PROYECTO PARA EL MEJORAMIENTO DEL LABORATORIO DEL GRUPO INVESTIGATIVO DE DELITOS INFORMÁTICOS DEL CUERPO TÉCNICO DE INVESTIGACIÓN "CTI" PASTO Y RESPALDO EN EL MEJORAMIENTO DE LA RED

ESTEFANÍA MUÑOZ CERÓN

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
SAN JUAN DE PASTO
2014

PROYECTO PARA EL MEJORAMIENTO DEL LABORATORIO DEL GRUPO INVESTIGATIVO DE DELITOS INFORMÁTICOS DEL CUERPO TÉCNICO DE INVESTIGACIÓN "CTI" PASTO Y RESPALDO EN EL MEJORAMIENTO DE LA RED

ESTEFANÍA MUÑOZ CERÓN

Informe final de pasantía para optar al título de Ingeniera Electrónica

ASESOR
ANDRÉS EDGAR CALVACHE GARCÍA
INGENIERO ELECTRÓNICO

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
SAN JUAN DE PASTO
2014

“Las ideas y conclusiones aportadas en el trabajo de grado son responsabilidad exclusiva de su autor.”

Artículo 1 del Acuerdo N. 324 de Octubre de 1966, emanado de Honorable Consejo Directivo de la Universidad de Nariño.

Nota de aceptación

_____
_____
_____
_____
_____
_____
_____

_____
Firma del jurado

Nota de aceptación

_____
_____
_____
_____
_____
_____
_____

_____
Firma del jurado

San Juan de Pasto, 2014.

DEDICATORIA

Este trabajo al igual que todos los proyectos en mi vida se lo dedico a Dios en agradecimiento por todas las bendiciones que ha puesto en mi vida, espero que con mi esfuerzo se vea retribuido todo lo que recibo. A mi madre Delia Cerón por ser mi guía y mi modelo de vida, por su sacrificio, por el amor y por el apoyo que me ha brindado en mis decisiones. A mi novio Marlon por brindarme su compañía y su comprensión en los momentos difíciles, por orientarme en momentos de confusión y por su amor incondicional

AGRADECIMIENTOS

Agradezco,

A la Fiscalía General de la Nación Seccional Pasto y su Cuerpo Técnico de Investigación

Al Ingeniero Pablo Andrés Gaviria coordinador del Grupo Investigativo de Delitos Informáticos del Cuerpo Técnico de Investigación CTI seccional Pasto

Al Esp. Andrés Edgar Calvache García Ingeniero Electrónico docente de la Universidad de Nariño, asesor del proyecto

Al Abogado Sebastián Gómez Master en Ingeniería del Software

A Héctor Rosero Mosquera Coordinador del Grupo Investigativo de Delitos Informáticos de Cuerpo Técnico de Investigación CTI seccional Medellín

Estefanía Muñoz Cerón

RESUMEN

El presente documento, describe el trabajo de grado en modalidad pasantía realizado con el Grupo Investigativo de Delitos Informáticos del Cuerpo Técnico de Investigación CTI de la Fiscalía seccional Pasto, para la formulación de un proyecto para la adecuación del laboratorio a cargo del grupo, orientada a la correcta manipulación del elemento material probatorio (E.M.P.). Proceso que va de la mano con el proyecto de Modernización Institucional por el que atraviesa la Fiscalía General de la Nación.

Se hace referencia especialmente a la norma NTC-ISO/IEC 17025 para la elaboración de una guía que oriente a la institución en actividades que permitan la acreditación del laboratorio Forense del Grupo de Delitos Informáticos, y se sugieren algunas tareas encaminadas a dar cumplimiento a clausulas relacionadas al perfil de la pasante

También se menciona las actividades que la pasante realizo en la administración de Red, teniendo en cuenta que esta es un miembro activo de la institución, con responsabilidades acordes a sus conocimientos.

ABSTRACT

This paper describes work done internship degree mode with Computer Crimes Investigative Group of the Cuerpo Tecnico Investigativo CTI Pasto sectional for the formulation of a project to laboratory adequacy of the group, oriented in the proper handling of material evidence. Process with follow the Institutional Modernization by passing through the Fiscalia General de la Nacion.

It referring especially to NTC-ISO/IEC 17025 to made a guide to orient the institution to accreditation activities for the Forensic Lab Computer Crime Group, and made tasks designed to satisfy the rule related to student's profile.

The student made activities performed in the through network management, considering that she is an active member of the institution, with responsibilities commensurate with their skills.

CONTENIDO

pág

INTRODUCCIÓN 17

1. MARCO TEÓRICO 19

1.1. INFORMATICA FORENSE 19

1.1.1. ¿QUE ES LA INFORMÁTICA FORENSE? 19

1.1.2. COMETIDO DE LA SECCION DE INFORMATICA FORENSE 19

1.1.3. ACTIVIDADES ILEGALES 20

1.1.4. TIPOS DE EVIDENCIAS 21

1.1.4.2. Terminales de telefonía móvil. 23

1.1.4.3. Dispositivos electrónicos. 23

1.1.5. ANÁLISIS FORENSE DE UN SOPORTE DIGITAL 24

1.1.6. INFORME PERICIAL 25

1.1.7. TELEFONIA 26

1.2. NORMA NTC ISO/IEC 17025:2005 28

1.2.1. Presentación de la Norma ISO/IEC 17025:2005 adaptada por el ICONTEC 28

1.2.2. La norma ISO/IEC 17025 internacional 29

1.2.3. Traducción de la Norma 30

1.2.4. Fundamentos de la Norma 30

2. PLANTEAMIENTO DEL PROBLEMA 32

2.1. FORMULACIÓN DEL PROBLEMA 32

3. JUSTIFICACIÓN 33

4. ANTECEDENTES 34

4.1. DISEÑO DE UN NUEVO ESQUEMA PARA EL PROCEDIMIENTO DE INDAGACIÓN DE LOS DELITOS INFORMÁTICOS. 34

4.2. TRIAGE IN-LAB: CASE BACKLOG REDUCTION WITH FORENSIC DIGITAL PROFILING (TRIAGE EN LABORATORIO REDUCCIÓN DE LISTAS DE ESPERA CON TÉCNICAS DE PERFILADO DIGITAL FORENSE) 34

4.3. ESTUDIO DE LECTORES DE BANDA MAGNÉTICA Y TECLADOS BANCARIOS, UTILIZADOS PARA EL CLONADO DE TARJETAS BANCARIAS MEDIANTE SKIMMERS MP3 35

4.4. ANTECEDENTES EN EL CTI DE LA FISCALIA GENERAL DE LA NACION 36

5. OBJETIVOS 37

5.1. OBJETIVOS GENERAL 37

5.2. OBJETIVOS ESPECÍFICOS 37

6. ALCANCE 38

7. DESCRIPCIÓN DE LA PASANTÍA 39

7.1. CUERPO TÉCNICO DE INVESTIGACIÓN C.T.I. 39

7.1.1. Misión..... 39

7.1.2. Visión 39

7.2. GRUPO DE DELITOS INFORMÁTICOS 39

7.2.1 ¿Qué servicios presta la Unidad de Delitos Informáticos del CTI? 40

8. DESARROLLO DE ACTIVIDADES..... 41

8.1. RECONOCIMIENTO DE LAS ACTIVIDADES A REALIZAR 41

8.2. RECOPILACIÓN DE INFORMACIÓN DEL ESTADO ACTUAL DEL LABORATORIO Y EQUIPO CON QUE CUENTA..... 42

8.2.1. Maquinas Forenses..... 43

8.2.2. Maquina Forense Portátil 45

8.2.3. UFED 46

8.2.4. Bloqueadores de escritura..... 47

8.3. CARACTERIZACIÓN DE EQUIPOS..... 50

8.4. INVESTIGACIÓN Y DOCUMENTACIÓN RESPECTO AL TEMA DE ADECUACIÓN DEL LABORATORIO DE DELITOS INFORMÁTICOS 51

8.5. DISEÑO DE LA PROPUESTA..... 77

8.5.1. Estado actual de la Propuesta..... 86

8.6. SUPERVISAR, ADMINISTRAR Y GESTIONAR EL MEJORAMIENTO DE LA RED87

8.6.1. Red de Acceso Inalámbrico 87

8.6.2. Telefonía IP 88

8.6.3. Puerta de enlace – Routers 90

CONCLUSIONES 93

RECOMENDACIONES 95

BIBLIOGRAFÌA 97

NETGRAFÍA 98

ANEXOS 99

LISTA DE TABLAS

pág

Tabla 1. DISTRIBUCIÓN DEPENDENCIAS Y NECESIDADES DE LA RED 41

Tabla 2. CARACTERIZACIÓN Y ADAPTACIÓN NORMA NTC ISO/IEC 17025 ...57

Tabla 3. GUÍA PARA LA IMPLEMENTACIÓN DE LABORATORIOS DE INFORMÁTICA FORENSE QUE CONTEMPLA ASPECTOS BÁSICOS DE HARDWARE Y SOFTWARE 82

LISTA DE FIGURAS

pág

Figura 1. EVIDENCIA INFORMÁTICA PORTABLE 22

Figura 2. EVIDENCIA INFORMÁTICA CONTENIDA EN EQUIPOS PORTÁTILES O DE MESA 22

Figura 3. EVIDENCIA EN TELEFONÍA MÓVIL 23

Figura 4. EVIDENCIA EN DISPOSITIVOS ELECTRÓNICOS 24

Figura 5. TORRE FORENSE I 44

Figura 6. TORRE FORENSE II 45

Figura 7. MÁQUINA FORENSE PORTÁTIL 46

Figura 8. UFED 47

Figura 9. PUENTE T35es 48

Figura 10. PUENTE T35es-RW 49

Figura 11. TABLEAU T8 50

Figura 12. CICLO DEMING DEL DESARROLLO DE LA PROPUESTA 84

Figura 13. DIAGRAMA ESTRUCTURAL DE LA PLANTA FÍSICA DEL LABORATORIO DE DELITOS INFORMÁTICOS DEL CTI SECCIONAL PASTO . 85

Figura 14. DIAGRAMA ESTRUCTURAL PROPUESTO PARA LA PLANTA FÍSICA DE DELITOS INFORMÁTICOS DEL CTI SECCIONAL PASTO 85

Figura 15. ESTADO ANTERIOR Y ESTADO ACTUAL DE LA RED INALÁMBRICA DEL CTI 88

Figura 16. ESTADO ANTERIOR Y ESTADO ACTUAL DE LA TELEFONÍA VoIP DEL CTI 90

Figura 17. ESTRUCTURA DE LA RED DE DATOS EL PRIMER DÍA DE LA PASANTÍA.....91
Figura 18. ESTRUCTURA DE LA RED DE DATOS AL FINALIZAR LA PASANTÍA 92

LISTA DE ANEXOS

pág
Anexo 1. FORMATO DE HOJAS DE VIDE DE EQUIPOS……...100

Anexo 2. HOJA DE VIDA ESTACION FORENSE 1..... .....……102

Anexo 3. HOJA DE VIDA ESTACION FORENSE 2……103

Anexo 4. HOJA DE VIDA ESTACION FORENSE 3……104

Anexo 5. HOJA DE VIDA PC-UFED……... …105

Anexo 6. HOJA DE VIDA UFED…… ..……...106

INTRODUCCIÓN

Una de las mayores preocupaciones a nivel mundial en cuanto a seguridad, es el cibercrimen. Entre los últimos 15 años este tipo de delitos que actualmente se conocen como los delitos informáticos, se han convertido en un fenómeno con tendencia de crecimiento exponencial y con alto impacto en la seguridad de las empresas e instituciones en todas las naciones, incluso dentro de los hogares no se está exento de ser víctima de un delincuente informático.

"El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones""[1], esto tipifica la llamada evidencia informática como un argumento válido en un proceso penal.

La situación coyuntural del cibercrimen en Colombia y acoplándose a la llegada de esta Ley al código penal colombiano, se creó una nueva división dentro de la policía judicial conocida como el Grupo de delitos informáticos, conformado por servidores con perfiles acordes para contrarrestar el perjuicio que dicho tipo de delitos generan en el país.

Cabe mencionar que a pesar de la vigencia y oportunidad de la ley en cuestión en nuestro País, la cantidad de procesos judiciales que hasta la actualidad se han tipificado bajo sus parámetros, no es significativa frente a su capacidad y alcance jurídico, en relación a la cantidad de denuncias que se reciben diariamente.

Lo anterior debido a la dificultad de consolidar y contar de manera tangible con evidencia digital que se encuentre soportada legalmente, bajo el respaldo de estándares en los procedimientos para su obtención y que faciliten la apropiación y dominio por parte de las autoridades que no cuenten con conocimientos técnicos relacionados con la materia, de manera que sean de fácil entendimiento para su manejo y uso argumentativo en los distintos procesos.

---

[1] GANDINI Isabella y otros. Ley de Delitos Informáticos en Colombia. Recuperado el 29 de Enero de 2014, de: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

La estandarización de los procedimientos que rodean la consecución de evidencia digital y la orientación hacia una acreditación, fortalecen el sistema de justicia al entregar herramientas apropiadas e indiscutibles para dictar sentencias definitivas.

1. MARCO TEÓRICO

1.1. INFORMATICA FORENSE

1.1.1. ¿QUE ES LA INFORMÁTICA FORENSE?

Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio electrónico, teniendo su fundamento en las leyes de la física, de la electricidad y el magnetismo. Lo que se conoce como Evidencia Digital.

Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

La criminalidad organizada en materia de nuevas tecnologías viene creciendo de manera exponencial. La pericia informática es uno de los medios probatorios con más auge en los procesos civiles, mercantiles y penales.

Este es el marco de competencias de los Laboratorios de Informática Forense.

1.1.2. COMETIDO DE LA SECCION DE INFORMATICA FORENSE

"Analizar el contenido de soportes digitales, dispositivos electrónicos o terminales de telefonía móvil, intervenidos con ocasión de la comisión de un acto delictivo, extraer las evidencias que sirvan de prueba judicial, (ficheros, imágenes) que estén relacionadas con el asunto investigado y presentarla de forma clara y ordenada en el Informe Pericial, respondiendo a los puntos de pericia solicitados por el juez en cada caso y posteriormente defender el IP en el Juicio Oral."[2]

Los investigadores de informática forense usan gran cantidad de técnicas para descubrir las evidencias, incluyendo herramientas de software que automatizan y aceleran el análisis.

---

[2] Comisaría General de Policía Científica. Pág. 4. Recuperado el 29 de enero de 2014, de: http://www5.poderjudicial.es/CVdi/TEMA02-ES.pdf

Las evidencias electrónicas pueden recogerse en diferentes lugares y de diferentes fuentes, y podrán encontrarse en cualquier elemento o sistema que se esté utilizando para transmitir o almacenar los datos.

En una investigación forense digital se presta una especial atención al cuidado en la manipulación de los soportes a analizar, para mantener la integridad de la evidencia. Los peligros para las evidencias digitales son muchos y graves, y van de la mano de los virus informáticos, del deterioro electromagnético o mecánico del soporte, e incluso con la presencia de trampas dejadas por el atacante.

Las reglas básicas que ayudan a asegurar que la evidencia no se destruya o quede alterada durante la investigación son:

- Utilizar solo herramientas y métodos que hayan sido probados y evaluados previamente para determinar su precisión y sensibilidad reales.

- Manipular lo menos posible la evidencia original para evitar cambiar los datos.

- Establecer y mantener una cadena de custodia.

- Documentar todo lo que se ha hecho.[3]

1.1.3. ACTIVIDADES ILEGALES

Entre los delitos más habituales investigados se encuentran:

- Amenazas, injurias, calumnias, por medio de correo electrónico, SMS, tablones de anuncios, foros, chat.

- Protección al menor: producción, distribución y posesión de pornografía infantil.

- Falsificación de moneda y estafas bancarias:

[3] Ibíd. Pág. 4, 5.

- Carding: uso de tarjetas de crédito ajenas o fraudulentas
- Phising: redirección mediante correo electrónico a falsas páginas simuladas trucadas (común en las mafias rusas).
- Cartas nigerianas: (segunda fuente de ingresos del país, según el FBI).

- Falsedad documental.
- Manipulación de cajeros.
- Agresiones sexuales.
- También puede ser cualquier tipo delictivo: Homicidios, Tráfico de Estupefacientes, secuestros, extorsiones, etc.

A parte de estas descritas, cualquier tipo delictivo que pueda dejar rastros en un soporte digital y hoy en día pueden ser todos.[4]

1.1.4. TIPOS DE EVIDENCIAS

Podemos establecer pues tres tipos de soportes:

1.1.4.1. Soportes Informáticos

- Soportes portátiles: aquellos que disponen de una carcasa que permite su traslado garantizando la integridad de la información en ellos contenida, por lo tanto hablamos de disquetes, discos CD o DVD, soportes de memoria del tipo compact flash, memoria stick, SD card, XD card y sus variantes del tipo micro o dúo y dispositivos USB (del tipo pendrive, MP3, MP4, Ipod o discos duros externos) o firewire.

[4] Ibíd. Pág. 5, 6.

Figura 1. EVIDENCIA INFORMÁTICA PORTABLE

Fuente: La autora.

➢ Soportes contenidos en equipos portátiles o sobremesa: incluye principalmente discos duros ubicados en el interior de equipos informáticos, discos duros de tipo IDE, SCSI o SATA en sus distintos tamaños de 3,5 pulgadas, 2.5 pulgadas y 1,8 pulgadas o microdrive. En este tipo también podrían incluirse dispositivos del tipo PDA o PALM.

Figura 2. EVIDENCIA INFORMÁTICA CONTENIDA EN EQUIPOS PORTÁTILES O DE MESA

Fuente: La autora.

1.1.4.2. Terminales de telefonía móvil.

Incluyendo tanto la memoria interna del teléfono como la tarjeta SIM. Las tarjetas de memoria adicional que incorporan algunos de teléfonos se podrían clasificar como un soporte informático portátil.

Figura 3. EVIDENCIA EN TELEFONÍA MÓVIL

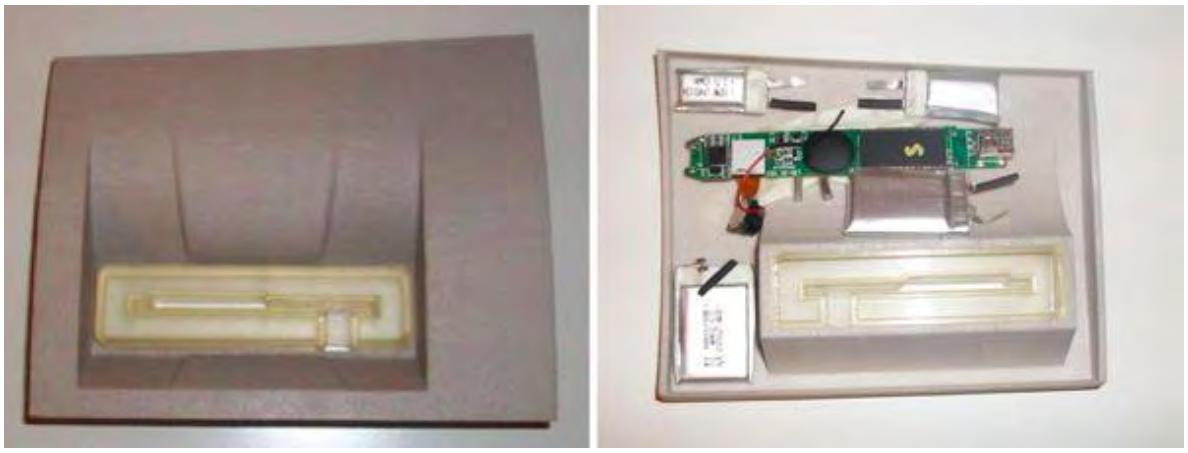
Fuente: La autora.

1.1.4.3. Dispositivos electrónicos.

En este grupo incluiríamos cualquier dispositivo electrónico capaz de almacenar información, tales como los skimmers usados en la falsificación de tarjetas, tarjetas de televisión de pago, etc.[5]

[5] Ibíd. Pág. 6, 7.

Figura 4. EVIDENCIA EN DISPOSITIVOS ELECTRÓNICOS



Fuente: La autora.

1.1.5. ANÁLISIS FORENSE DE UN SOPORTE DIGITAL

El objetivo es encontrar toda la información relacionada con el asunto investigado que se encuentre almacenada en el soporte analizado. En primer lugar hay que plantearse el tipo de soporte a analizar, estado físico del mismo, sistema operativo, etc.

Las fases de un análisis forense son:

1. Duplicar
2. Analizar
3. Presentar: Redactar el Informe Pericial

Duplicar quiere decir, realizar una copia exacta de la evidencia para analizarla. Existen dos formas:

- Volcado: Traspaso de datos originales en un formato apto para ser tratado por la herramienta de análisis que se vaya a utilizar.

- Clonado: Copia exacta del original, realizada bit-a-bit.

Duplicar la evidencia (IMAGING) presenta una serie de inconvenientes como son, el tiempo requerido y la necesidad de un soporte para el volcado; a su vez presenta muchas ventajas como son, mantener la integridad de la evidencia y la posibilidad de repetir el análisis las veces que sea necesario.

A la hora de analizar la información nos encontramos con una serie de dificultades:

- Tamaño de la muestra.
- Ficheros de tipo desconocido.
- Desconocimiento del funcionamiento de las aplicaciones informáticas, motivo por el cual se debe estar en constante formación.
- Cambios en la apariencia de la información (extensiones de ficheros/signaturas).
- Ficheros borrados.
- Ficheros protegidos.
- Ficheros cifrados.
- Esteganografia.[6]

1.1.6. INFORME PERICIAL

"El informe del investigador o perito del laboratorio deberá tener las siguientes características:

- La descripción clara y precisa del elemento material probatorio y evidencia física examinados.
- La descripción clara y precisa de los procedimientos técnicos empleados en la realización del examen y, además, informe sobre el grado de aceptación de dichos procedimientos por la comunidad técnico-científica.
- Relación de los instrumentos empleados e información sobre su estado de mantenimiento al momento del examen.

