB/s, con este ya no se necesita utilizar los cables de puente y este modelo permite escanear automáticamente el bus SCSI.[76]

## 7.21 PROCEDIMIENTOS DEL LIF

A continuación se relacionan las diferentes actividades que se van a llevar a cabo en el LIF de la UAO:

[76] INTRASOFT PANAMA [en línea] Panamá [consultado en noviembre de 2013] Disponible en internet: http://www.intrasoftpanama.com/index.php?option=com_content&view=article&id=21&Itemid=16&limitstart=3

- Análisis técnico factico.
- Identificar de los medios de almacenamiento implicado en la investigación.
- Inicio de la conservación de la evidencia digital.
- Captura de los medios almacenamientos originales.
- Volcado de las imágenes forense en el laboratorio.
- Recuperación d datos borrados y de ambiente.
- Filtrado y análisis de documentos relevantes.
- Identificar y extracción de las pruebas.
- Reconstrucción de la cadena de acontecimientos.
- Presentación de resultados, elaboración del informe final o base opinión pericial a las autoridades.

# 8. CONCLUSIONES

Los resultados obtenidos con el desarrollo de este proyecto son los siguientes:

- La herramienta a utilizar es FTK, debido a su fácil manejo y amplio respaldo de la firma Accessdata, esto para empezar y sin rechazar la opción de adquirir posteriormente la licencia de ENCASE.

- Para el montaje del LIF se debe contar con los recursos relacionados en la siguiente tabla:

Cuadro 12. Opción recomendada

| PAQUETE | COSTO | VENTAJAS | DESVENTAJAS | COSTO TOTAL |
|---|---|---|---|---|
| SOFTWARE FTK PARA TRES EQUIPOS | $ 31.989.018 | Respaldo por parte de la casa desarrolladora del software de análisis forense . | El costo de esta opción es más elevado. | $ 402.448.022 |
| 1 ESTACION FORENSE FRED SR | $ 122.000.000 | | | |
| 1 ESTACION FORENSE FRED L | $ 85.000.000 | La operación del software licenciado es más sencilla. | | |
| 1 ULTRAKIT III (KIT DE BLOQUEADORES) | $ 14.000.000 | | | |
| MEDIOS DE ALMACENAMIENTO PARA EVIDENCIAS | $ 27.000.000 | | | |
| 1 CÁMARA FOTOGRÁFICAS SONY CYBERSHOT | $ 499.000 | | | |
| HERRAMIENTA XRY (DISPOSITIVOS MOVILES) | $ 19.460.004 | | | |
| DUPLICADOR DE DISCOS FORENSE | $ 20.000.000 | | | |
| CAPACITACION EN CADA UNO DE LOS MODULOS DE LA APLICACION (PARA TRES FUNCIONARIOS | $ 82.500.000 | El uso de este software tiene una trazabilidad a nivel mundial. | | |

- De esta información se obtiene que el montaje del LIF tiene un costo estimado de $402.448.022 sumando el valor de $110.760.000 que vale el personal durante un año se obtiene un costo total de $ 513.208.022.pesos colombianos.
- La puesta en marcha del LIF en la UAO (o segunda etapa de este proyecto) fomenta la creación de semilleros de estudiantes interesados en la especialidad de “informática forense”.

# 9. RECOMENDACIONES

Existen aspectos muy importantes a tener en cuenta para el montaje de un LIF, tales como:

- Infraestructura: se debe contar con espacios que faciliten la labor de los expertos forenses, debe haber un área mínima de 5mx5m en el lugar donde se realiza el proceso de análisis a la evidencia, adicionalmente se debe tener un lugar para el almacenamiento del material probatorio, el cual debe estar seco, evitando las temperaturas extremas (no mayor de 46°c ni menor de 16°c)[77] y campos magnéticos.

- Control de documentos: el laboratorio debe establecer y mantener procedimientos para el control de todos los documentos que forman parte de su sistema de gestión (generados internamente o de fuentes externas), tales como la reglamentación, las normas y otros documentos normativos, el software, las especificaciones, las instrucciones y los manuales[78].

- El laboratorio debe tener políticas y procedimientos para asegurar la protección de la información confidencial y los derechos de propiedad de sus clientes, incluidos los procedimientos para la protección del almacenamiento y la transmisión electrónica de los resultados (en caso de requerirse esta última).

- El laboratorio debe contar con suficientes instalaciones eléctricas y todas deben estar debidamente aterrizadas[79] para proteger los equipos de cómputo de descargas eléctricas, así como también se debe tener redundancia del servicio eléctrico por medio de ups y/o plantas eléctricas.