[6] Ibíd. Pág. 7, 8.

- Explicación del principio o principios técnicos y científicos aplicados e informe sobre el grado de aceptación por la comunidad científica.

- Descripción clara y precisa de los procedimientos de su actividad técnico-científica.

- Interpretación de esos resultados."[7]

1.1.7. TELEFONIA

Lo más interesante, desde el punto de vista forense, es su capacidad para almacenar información. Un teléfono inteligente está compuesto habitualmente de los siguientes componentes con capacidad para almacenar información:

1. Un terminal

2. Una o varias tarjetas SIM

3. Una o varias tarjetas de memoria adicional

Un terminal de telefonía móvil contiene dos tipos de memoria: memoria volátil y memoria no volátil. La memoria volátil es similar a la que todos conocemos como memoria RAM en los ordenadores personales. Es aquella cuya información se pierde al interrumpirse el flujo de corriente eléctrica. La no volátil es aquella cuyo contenido no se pierde al interrumpirse el flujo eléctrico que la alimenta. Esta última es la memoria que nosotros vamos a tener en consideración.

En la memoria no volátil de teléfono móvil es donde se almacenan todos los datos relativos a sistema operativo y programas, pero también los datos de usuario como pueden ser:

- Archivos de texto, imagen, sonido, vídeo.

- Agenda telefónica, registros de llamadas, mensajes SMS o multimedia

---

[7] DEFENSORIA DEL PUEBLO. Código de Procedimiento Penal. Pág. 132. Recuperado el 15 de enero de 2014, de: http://www.defensoria.org.co/red/anexos/publicaciones/cod_prospenal.pdf

- Correos electrónicos, registros de visitas a páginas Web.

- Agenda personal, notas, citas, etc.

Las estructuras de estas memorias también varían entre fabricantes y entre los distintos modelos y versiones de terminales de cada fabricante. Este es el mayor problema con el que nos encontramos para poder acceder a los datos en ellas contenidos.

La tarjeta SIM es un componente removible que contiene información esencial sobre el abonado. La función principal de la Tarjeta SIM es la autenticación del usuario del teléfono móvil a la red para obtener acceso a los servicios que tiene contratados.

Las tarjetas SIM están protegidas de acceso mediante un código de identificación personal (PIN). Este código PIN (número de 4 cifras) puede ser modificado por el abonado, de tal forma que sea la única persona que tenga conocimiento del mismo.

El código de desbloqueo se denomina código PUK y es proporcionado por las compañías telefónicas que gestionan la tarjeta SIM bloqueada.

Datos contenidos en una SIM:

1. Información relativa al servicio prestado por la compañía telefónica.

2. Agenda de teléfonos e información sobre llamadas, realizadas, recibidas y perdidas.

3. Información relativa a mensajes de texto, tanto SMS (mensajes de texto), como EMS (SMS, mejorado con animaciones, melodías, sonidos,…) y mensajes multimedia.

4. Información de localización.[8]

[8] Comisaría General de Policía Científica. Pág. 10, 11. Recuperado el 29 de enero de 2014, de: http://www5.poderjudicial.es/CVdi/TEMA02-ES.pdf

1.2. NORMA NTC ISO/IEC 17025:2005

1.2.1. Presentación de la Norma ISO/IEC 17025:2005 adaptada por el ICONTEC

El Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La NTC-ISO/IEC 17025 (Primera actualización) fue ratificada por el Consejo Directivo de 2005-10-26.

Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico 21 Evaluación de la Conformidad.

ACEGRASAS S. A.
ACUEDUCTO DE BOGOTÁ S. A. ESP
ALPINA PRODUCTOS ALIMENTICIOS S. A.
AMG E. U
ASOPESAJE
BASCUTE
BCI
BUREAU VERITAS QUALITAS
INTERNATIONAL BVQI COLOMBIA
CENTROAGUAS S. A. ESP
CENTRO DE INVESTIGACIONES
METROLÓGICAS GLOBAL METRIC
CHALLENGER S. A.
CIBA ESPECIALIDADES QUÍMICAS
COLCERÁMICA S. A.

COLGATE –PALMOLIVE–
CONSECIONARIA TIBITOC S. A.
COTECMAR
COTECNA CERTIFICADORA SERVICES
DIRIMPEX LTDA.
ELECTROMANUFACTURAS
EMPRESA COLOMBIANA DE PETRÓLEOS –ECOPETROL–
EMPRESA COLOMBIANA DE SOPLADO E INYECCIÓN S.A. –ECSI–
EMPRESA DE LICORES DE CUNDINAMARCA
ENGICAST LTDA.
EQUIPOS & CONTROLES
FUNDACIÓN GILLÓN
HOLCIM COLOMBIA S. A.
IDEAM
IMPROTEC LTDA.
METRON QUALITY CONSULTING
PINZUART LTDA.
PROGEN LTDA.
QUALITAS INGENIERÍA
SENA LABORATORIO MEDICIONES–LONGITUDES–
SGS COLOMBIA S. A.
SHELL COLOMBIA S. A.
SIG-MA
SIKA COLOMBIA S. A.
SMS CALIDAD & PROCEDIMIENTOS
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
TECNIBÁSCULAS LA GARANTÍA LTDA.
UNIVERSIDAD DEL NORTE
UNIVERSIDAD DE LA SABANA
UNIVERSIDAD NACIONAL DE COLOMBIA

1.2.2. La norma ISO/IEC 17025 internacional

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los organismos nacionales miembros de ISO e IEC participan en el desarrollo de las Normas Internacionales a través de comités técnicos establecidos por la organización respectiva, para tratar con campos particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, públicas y privadas, vinculadas a ISO e IEC, también participan en el trabajo. En el campo de la evaluación de la conformidad, el Comité de ISO para la evaluación de la conformidad (CASCO) es responsable del desarrollo de Normas y Guías Internacionales

Las Normas Internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las Directivas ISO/IEC.
Los Proyectos de Normas Internacionales se circulan a los organismos nacionales para votación. La publicación como Norma Internacional requiere la aprobación por al menos el 75 % de los organismos nacionales con derecho a voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO e IEC no se responsabilizan por la identificación de ningún derecho de patente.

La Norma ISO/IEC 17025 fue preparada por el Comité de ISO para la evaluación de la conformidad (CASCO).

Fue circulada para su voto a los organismos nacionales tanto de ISO como de IEC, y fue aprobada por ambas organizaciones.

Esta segunda edición anula y reemplaza a la primera edición (ISO/IEC 17025:1999), la cual ha sido revisada técnicamente.

1.2.3. Traducción de la Norma

Esta Norma Internacional ha sido traducida por el Grupo de Trabajo “Spanish Translation Working Group” del Comité ISO/CASCO, Comité para la evaluación de la conformidad, en el que participan representantes de los organismos nacionales de normalización y representantes del sector empresarial de los siguientes países:

Argentina, Brasil, Bolivia, Chile, Colombia, Costa Rica, Cuba, España, Estados Unidos de América, México, República Dominicana, Uruguay y Venezuela.

Igualmente, en el citado Grupo de Trabajo participan representantes de COPANT (Comisión Panamericana de Normas Técnicas) e IAAC (Cooperación Interamericana de Acreditación).

Esta traducción es el resultado del trabajo que el Grupo ISO/CASCO STWG viene desarrollando desde 2002 para lograr la unificación de la terminología en lengua española en el ámbito de la evaluación de la conformidad.

1.2.4. Fundamentos de la Norma

La primera edición (1999) de esta Norma Internacional fue producto de la amplia experiencia adquirida en la implementación de la Guía ISO/IEC 25 y de la Norma EN 45001, a las que reemplazó. Contiene todos los requisitos que tienen que cumplir los laboratorios de ensayo y de calibración si desean demostrar que poseen un sistema de gestión, son técnicamente competentes y son capaces de generar resultados técnicamente válidos.

La primera edición hacía referencia a las Normas ISO 9001:1994 e ISO 9002:1994. Dichas normas han sido reemplazadas por la Norma ISO 9001:2000, lo que hizo necesario alinear la Norma ISO/IEC 17025. En esta segunda edición se han modificado o agregado apartados sólo en la medida que fue necesario a la luz de la Norma ISO 9001:2000.

Es conveniente que los organismos de acreditación que reconocen la competencia de los laboratorios de ensayo y de calibración se basen en esta Norma Internacional para sus acreditaciones. El capítulo 4 establece los requisitos para una gestión sólida. El capítulo 5 establece los requisitos para la competencia técnica en los tipos de ensayos y/o de calibraciones que el laboratorio lleva a cabo.

El creciente uso de los sistemas de gestión ha producido un aumento de la necesidad de asegurar que los laboratorios que forman parte de organizaciones mayores o que ofrecen otros servicios, puedan funcionar de acuerdo con un sistema de gestión de la calidad que se considera que cumple la Norma ISO 9001 así como esta Norma Internacional. Por ello, se ha tenido el cuidado de incorporar todos aquellos requisitos de la Norma ISO 9001 que son pertinentes al alcance de los servicios de ensayo y de calibración cubiertos por el sistema de gestión del laboratorio.

Los laboratorios de ensayo y de calibración que cumplen esta Norma Internacional funcionarán, por lo tanto, también de acuerdo con la Norma ISO 9001.

La conformidad del sistema de gestión de la calidad implementado por el laboratorio, con los requisitos de la Norma ISO 9001, no constituye por sí sola una prueba de la competencia del laboratorio para producir datos y resultados técnicamente válidos. Por otro lado, la conformidad demostrada con esta Norma Internacional tampoco significa que el sistema de gestión de la calidad implementado por el laboratorio cumple todos los requisitos de la Norma ISO 9001.

La aceptación de los resultados de ensayo y de calibración entre países debería resultar más fácil si los laboratorios cumplen esta Norma Internacional y obtienen la acreditación de organismos que han firmado acuerdos de reconocimiento mutuo con organismos equivalentes que utilizan esta Norma Internacional en otros países.

El uso de esta Norma Internacional facilitará la cooperación entre los laboratorios y otros organismos y ayudará al intercambio de información y experiencia, así como a la armonización de normas y procedimientos.

2. PLANTEAMIENTO DEL PROBLEMA

Bajo el ánimo del proyecto de Modernización Institucional[9] por el que atraviesa la Fiscalía General de la Nación, es necesario identificar las opciones de mejoramiento, las cualidades y los aspectos que requieren intervención para llegar a la construcción de soluciones que permitan avanzar y alcanzar estándares de excelencia.

Entre las opciones de mejoramiento aparece la oportunidad de adecuación del laboratorio a cargo del Grupo Investigativo de Delitos Informáticos del Cuerpo Técnico de Investigación "CTI" de la Fiscalía General de la Nación Seccional Pasto, atendiendo las necesidades y requerimientos de conservación del elemento material probatorio (E.M.P.) [10].

Además, cabe resaltar que dentro de cualquier organización un elemento importante es el manejo de la información, y para el CTI de la Fiscalía, se convierte en una continua necesidad el correcto manejo, seguridad y disponibilidad de la misma, pues dicha información articula un marco fundamental en su actuación, concentrando como materia prima, bases de datos, decisiones judiciales, actividades de Policía Judicial y los resultados a sus investigaciones; información que puede verse afectada por factores externos e internos, entre los cuales se cuentan: cortes de fluido eléctrico, que afectan la vida útil de los elementos de red; deficiencias en la utilización óptima de los recursos y tecnologías de comunicación; inadecuada adecuación física y ambiental; la ausencia de personal con dedicación exclusiva y capacitado para hacer frente a los aspectos de red en su soporte físico y lógico, por mencionar algunas.

2.1. FORMULACIÓN DEL PROBLEMA

¿Cómo se puede aportar al mejoramiento del Laboratorio Forense del Grupo Investigativo del CTI de la Fiscalía General de la Nación Seccional Pasto y respaldar las labores de supervisión, administración y gestión del mejoramiento de la red?

---

[9] LA REFORMA*, Boletín Informativo del proyecto de modernización Institucional de la Fiscalía.* Fiscalía General de la Nación. Edición 1. Mayo del 2013.

[10] Fiscalía General de la Nación. Reglamento Interno para el manejo del Elemento Material Probatorio (E.M.P). Recuperado el 02 de mayo de 2013, de: Fiscalnet.

3. JUSTIFICACIÓN

Desarrollar una pasantía dentro del Cuerpo Técnico de Investigación “CTI” de la Fiscalía General de la Nación seccional Pasto genera vínculos académicos que permiten al estudiante enfrentar un reto profesional real en el campo laboral, donde se tiene la oportunidad de poner en práctica los conocimientos adquiridos en las aulas de clase.

Para el CTI es un momento coyuntural ideal en el cual las condiciones están dadas para obtener el mayor provecho de la iniciativa planteada.

La formulación del proyecto de adecuación del laboratorio a cargo del Grupo Investigativo de Delitos Informáticos del Cuerpo Técnico de Investigación “CTI” de la Fiscalía General de la Nación Seccional Pasto, fomenta una mayor inversión del presupuesto nacional en innovación y desarrollo local, partiendo del hecho que sería uno de los laboratorios al servicio de la Entidad, que brinde mayores garantías en el campo técnico, frente a la protección y el manejo de evidencias de características digitales y electrónicas.

En cuanto al manejo y la administración en cada uno de los elementos que hacen parte de las tecnologías de comunicación, las mejoras aportan tanto al orden como al correcto funcionamiento de la Entidad como conjunto y como grupos investigativos en torno a las prácticas que se desarrollen, conjugando un aporte a una área con necesidades mayores como lo es el CTI.

Al tener en consideración la naturaleza del laboratorio que es el centro de trabajo del presente proyecto, relacionado con delitos de tipo tecnológico y para dar una pronta respuesta a la gran cantidad procesos, es necesario que dicho laboratorio se encuentre ajustado a una serie de requerimientos que permitan su fácil adaptación y actualización, acorde a estándares nacionales e internacionales; logrando mayor competencia y efectividad en la administración de justicia.

4. ANTECEDENTES

Los antecedentes que se mencionan a continuación se refieren a proyectos en los que se ha trabajado con respecto a laboratorios de informática forense:

4.1. DISEÑO DE UN NUEVO ESQUEMA PARA EL PROCEDIMIENTO DE INDAGACIÓN DE LOS DELITOS INFORMÁTICOS.

Esta tesis presentada a la facultad de Ingenierías de la Universidad Politécnica Salesiana de Guayaquil Ecuador tiene como objetivo establecer las formas de delito informático con herramientas tecnológicas, mediante un esquema que cuenta con procedimientos, funciones y requerimientos mínimos para combatir los mismos.

Expone la inexistencia de acciones procedimentales en el Ecuador, establecidos para resolver los casos de delitos informáticos y la falta de conocimiento sobre herramientas para adquirir, preservar y recuperar evidencias digitales.

Propone el diseño de un esquema para el procedimiento de indagación de los delitos informáticos, estableciendo los requerimientos mínimos necesarios para que la entidad pueda ejercer sus actividades de una manera eficiente, contando con funciones bien definidas según las necesidades actuales y con los recursos con los que cuentan, estableciendo también procesos y procedimientos que permitan controlar las funciones y realizar monitoreo

La importancia científica de la propuesta es la de aportar a la Administración de Justicia lineamientos que permitan planificar, motivar y Gestionar rápidamente la indagación de delitos informáticos.

4.2. TRIAGE IN-LAB: CASE BACKLOG REDUCTION WITH FORENSIC DIGITAL PROFILING (TRIAGE EN LABORATORIO REDUCCIÓN DE LISTAS DE ESPERA CON TÉCNICAS DE PERFILADO DIGITAL FORENSE)

Este trabajo académico describe la experimentación y desarrollo de un software propio para triage forense utilizando técnica de perfilado digital forense, basado en técnicas algorítmicas para contrarrestar la enorme acumulación de casos relacionados a delitos informáticos y los pocos especialistas forenses digitales en el Sistema de Justicia.

Desarrollando una nueva herramienta de clasificación, que trata de atrapar un perfil criminal con un clasificador predictivo automatizado centrado en la pornografía infantil y el robo de propiedad intelectual. Este software detecta algunos atributos críticos en la evidencia digital y se comparan con otros vectores de características extraídos de un corpus de datos digital basada en dispositivos de casos anteriores. Como resultado de este proceso automatizado, se hace una predicción perfil penal.

Esta herramienta busca ayudar a los expertos en informática forense, con el fin de tomar decisiones acerca de las prioridades para hacer un análisis completo de los dispositivos sospechosos o descartarlos con bajas probabilidades de perder la evidencia digital. Este enfoque debe ser útil para mitigar el retraso de los laboratorios de informática forense.

4.3. ESTUDIO DE LECTORES DE BANDA MAGNÉTICA Y TECLADOS BANCARIOS, UTILIZADOS PARA EL CLONADO DE TARJETAS BANCARIAS MEDIANTE SKIMMERS MP3

Un tipo de estudio que hace el Grupo de Electrónica de la Sección de Informática Forense es el estudio de lectores de banda magnética y teclados bancarios, utilizados para el clonado de tarjetas bancarias.

Miembros del Instituto Universitario de Investigación en Ciencias Policiales (IUICP) desarrollaron en conjunto con la Universidad de Alcalá de Henares y la colaboración de la Guardia Civil, un software y un hardware que permite recuperar y leer la información que almacenan los skimmers MP3 (un tipo de falsos lectores de bandas magnéticas que se adaptan en las bocas de inserción de las tarjetas en los cajeros para grabar las lecturas de las bandas magnéticas) y así poder saber la numeración de las tarjetas que han sido copiadas.

El Grupo de Electrónica de esta Sección es capaz de poder obtener la información total de los dispositivos MP3 acoplados a los cajeros, y que es grabada en forma de archivo de sonido

La información que contienen las tarjetas magnéticas o tarjetas de crédito/debito son leídas a través de un cabezal lector de bandas que lee la pista DOS de las tarjetas (pista que contiene la numeración de la tarjeta) y grabado en el MP3 de

forma analógica por el conector de entrada al micro, quedando así los datos grabados en un archivo de sonido.

La importancia de este desarrollo para la recuperación de los datos de los skimmers MP3, viene dada por ser los pioneros en Europa en poder desarrollar un programa, acceder a los datos y ser capaces de descodificarlos para obtener la información de las bandas magnéticas.

4.4. ANTECEDENTES EN EL CTI DE LA FISCALIA GENERAL DE LA NACION

De manera interna en el cuerpo técnico investigativo de la Fiscalía no se encontraron antecedentes relacionados al proyecto de mejoramiento del laboratorio de informática forense, esto debido a que "la estructura organizacional de la fiscalía general de la nación no ha presentado cambios de fondo desde hace 20 años"[11] y que el grupo de delitos informáticos con 5 años de funcionamiento es relativamente nuevo.

La formulación del proyecto de adecuación del laboratorio a cargo del Grupo Investigativo de Delitos Informáticos del Cuerpo Técnico de Investigación "CTI" de la Fiscalía General de la Nación Seccional Pasto, fomenta una mayor inversión del presupuesto nacional en innovación y desarrollo local, dado que brinda la oportunidad de convertirse en el primer laboratorio a nivel Nacional, acreditado con normas ICONTEC en la protección y el manejo de evidencias de características electrónicas y digitales.

[11] LA REFORMA*, Boletín Informativo del proyecto de modernización Institucional de la Fiscalía.* Fiscalía General de la Nación. Edición 1. Mayo del 2013.

5. OBJETIVOS

5.1. OBJETIVOS GENERAL

Brindar apoyo profesional desde el campo de la Ingeniería Electrónica al Cuerpo Técnico de Investigación “CTI.” de la Fiscalía General de la Nación Seccional Pasto, formulando un proyecto de mejoramiento del laboratorio con que cuenta el Grupo Investigativo de Delitos Informáticos; así como también, respaldar las labores de supervisión, administración y gestión del mejoramiento de la red.

5.2. OBJETIVOS ESPECÍFICOS

- Realizar un reconocimiento de las actividades a realizar.

- Recopilar información actual frente al estado del laboratorio y equipo con que cuenta.

- Realizar caracterización de equipos mediante la elaboración de hojas la hoja de vida de los mismos.

- Investigar y documentar información respecto al tema de adecuación del laboratorio de Delitos Informáticos.

- Diseñar la propuesta de mejoramiento para el laboratorio de delitos informaticos.

- Supervisar, administrar y gestionar el mejoramiento de la red.

6. ALCANCE

Como resultado del desarrollo del presente trabajo de pasantía se entregara al CTI de la Fiscalía la formulación de un proyecto de mejoramiento del laboratorio con que cuenta el Grupo Investigativo de Delitos Informáticos, teniendo como fundamento la norma NTC ISO/IEC 17025:2005.

Es necesario aclarar que no se realizará ejecución del proyecto de adecuación del laboratorio debido a que existen procedimientos definidos por Nivel Central[12], donde se debe lograr aprobación en diferentes etapas, situación que lleva tiempo mayor al disponible para esta pasantía; de modo tal que se llegará hasta la etapa de formulación y socialización con las Directivas del Cuerpo Técnico de Investigación "CTI" de la Fiscalía General de la Nación Seccional Pasto.

Gracias a la experiencia en el manejo de la red y a la documentación que se realice respecto de la misma, se generará una serie de recomendaciones, aplicables en la realidad del contexto, que cuenten con alta viabilidad de implementación y permitan garantizar mejoras en la eficiencia y disponibilidad de la red.

Debido a que la figura de pasante no se considera como funcionario de la Entidad, no se permitió la participación de esta en las actividades de investigación ni el acceso a los equipos destinados a la investigación, refiriéndonos al laboratorio de delitos informáticos, por lo cual la propuesta se basa en información proporcionada por los funcionarios, la cual se debe manejar con la debida reserva. Tal situación se certifica en el oficio de 14 de febrero de 2014, suscrito por el Director del Cuerpo Técnico de Investigación y el Coordinador del Grupo Investigativo de Delitos Informáticos

[12] Organismo que encierra todas las divisiones de la Fiscalía General de la Nación a nivel nacional

7. DESCRIPCIÓN DE LA PASANTÍA

7.1. CUERPO TÉCNICO DE INVESTIGACIÓN C.T.I.

El Cuerpo Técnico de Investigación C.T.I. es una dependencia investigativa al servicio exclusivo de la Fiscalía General de la Nación. Mediante esta dependencia se definen políticas y estrategias para la Policía Judicial en temas de investigación criminal, servicios forenses, de genética y en la administración de la información técnica y judicial para las investigaciones penales. El CTI planea, organiza, dirige, controla y ejecuta las funciones de Policía Judicial de la Fiscalía General de la Nación, organiza y controla el cumplimiento de las políticas y estrategias de investigación, servicios forenses, de genética y de administración de la información. Promueve además el intercambio de información entre las distintas ramas de la fuerza pública.

7.1.1. Misión

La Fiscalía General de la Nación ejerce la acción penal y elabora y ejecuta la política criminal del Estado; garantiza la tutela judicial efectiva de los derechos de los intervinientes en el proceso penal; genera confianza y seguridad jurídica en la sociedad mediante la búsqueda de la verdad, la justicia y la reparación.

7.1.2. Visión

La Fiscalía General de la Nación pondrá en ejecución un sistema de investigación integral, y será reconocida por el diseño y ejecución de políticas públicas vanguardistas que le permitirán enfrentar las diversas formas de criminalidad; su tarea se verá apoyada en la profesionalización del talento humano y el desarrollo y aplicación de herramientas innovadoras de tecnología y comunicación, que garanticen la independencia, autonomía y acceso a la justicia.

7.2. GRUPO DE DELITOS INFORMÁTICOS

La Fiscalía General de la Nación con el fin de contrarrestar las nuevas modalidades delictivas generadas con los avances tecnológicos, conformó mediante resolución 010 del 2008 las unidades Investigativas de Delitos

Informáticos, las cuales cuentan con personal idóneo y altamente capacitado, además de laboratorios de Informática Forense de tecnología de punta.

7.2.1 ¿Qué servicios presta la Unidad de Delitos Informáticos del CTI?

La unidad de delitos informáticos además de llevar a cabo investigaciones especializadas enmarcadas dentro del código penal colombiano, también cuenta con el Laboratorio de Informática Forense, que tiene equipos de tecnología de punta, los cuales sirven para la recuperación y análisis de información en medios tecnológicos, esta actividad eta al servicio de las autoridades judiciales y de la comunidad en general, en eventos en los cuales se requiera un Perito experto en Informática Forense. Los servicios bridados por la Unidad son:

En el ámbito Investigativo:

- Investigación de hechos delictivos mediante la utilización de páginas web.
- Investigación de hechos delictivos en comunicaciones telefónicas, informáticas y/o telemáticas.
- Investigación de hechos delictivos sobre elementos informáticos y/o telemático.
- Investigación de hechos delictivos mediante la utilización de cuentas de correo electrónico.

En el ámbito pericial:

- Análisis y/o recuperación de información de medios digitales de almacenamiento de información digital.
- Rastreo de direcciones I.P.
- Análisis de páginas Web.
- Análisis de Software: Licenciamiento de software
  Comparación de software
- Análisis de Sistemas de Información.
- IRC (Respuesta a Incidentes Cibernéticos).
- Asesoría Especializada.

8. DESARROLLO DE ACTIVIDADES

8.1. RECONOCIMIENTO DE LAS ACTIVIDADES A REALIZAR

Para el desarrollo de la presente pasantía, se realizó la asignación de la suscrita al grupo investigativo de delitos informáticos del Cuerpo Técnico de Investigación "CTI", como el lugar desde el cual se brindara apoyo a las tareas, debido a la afinidad profesional entre los funcionarios de dicho grupo y el área de atención de las tareas a desarrollar por la pasante.

En primera instancia se realizó por el método de observación directa respecto de los recursos con que cuenta el CTI, a red eléctrica y la red de datos, y algunos elementos de estas como, las UPS[13] y el RACK[14] eléctrico del edificio; un RACK de comunicaciones secundario, en el cual se concentra la red de la dependencia de Telecomunicaciones y la dependencia de seguridad y transporte; y el RACK principal del edificio que contiene los switches que se conectan con la Ethernet Nacional, Planta Telefónica, Servidores, entre otros.

Adicional a lo anterior, se hizo un reconocimiento de cada uno de los grupos investigativos con el fin de recolectar información acerca de las necesidades y falencias de cada uno de ellos en específico, en cuanto a la red eléctrica y de datos; en la tabla 1 se presentan las necesidades planteadas en cada dependencia, y se define si son tareas acordes a las funciones de la pasante:

Tabla 1. DISTRIBUCIÓN DEPENDENCIAS Y NECESIDADES DE LA RED

Dependencia	Necesidad	Acorde con el perfil de la pasante	Se soluciono
Laboratorio de Química y Balística	Ninguna	N/A	N/A
Gestión Documental	Ninguna	N/A	N/A
Seguridad y Soporte Logístico	Ninguna	N/A	N/A
Capturas	Ninguna	N/A	N/A

[13] UPS (uninterruptible power supply), es un dispositivo que puede proporcionar energía eléctrica por un tiempo limitado.
[14] Armario o cuarto de cableado eléctrico y/o de datos

Medicina	Ninguna	N/A	N/A
Grafología	Red de Datos	SI	SI
Arquitectura y Topografía	Adquisición de Licencias	NO	SI
Lofoscopia	Ninguna	N/A	N/A
Automotores	Ninguna	N/A	N/A
Administración Publica	Ninguna	N/A	N/A
Coordinación y Capacitación	Red Inalámbrica	SI	SI
Jefatura Seccional	Telefonía	SI	SI
Sección de Análisis Criminalístico S.A.C.	Telefonía, Red de Datos	SI	SI
Control Telemático	Red Inalámbrica	SI	SI
Telecomunicaciones	Ninguna	N/A	N/A
Delitos Informáticos	Laboratorio	SI	SI
Vida y Homicidios	Red de Datos	SI	SI
Sección Desaparecidos NN	Ninguna	N/A	N/A
Dirección	Telefonía	SI	SI

Fuente: La autora.

Las necesidades indicadas fueron atendidas durante el transcurso de la pasantía, entre otras tareas que se presentaron más adelante, en el numeral 8.6 se da detalle de estas tareas.

De esta actividad se dio mayor relevancia y se formuló el proyecto de trabajo para alcanzar el título de Ingeniera Electrónica a la tarea de mejorar el laboratorio del grupo de delitos informáticos mediante la formulación del PROYECTO PARA EL MEJORAMIENTO DEL LABORATORIO DEL GRUPO INVESTIGATIVO DE DELITOS INFORMÁTICOS DEL CUERPO TÉCNICO DE INVESTIGACIÓN "CTI" PASTO Y RESPALDO EN EL MEJORAMIENTO DE LA RED, en primer lugar, porque es el grupo desde el cual se llevaran a cabo todas las tareas, y segundo, porque esto dejaría un producto tangible del desarrollo de la pasantía.

8.2. RECOPILACIÓN DE INFORMACIÓN DEL ESTADO ACTUAL DEL LABORATORIO Y EQUIPO CON QUE CUENTA

Como punto de partida, para la adecuación del laboratorio, se realizó un diagnóstico del estado actual del mismo. Para esto, se inspeccionó desde la disposición del espacio, hasta la dotación de los equipos con que cuenta actualmente el Grupo Investigativo de Delitos Informáticos del CTI de la Fiscalía.

Dentro de este proceso se elaboró un inventario de los bienes técnicos y tecnológicos, que son de uso habitual en las actividades del laboratorio forense, y se obtuvieron las siguientes apreciaciones con respecto a los elementos de interés:

En cuanto al espacio:

- Existe una mala disposición del lugar de trabajo, tanto en el orden como en el almacenamiento. Se trabaja sobre escritorios de madera, los cuales son inadecuados para la manipulación de evidencia digital y para trabajar en las maquinas forenses.

- Teniendo en cuenta la intensidad del trabajo que conlleva para los equipos un análisis forense, se hace evidente la necesidad de un sistema de aire acondicionado con el que actualmente no cuentan, esto debido a que en muchas ocasiones las maquinas forenses trabajan semanas en una sola evidencia, sin ser apagadas; y ya que este proceso se repite durante todos los meses, el factor calor puede deteriorar los equipos.

- No se tienen definidos protocolos para la manipulación de la evidencia digital durante un análisis forense, tales como uso de guantes o transporte en bolsas de plástico o de Faraday[15] según la evidencia.

- Se carece de filtros de seguridad para acceso al laboratorio, solo prohibiciones verbales, ni tampoco existen medidas especiales para el aseo del laboratorio.

Equipo con que cuentan:

8.2.1. Maquinas Forenses

También conocidas como F.R.E.D. (Forensic Recovery of Evidence Device) es una estación de trabajo forense. Dotado de plataformas de procesamiento forenses integradas, esta máquina está diseñada tanto para la extracción como para el análisis de evidencia digital. Tiene la capacidad de duplicar la evidencia

[15] La Bolsa Faraday causa que el campo electromagnético al interior de esa sea nulo.

directamente de IDE/ SAS/ SATA de los discos duros, de dispositivos USB, dispositivos Firewire, CD, DVD, cintas LTO-4 y PC Card/ SmartMedia/ SD-MMC/ Memory Stick/ media Compact Flash en un entorno de análisis forense. F.R.E.D. es capaz de archivar o adquirir pruebas a partir de cintas DLT-V4. Con la opción de RAID FRED tiene una increíble 2.0 TB de almacenamiento RAID interno.

Todos los sistemas F.R.E.D. incluyen la UltraBay, conexiones del panel frontal personalizado, y bandejas de unidad extraíbles lo que no hay necesidad de abrir el sistema de procesamiento de instalar unidades o arrastrarse por la parte trasera de la unidad para conectar dispositivos. Esta máquina tiene un costo cercano a los doce millones de pesos colombianos ($12’000.000)

En la figura 5 y la figura 6 se muestran las maquinas forenses F.R.E.D. que están a disposición de los funcionario del grupo de delitos informáticos del CTI Pasto.

Figura 5. TORRE FORENSE I

Fuente: La autora.

Figura 6. TORRE FORENSE II

Fuente: La autora.

8.2.2. Maquina Forense Portátil

También conocida como F.R.E.D.D.I.E. (Forensic Recovery of Evidence Device Diminutive Interrogation Equipment) es una estación de trabajo forense portable ideal para allanamientos (operativos fuera del laboratorio), en los cuales, no es posible llevar la evidencia digital hasta las instalaciones del laboratorio o se corre el riesgo de que durante el transporte se pueda afectar la integridad del elemento material probatorio (E.M.P).

El F.R.E.D.D.I.E. al igual que la maquina forense F.R.E.D. tiene la facultad de extraer informacion para el análisis de evidencia digital y la duplica directamente de IDE/ SAS/ SATA de los discos duros, de dispositivos USB, dispositivos Firewire, CD, DVD, cintas LTO-4 y PC Card/ SmartMedia/ SD-MMC/ Memory Stick/ media Compact Flash.

Es la solución definitiva del procesamiento forense móvil. La figura 7 muestra el F.R.E.D.D.I.E. con el que cuenta el laboratorio de informática forense del CTI Pasto, en esta imagen se puede verificar el tamaño de esta máquina similar al de una computadora portátil lo que lo hace apropiado para su transporte

Figura 7. MÁQUINA FORENSE PORTÁTIL

Fuente: La autora.

8.2.3. UFED

El UFED (Universal Forensic Extraction Device) es una herramienta de análisis forense para la detección de malware, decodificación mejorada y funciones de informes, análisis de proyectos, grafico de línea de tiempo, la exportación de las capacidades de datos y más. Este dispositivo es capaz de duplicar toda la información almacenada en equipos de telefonía móvil, sin embargo, a diferencia de las maquinas forenses F.R.E.D. Y F.R.E.D.D.I.E., no cuenta con la capacidad de recuperar la información que ha sido eliminada.

Soporta una amplia gama de dispositivos móviles y versiones de sistemas operativos, y debe ser actualizado constantemente para incorporar más recientes dispositivos, plataformas y sistemas operativos.

Adicional a las funciones básicas el UFED cuenta con capacidades avanzadas para:

- Eludir contraseñas simples y complejas al realizar extracciones físicas y del sistema de archivos en determinados dispositivos con iOS 3.0 o superior, incluyendo iOS 6
- Desencriptar y decodificar en tiempo real de datos, aplicaciones y desencriptado de llavero en tiempo real, revelando contraseñas de usuario.
- Desencriptar en tiempo real de contenido protegido por contraseña de determinados dispositivos BlackBerry con OS 4 o posterior.
- Decodificación avanzada de aplicaciones.

- Decodificar mensajes de BlackBerry Messenger (BBM), correos electrónicos, ubicaciones, aplicaciones y más
- Decodificar todas las extracciones físicas realizadas en dispositivos Android en cualquiera de sus versiones
- Decodificar aplicaciones y archivos de aplicaciones.
- Extraer y decodificar dispositivos GPS portátiles
- Extraer de manera física archivos de registro de viaje Tom Tom

El UFED con que cuenta el laboratorio de informática forense del CTI Pasto es un dispositivo de fácil manipulación y pocos comandos como se puede apreciar en la figura 8.

Figura 8. UFED

Fuente: La autora.

8.2.4. Bloqueadores de escritura

La colección de inhibidores de escritura forense hace interfaz con la maquina forense a través de FireWire-A, FireWire-B, y las interfaces USB 2.0. El bloqueador de escritura restringe y/o deshabilita la opción de escritura en el disco, ya que mantener activa esta opción provocaría una alteración no deseada en los medios.

Los bloqueadores de escritura con que cuentan en el laboratorio de delitos informáticos del CTI Pasto son de la empresa Tableau.

- Ultrablock USB 3 IDE / SATA (sólo lectura)

El sólo lectura UltraBlock USB 3 IDE / SATA (Figura 9) se utiliza para adquirir datos de un IDE o disco duro SATA en un entorno protegido contra escritura válida a efectos legales. Ofrece más opciones de conexión nativa del equipo host y del dispositivo que cualquier otro bloqueador de escritura que se encuentra hoy disponible. Gracias al T35es de su kit de herramientas forenses, dispone de un puente forense sólido y fiable con cuatro conexiones diferentes de la interfaz de host (eSATA, FireWire 800, FireWire 400 y USB) y de dos conexiones para dispositivos (SATA e IDE).

Es el primer puente de Tableau con una conexin eSATA del host. La interfaz eSATA permitirá que los profesionales forenses adquieran imágenes de las unidades objeto de análisis SATA e IDE a una velocidad superior a FireWire 800.

Figura 9. PUENTE T35es

Fuente: La autora.

- Ultrablock USB 3 IDE / SATA (Lectura y escritura)

La lectura y escritura UltraBlock USB 3 IDE / SATA (Figura 10) se utiliza para escribir datos en un IDE o disco duro SATA de manera segura (Figura 10). La carcasa amarilla es idéntica a la negra habitual del T35es, exceptuando que el T35es-RW está previamente configurado de fábrica para un funcionamiento de lectura-escritura.

Este equipo cuenta exclusivamente con la capacidad de realizar copias de una evidencia forense. La carcasa amarilla destaca el hecho de que se puede escribir en el T35es-RW y eliminar así un posible uso incorrecto durante los exámenes forenses.

A menudo, un kit completo de análisis forense incluirá tanto el puente forense bloqueado contra escritura (negro) como el de lectura-escritura (amarillo).

Figura 10. PUENTE T35es-RW

Fuente: La autora.

- Ultrablock eSATA IDE / SATA (sólo lectura)

El sólo lectura UltraBlock eSATA IDE / SATA (Figura 11) se utiliza para adquirir datos de un IDE o disco duro SATA en un entorno protegido contra escritura válida a efectos legales (Figura 11).

Es el bloqueador de escritura más moderno de Tableau, el puente forense SATA/IDE T35e proporciona un rendimiento y funciones sólidas.

Diseñado para admitir las imágenes de las unidades SATA e IDE de un único paquete clásico, T35e proporciona el rendimiento con el que no pueden competir otros bloqueadores de escritura de hardware.

Figura 11. TABLEAU T8

Fuente: La autora.

8.3. CARACTERIZACIÓN DE EQUIPOS

Una vez realizado el inventario de los equipos del laboratorio forense se realizó la caracterización de los equipos inventariados, mediante el diligenciamiento de las hojas de vida de cada equipo (ANEXO 1).

Este proceso se llevó a cabo con seguimiento de las INSTRUCCIONES PARA EL DILIGENCIAMIENTO DEL FORMATO DE HOJAS DE VIDA DE EQUIPOS, (ANEXO 2).

8.4. INVESTIGACIÓN Y DOCUMENTACIÓN RESPECTO AL TEMA DE ADECUACIÓN DEL LABORATORIO DE DELITOS INFORMÁTICOS

A nivel nacional se hace latente la preocupación actual con el crecimiento que presentan los delitos informáticos o de ciberseguridad[16] y se encuentra muchos recursos con los que las autoridades buscan contrarrestar el incremento de las amenazas informáticas que afectan significativamente al país, la ciberdefensa[17]. Como referencia a ello encontramos el documento CONPES 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa, el artículo 210 del CCP (Código de procedimiento Penal Colombiano): Informe de Investigador de Laboratorio, la creación de colCERT (Equipo de Respuesta a Emergencias Informáticas de Colombia), entre otros.

Desafortunadamente a nivel nacional a pesar de que se han desarrollado muchos sistemas de seguridad para la prevención, ciberseguridad y ciberdefensa, aún no se han desarrollado mecanismos de reparación eficientes, pero esto acapara actualmente todo el interés de las autoridades Nacionales. Actualmente la Policía Nacional se está fortaleciendo en el tema, apoyados de entidades como la INTERPOL y asesorados por instituciones universitarias como la UNIANDES.

Yendo más allá, vemos como esta tendencia tiene el mismo impacto en todo el mundo, es una preocupación compartida por todas las naciones. En búsqueda de soluciones, han mostrado su interés en el tema organizaciones tales como: la UIT (Unión Internacional de Telecomunicaciones), la IOCE (International Organization on Computer Evidence), la IEEE (Institute of Electrical and Electronics Engineers), la ASCLD (American Society of Crime Laboratory Directors), y una gran cantidad de Universidades y cuerpos de defensa de diferentes países, quienes han desarrollado grandes aportes para la lucha contra los delincuentes informáticos.

Con el fin de mejorar el laboratorio objeto de trabajo, se buscaba identificar una acreditación que alcanzar para encaminarse hacia ella como meta, y de esta manera definir las necesidades a satisfacer de manera más clara.

---

[16] Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética

[17] Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional

La propuesta de mejoramiento del laboratorio del grupo investigativo de delitos informáticos del CTI, se planteó con el fin de realizar un aporte importante a la Fiscalía en su plan de reestructuración. Se pretende desde esta área aportar al reconocimiento de los procesos y actividades ejercidas por la Institución, mediante una legitimización del accionar del laboratorio como respaldo a las decisiones que puedan ser resultado de un peritaje informático.

Es por esta razón que se pretende que la propuesta que aquí se presenta y todo accionar que se realice más adelante este encaminado en alcanzar una acreditación, que respalde y dé valor jurídico a toda evidencia digital resultante de un análisis forense en el laboratorio de delitos informáticos. Claramente un objetivo de esta magnitud requiere mucho tiempo de trabajo y experiencia, sin embargo, se contempla la información aquí contenida como el punto de partida para dicho proceso. Para esto, se buscó orientación en herramientas como guías y normas de organizaciones y comisiones nacionales e internacionales

Como resultado, se encontró que los laboratorios de informática forense se acreditan bajo estándares internacionales ISO 17025:2005. Actualmente hay alrededor de 82 laboratorios de informática forense acreditados en el mundo.

Para el desarrollo de esta propuesta se utilizó la Norma Técnica Colombiana NTC-ISO/IEC 17025, la cual establece cerca de 122 cláusulas plausibles de aplicación para acreditar un laboratorio de ensayo y calibración. No está definido con precisión cuáles de ellas son aplicables a un laboratorio de informática forense. En algunas de ellas se evidencia su correspondencia a otras disciplinas. No está claro qué elementos objetivos se requieren para dar conformidad a una cláusula, por eso se realizó un análisis que permitiera aproximar cada clausula a la realidad de la Institución.

Normalmente en algunos casos era claro que una determinada cláusula no aplica a la especialidad y simplemente se colocó "NO APLICA" en la lista de chequeo. En otros casos hubo que analizar hasta qué punto es viable dar cumplimiento a la cláusula, lo cual requiere de mayor intervención por parte de una autoridad competente.

A continuación se presenta una tabla donde se encuentran los ítems definidos por la Norma NTC-ISO/IEC 17025 hasta su último nivel de desagregación y se realiza el respectivo análisis de oportunidad y aplicabilidad a la Fiscalía General de la Nación (Columna 2), de lo cual, posteriormente se propone un ajuste al ítem de

modo tal que se encuentre estrechamente ligado a la realidad de dicha Entidad (Columna 3). Una vez efectuado esto, se verifica su cumplimiento o no en la actualidad de la Institución (Comuna 4).