- Al personal que esté encargado de llevar a cabo la segunda fase de este proyecto se le recomienda llevar a cabo un estudio del mercado por medio del cual se obtenga información como valores a cobrar por los servicios (actualizados) y clientes potenciales del LIF.

---

[77] Información obtenida de la página web http://www.taringa.net/posts/info/5010222/Cuatro-Consejos-para-Cuidar-y-No-Danar-los-Discos-Rigidos.html

[78] Numeral 4.3.1 Generalidades de la norma ISO 17025 para la competencia de laboratorios, ver anexo 4 página 54 del archivo “anexos.docx”.

[79] Se entiende como aterrizada a una línea eléctrica que cuenta con polo a tierra para proteger el cableado de descargas producidas por las tormentas eléctricas.

- Para la etapa de implantación del LIF (segunda fase de este proyecto) tener en cuenta que los precios y costos mencionados en este documento fueron cotizados en el año 2014.

- Se recomienda crear conciencia en la población en general en cuanto a que "si esta encendido, no lo apagues, y si esta apagado, no lo enciendas". En caso de que esté encendido lo más común es simplemente fotografiar la pantalla y tirar del cable de la pared. Se deberá anotar que desconectó el cable para tener en cuenta más tarde que el SO puede estar en un estado inconsistente. Esto es útil saberlo para asi no alterar la evidencia y posteriormente iniciar el sistema de nuevo en un entorno seguro. [80]

[80] Recomendación tomada de las buenas prácticas del documento de D. Manuel José Lucena López, del Departamento de Informática de la Universidad de Jaén.

## BIBLIOGRAFIA


ALEJANDRO RAMOS [En línea]. Historia de la informatica forense [Consultado el día 08 de abril de 2014], Disponible en internet: http://www.securitybydefault.com/2011/03/historia-de-la-informatica-forense.html

ASOTO TECHNOLOGY GROUP [En línea].Bogotá D.C. Colombia [Consultado el día 10 de junio de 2013], Disponible en internet: http://www.asoto.com/

AVANTEL [En línea]. Equipos [Consultado el día 15 de mayo de 2013], Disponible en internet: http://comercial.avantel.com.co/equipos/

BLOG DE MARKETING [En línea]. El marqueting y sus fases [Consultado el día 16 de febrero de 2014], Disponible en internet: http://www.blogdemarketing.com/?p=19

CCN-CERT [En línea].Seguridad Informática [Consultado el día 11 de junio de 2013], Disponible en internet: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/http://msnseguridad.blogspot.com/2012/08/seguridad-informatica-la-seguridad.html

CELLEBRITE [En línea]. Ufed 4pc [Consultado el día 08 de abril de 2014], Disponible en internet: http://www.cellebrite.com/es/mobile-forensics/products/pc-based/ufed-4pc-logicall

CENTRO CIBERNETICO POLICIAL [En línea].Csirt, Bogotá, Colombia [Consultado el día 05 de junio de 2013], Disponible en internet: http://www.ccp.gov.co/gilaf.php

DAN BOONE [En línea]. Material que afecta la señal de celular [Consultado el día 08 de abril de 2014], Disponible en internet: http://www.ehowenespanol.com/materiales-afectan-senales-celulares-info_468322/

DIGITAL INTELLIGENCE [En línea].Nuevo Berlin, Alemania [Consultado el día 12 de diciembre de 2013]. Disponible en internet: https://www.digitalintelligence.com/

EDUARDO DIAZ [En línea]. Informatica Forense [Consultado el día 01 de octubre de 2013], Disponible en internet: http://informaticacefac.blogspot.com/

FBI [En línea]. Washington D.C., USA [Consultado el día 04 de junio de 2013], Disponible en internet: http://www.fbi.gov

FERNANDO ALCAZAR DEVIA ARIAS, GABRIEL RAMON JAIMES DURAN, INGRITH PATRICIA REYES VERGARA, JAMES TROY VALENCIA VARGAS, JUAN CARLOS BERMÚDEZ BERMÚDEZ, JUAN CARLOS JIMENEZ LEAL, MAGDA VICTORIA ACOSTA WALTEROS, MARTÍN ENRIQUE DÍAZ PARDO [En línea]. Manual de procedimientos del sistema de cadena de custodia [Consultado el día 07 de septiembre de 2013], Disponible en internet: http://www.usergioarboleda.edu.co/derecho_penal/pdf/2004-MANUAL%20CADENA%20DE%20CUSTODIA.pdf

GOBIERNO DE ESPAÑA [En línea]. Metodologia magerit, Madrid, España [Consultado el día 21 de agosto de 2013], Disponible en internet: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/Libro_I_metodo.pdf

GUSTAVO PAREDES, Curso de especializacion en informatica forense, Laboratorios desarrollados el mes de noviembre de 2013.