CONTENIDO DE LA NORMA NTC-ISO/IEC 17025

1. OBJETO Y CAMPO DE APLICACIÓN
   1.1.
   1.2.
   1.3.
2. REFERENCIAS NORMATIVAS
3. TERMINOS Y DEFINICIONES
4. REQUISITOS RELATIVOS A LA GESTION
   4.1. ORGANIZACIÓN
      4.1.1.
      4.1.2.
      4.1.3.
      4.1.4.
      4.1.5.
      4.1.6.
   4.2. SISTEMA DE GESTION
      4.2.1.
      4.2.2.
      4.2.3.
      4.2.4.
      4.2.5.
      4.2.6.
      4.2.7.
   4.3. CONTROL DE DOCUMENTOS
      4.3.1. Generalidades
      4.3.2. Aprobación y emisión de documentos
         4.3.2.1.
         4.3.2.2.
         4.3.2.3.
      4.3.3. Cambios a las documentaciones
         4.3.3.1.
         4.3.3.2.
         4.3.3.3.
         4.3.3.4.
   4.4. REVISION DE LOS PEDIDOS, OFERTAR Y CONTRATOS
      4.4.1.
      4.4.2.
      4.4.3.
      4.4.4.

4.4.5.
4.5. SUBCONTRATACION DE ENSAYOS Y DE CALIBRACIONES
4.5.1.
4.5.2.
4.5.3.
4.5.4.
4.6. COMPRA DE SERVICIOS Y DE SUMINISTRO
4.6.1.
4.6.2.
4.6.3.
4.6.4.
4.7. SERVICIO AL CLIENTE
4.7.1.
4.7.2.
4.8. QUEJAS
4.9. CONTROL DE TRABAJOS DE ENSAYO Y/O CALIBRACIONES NO CONFORMES
4.9.1.
4.9.2.
4.10. MEJORA
4.11. ACCIONES CORRECTIVAS
4.11.1.
4.11.2. Análisis de las causas
4.11.3. Selección e implementación de acciones correctivas
4.11.4. Seguimiento de las acciones correctivas
4.11.5. Auditorias adicionales
4.12. ACCIONES PREVENTIVAS
4.12.1.
4.12.2.
4.13. CONTROL DE LOS REGISTROS
4.13.1. Generalidades
4.13.1.1.
4.13.1.2.
4.13.1.3.
4.13.1.4.
4.13.2. Registros técnicos
4.13.2.1.
4.13.2.2.
4.13.2.3.
4.14. AUDITORIAS INTERNAS
4.14.1.
4.14.2.
4.14.3.
4.14.4.
4.15. REVISIONES POR LA DIRECCION

4.15.1.
4.15.2.
5. REQUISITOS TECNICOS
5.1. GENERALIDADES
5.1.1.
5.1.2.
5.2. PERSONAL
5.2.1.
5.2.2.
5.2.3.
5.2.4.
5.3. INSTALACIONES Y CONDICIONES AMBIENTALES
5.3.1.
5.3.2.
5.3.3.
5.3.4.
5.3.5.
5.4. METODOS DE ENSAYO Y DE CALIBRACION Y VALIDACION DE LOS METODOS
5.4.1. Generalidades
5.4.2. Selección de los métodos
5.4.3. Métodos desarrollados por el laboratorio
5.4.4. Métodos no normalizados
5.4.5. Validación de los métodos
5.4.5.1.
5.4.5.2.
5.4.5.3.
5.4.6. Estimación de la incertidumbre de la medición
5.4.6.1.
5.4.6.2.
5.4.6.3.
5.4.7. Control de los datos
5.4.7.1.
5.4.7.2.
5.5. EQUIPOS
5.5.1.
5.5.2.
5.5.3.
5.5.4.
5.5.5.
5.5.6.
5.5.7.
5.5.8.
5.5.9.
5.5.10.

5.5.11.
5.5.12.

5.6. TRAZABILIDAD DE LAS MEDICIONES

5.6.1. Generalidades

5.6.2. Requisitos específicos

5.6.2.1. Calibración

5.6.2.1.1.

5.6.2.1.2.

5.6.2.2. Ensayos

5.6.2.2.1.

5.6.2.2.2.

5.6.3. Patrones de referencia y materiales de referencia

5.6.3.1. Patrones de referencia

5.6.3.2. Materiales de referencia

5.6.3.3. Verificaciones intermedias

5.6.3.4. Transporte y almacenamiento

5.7. MUESTREO

5.7.1.

5.7.2.

5.7.3.

5.8. MANIPULACION DE LOS ITEMS DE ENSAYO Y CALIBRACION

5.8.1.

5.8.2.

5.8.3.

5.8.4.

5.9. ASEGURAMIENTO DE LA CALIDAD DE LOS RESULTADOS DE ENSAYO Y DE CALIBRACION

5.9.1.

5.9.2.

5.10. INFORME DE LOS RESULTADOS

5.10.1. Generalidades

5.10.2.

5.10.3. Informes de ensayos

5.10.3.1.

5.10.3.2.

5.10.4. Certificados de calibración

5.10.4.1.

5.10.4.2.

5.10.4.3.

5.10.4.4.

5.10.5. Opiniones e interpretaciones

5.10.6.

5.10.7. Transmisión electrónica de los resultados

5.10.8. Presentación de los informes y de las certificaciones

5.10.9.

Tabla 2. CARACTERIZACIÓN Y ADAPTACIÓN NORMA NTC ISO/IEC 17025

NORMA NTC-ISO/IEC 17025		APLICA	ÍTEM DE LA NORMA AJUSTADO A LA ENTIDAD	CUMPLE
1. OBJETO Y CAMPO DE APLICACIÓN				
			Los laboratorios de Informática Forense se clasifican como Laboratorio de ensayo, debido a sus actividades de extracción y análisis de información de lo que para nuestro interés seria la evidencia digital.	
2. REFERENCIAS NORMATIVAS				
			Aplica igual a la original	
3. TERMINOS Y DEFINICIONES				
			Aplica igual a la original	
4. REQUISITOS RELATIVOS A LA GESTION				
4.1	4.1.1	SI	La entidad de la cual es parte el laboratorio es una entidad con responsabilidad legal.	SI
	4.1.2	SI	Es responsabilidad del laboratorio realizar sus actividades de mantenimiento de modo que se cumplan los requisitos de esta guía y se satisfagan las necesidades de las autoridades competentes u organizaciones que otorgan reconocimiento.	NO
	4.1.3	SI	El sistema de gestión debe cubrir las actuaciones realizadas en las instalaciones permanentes del laboratorio, en sitios fuera de sus instalaciones permanentes (allanamientos) o en instalaciones temporales o móviles asociadas.	NO
	4.1.4	SI	Se debe definir las responsabilidades del coordinador del grupo a cargo del laboratorio, con el fin de identificar potenciales conflictos de intereses con sus actividades diferentes a la de analista forense.	NO

	4.1.5	SI	El laboratorio debe: a) Contar con un grupo en el cual este incluido el coordinador del grupo, que tenga, independientemente de toda otra responsabilidad, la autoridad y los recursos necesarios para desempeñar sus tareas, incluida la implementación, el mantenimiento y la mejora del sistema de gestión, y para identificar la ocurrencia de desvíos del sistema de gestión o de los procedimientos de análisis forense, e iniciar acciones destinadas a prevenir o minimizar dichos desvíos. b) Tomar medidas para asegurarse de que el grupo investigativo está libre de cualquier presión o influencia indebida, interna o externa, comercial, financiera o de otro tipo, que pueda perjudicar la calidad de su trabajo. c) Tener políticas y procedimientos para asegurar la protección de la información confidencial, incluidos los procedimientos para la protección del almacenamiento y el cumplimiento de los procesos de cadena de custodia. d) Tener políticas y procedimientos para evitar intervenir en cualquier actividad que pueda disminuir la confianza en su competencia, imparcialidad, juicio o integridad operativa. e) Definir la organización y la estructura de gestión del laboratorio, su ubicación dentro de una organización estructural desde nivel central, y las relaciones entre la gestión de la calidad, las operaciones técnicas y los servicios de apoyo. f) Especificar la responsabilidad, autoridad e interrelación de los investigadores que dirigen, realizan o verifican actuaciones que afectan la calidad del análisis forense. g) Proveer adecuada supervisión a los investigadores encargados de las extracciones y/o inspecciones, incluidos los que están en formación, por investigadores familiarizados con los métodos y procedimientos, el objetivo de cada actuación y con la evaluación de los resultados de los análisis forenses. h) Tener un coordinador con la responsabilidad total por las operaciones técnicas y la gestión de los recursos necesarios para asegurar la calidad requerida de las operaciones del laboratorio. i) Nombrar un investigador como responsable de la calidad, quien, independientemente de otras obligaciones y responsabilidades, debe tener definidas la responsabilidad y la autoridad para asegurarse de que el sistema de gestión relativo a la calidad será implementado y respetado en todo momento; el responsable de la calidad debe tener acceso directo al líder de sistema de gestión integral para la toma de decisiones sobre la política y los recursos del laboratorio. j) Nombrar sustitutos para los investigadores que lideren la gestión de calidad. k) Asegurarse de que los investigadores son conscientes de la pertinencia e importancia de sus actuaciones y de la manera en que contribuyen al logro de los objetivos del sistema de gestión.	NO
	4.1.6	SI	El encargado del sistema de gestión de calidad debe asegurarse de que se establecen los procesos de comunicación apropiados dentro del laboratorio y de que la comunicación se efectúa considerando la eficacia del sistema de gestión.	NO

4.2	4.2.1	SI	El laboratorio debe establecer, implementar y mantener un sistema de gestión apropiado al alcance del procedimiento y los resultados de sus análisis forenses. El laboratorio debe documentar sus políticas, sistemas, programas, procedimientos e instrucciones tanto como sea necesario para asegurar la calidad de los resultados de los análisis forenses. La documentación del sistema debe ser comunicada a los investigadores del grupo, debe estar a su disposición y debe ser comprendida e implementada por todos.	NO
	4.2.2	SI	Las políticas del sistema de gestión del laboratorio concernientes a la calidad, incluida una declaración de la política de la calidad, deben estar definidas en un manual de la calidad. Los objetivos generales deben ser establecidos y revisados durante la revisión por el líder del equipo de sistema de gestión integral. La declaración de la política de la calidad debe ser emitida bajo la autoridad de la alta dirección. Como mínimo debe incluir lo siguiente: a) El compromiso del coordinador del grupo a cargo del laboratorio con la buena práctica profesional y con la calidad de sus análisis forenses como respuesta a una actuación. b) Una declaración del director con respecto al tipo de actuaciones posibles en el laboratorio. c) El propósito del sistema de gestión concerniente a la calidad. d) Un requisito de que todos los investigadores encargados de realizar análisis forense dentro del laboratorio se familiaricen con la documentación de la calidad e implemente las políticas y los procedimientos en su trabajo. e) El compromiso del coordinador del laboratorio de cumplir esta guía y mejorar continuamente la eficacia del sistema de gestión.	NO
	4.2.3	SI	El líder del equipo de sistema de gestión integral debe proporcionar evidencias del compromiso con el desarrollo y la implementación del sistema de gestión y con mejorar continuamente su eficacia.	NO
	4.2.4.	SI	El líder del equipo de sistema de gestión integral debe comunicar a la entidad la importancia de satisfacer los requisitos legales y reglamentarios.	NO
	4.2.5	SI	El manual de la calidad debe contener o hacer referencia a los procedimientos de apoyo, incluidos los procedimientos técnicos. Debe describir la estructura de la documentación utilizada en el sistema de gestión.	NO
	4.2.6	SI	En el manual de la calidad deben estar definidas las funciones y responsabilidades del coordinador y del responsable de la calidad, incluida su responsabilidad para asegurar el cumplimiento de esta guía.	NO
	4.2.7	SI	El líder del equipo de sistema de gestión integral debe asegurarse de que se mantiene la integridad del sistema de gestión cuando se planifican e implementan cambios en éste.	NO

4.3	4.3.1		SI	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, los métodos de análisis forense, así como el software, las especificaciones, las instrucciones y los manuales.	NO
	4.3.2	4.3.2.1	SI	Todos los documentos distribuidos entre los investigadores del laboratorio como parte del sistema de gestión deben ser revisados y aprobados, para su uso, por el líder del equipo de sistema de gestión integral antes de su emisión. Se debe tener esta información disponible en la estructura documental de la intranet de la fiscalía, identificando el estado de revisión vigente y la distribución de los documentos del sistema de gestión, la cual debe ser fácilmente accesible con el fin de evitar el uso de documentos no válidos u obsoletos.	NO
		4.3.2.2	SI	Los procedimientos adoptados deben asegurar que: a) Las ediciones autorizadas de los documentos pertinentes estén disponibles en todos los sitios en los que se llevan a cabo operaciones esenciales para el funcionamiento eficaz del laboratorio. b) Los documentos sean examinados periódicamente y, cuando sea necesario, modificados para asegurar la adecuación y el cumplimiento continuos con los requisitos aplicables. c) Los documentos no válidos u obsoletos serán retirados inmediatamente de todos los puntos de emisión o uso, o sean protegidos, de alguna otra forma, de su uso involuntario. d) Los documentos obsoletos, retenidos por motivos legales o de preservación del conocimiento, sean adecuadamente marcados.	NO
		4.3.2.3	SI	Los documentos del sistema de gestión generados por el laboratorio deben ser identificados unívocamente. Dicha identificación debe incluir la fecha de emisión y/o una identificación de la revisión, la numeración de las páginas, el número total de páginas o una marca que indique el final del documento, y la o las personas autorizadas a emitirlos.	NO

	4.3.3	4.3.3.1	SI	Los cambios a los documentos deben ser revisados y aprobados por el líder del equipo de sistema de gestión integral que realizó la revisión original, a menos que se designe específicamente a otra función. El investigador designado debe tener acceso a los antecedentes pertinentes sobre los que basará su revisión y su aprobación.	NO
		4.3.3.2	SI	Cuando sea posible, se debe identificar el texto modificado o nuevo en el documento o en los anexos apropiados.	NO
		4.3.3.3	SI	Si el sistema de control de los documentos del laboratorio permite modificar los documentos a mano, hasta que se edite una nueva versión, se deben definir los procedimientos y las personas autorizadas para realizar tales modificaciones. Las modificaciones deben estar claramente identificadas, firmadas y fechadas. Un documento revisado debe ser editado nuevamente tan pronto como sea posible.	NO
		4.3.3.4	SI	Se deben establecer procedimientos para describir cómo se realizan y controlan las modificaciones de los documentos conservados en la estructura documental de la intranet de la Fiscalía.	NO
4.4	4.4.1		NO		
	4.4.2		SI	Se deben conservar los registros de las revisiones, incluidas todas las modificaciones significativas. También se deben conservar las copias de las órdenes judiciales relacionadas con la actuación mientras estas tengan vigencia.	NO
	4.4.3		NO		
	4.4.4		SI	Se debe informar a la autoridad competente de cualquier desviación con respecto a la actuación.	SI
	4.4.5		SI	Si una actuación necesita ser modificada después de comenzar el análisis forense, se debe repetir el análisis y se deben comunicar los cambios al investigador encargado.	SI
4.5			NO		

4.6	4.6.1	SI	El laboratorio debe tener una política y procedimientos para la gestión y solicitud de los servicios y suministros que utiliza y que afectan a la calidad de las extracciones y/o inspecciones. Deben existir procedimientos para la compra, la recepción y el almacenamiento de los reactivos y materiales consumibles de laboratorio que se empleen en los análisis forenses.	SI
	4.6.2	SI	El laboratorio debe asegurarse de que los equipos, los implementos y los materiales consumibles comprados, que afectan a la calidad de los análisis forenses, no sean utilizados hasta que no hayan sido probados, o verificados de alguna otra forma, como que cumplen las especificaciones normalizadas o los requisitos definidos en los métodos relativos al análisis forense concerniente. Estos servicios y suministros deben cumplir con los requisitos especificados. Se deben mantener registros de las acciones tomadas para verificar el cumplimiento.	NO
	4.6.3	SI	Los documentos de compra de los elementos que afectan a la calidad de las prestaciones del laboratorio deben contener datos que describan los servicios y suministros solicitados. Estos documentos de compra deben ser revisados y aprobados en cuanto a su contenido técnico antes de ser liberados.	NO
	4.6.4	SI	El laboratorio debe evaluar a los proveedores de los productos consumibles, suministros y servicios críticos que afectan a la calidad de los análisis forenses, y debe mantener los registros de dichas evaluaciones.	NO
4.7	4.7.1	SI	El laboratorio debe estar dispuesto a cooperar con las autoridades competentes para aclarar la actuación solicitada y para realizar el seguimiento del desempeño del laboratorio en relación con el trabajo realizado. El laboratorio debe garantizar la confidencialidad de sus resultados.	SI
	4.7.2	SI	El laboratorio debe procurar obtener información de retorno, tanto positiva como negativa, de la autoridad competente. La información de retorno debe utilizarse y analizarse para mejorar el sistema de gestión y las actividades del laboratorio.	NO
4.8		SI	El laboratorio debe tener una política y un procedimiento para la resolución de inconformidades de las autoridades competentes o de otros autores. Se deben mantener los registros de todas las quejas así como de las investigaciones y de las acciones correctivas llevadas a cabo por el laboratorio.	NO

4.9	4.9.1	SI	El laboratorio debe tener una política y procedimientos que se deben implementar cuando cualquier aspecto del análisis forense, no es conformes con sus propios procedimientos o con los requisitos de la autoridad competente. La política y los procedimientos deben asegurar que: a) Cuando se identifique el trabajo no conforme, se asignen las responsabilidades y las autoridades para la gestión del trabajo no conforme, definan y tomen las acciones. b) Se evalúe la importancia del trabajo no conforme. c) Se realice la corrección inmediatamente y se tome una decisión respecto de la aceptabilidad de los trabajos no conformes. d) Si fuera necesario, se notifique a la autoridad competente y se anule la actuación. e) Se defina la responsabilidad para autorizar la reanudación del trabajo.	NO
	4.9.2	SI	Cuando la evaluación indique que el trabajo no conforme podría volver a ocurrir o existan dudas sobre el cumplimiento de las operaciones del laboratorio con sus propias políticas y procedimientos, se deben seguir rápidamente los procedimientos de acciones correctivas.	NO
4.10		SI	El laboratorio debe mejorar continuamente la eficacia de su sistema de gestión mediante el uso de la política de la calidad, los objetivos de la calidad, los resultados de las auditorías, el análisis de los datos, las acciones correctivas y preventivas y la revisión por la dirección.	NO
4.11	4.11.1	SI	El laboratorio debe establecer una política y un procedimiento para la implementación de acciones correctivas cuando se haya identificado un trabajo no conforme o desvíos de las políticas y procedimientos del sistema de gestión o de las operaciones técnicas, y debe designar personas apropiadamente autorizadas para implementarlas.	NO
	4.11.2	SI	El procedimiento de acciones correctivas debe comenzar con una investigación para determinar la o las causas raíz del problema.	SI
	4.11.3	SI	Cuando se necesite una acción correctiva, el laboratorio debe identificar las acciones correctivas posibles. Debe seleccionar e implementar la o las acciones con mayor posibilidad de eliminar el problema y prevenir su repetición.	SI
	4.11.4	SI	El laboratorio debe realizar el seguimiento de los resultados para asegurarse de la eficacia de las acciones correctivas implementadas.	SI
	4.11.5	SI	Cuando la identificación de no conformidades o desvíos ponga en duda el cumplimiento del laboratorio con sus propias políticas y procedimientos, o el cumplimiento con esta guía, el laboratorio debe asegurarse de que los correspondientes sectores de actividades sean auditados.	NO

4.12	4.12.1		SI	Se deben identificar las mejoras necesarias y las potenciales fuentes de no conformidades. Cuando se identifiquen oportunidades de mejora o si se requiere una acción preventiva, se deben desarrollar, implementar y realizar el seguimiento de planes de acción, a fin de reducir la probabilidad de ocurrencia de dichas no conformidades y aprovechar las oportunidades de mejora.	NO
	4.12.2		SI	Los procedimientos para las acciones preventivas deben incluir la iniciación de dichas acciones y la aplicación de controles para asegurar que sean eficaces.	NO
4.13	4.13.1	4.13.1.1	SI	El laboratorio debe establecer y mantener procedimientos para la identificación, la recopilación, la codificación, el acceso, el archivo, el almacenamiento, el mantenimiento y la disposición de los registros de la calidad y los registros técnicos. Los registros de la calidad deben incluir los informes de las auditorías internas y de las revisiones del líder del equipo de sistema de gestión integral, así como los registros de las acciones correctivas y preventivas.	NO
		4.13.1.2	SI	Todos los registros deben ser legibles y se deben almacenar y conservar de modo que sean fácilmente recuperables en instalaciones que les provean un ambiente adecuado para prevenir los daños, el deterioro y las pérdidas. Se debe establecer el tiempo de retención de los registros.	NO
		4.13.1.3	SI	Todos los registros deben ser conservados en sitio seguro y en confidencialidad.	NO
		4.13.1.4	SI	El laboratorio debe proteger y salvaguardar los registros almacenados en la estructura documental de la intranet de la Fiscalía y prevenir el acceso no autorizado o la modificación de dichos registros.	NO

	4.13.2	4.13.2.1	SI	El laboratorio debe conservar, por un período determinado, los registros de las observaciones originales, de los datos derivados y de información suficiente para establecer un protocolo de control, los registros de mantenimiento, los registros del personal y una copia de cada informe resultado de una actuación. Los registros correspondientes a cada extracción y/o inspección deben contener suficiente información para facilitar, cuando sea posible, la identificación de los factores que afectan a la veracidad y posibilitar que la extracción y/o inspección sean repetidas bajo condiciones lo más cercanas posible a las originales. Los registros deben incluir la identidad del investigador responsable de la actuación y del triage forense.	NO
		4.13.2.2	SI	Las observaciones, extracciones y/o inspecciones y el triage se deben registrar en el momento de hacerlos y deben poder ser relacionados con la actuación en cuestión.	NO
		4.13.2.3	SI	Cuando ocurran errores en los registros, cada error debe ser tachado, no debe ser borrado, hecho ilegible ni eliminado, y el valor correcto debe ser escrito al margen. Todas estas alteraciones a los registros deben ser firmadas o visadas por la persona que hace la corrección. En el caso de los registros cargados al SPOA se deben tomar medidas similares para evitar pérdida o cambio de los datos originales.	NO
4.14	4.14.1		SI	El laboratorio debe efectuar periódicamente, de acuerdo con un calendario y un procedimiento predeterminados, auditorías internas de sus actividades para verificar que sus operaciones continúan cumpliendo con los requisitos del sistema de gestión y de esta guía. El programa de auditoría interna debe considerar todos los elementos del sistema de gestión, incluidas las actividades de análisis forense. Es el responsable de la calidad quien debe planificar y organizar las auditorías según lo establecido en el calendario y lo solicitado por el líder del equipo de sistema de gestión integral. Tales auditorías deben ser efectuadas por personal formado y calificado, quien será, siempre que los recursos lo permitan, independiente de la actividad a ser auditada.	NO
	4.14.2		SI	Cuando los hallazgos de las auditorías pongan en duda la eficacia de las operaciones o la exactitud o validez de los resultados de los análisis forenses del laboratorio, éste debe tomar las acciones correctivas oportunas y, si las investigaciones revelaran que los resultados del laboratorio pueden haber sido afectados, debe notificarlo por escrito a las autoridades competentes que puedan verse afectadas.	NO

	4.14.3	SI	Se deben registrar el sector de actividad que ha sido auditado, los hallazgos de la auditoría y las acciones correctivas que resulten de ellos.	NO
	4.14.4	SI	Las actividades de la auditoría de seguimiento deben verificar y registrar la implementación y eficacia de las acciones correctivas tomadas.	NO
4.15	4.15.1	SI	El coordinador del grupo encargado del laboratorio debe efectuar periódicamente, de acuerdo con un calendario y un procedimiento predeterminados, una revisión del sistema de gestión y de las actividades de análisis forense del laboratorio, para asegurarse de que se mantienen constantemente adecuados y eficaces, y para introducir los cambios o mejoras necesarios. La revisión debe tener en cuenta los elementos siguientes: - La adecuación de las políticas y los procedimientos. - Los informes del personal directivo y de supervisión. - El resultado de las auditorías internas recientes. - Las acciones correctivas y preventivas. - Las evaluaciones por organismos externos. - Los resultados de las comparaciones interlaboratorios. - Todo cambio en el volumen y el tipo de trabajo efectuado. - La retroalimentación de los fiscales. - Las quejas. - Las recomendaciones para la mejora. - Otros factores pertinentes, tales como las actividades del control de la calidad, los recursos y la formación de los investigadores.	NO
	4.15.2	SI	Se deben registrar los hallazgos de las revisiones del coordinador y las acciones que surjan de ellos. El coordinador debe asegurarse de que estas acciones sean realizadas dentro de un plazo apropiado y acordado.	NO
5. REQUISITOS TECNICOS				
5.1	5.1.1	SI	Muchos factores determinan la exactitud y la confiabilidad de los análisis forenses realizados por un laboratorio. Estos factores incluyen elementos provenientes: - De los factores humanos. - De las instalaciones y condiciones ambientales. - De los métodos de extracción y/o inspección, y de la validación de los métodos. - De los equipos. - De las consideraciones del triage pericial.	NO

	5.1.2	SI	El grado con el que los factores contribuyen a la efectividad de los análisis forenses difiere considerablemente según la extracción y/o inspección. El laboratorio debe tener en cuenta todos los factores al desarrollar los métodos y procedimientos de los análisis forenses, en la formación y la calificación del personal, así como en la selección y el mantenimiento de los equipos utilizados.	NO
5.2	5.2.1	SI	La alta dirección debe asegurar la competencia de todos los investigadores asignados al grupo, quienes operan equipos específicos, realizan análisis forense y generan informes. Cuando emplea investigadores en formación, debe proveer una supervisión apropiada. El personal que realiza tareas específicas debe estar calificado sobre la base de una educación, una formación, una experiencia apropiadas y/o de habilidades demostradas, según sea requerido.	NO
	5.2.2	SI	La alta dirección debe apoyar al coordinador del grupo en la formulación de metas con respecto a la educación, la formación y las habilidades de los investigadores asignados al laboratorio. El laboratorio debe tener una política y procedimientos para identificar las necesidades de formación de investigadores y para proporcionarla. El programa de formación debe ser pertinente a las tareas presentes y futuras del laboratorio. Se debe evaluar la eficacia de las acciones de formación implementadas.	NO
	5.2.3	SI	Cuando utilice personal técnico y de apoyo clave, ya sea bajo contrato o a título suplementario, el laboratorio debe asegurarse de que dicho personal sea supervisado, que sea competente, y que trabaje de acuerdo con el sistema de gestión del laboratorio.	NO
	5.2.4	SI	El laboratorio debe mantener actualizados los perfiles de los investigadores del grupo de delitos informáticos encargados de los análisis forenses.	SI

	5.2.5	SI	La dirección debe autorizar a miembros específicos del personal para realizar tipos particulares extracciones y/o inspecciones, para realizar triage, para emitir opiniones e interpretaciones y para operar tipos particulares de equipos. El laboratorio debe mantener registros de las autorizaciones pertinentes, de la competencia, del nivel de estudios y de las calificaciones profesionales, de la formación, de las habilidades y de la experiencia de todos los investigadores. Esta información debe estar fácilmente disponible y debe incluir la fecha en la que se confirma la autorización y/o la competencia.	NO
5.3	5.3.1	SI	Las instalaciones del laboratorio, incluidas, pero no en forma excluyente, las fuentes de energía, la iluminación y las condiciones ambientales, deben facilitar la realización correcta del análisis forense. El laboratorio debe asegurarse de que las condiciones ambientales no invaliden los resultados ni comprometan la calidad requerida. Se deben tomar precauciones especiales cuando las extracciones y/o inspecciones se realicen en sitios distintos de la instalación permanente del laboratorio (allanamientos). Los requisitos técnicos para las instalaciones y las condiciones ambientales que puedan afectar a los resultados los resultados de los análisis forenses deben estar documentados.	NO
	5.3.2	SI	El laboratorio debe realizar el seguimiento, controlar y registrar las condiciones ambientales según lo requieran las especificaciones, métodos y procedimientos correspondientes, o cuando éstas puedan influir en la calidad de los resultados. Se debe prestar especial atención, por ejemplo, a la estática, la interferencia electromagnética, las ondas de radio, la radiación, la humedad, el suministro eléctrico, y la temperatura. Cuando las condiciones ambientales comprometan los resultados de los análisis forenses, éstos se deben interrumpir.	NO
	5.3.3	SI	Debe haber una separación eficaz entre áreas vecinas en las que se realicen actividades incompatibles. Se deben tomar medidas para prevenir la contaminación cruzada.	NO
	5.3.4	SI	Se deben controlar el acceso y el uso de las áreas que afectan a la calidad de los análisis forenses. El laboratorio debe determinar la extensión del control en función de sus circunstancias particulares.	NO

	5.3.5	SI	Se deben tomar medidas para asegurar el orden y la limpieza del laboratorio. Cuando sean necesarios se deben preparar procedimientos especiales.	NO
5.4	5.4.1	SI	El laboratorio debe aplicar métodos y procedimientos apropiados para todos los análisis forenses dentro de su alcance. Estos incluyen cadena de custodia, la manipulación, el almacenamiento y el triage forense, la estimación de la veracidad de los resultados. El laboratorio debe tener instrucciones para el uso y el funcionamiento de todo el equipamiento pertinente, y para la manipulación y la preparación de la información deseada, cuando la ausencia de tales instrucciones pudiera comprometer los resultados de los análisis forenses. Todas las instrucciones, normas, manuales y datos de referencia correspondientes al trabajo del laboratorio se deben mantener actualizados y deben estar fácilmente disponibles para el investigador. Las desviaciones respecto de los métodos de análisis forense deben ocurrir solamente si la desviación ha sido documentada, justificada técnicamente, autorizada y aceptada por la autoridad competente.	NO
	5.4.2	SI	El laboratorio debe utilizar los métodos de análisis forense, incluidos los del triage, que satisfagan las necesidades de la autoridad competente y que sean apropiados para la actuación que realiza. Se deben utilizar preferentemente los métodos publicados como acuerdos internacionales, nacionales o regionales. Cuando sea necesario, la guía debe ser complementada con detalles adicionales para asegurar una aplicación coherente. Cuando no se especifique el método a utilizar, el laboratorio debe seleccionar los métodos apropiados que hayan sido validados por nivel central, normas nacionales o regionales, por organizaciones técnicas reconocidas, libros o revistas científicas especializados, o especificados por el fabricante del equipo. También se pueden utilizar métodos desarrollados por el laboratorio o los métodos adoptados por el laboratorio si son apropiados para el uso previsto y si han sido validados. La autoridad competente debe ser informada del método usado. El laboratorio debe confirmar que puede aplicar correctamente los métodos antes de utilizarlos para los análisis forenses. Si el método normalizado cambia, se debe repetir la confirmación.	NO

	5.4.3		SI	La introducción de los métodos de análisis forenses desarrollados por el laboratorio para su propio uso debe ser una actividad planificada y debe ser asignada a personal calificado, provisto de los recursos adecuados.	NO
	5.4.4		SI	Cuando sea necesario utilizar métodos no normalizados, éstos deben ser acordados con la autoridad correspondiente y deben incluir una especificación clara de los requisitos de la actuación y de la manipulación del elemento material probatorio. El método desarrollado debe haber sido validado adecuadamente antes del uso.	NO
	5.4.5	5.4.5.1	SI	La validación es la confirmación, a través de experiencias acertadas, que validen el cumplimiento de los requisitos particulares para un uso específico previsto.	NO
		5.4.5.2	SI	El laboratorio debe validar los métodos no normalizados, los métodos que diseña o desarrolla, los métodos normalizados empleados fuera del alcance previsto, así como las ampliaciones y modificaciones de los métodos normalizados, para confirmar que los métodos son aptos para el fin previsto. La validación debe ser tan amplia como sea necesario para satisfacer las necesidades del tipo de aplicación o del campo de aplicación de dados. El laboratorio debe registrar los resultados obtenidos, el procedimiento utilizado para la validación y una declaración sobre la aptitud del método para el uso previsto.	NO
		5.4.5.3	SI	La gama y la exactitud de la información que se obtienen empleando métodos validados tal como fueron fijadas para el uso previsto, deben responder a las necesidades de la autoridad competente.	NO
	5.4.6	5.4.6.1	SI	El laboratorio debe tener y debe aplicar un procedimiento para estimar la veracidad de la información obtenida del análisis forense y todos los resultados que de este se puedan obtener.	NO
		5.4.6.2	SI	El laboratorio debe tener y debe aplicar procedimientos para estimar los factores que desestiman la veracidad de la medición. Para ello el laboratorio debe, por lo menos, tratar de identificar todos los componentes de la incertidumbre y hacer una estimación razonable, y debe asegurarse de que la forma de informar el resultado no dé una impresión equivocada de la incertidumbre. Una estimación razonable se debe basar en un conocimiento del desempeño del método y en el alcance de la extracción y/o inspección y debe hacer uso, por ejemplo, de la experiencia adquirida y de los datos de validación anteriores.	NO

		5.4.6.3	SI	Cuando se estima el error que conlleva la extracción y/o inspección, se deben tener en cuenta todos los componentes de la incertidumbre que sean de importancia en la actuación dada, utilizando métodos apropiados de análisis.	NO
	5.4.7	5.4.7.1	SI	Los resultados obtenidos del análisis forense deben estar sujetos a verificaciones adecuadas llevadas a cabo de una manera sistemática.	NO
		5.4.7.2	SI	El laboratorio debe asegurarse de que: a) El software empleado para el análisis forense documente con el detalle suficiente y haya sido convenientemente validado, de modo que se pueda asegurar que es adecuado para el uso. b) Se establecen e implementan procedimientos para proteger los datos; tales procedimientos deben incluir, pero no limitarse a, la integridad y la confidencialidad de la evidencia y triage, su almacenamiento, transmisión y procesamiento. c) Se hace el mantenimiento de las computadoras y equipos con el fin de asegurar que funcionan adecuadamente y que se encuentran en las condiciones ambientales y de operación necesarias para preservar la integridad de la información recuperada.	NO
5.5	5.5.1		SI	El laboratorio debe estar provisto con todos los equipos para extracción e inspección, requeridos para la correcta ejecución del análisis forense. En aquellos casos en los que el laboratorio necesite utilizar equipos que estén fuera de su control permanente, debe asegurarse de que se cumplan los requisitos de esta guía.	SI
	5.5.2		SI	Los equipos y su software utilizado para el análisis forense deben permitir lograr la exactitud requerida y deben cumplir con las especificaciones pertinentes para los análisis forenses concernientes. Se deben establecer programas de mantenimiento de los instrumentos cuando sus propiedades afecten significativamente a los resultados. Antes de poner en servicio un equipo se lo debe probar o verificar su funcionamiento con el fin de asegurar que responde a las exigencias especificadas del laboratorio y cumple las especificaciones normalizadas pertinentes. El equipo debe ser examinado antes de su uso.	NO
	5.5.3		SI	Los equipos deben ser operados por personal autorizado. Las instrucciones actualizadas sobre el uso y el mantenimiento de los equipos (incluido cualquier manual pertinente suministrado por el fabricante del equipo) deben estar disponibles para ser utilizadas por los investigadores del grupo.	NO

	5.5.4	SI	Cada equipo y su software utilizado para los análisis forenses, que sea importante para el resultado, debe, en la medida de lo posible, estar unívocamente identificado.	NO
	5.5.5	SI	Se deben establecer registros de cada componente del equipamiento y su software que sea importante para la realización del análisis forense. Los registros deben incluir por lo menos lo siguiente: a) La identificación del equipo y su software. b) El nombre del fabricante, la identificación del modelo, el número de serie u otra identificación única. c) Las verificaciones de la conformidad del equipo con la especificación. d) La ubicación actual, cuando corresponda. e) Las instrucciones del fabricante, si están disponibles, o la referencia a su ubicación. f) Las fechas, los resultados y las copias de los informes y de los certificados de todos los mantenimientos, los criterios de aceptación, y la fecha prevista del próximo mantenimiento. g) Todo daño, mal funcionamiento, modificación o reparación del equipo.	NO
	5.5.6	SI	El laboratorio debe tener procedimientos para la manipulación segura, el transporte, el almacenamiento, el uso y el mantenimiento planificado de los equipos con el fin de asegurar el funcionamiento correcto y de prevenir la contaminación o el deterioro.	NO
	5.5.7	SI	Los equipos que hayan sido sometidos a una sobrecarga o a un uso inadecuado, que den resultados dudosos, o se haya demostrado que son defectuosos o que están fuera de los límites especificados, deben ser puestos fuera de servicio. Se deben aislar para evitar su uso o se deben rotular o marcar claramente como que están fuera de servicio hasta que hayan sido reparados y se haya demostrado por ensayo que funciona correctamente. El laboratorio debe examinar el efecto del defecto o la probabilidad de error en el análisis anterior y debe aplicar el procedimiento de "control del trabajo no conforme”.	NO
	5.5.8	SI	Cuando sea posible, todos los equipos bajo el control del laboratorio que requieran mantenimiento o actualización, deben ser rotulados, codificados o identificados de alguna manera para indicar el estado funcionamiento, incluida la fecha en la que tuvieron mantenimiento por última vez y su fecha de vencimiento o el criterio para la próxima revisión.	NO

	5.5.9			SI	Cuando, el equipo quede fuera del control directo del laboratorio, éste debe asegurarse de que se verifican el funcionamiento del equipo y de que los resultados son satisfactorios, antes de que el equipo sea reintegrado al servicio.	NO
	5.5.10			SI	Cuando se necesiten verificaciones intermedias para mantener la confianza en el estado de funcionamiento de los equipos, éstas se deben efectuar según un procedimiento definido.	NO
	5.5.11			SI	Cuando los mantenimientos den lugar a un conjunto de factores de corrección, el laboratorio debe tener procedimientos para asegurarse de que las copias (por ejemplo, en el software), se actualizan correctamente.	NO
	5.5.12			SI	Se deben proteger los equipos, tanto el hardware como el software, contra ajustes que pudieran invalidar los análisis forenses.	NO
5.6	5.6.1			SI	Todos los equipos utilizados para los análisis forenses, incluidos los equipos para tareas auxiliares que tengan un efecto significativo en la validez de los resultados del análisis forense, deben ser probados y revisados antes de ser puestos en servicio. El laboratorio debe establecer un programa y un procedimiento para la evaluación de sus equipos.	NO CUMPLE
	5.6.2	5.6.2.1		NO		
		5.6.2.2	5.6.2.2.1	NO		
			5.6.2.2.2	SI	Para los laboratorios de informática forense, el programa de mantenimiento de los equipos debe ser diseñado y operado de modo que se asegure que los análisis forenses hechos por el laboratorio sean reconocidos por un tribunal. Se debe determinar un mecanismo para comprobar la eficacia del laboratorio de informática forense. La eficacia de sus resultados debe contar con un método de ensayo para determinar el estado de funcionamiento de los equipos. Se debe buscar una referencia al cual soportar los resultados obtenidos del análisis forense. Cuando se utilicen servicios de mantenimiento externos, se debe asegurar la eficiencia de dichos mantenimientos mediante un proceso similar al descrito anteriormente.	NO
	5.6.3			NO		
5.7				NO		

5.8	5.8.1	SI	El laboratorio debe tener procedimientos para el transporte, la recepción, la manipulación, la protección, el almacenamiento, la conservación y/o la disposición final de la información obtenida de un análisis forense, incluidas todas las disposiciones necesarias para proteger la integridad del elemento de cadena de custodia resultante.	NO
	5.8.2	SI	El laboratorio debe tener un sistema para la identificación de las actuaciones necesarias que atender con el análisis forense. La identificación debe conservarse durante el proceso de triage en el laboratorio. El sistema debe ser diseñado y operado de modo tal que asegure que los ítems del triage no puedan ser confundidos físicamente ni cuando se haga referencia a ellos en registros u otros E.M.P o documento. Cuando corresponda, el sistema debe prever una subdivisión en grupos de ítems y la transferencia de los ítems dentro y desde el laboratorio.	SI
	5.8.3	SI	Al recibir el ítem para triage forense, se deben registrar las anomalías o los desvíos en relación con las condiciones de la información obtenida, según se describen en el correspondiente método de análisis forense. Cuando exista cualquier duda respecto a la adecuación de un ítem para una extracción y/o inspección, o cuando un ítem no cumpla con la descripción provista, o el análisis no especifique con suficiente detalle la actuación requerida, el laboratorio debe solicitar a la autoridad competente instrucciones adicionales antes de proceder y debe registrar lo tratado.	NO
	5.8.4	SI	El laboratorio debe tener procedimientos e instalaciones apropiadas para evitar el deterioro, la pérdida o el daño de la información resultante durante el almacenamiento, la manipulación y la preparación. Se deben seguir las instrucciones para la manipulación provistas para la información. El laboratorio debe tener disposiciones para el almacenamiento y la seguridad que protejan la condición e integridad de la información resultante de las extracciones y/o inspecciones.	NO
5.9		NO		

5.10	5.10.1		SI	Los resultados de cada análisis forense efectuado por el laboratorio, deben ser informados en forma exacta, clara, no ambigua y objetiva, de acuerdo con las instrucciones específicas de los métodos de análisis forense. Los resultados deben ser informados en un informe judicial y deben incluir toda la información requerida por la autoridad competente y necesaria para la interpretación de los resultados de la actuación.	NO
	5.10.2		SI	Cada informe judicial debe incluir la siguiente información, salvo que el laboratorio tenga razones válidas para no hacerlo así: a) Un título. b) El grupo investigativo responsable de la actuación (de no ser delitos informáticos, justificar el apoyo solicitado). c) La identificación de orden de trabajo y el No de informe en cada página una identificación para asegurar que la página es reconocida como parte del informe judicial, y una clara identificación del final del informe. d) La identificación la autoridad solicitante. e) La identificación de las acciones ejecutadas para cumplir con la actuación. f) Una descripción, la condición y una identificación no ambigua de la información obtenida de las extracciones y/o inspecciones. g) Las fechas entre las cuales se realizó el análisis forense. h) Una referencia al plan y a los procedimientos utilizados por el laboratorio u otros organismos, cuando éstos sean pertinentes para la validez o la aplicación de los resultados. i) Los resultados finales del análisis forense como respuesta a lo solicitado por una autoridad competente. j) El o los nombres, cargo y firmas del o los investigadores que realizaron el análisis.	NO
	5.10.3	5.10.3.1	SI	Además de los requisitos indicados en el apartado, los informes de los análisis forenses deben incluir, en los casos en que sea necesario para la interpretación de los resultados del análisis forense, lo siguiente: a) Las variaciones, adiciones o exclusiones del método establecido para el análisis e información sobre condiciones específicas, tales como las condiciones ambientales. b) Cuando corresponda, una declaración sobre el cumplimiento o no cumplimiento con los requisitos y/o las especificaciones. c) Cuando sea apropiado y necesario, las opiniones e interpretaciones. d) La información adicional que pueda ser requerida por métodos específicos o una autoridad competente.	NO CUMPLE

	5.10.3.2	NO		
5.10.4		NO		
5.10.5		SI	Cuando se incluyan opiniones e interpretaciones, el laboratorio debe asentar por escrito las bases que respaldan dichas opiniones e interpretaciones. Las opiniones e interpretaciones deben estar claramente identificadas como tales en un informe judicial.	NO
5.10.6		NO		
5.10.7		SI	Cuando el informe forense se cargue al SPOA a través de la intranet, se deben cumplir los requisitos de esta guía.	NO
5.10.8		SI	La presentación del informe debe ser concebida para responder a cada análisis forense efectuado y para minimizar la posibilidad de mala interpretación o mal uso.	NO
5.10.9		NO		

Fuente: La autora.