HACKTIMES [En línea]. Extrayendo la sam de windows [Consultado el día 25 de noviembre de 2013], Disponible en internet: http://www.hacktimes.com/contrasenas_de_windows/

HÉCTOR ACEVEDO JUÁREZ [En línea]. ITIL, para qué sirve? [Consultado el día 10 de junio de 2013], Disponible en internet: http://www.magazcitum.com.mx/?p=50

INFORMATICA FORENSE [En línea].Buenos Aires, Argentina [Consultado el día 01 de octubre de 2013], Disponible en internet: http://www.informaticaforense.com.ar/informatica_forense.htm

INIF [En línea].Lima, Peru [Consultado el día 10 de junio de 2013], Disponible en internet: http://www.sedeforense.edu.pe/

INIF [En línea].Lima, Peru [Consultado el día 10 de junio de 2013]. Disponible en internet: http://blogs.peru21.pe/atajosweb/2012/10/el-instituto-nacional-de-investigacion-forense-inif.html
INTECO [En línea].Madrid, España [Consultado el día 04 de junio del 2013], Disponible en internet:http://cert.inteco.es

INTERNET SOLUTIONS S.A.S. [En línea]. Bogotá, Colombia [Consultado el día 29 de enero de 2014], Disponible en internet: http://www.internet-solutions.com.co/emp.php

INTRASOFT [En línea].Consultado el día 10 de junio de 2013. Disponible en internet:http://www.intrasoftpanama.com/

IT PROCESS MAPS [En línea]. ITIL Gestión del riesgo [Consultado el día 17 de agosto de 2013], Disponible en internet:
http://wiki.es.it-processmaps.com/index.php/ITIL_Gestion_del_Riesgo

JHON JAIRO HERNANDEZ [En línea].Cadena de custodia [Consultado el día 10 de junio de 2013], Disponible en internet:
http://world-of-dino.blogspot.com/2012/10/cadena-de-custodia-resolucion-0-6394.html

UNIVERSIDAD DE LOS ANDES [En línea]. Laboratorio de Informatica Forense [Consultado el día 28 de septiembre de 2013], Disponible en internet: http://sistemas.uniandes.edu.co/main/laboratorios/laboratorio-de-informatica-forense

NFORMATICA FORENSE COLOMBIA [En línea]. Ley 527 de 1999 [Consultado el día 20 de diciembre de 2013], Disponible en internet:
http://www.informaticaforense.com.co/index.php?option=com_content&view=article&id=62:ley-527-de-1999&catid=36:colombia&Itemid=69

INFORMATICA FORENSE COLOMBIA [En línea]. Ley 1273 de 2009 [Consultado el día 20 de diciembre de 2013], Disponible en internet:
http://www.informaticaforense.com.co/index.php?option=com_content&view=article&id=61:ley-1273-de-2009&catid=36:colombia&Itemid=69

MATTICA [En línea].Mexico D.F. [Consultado el día 26 de marzo de 2013], Disponible en internet:http://www.mattica.com/2009/09/computo-forense-al-servicio-de-la-ley-para-delitos-informaticos/

REVISTA AUTÓNOMA AL DÍA VERSIÓN OCTUBRE DE 2013 [En línea].Conceptos basicos en seguridad informática [Consultado el día 08 de octubre de 2013] Disponible en internet:. http://www.uao.edu.co/

SEGURIDAD INFORMÁTICA [En línea]. Metodologia Magerit [Consultado el día 17 de agosto de 2013], Disponible en internet: http://seguridadinformaticaufps.wikispaces.com/MAGERIT

SLIDES SHARE [En línea]. Informatica Forense [Consultado el día 01 de octubre de 2013],Disponible en internet: http://www.slideshare.net/leidyjohanagarciaortiz/informatica-forense-17521392

SOFTWARE ENGINEERING INSTITUTE [En línea]. Octave, Pittsburgh, PA, U.S.A. [Consultado el día 17 de agosto de 2013]. Disponible en internet: http://www.cert.org/octave/

SUSCERTE [En línea]. Cenif, Caracas, Venezuela [Consultado el día 26 de marzo de 2013]. Disponible en internet: http://www.suscerte.gob.ve/index.php/es/seguridad-de-la-informacion/cenif

THE MURO GROUP INTERNATIONAL [En línea].Soluciones seguridad [Consultado el día 10 de junio de 2013]. Disponible en internet: http://www.themurogroup.com/analisis_forense.html

XRY [En línea]. [Consultado el día 08 de abril de 2014], Disponible en internet: http://www.msab.com/xry/xry-complete

YANAPTI [En línea].[Consultado el día 26 de marzo de 2013], Disponible en internet: http://www.yanapti.com/