8.5. DISEÑO DE LA PROPUESTA

El diseño de la propuesta está plasmado en la tercera columna “Ítem de la Norma ajustado a la Entidad” de la Tabla 3. “Caracterización y adaptación Norma NTC-ISO/IEC 17025”, mencionada previamente. Aquí se propone un completo plan de trabajo a desarrollarse a partir del presente 2014, se describen tareas específicas como logros a alcanzarse encaminadas a la acreditación del laboratorio. Hay que resaltar que esta es una labor interdisciplinaria que requiere la conformación de una mesa de trabajo, donde de manera conjunta den cumplimiento a cada ítem que hasta el momento no se satisface.

La propuesta contiene requerimientos tanto administrativos como técnicos, pues para alcanzar la meta de acreditación, estas actividades deben ir de la mano. La propuesta se desarrolló en ambos aspectos, de modo que cuando se presente un trabajo final se muestre una propuesta completa y que no solo se limite a aspectos técnicos.

Para realizar el ajuste de las clausulas originales enfocado a las actividades específicas de un laboratorio de informática forense, se tomó como referencia la ASCLD/LAB (American Society of Crime Laboratory Directors/ Laboratory Accreditation Board). La ASCLD/LAB para laboratorios forenses, define normativas semejantes a la ISO/IEC 17025:2005, sin embargo, han contemplado sus definiciones en un marco jurídico que se encuentra ligado a las actividades de análisis forense del laboratorio, resaltando la importancia del E.M.P. y de la figura de cadena de custodia, así como términos de una investigación judicial.

No se realizó la propuesta con base a la ASCLD/LAB, porque se trata de una sociedad Americana y a pesar de haber acreditado ya 19 laboratorios fuera de Estados Unidos, la norma ISO tienen mayor reconocimiento a nivel mundial y es el ICONTEC la figura más reconocida a nivel nacional en cuanto a normalización.

Adicional a esto se resaltó la necesidad latente e imprescindible para un investigador informático de conservar la idoneidad, metodología y la técnica para obtener la evidencia digital, para que esta información pueda ser efectiva en una indagación judicial, por ello se tuvo como marco de referencia la NTC-ISO/IEC 27037:2012 la cual especifica directrices para la identificación, recolección, adquisición y preservación de la evidencia digital, manteniendo así, características del derecho informático.

Lo más destacable para el trabajo realizado y que se debe tener en cuenta en las actividades que continúan, es que todos los procedimientos realizados con evidencia digital tienen que garantizar los tres pilares de la información: Confidencialidad, Integridad y Disponibilidad[18].

A continuación se presentan algunas propuestas que pueden ser de interés para dar cumplimiento a algunos ítems:

- Teniendo en cuenta que el objeto de análisis (Evidencia Digital) de un análisis forense son datos que han sido procesados electrónicamente y guardados en un medio electrónico, teniendo su fundamento en las leyes de la física, de la electricidad y el magnetismo, se le debe prestar mayor atención a factores ambientales que puedan afectar la integridad de la evidencia y de los equipos.

El laboratorio y el edificio en el que este se encuentra, no cuenta con un sistema de protecciones eléctricas de acuerdo al reglamento técnico de instalaciones eléctricas "RETIE". Por lo cual sería necesario implementar por lo menos los tres niveles de protección definidos en este reglamento.

a. Sistema de apantallamiento contra descargas atmosféricas

Implementar un sistema de pararrayos Ionizante (no radiactivo) con dispositivo de cebado, que cumple con la teoría de la esfera ficticia[19] y es una forma sencilla que brinda una protección contra rayos eficiente. Este sistema presenta un amplio radio de cobertura, el cual depende de un sencillo cálculo del modelo electrogeométrico y el cumplimiento de la teoría de la esfera ficticia de mayor distancia, este es un modelo de fácil aplicación.

Permite la captación de hasta ocho impactos directos de rayos continuos sin saturarse, captando los rayos y canalizándolos hasta la malla de puesta a tierra del pararrayos para disipar su energía en el subsuelo, sin que ocasione daños irreparables en instalaciones

[18] CENTRO CIBERNÉTICO POLICIAL. Evidencia Digital. Recuperado el 15 de enero de 2014, de: http://www.ccp.gov.co/articulo-imagen.php?id=141

[19] La teoría de la esfera ficticia está basada en la suposición de que el punto de impacto de un rayo queda definido cuando el líder descendente está a una distancia determinada de un punto de una estructura (edificio, objeto o suelo)

eléctricas, equipos eléctricos y electrónicos y, principalmente protegiendo la integridad física de los funcionarios.

b. Sistemas de puestas a tierra

Un correcto diseño del sistema de puesta a tierra es fundamental para asegurar la correcta conducción de la descarga eléctrica del rayo. En el sistema que se implemente se debe contemplar que no existan bucles que produzcan tensiones inducidas.

Se debe realizar los cálculos, el diseño y la instalación del sistema de protección de puestas a tierra y malla del servicio, para aterrizar las sobrecargas tanto atmosféricas como de conmutaciones internas y fluctuaciones de tensión en las redes de alimentación eléctrica que contenga el laboratorio.

Se propone implementar sistemas tradicionales en mallas de puesta tierra, con tecnología de última generación como las “Unidades de Tratamiento de Suelos“(UTS) y la Hidrosolta. Las mediciones de resistencia de suelos se deben realizar empleando el método de medición de la “curva de caída de tensión”, mediante la utilización de equipos aptos como el Telurómetro digital.

c. Protecciones contra sobrevoltajes transitorios.

Prácticamente todas las conmutaciones en las redes a gran escala, y particularmente las de elevada potencia, producen sobretensiones. La apertura de circuitos de protección o de mando compuestos por contactores y relés, en aplicaciones de transferencia de redes, bancos de condensadores, puesta en marcha de motores de gran potencia, encendido de soldadores y balastros. Estas maniobras generan sobretensiones de tipo oscilatorio, de alta frecuencia y con tiempos de amortiguación rápida. Estos transitorios pueden perturbar el funcionamiento de los equipos del laboratorio.

Los dispositivos de protección contra sobretensiones transitorias (DPS) según la norma NTC 4552 son dispositivos destinados a limitar las sobretensiones transitorias, evacuando las corrientes asociadas a dicho sobrevoltaje.

Es necesario discernir entre las categorías tipo A y B de supresores que mejor se adapte a las necesidades del laboratorio dependiendo de su utilización y del costo.

Adicionalmente se recomienda considerar la independencia de los circuitos del laboratorio forense y realizar estas consideraciones, desde el escenario actual y el que contempla la independencia de los circuitos.

Otro factor de consideración es la estática. La estática es una parte de un campo de alto voltaje no equilibrado sobre una superficie no conductora, como la palma de la mano. Los circuitos integrados son especialmente sensibles a las descargas electroestáticas, como procesadores, memoria, chips de cache y tarjetas de expansión, entre otros.

Actualmente no se manejan protocolos a modo de prevenir este tipo de daños, para lo cual es se deben tomar medidas como el uso de guantes o manillas antiestáticas, uso de bata en el laboratorio y adecuaciones mayores que ayuden a reducir el impacto de estos fenómenos físicos en la evidencia digital como dotar el laboratorio con mesas fijas, se puede optar por mesas de concreto para que no afecten la estabilidad, impidiendo vibraciones e inestabilidad, con una superficie de cerámica que minimice los efectos de la estática durante la manipulación del E.M.P. y el análisis forense. Esto mejora también otros factores como la humedad o la temperatura teniendo en cuenta que durante un análisis forense un F.R.E.D. puede estar encendido hasta un mes. Para esto se pueden consultar manuales de normas de procedimiento existentes para el laboratorio forense, o diseñarlo teniendo en cuenta todos los factores ambientales que influyen en un análisis forense.

- Uno de los protocolos para el análisis forense de telefonía móvil consiste en la activación de un inhibidor de frecuencias.

Un inhibidor de frecuencias emite ondas electromagnéticas con energía suficiente para colisionar con las señales de los teléfonos móviles y tirar las comunicaciones o impedir el servicio.

La importancia de este procedimiento radica en preservar la integridad de la evidencia digital durante el análisis forense. El fundamento de este protocolo está norma NTC-ISO/IEC 27037, donde se estipula que el E.M.P. dentro de su

protocolo de cadena de custodia conserve las características impuestas en esta norma.

Actualmente en el laboratorio de informática forense del CTI no se cumple este protocolo, esto, debido a la cercanía que tiene con el grupo de control telemático, pues se corre el riesgo de que la activación del inhibidor afecte sus actividades.

Frente a esta situación se propuso hacer el estudio de los patrones de radiación, para tener conocimiento real de la cobertura del inhibidor y de los elementos que puedan verse afectados. Con los resultados de este estudio se puede optimizar la ubicación del inhibidor de frecuencias y crear un sistema para aislar el laboratorio, basado en la Jaula de Faraday (modelo utilizado también para el apantallamiento contra descargas atmosféricas).

- Cuando se habla de triage forense se hace referencia a una de las fases del peritaje informático que también se conoce como el análisis, se realiza después de duplicar la evidencia con el fin de depurar la información no necesaria y recaudar la mayor cantidad de información de interés con respecto a la actuación que se generó por parte de la autoridad competente.

En el laboratorio de delitos informáticos del CTI este proceso se realiza de manera manual, por lo tanto depende exclusivamente de la pericia y criterio del investigador, lo cual puede arrojar resultados variables de un investigador a otro.

Ya que el propósito de normalizar los procedimientos del laboratorio forense, requiere una estandarización de los mismos se deben implementar métodos que minimicen el error que pueda generar el triage de la manera que se realiza actualmente, siendo este un procedimiento rezagado.

Para ello existen en el mercado varias herramientas enfocadas exclusivamente en el triage forense como las que ofrecen compañías como Access Data y Mattica; e incluso se pueden desarrollar a nivel institucional teniendo como base proyectos de esta clase que ya se han realizado como el perfilado digital enfocado a minimizar el error resultante del triage, el cual considera factores como: tamaño de la muestra, ficheros de tipo desconocido, desconocimiento del funcionamiento de las aplicaciones informáticas (motivo por el cual se debe estar en constante formación), cambios en la apariencia de la información (extensiones de ficheros/signaturas), ficheros borrados, ficheros protegidos, ficheros cifrados, entre otros.

El perfilado digital realizado en el marco de una pericia informática legalmente solicitada por una autoridad competente no puede recibir cuestionamientos. Simplemente se trata de una técnica forense que se aplica en el marco de una metodología que utiliza procedimientos formalmente aprobados y que garantiza en todo momento la integridad de la evidencia digital.

- En cuanto a los equipo se aportó la siguiente información para cumplir de manera básica los requisitos de la norma.

En la tabla 4 se documenta las necesidades básicas que debe cubrir el laboratorio con respecto a equipos para cumplir con la norma, adicional a esto y teniendo en cuenta la información recolectada de los equipos con que el laboratorio cuenta actualmente, frente a cada uno de los requerimientos se marca con un visto los que cumple el laboratorio del CTI y con una equis los que no, así se hace claridad a los aspectos para solucionar:

Tabla 3. GUÍA PARA LA IMPLEMENTACIÓN DE LABORATORIOS DE INFORMÁTICA FORENSE QUE CONTEMPLA ASPECTOS BÁSICOS DE HARDWARE Y SOFTWARE

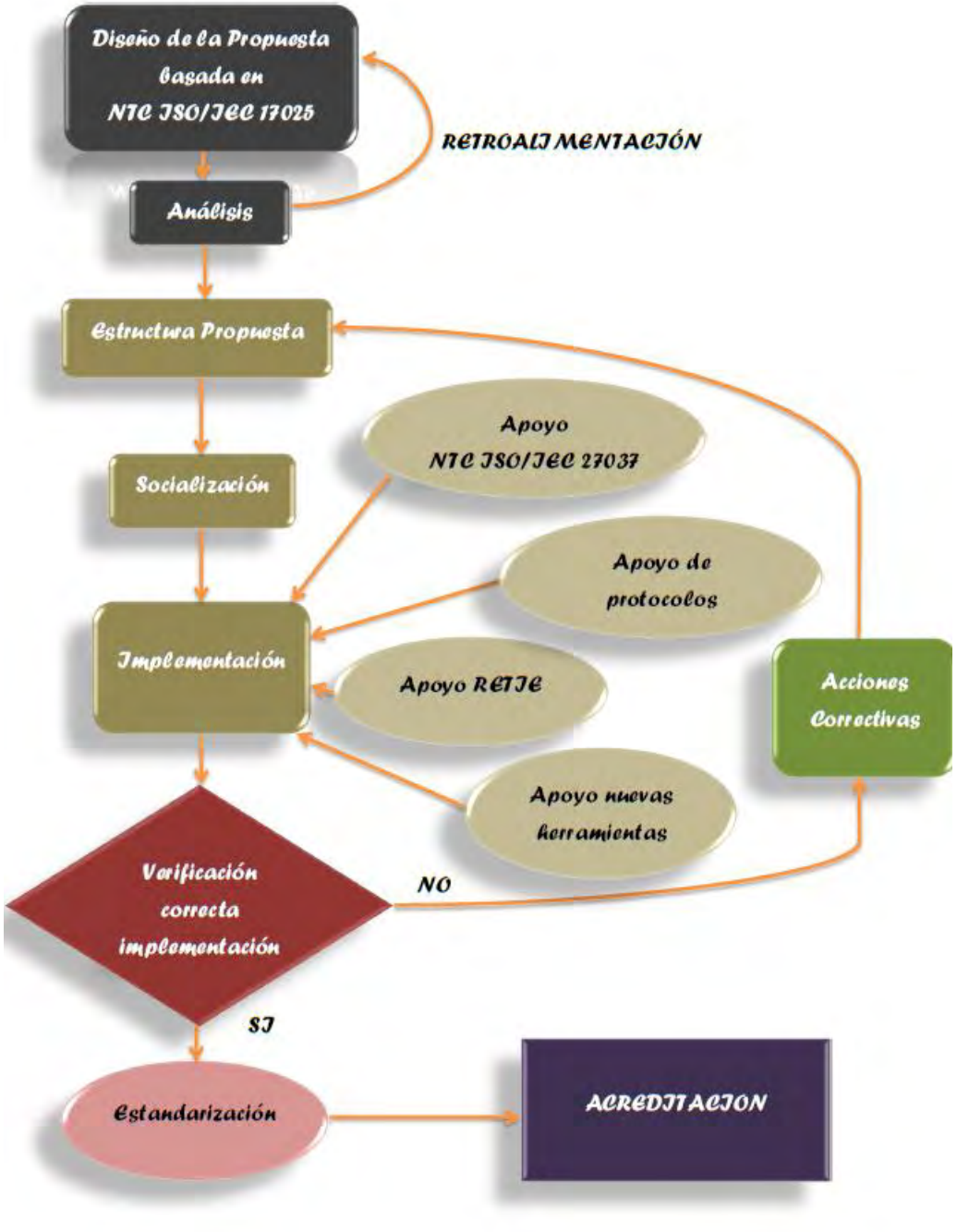
No.	ÍTEM	REQUISITOS MÍNIMOS	
1	SERVIDOR DEL LABORATORIO	Almacenamiento de 4,5 Tb en discos SAS	☒
		S.O. que brinde servicios de Terminal Server para inicio de sesiones remotas	☒
		UPS acordes al Servidor del Laboratorio	☒
2	RED INTERNA DE LABORATORIO DE TIPO GIGABIT ETHERNET	Rack	☒
		Switch	☒
		Placas de Red para cada puesto	☒
		Cableado Estructurado	☒
		Red eléctrica separada para conexión de equipos informáticos	☒
3	PROTECTORES	Tableau T8	☑

	CONTRA ESCRUTURA (WRITE BLOCKERS) Y DUPLICADORES	Tableau TD1	☑
		Disk Jockey Pro Forensic Kit	☒
		Caja de Faraday para el Laboratorio	☒
		Bolsas de Faraday	☑
4	TELEFONIA CELULAR	Device Seizure Toolbox	☑
		Lector de memorias + Cargador externo	☑
		CSI Stick	☒
		Computador portátil	☑
5	EQUIPO INFORMATICO FORENSE MOVIL	Impresora portátil	☑
		Equipo forense portátil	☒
		Memoria RAM de 4Gb mínimo	☑
		Monitor LCD 22"	☒
		RAID-0 de 750 Gb mínimo	☑
6	EQUIPO INFORMATICO FORENSE PARA LABORATORIO	Placa de red Ethernet Gigabit	☑
		SO Windows 7 Ultimate	☑
		Interfaces para conexión de dispositivos externos: USB, P-ATA, S-ATA, FIREWIRE, etc	☑
		Impresora láser con conexión a red	☑
7	PERIFERICOS DEL LABORATORIO	Cámara digital	☑
		Software gratuito: Helix, Liveview!, FTK Imager, etc	☑
		1 licencia de EnCase por puesto de trabajo	☑
8	SOFTWARE FORENSE	Device Seizure (opcional)	☒
		Mount Imager Pro (opcional)	☒
		Vmware Workstation (opcional)	☒

Fuente: La autora.

El siguiente esquema, basado en el ciclo Deming, representa el proceso de mejora para el laboratorio, de acuerdo a la propuesta presentada.

Figura 12. CICLO DEMING DEL DESARROLLO DE LA PROPUESTA

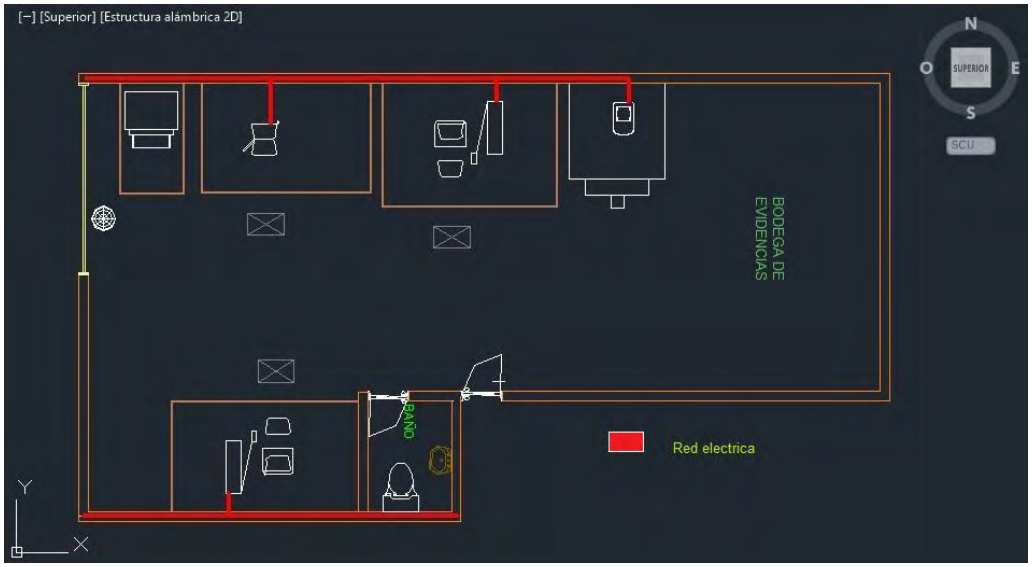


Fuente: La autora.

Gran parte de la propuesta no podría hacerse tangible de manera física, pues establece lineamientos, parámetros y protocolos del accionar dentro del mismo.

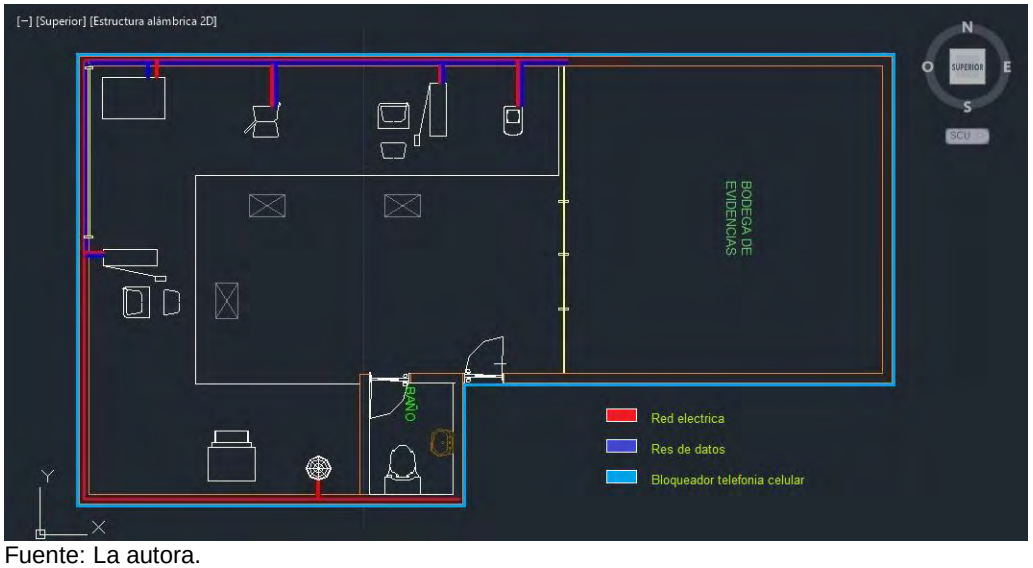
En la figura 13 y la figura 14 se evidencian los cambios de infraestructura que se llevarían a cabo con la aplicación de la propuesta:

Figura 13. DIAGRAMA ESTRUCTURAL DE LA PLANTA FÍSICA DEL LABORATORIO DE DELITOS INFORMÁTICOS DEL CTI SECCIONAL PASTO



Fuente: La autora.

Figura 14. DIAGRAMA ESTRUCTURAL PROPUESTO PARA LA PLANTA FÍSICA DE DELITOS INFORMÁTICOS DEL CTI SECCIONAL PASTO



Fuente: La autora.

8.5.1. Estado actual de la Propuesta

Inicialmente el PROYECTO PARA EL MEJORAMIENTO DEL LABORATORIO DEL GRUPO INVESTIGATIVO DE DELITOS INFORMÁTICOS DEL CUERPO TÉCNICO DE INVESTIGACIÓN "CTI" PASTO pasó por la revisión del coordinador del Grupo de Delitos Informáticos del CTI seccional Pasto, el cual sugirió ajustes antes de ser presentada a la Dirección del CTI de la ciudad.

En el mes de enero del presente año se presentó el proyecto a la Dirección del CTI, quien con conocimiento del tema del proyecto, solicitó la revisión del líder del equipo de gestión integral del CTI, quien dio viabilidad para enviar el proyecto a Nivel Central en busca de aprobación para iniciar con un trabajo en torno al proyecto, con el fin de alcanzar la acreditación NTC-ISO/IEC 17025 para todos los laboratorios de informática forense del CTI de la Fiscalía General de la Nación.

El proyecto se envió a Nivel Central en Enero del presente año, y en Febrero del mismo se dio a conocer a todos los coordinadores de los grupos de Delitos Informáticos a Nivel Nacional, de lo cual se acordó realizar una reunión en el mes de Marzo con fecha exacta por definirse en la ciudad de Medellín, con el fin de socializar la propuesta y concretar la aceptación del proyecto a nivel nacional, así como el calendario de trabajo que se planee para la ejecución.

8.6. SUPERVISAR, ADMINISTRAR Y GESTIONAR EL MEJORAMIENTO DE LA RED

8.6.1. Red de Acceso Inalámbrico

Se realizó la supervisión en la prestación de servicios, consistentes en conceder a la planta física el servicio de acceso inalámbrico a la red de datos de la institución. Esto consistió en la implementación de 4 Access point HP MSM-802.11n que realizan la función de puntos de enlace para los usuarios remotos. Para esto la empresa a la que se le adjudicó el contrato, se encargó de la dotación de los equipos y los entregó funcionando dentro de la red Ethernet de la Fiscalía, una vez hecho esto y dentro de la autonomía del CTI, fue necesario adecuar su configuración a la seguridad requerida por la institución lo cual se logró una vez estudiado el manual del equipo.

Durante este proceso se encontró que estos equipos no podían proveer el servicio de conexión DHCP a sus clientes, pues a diferencia de la mayoría de access point en el mercado, estos equipos no actuaban como routers y solo funcionaban como puntos de acceso a la red.

Igualmente, se evaluó las diferentes opciones para sobrellevar este inconveniente, por lo cual inicialmente todos los equipos fueron dotados de IP estática de manera manual, siendo esta una labor tediosa. Finalmente se propuso como solución la adquisición de un AP controller y fue solicitado a la empresa proveedora del servicio debido a que su solución inicial no satisfacía las necesidades planteadas por el CTI.

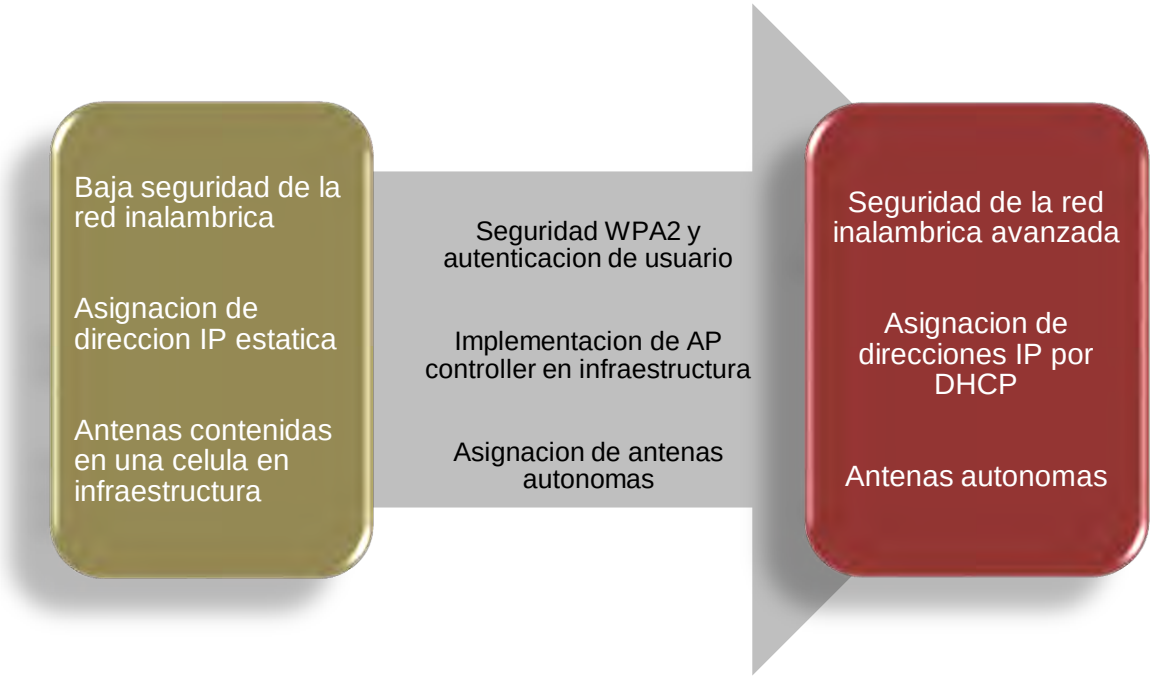
Algunos meses después enviaron un controlador de acceso HP serie WX5000, a las instalaciones del CTI, pero no enviaron personal capacitado para configurarlo de acuerdo a las necesidades institucionales.

Con base al manual del usuario incluido con el equipo y a las necesidades presentadas se instaló el AP controller en el RACK de telecomunicaciones principal del edificio en Infraestructura a las antenas, creando así una única célula de mayor tamaño dependiente del controlador.

Posteriormente se solicitó que uno de los Access Point quedara externo de la célula, esto debido a que funcionaria en el Grupo de Telemática, el cual mantiene con mayor restricción sus comunicaciones. Para ello se definió desde el

controlador una antena como independiente, limitando el acceso a la misma desde el AP Controller y sin embargo este continuaba proveyendo a su célula de direcciones DHCP, incluida la antena independiente.

Figura 15. ESTADO ANTERIOR Y ESTADO ACTUAL DE LA RED INALÁMBRICA DEL CTI



Fuente: La autora.

8.6.2. Telefonía IP

Se realizó un proceso de reestructuración de la telefonía IP dentro de las instalaciones del CTI, teniendo en cuenta las sugerencias y necesidades planteadas por algunas dependencias que se muestran en la Tabla 1. “Distribución dependencias y necesidades de la Red”.

Para esto se consultaron servicios específicos requeridos por dichas dependencias, entre los cuales estaban:

- Grabación de las llamadas entrantes y salientes.
- Servicio de buzón de mensajes para la recepción de denuncias.
- Recepción de Fax en las extensiones

- Enlace de teléfonos en instalaciones aledañas, con puerta de enlace diferente a la de la planta.

- Creación y adición de nuevas troncales.

Para dar cumplimiento a estas necesidades se revisó el manual de la planta y de los teléfonos y adicionalmente se obtuvo información referente al tema de trabajos relacionados[20].

Para el servicio de buzón de mensajes simplemente se revisó el manual del usuario y se configuro la opción de la planta al mismo comando del teléfono para habilitar el buzón.

Se adquirió una nueva planta Zycoo ZX50-A8 para crear una nueva troncal en otra sede del CTI, la cual se configuro de manera similar a la planta del edificio principal teniendo en cuenta el manual del usuario e igualmente se adiciono esta nueva troncal en las otras plantas. Debido a que la planta iba a tener no más de 15 usuarios no fue necesario realizar estudios adicionales con respecto a la saturación del ancho de banda de la Fiscalía General de la Nación y se pudo usar la misma referencia de equipos utilizados por las demás dependencias.

Para poder recibir fax en las extensiones se sugirió la implementación de un equipo ATA, que hiciera la función de interconectar la red conmutada con la red IP, sin tener que adquirir equipos de fax con IP que generarían mayores costos. Sin embargo por el momento se prefirió continuar con una única línea telefonica independiente a la planta para el servicio de Fax.

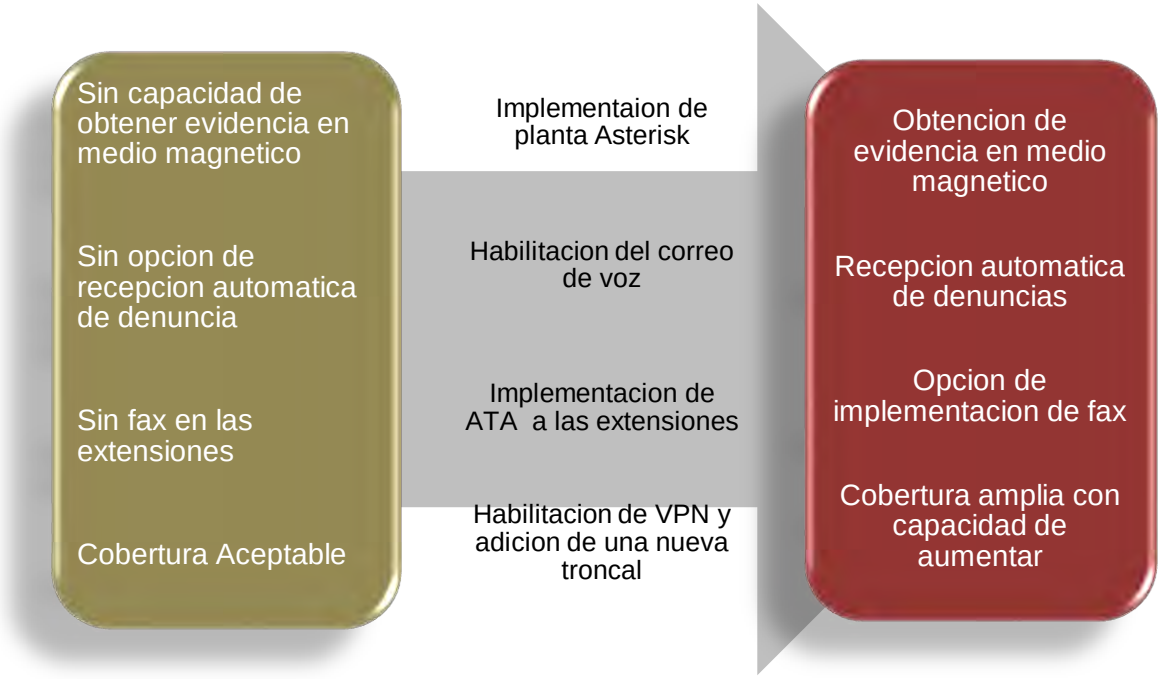
Fue necesario crear una nueva planta en software libre para la grabación de las llamadas entrantes y salientes. Se pretendía que esta planta se enlazara con la actual para que actuara como apoyo, pero finalmente se la dejo independiente. Esta planta se creó en Asterisk y solo se vincularon los teléfonos de la Sección de Análisis Criminalístico SAC.

Finalmente el enlace de los teléfonos del Grupo de BACRIM que se encuentra en instalaciones aledañas y cuenta con puerta de enlace diferente a la de la planta no

[20] FLOREZ PADILLA Mario Andres, RAMIREZ MELO Edgar Camilo. Caracterización de tráfico en la migración de la red de voz sobre IP en la Universidad de Nariño. Universidad de Nariño. 2014.

se pudo realizar pues requería autorización de nivel central quienes manejan toda la seguridad de la red y no permitieron que se habilite una VPN para los teléfonos.

Figura 16. ESTADO ANTERIOR Y ESTADO ACTUAL DE LA TELEFONÍA VoIP DEL CTI



Fuente: La autora.

8.6.3. Puerta de enlace – Routers

En el sector donde se encuentran las instalaciones de CTI Pasto se presentaron una serie de fallas en el suministro de energía eléctrica, que ocasionaron que los routers de la Entidad salieran de funcionamiento, y al reactivarse entraron en un estado de falla, por lo cual CTI Pasto estuvo desconectado de la Ethernet de CTI Colombia.

Debido a que la garantía de los equipos requería varios días de espera para solucionar este inconveniente, situación que obstruiría el desarrollo de la labor Institucional, se permitió tomar acciones correctivas por parte de la pasante. Para ello se consultó de manera virtual información referente a los equipos y a problemas similares en estos, pues no se conocía la configuración interna.

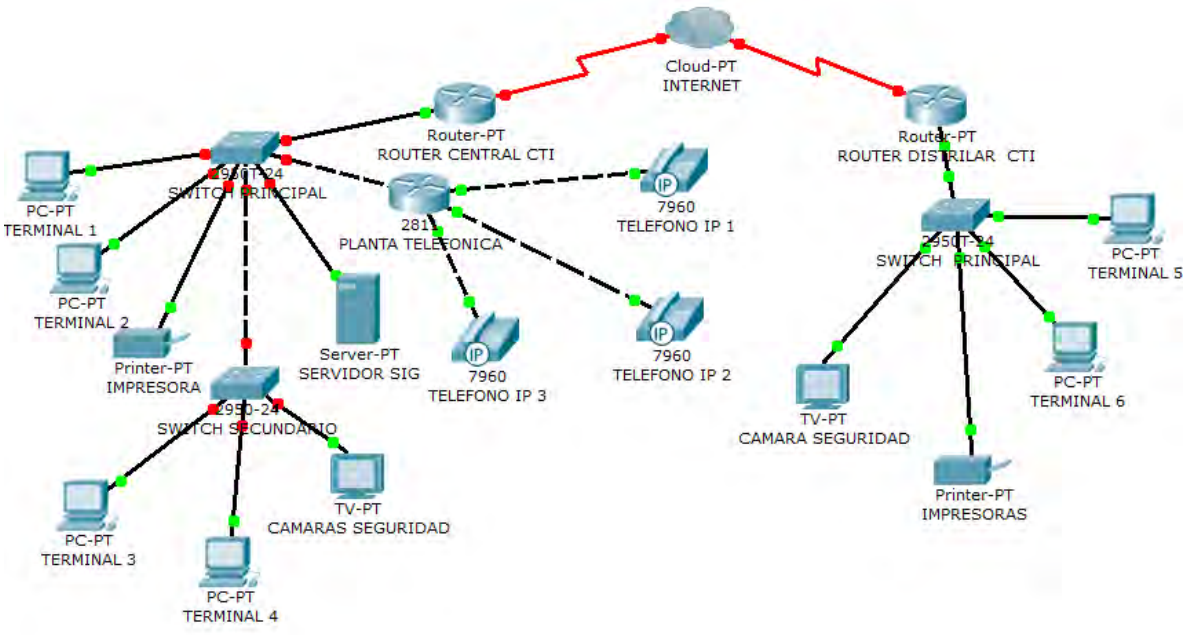
Provisionalmente se utilizó un Swith de tan solo 24 puertos para todo el edificio que cuenta con cerca de 100 puntos de red, con el objetivo de conectar por lo

menos un servidor por dependencia, este proceso se dificulto en gran medida, debido a que la red del edificio no está estandarizada bajo las normas Internacionales de cableado estructurado, como la ANSI/EIA/TIA-606 que proporciona un esquema de administración uniforme independiente de las aplicaciones que se le dan al sistema de cableado con el propósito de guiar en cuanto a la infraestructura de telecomunicaciones, por lo cual el proceso se realizó de manera intuitiva, conectando y desconectando usuarios hasta encontrar el adecuado.

Después de 2 días fuera de red, se accedió a los switches en estado de fault mediante una a través del protocolo SSH de Putty y se encontró que una de las librerías de inicio había sido borrada durante el apagón, pero el mismo equipo guardaba copias de seguridad y gracias a eso se pudo reasignar una copia de la librería a la librería original.

La siguiente grafica muestra la estructura de la red de datos en el momento inicial de la pasantía, y se resalta el momento más crítico ocurrido durante el desarrollo de la misma.

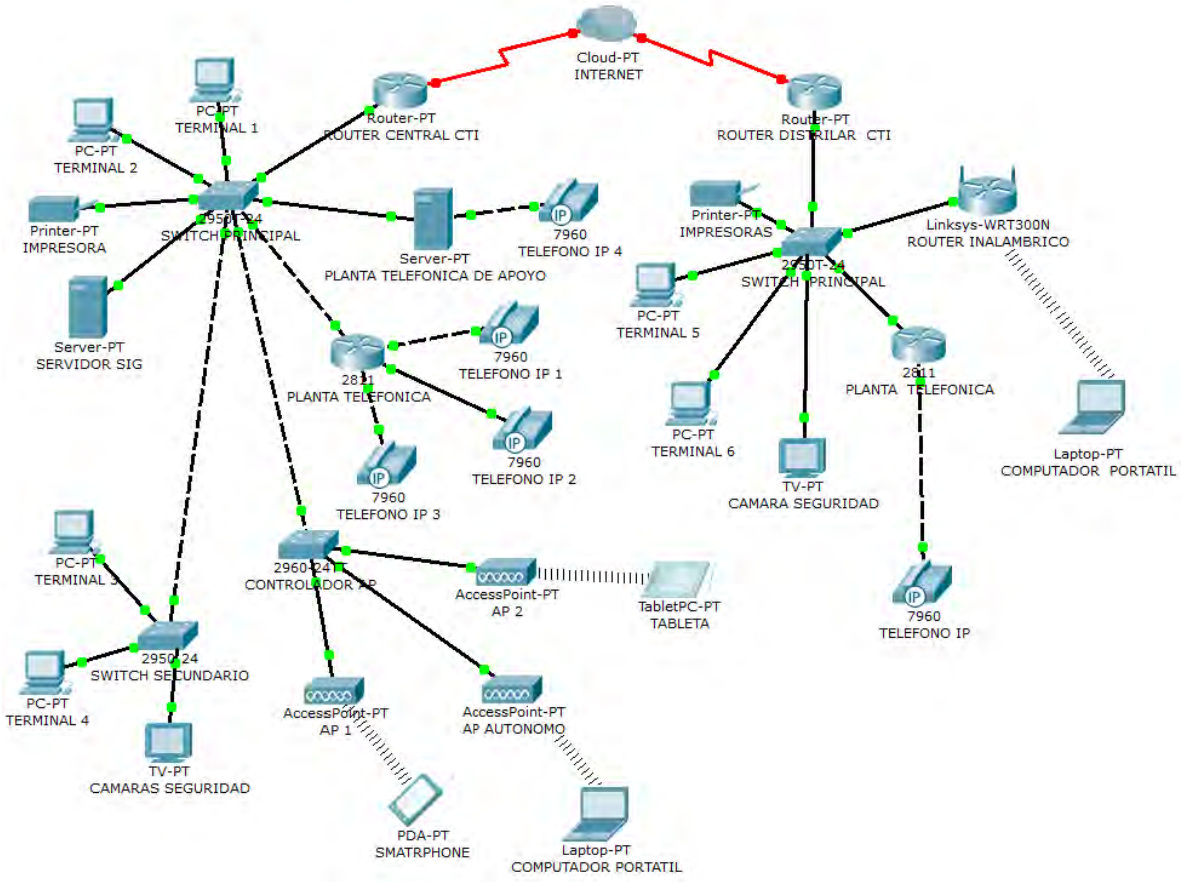
Figura 17. ESTRUCTURA DE LA RED DE DATOS EL PRIMER DÍA DE LA PASANTÍA



Fuente: La autora.

A continuación se puede ver el esquema de la red de datos al finalizar el periodo de la pasantía, con las mejoras que se realizaron.

Figura 18. ESTRUCTURA DE LA RED DE DATOS AL FINALIZAR LA PASANTÍA



Fuente: La autora.

CONCLUSIONES

- Es fundamental destacar la importancia de los vínculos interinstitucionales Universidad – Estado, puesto que son estos los que permiten una mejor dinámica en la generación de conocimiento y la investigación. En razón a esto, se logra un gran aporte a la Fiscalía General de la Nación en su búsqueda de acreditación de sus laboratorios de delitos informáticos a nivel nacional, puesto que todos deben guiarse bajo un mismo estándar.

- El aporte resultante del proceso de investigación deja latente la necesidad de generar nuevos espacios e involucrar directamente en el proceso, a profesionales del área de Ingeniería Electrónica, logrando una interdisciplinariedad que fortalezca la función de administración de justicia de la Fiscalía General de la Nación.

- Al ser el tema de los delitos informáticos una preocupación global, las cooperaciones internacionales marcan un factor importante para atenuar el perjuicio que estos puedan generar.

- La normalización en los procesos es la mejor forma de asegurar la eficacia de las actividades del laboratorio forense y las que se realizan en torno a él, sin embargo, es de gran importancia realizar un análisis de las clausulas con respecto a la realidad de la institución en busca de cumplir de manera pertinente a los requerimientos, sin faltar a otros procedimientos a los que una investigación se debe regir.

- Es importante resaltar que la mayoría de requerimientos especificados por la Norma NTC ISO/IEC 17025, y a su vez ajustados al contexto de la entidad en este proyecto, no se cumplen a pesar de su aplicabilidad y pertinencia a la labor misional.

- La Fiscalía General de la Nación tiene la disposición para mejorar los procedimientos de sus áreas de investigación, y a pesar de no generar propuestas por su iniciativa debido al desconocimiento de labores específicas, las directivas de la institución respaldan y acompañan las iniciativas que encaminen a la institución a fortalecerse de manera gradual y creciente.

- Enfocar un proceso de adecuación de un laboratorio hacia una acreditación, crea caminos y tareas claras hacia una meta, así, cada actividad que se quiera realizar para el mejoramiento del mismo, tendrá un objetivo presente establecido y se facilitara los mecanismos de medición para verificar su cumplimiento.

- La importancia del amplio análisis que se realizó para generar una propuesta de mejoramiento específica para el laboratorio forense del CTI de la Fiscalía radica en la magnitud del proceso que envuelve esta actividad, pues no se limita a realizar el peritaje forense y generar un resultado a un usuario, sino que hace parte de un proceso judicial cuyo desarrollo no tiene un punto de cierre establecido, y que en muchas ocasiones debe ser sometido a re-alimentación (retroalimentación).

- La interdisciplinariedad es un factor fundamental para lograr buenos resultados en un proceso de mejoramiento, pues permite analizar todos los factores de interés desde un panorama más amplio e incluyente desde el ámbito de diferentes profesiones que conocen y ejercen en la materia.

- Es necesario prestar mayor atención a la red del CTI Pasto tanto en los aspectos técnicos, como en la manipulación de los elementos de la misma, teniendo en cuenta que esta es vulnerable a factores externos e internos. La red de la institución es una pieza clave para el correcto funcionamiento del que hacer misional, y las fallas que presenta recurrentemente, son consecuencia del poco interés en capacitación sobre su manejo que recibe por parte de las directivas y el personal.

- El analista de sistemas de la Fiscalía General de la Nación no da abasto con los requerimientos de todas las sedes de la institución (CTI principal y sedes, Administrativa y Fiscalías), por lo cual la red del CTI Pasto no recibe atención oportuna ante las posibles anomalías que se presentan, ni recibe el mantenimiento necesario para evitar que algunas de ellas ocurran.

RECOMENDACIONES

- Implementar la guía que en este trabajo se propone, permitiendo al laboratorio de delitos informáticos del CTI, aspirar a conseguir una acreditación NTC-ISO/IEC 17025, que respalde los procesos judiciales que impliquen dicha clase de delitos y de igual manera fortalezcan la parte penal que gira en torno a estos.

- Encaminarse hacia la acreditación del laboratorio de delitos informáticos, convertiría a la Fiscalía en la primera y única Entidad en Colombia en contar con dicha acreditación, mostrando el interés de las autoridades por mejorar sus procesos y brindarles mayor seguridad y efectividad

- Contar con un laboratorio de delitos informáticos acreditado en Colombia se convertiría en una gran fortaleza en la lucha en contra el crimen y un paso trascendental para enfrentar a los delincuentes informáticos.

- Fortalecer el área de delitos informáticos no solo mejora la calidad de los procesos que impliquen dicho tipo de delitos, sino también el de cualquier caso en que el E.M.P. se soporte en una evidencia digital.

- De la mano con el proyecto de reestructuración institucional de la Fiscalía General de la Nación, perfilar de manera coherente el trabajo a desarrollar por cada uno de los funcionarios de la Entidad, de modo que exista una relación directa entre la especialidad académica de cada servidor, así como su nivel de formación, frente a las funciones y responsabilidad asignadas a cada uno de ellos. Esto generaría beneficios mutuos, tanto para los trabajadores como para la Entidad, generando escenarios en los cuales se aprovechen las verdaderas capacidades y competencias de cada persona.

- Establecer una metodología acorde a la disposición de los funcionarios de la entidad para facilitar la selección y distribución de los perfiles previamente definidos, haciendo eficiente el uso de los talentos, capacidades y formación de dichos trabajadores.

- Socializar la propuesta contenida en este proyecto, a nivel nacional, permitiendo una retroalimentación constructiva, que involucre a todas las partes

interesadas y que facilite la divulgación, conocimiento y estandarización de lo acordado.

- Implementar mejoras a la estructura de red del CTI Pasto de manera que cumpla con los estándares internacionales de cableado estructurado ANSI/EIA/TIA, para que se facilite la atención a las complicaciones de la red y se disminuya el riesgo de fallas consecuentes a la mala distribución y referenciación que presenta actualmente

- Asignar un funcionario vinculado al CTI de la Fiscalía en la ciudad de Pasto, que se encuentre capacitado, para que tenga dedicación exclusiva a atender las necesidades de la red eléctrica y de datos. Este cumplirá como veedor de las contrataciones que se desarrollen para el mejoramiento de la red, atenderá de manera inmediata las fallas que se presenten y gestionara la inversión por parte de la institución en desarrollo tecnológico; entre otras funciones que se le puedan presentar más adelante.

BIBLIOGRAFÌA

- ✓ ASCLD/LAB INTERNATIONAL. ASCLD/LAB Guidance on Measurement Traceability – Measurement Assurance. Mayo de 2013.
- ✓ ASCLD/LAB INTERNATIONAL. ASCLD/LAB Policy on Measurement Traceability. Mayo de 2013.
- ✓ CHANG LASCANO Cindy Melina, CORTEZ DIAZ Aracely del Rocío. Diseño de un nuevo esquema para el procedimiento de indagación de los delitos informáticos. Universidad Politécnica Salesiana. Guayaquil, Ecuador. 2012.
- ✓ FISCALIA GENERAL DE LA NACION. La Reforma: Boletín Informativo del proyecto de modernización Institucional de la Fiscalía. Fiscalía General de la Nación. Edición 1. Mayo del 2013.
- ✓ FLOREZ PADILLA Mario Andrés, RAMIREZ MELO Edgar Camilo. Caracterización de tráfico en la migración de la red de voz sobre IP en la Universidad de Nariño. Universidad de Nariño. 2014.
- ✓ GARZA GONZALES Mario. Modelos de indicadores de calidad. Editorial Yla wmbo. Marzo de 2011.
- ✓ ICONTEC. Norma Técnica Colombiana NTC ISO/IEC 17025. Requisitos generales para la competencia de los laboratorios de ensayo y calibración. Octubre del 2005.
- ✓ ISO. ISO/IEC 27037: Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. Primera Edición. Suiza. 2012.
- ✓ M. GOMEZ Leopoldo Sebastián. Triage in-Lab: case backlog reduction with forensic digital profiling. Junio del 2012.
- ✓ MINISTERIO DE MINAS Y ENERGIA. Reglamento técnico de Instalaciones Eléctricas RETIE. Resolución No. 9-0708. Agosto de 2013.
- ✓ SIERRA RODRIGUEZ Antonio. Instalación de un sistema VoIP corporativo basado en Asterisk. Escuela técnica superior de ingeniería de telecomunicación universidad politécnica de Cartagena. Septiembre de 2008.

NETGRAFÍA

- ✓ CENTRO CIBERNÉTICO POLICIAL. Evidencia Digital. Recuperado el 15 de enero de 2014, de: http://www.ccp.gov.co/articulo-imagen.php?id=141
- ✓ COMISARÍA GENERAL DE POLICÍA CIENTÍFICA. Recuperado el 29 de enero de 2014, de: http://www5.poderjudicial.es/CVdi/TEMA02-ES.pdf
- ✓ DEFENSORIA DEL PUEBLO. Código de Procedimiento Penal. Recuperado el 15 de enero de 2014, de: http://www.defensoria.org.co/red/anexos/publicaciones/cod_prospenal.pdf
- ✓ FISCALÍA GENERAL DE LA NACIÓN. Reglamento Interno para el manejo del Elemento Material Probatorio (E.M.P). Recuperado el 02 de mayo de 2013, de: Fiscalnet.
- ✓ GANDINI Isabella y otros. Ley de Delitos Informáticos en Colombia. Recuperado el 29 de Enero de 2014, de: http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

ANEXOS

FISCALIA GENERAL DE LA NACION	SUBPROCESO INFORMÁTICA Y TELEMÁTICA	Código: FGN-12000-F-18
	FORMATO HOJA VIDA COMPUTADORES Y RECIBIDO	Versión: 04
		Pagina ___ de ___

FECHA : _____

IDENTIFICACION CPU				
No. HOJA VIDA	MARCA	TIPO	MODELO	SERIAL
NOMBRE DEL EQUIPO		DIRECCION MAC		PLACA

CARACTERISTICAS TÉCNICAS				
ELEMENTOS	MARCA	TIPO	CANTIDAD	VELOCIDAD/CAPACIDAD
PROCESADOR				
MEMORIA RAM				
DISCO DURO INTERNO				
TARJETA DE VIDEO				
TARJETA DE RED				
TARJETA PARALELA				
OTRAS TARJETAS				
OBSERVACIONES				

PERIFERICOS				
COMPONENTES COMPUTADOR	MARCA	MODELO	SERIAL	PLACA
MONITOR				
TECLADO				
MOUSE				
PARLANTES				

RESPONSABLE DEL ACTIVO				
TIPO RESPONSABLE ACTIVO	NOMBRES Y APELLIDOS	CEDULA	FECHA ASIGNACION (DD/MM/AAAA)	TELEFONO

FUNCION PRINCIPAL	UBICACIÓN			
SECCIONAL	MUNICIPIO	AREA	DEPENDENCIA	DIRECCION FISICA

NUMERO CONTRATO	FECHA CONTRATO (DD/MM/AAAA)	CONTRATISTA/TELEFONO	INICIO GARANTIA (DD/MM/AAAA)	FIN GARANTIA (DD/MM/AAAA)

SOFTWARE INSTALADO						
NOMBRE SOFTWARE	VERSION	LICENCIA No.	ORIGEN LICENCIA	FABRICANTE	FECHA INSTALACION (DD/MM/AAAA)	REFERENCIA INVENTARIO LICENCIA

MANTENIMIENTOS								
FECHA			SOFTWARE	HARDWARE	PREV.	CORR.	PROCEDIMIENTO EFECTUADO	REALIZADO POR
DD	MM	AAAA						

EL usuario es responsable de la custodia del equipo y la confidencialidad de la información oficial contenida en los recursos informáticos que le han sido asignados por la Entidad

!IMPORTANTE! Recuerde que la clave es personal e intrasferible

Verificó que el equipo esta operando bien y tiene todos las aplicaciones y software requerido

INSTRUCCIONES PARA EL DILIGENCIAMIENTO DEL FORMATO

IDENTIFICACIÓN CPU: Detalles de la hoja de vida del computador y el contrato con el cual llego el computador a la FGN

No. HOJA DE VIDA. Numero consecutivo asignado por el administrador del inventario.

MARCA. Marca del equipo (Hp, Dell, Compaq, etc.).
TIPO. Campo para ingresar si el computador es de escritorio o portátil.

MODELO. Modelo del equipo (Evo, Optiplex, etc.). MODELO. Modelo del equipo (Evo, Optiplex, etc.).
SERIAL. Campo para ingresar el número de serie del equipo.
NOMBRE DEL EQUIPO. Campo para ingresar el nombre del equipo en la red.
DIRECCION MAC. Campo para ingresar la dirección física del equipo.
PLACA. Corresponde al código de barras o numero asignado por inventarios.

CARACTERISTICAS TECNICAS: Elementos del hardware que forman parte del equipo: PROCESADOR, MEMORIA RAM, DISCO DURO INTERNO, UNIDAD CD, UNIDAD DVD, TARJETAS (RED, SONIDO,

RESPONSABLE : Datos del usuario responsable del uso del computador

NOMBRES Y APELLIDOS. Corresponde a los nombres y apellidos del responsable del activo.

CEDULA. Número de la cedula de ciudadanía del responsable del activo.

TELEFONO/CORREO. Número telefónico o dirrección del correo del responsable del activo.

UBICACIÓN:

SECCIONAL. Nombre de la Seccional o área donde se encuentra el activo.
MUNICIPIO. Nombre del municipio donde se encuentra el activo.
AREA. Nombre del área donde se encuentra el activo.
DEPENDENCIA. Nombre de la Dependencia donde se encuentra el activo.
DIRECCION FISICA. Dirección de la sede donde se encuentra el activo.

No. CONTRATO. Campo para ingresar el número de contrato al que pertenece el equipo.

FECHA CONTRATO. Campo para ingresar la fecha del contrato en formato (DD/MM/AAAA).

CONTRATISTA/TELEFONO. Nombre y número de telefónico del proveedor del equipo.

INICIO GARANTIA. Fecha cuando inicia la garantía del equipo en formato (DD/MM/AAAA).

FIN GARANTIA. Fecha de finalización de la garantía del equipo en formato (DD/MM/AAAA).

SOFTWARE INSTALADO

NOMBRE SOFTWARE. Nombre del software instalado.
VERSION. Versión actual del software.
LICENCIA No. Numero de licencia del software instalado.
ORIGEN LICENCIA. El origen de la licencia pude ser comercial, libre o gratuita.
FABRICANTE. Nombre del fabricante del software.
FECHA INSTALACION. Fecha cuando se instala el software en formato (DD/MM/AAAA).

MANTENIMIENTOS: Corresponde a los datos de los mantenimientos preventivos y/o correctivos realizados al activo y contiene los siguientes datos:

FECHA. Campo en el cual se deberá diligenciar la fecha en que se efectúa el mantenimiento de Hardware o de Software en formato (DD/MM/AAAA).

SOFTWARE. Casilla para colocar una X en caso de que el mantenimiento haya sido al software. Va relacionada con la casilla PREV o CORR, dependiendo de si dicho mantenimiento es Preventivo o Correctivo.

HARDWARE. Casilla para colocar una X en caso de que el mantenimiento haya sido al hardware. Va relacionada con la casilla PREV o CORR, dependiendo de si dicho mantenimiento es Preventivo o Correctivo.

PREV. PREVENTIVO. Casilla para colocar una X en caso de que el mantenimiento haya sido Preventivo.

CORRE. CORRECTIVO. Casilla para colocar una X en caso de que el mantenimiento haya sido Correctivo.
reinstalar controlador, se informó al funcionario encargado de redes, etc.

REALIZADO POR. Nombre de la persona que efectúa el mantenimiento.

FISCALIA GENERAL DE LA NACION	SUBPROCESO INFORMÁTICA Y TELEMÁTICA	Código: FGN-12000-F-18
	FORMATO HOJA VIDA COMPUTADORES Y RECIBIDO	Versión: 04 Pagina ___ de ___

FECHA : _____

IDENTIFICACION CPU				
No. HOJA VIDA	MARCA	TIPO	MODELO	SERIAL
LAB-DELINFO-01	Forensic Computers		Forensic Tower III	FT-III-0109-0077
NOMBRE DEL EQUIPO		DIRECCION MAC		PLACA
ESTACION FORENSE I				SIN

CARACTERISTICAS TÉCNICAS				
ELEMENTOS	MARCA	TIPO	CANTIDAD	VELOCIDAD/CAPACIDAD
PROCESADOR	INTEL	XEON E5335	1	2,00 GHZ
MEMORIA RAM	4 GB			
DISCO DURO INTERNO	D0: 139,73 GB, D1:931,51 GB, D2: 931,51 GB, D3: 931,51 GB			
TARJETA DE VIDEO	NVIDIDIA	GEFORCE 9400 GT	1	
TARJETA DE RED	INCLUIDA			
TARJETA PARALELA	INCLUIDA			
OTRAS TARJETAS	INCLUIDA			
OBSERVACIONES				

PERIFERICOS				
COMPONENTES COMPUTADOR	MARCA	MODELO	SERIAL	PLACA
MONITOR	DELL		CN-0F532H-71618-88°-100S	SIN
TECLADO	ASKA		20070708071	SIN
MOUSE	Alltec		50004154	SIN
PARLANTES	DELL		CN-0C730C-71623-886-6877	SIN

RESPONSABLE DEL ACTIVO				
TIPO RESPONSABLE ACTIVO	NOMBRES Y APELLIDOS	CEDULA	FECHA ASIGNACION (DD/MM/AAAA)	TELEFONO

FUNCION PRINCIPAL	UBICACIÓN			
SECCIONAL	MUNICIPIO	AREA	DEPENDENCIA	DIRECCION FISICA
PASTO	PASTO	SECCION INVESTI.	DELITOS INFORMATICOS	CLLA 19 N. 21-10 QUINTO PISO

NUMERO CONTRATO	FECHA CONTRATO (DD/MM/AAAA)	CONTRATISTA/TELEFONO	INICIO GARANTIA (DD/MM/AAAA)	FIN GARANTIA (DD/MM/AAAA)

SOFTWARE INSTALADO						
NOMBRE SOFTWARE	VERSION	LICENCIA No.	ORIGEN LICENCIA	FABRICANTE	FECHA INSTALACION (DD/MM/AAAA)	REFERENCIA INVENTARIO LICENCIA
WINDOWS XP	2003 SP 2			MICROSOFT		
ENCASE	6.19.4	C1002042514		GUIDANCE SOFTWARE		
ENCASE	6.19.6	C1002042515		GUIDANCE SOFTWARE		
ENCASE	6.19.7	C1002042516		GUIDANCE SOFTWARE		
ENCASE	7.04	C1002042517		GUIDANCE SOFTWARE		
ENCASE	7.05	C1002042518		GUIDANCE SOFTWARE		
ENCASE	7.05.02	C1002042519		GUIDANCE SOFTWARE	06/04/2013	
QUICK VIEW PLUS	10.1.0			AVANTSTAR		
FTK IMAGER	3.1.1.8			ACCESDATA		

MANTENIMIENTOS								
FECHA			SOFTWARE	HARDWARE	PREV.	CORR.	PROCEDIMIENTO EFECTUADO	REALIZADO POR
DD	MM	AAAA						

EL usuario es responsable de la custodia del equipo y la confidencialidad de la información oficial contenida en los recursos informáticos que le han sido asignados por la Entidad

!IMPORTANTE! Recuerde que la clave es personal e intrasferible

Verificó que el equipo esta operando bien y tiene todos las aplicaciones y software requerido

FIRMA RESPONSABLE DEL EQUIPO: _____ _____

NUMERO CEDULA: _____

NOMBRES Y APELLIDOS TECNICO: _____

FISCALIA GENERAL DE LA NACION	SUBPROCESO INFORMÁTICA Y TELEMÁTICA	Código: FGN-12000-F-18
	FORMATO HOJA VIDA COMPUTADORES Y RECIBIDO	Versión: 04
		Pagina ___ de ___

FECHA : _____

IDENTIFICACION CPU				
No. HOJA VIDA	MARCA	TIPO	MODELO	SERIAL
LAB-DELINFO-02	Digital Intelligence		FRED	F008B030978
NOMBRE DEL EQUIPO		DIRECCION MAC		PLACA
ESTACION FORENSE II				SIN

CARACTERISTICAS TÉCNICAS				
ELEMENTOS	MARCA	TIPO	CANTIDAD	VELOCIDAD/CAPACIDAD
PROCESADOR	INTEL	CORE 2 QUAD	1	2,40 GHZ
MEMORIA RAM	8 GB			
DISCO DURO INTERNO	D0:931,51 GB, D1:465,76 GB, D2: 931,51 GB.			
TARJETA DE VIDEO	NVIDIDIA	GEFORCE 9600 GT	1	
TARJETA DE RED	MARVELL	YUJKON 88E8656PCI-E	1	
TARJETA PARALELA	INCLUIDA			
OTRAS TARJETAS	INCLUIDA			
OBSERVACIONES				

PERIFERICOS				
COMPONENTES COMPUTADOR	MARCA	MODELO	SERIAL	PLACA
MONITOR	Viewsonic		QCC083880948	SIN
TECLADO	Microsoft		P/N: 9231710278294	SIN
MOUSE	Microsoft		P/N: X814719-003	SIN
PARLANTES	SIN		SIN	SIN

RESPONSABLE DEL ACTIVO				
TIPO RESPONSABLE ACTIVO	NOMBRES Y APELLIDOS	CEDULA	FECHA ASIGNACION (DD/MM/AAAA)	TELEFONO
DELITOS INFORMATICOS	PABLO ANDRES GAVIRIA	5,204,498	05/04/2013	7215532

FUNCION PRINCIPAL	UBICACIÓN			
SECCIONAL	MUNICIPIO	AREA	DEPENDENCIA	DIRECCION FISICA
PASTO	PASTO	SECCION INVESTI.	DELITOS INFORMATICOS	CLLA 19 N. 21-10 QUINTO PISO

NUMERO CONTRATO	FECHA CONTRATO (DD/MM/AAAA)	CONTRATISTA/TELEFONO	INICIO GARANTIA (DD/MM/AAAA)	FIN GARANTIA (DD/MM/AAAA)

SOFTWARE INSTALADO						
NOMBRE SOFTWARE	VERSION	LICENCIA No.	ORIGEN LICENCIA	FABRICANTE	FECHA INSTALACION (DD/MM/AAAA)	REFERENCIA INVENTARIO LICENCIA
WINDOWS 7	2003 SP 2			MICROSOFT		
ENCASE	6.19.4	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	6.19.6	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	6.19.7	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	7.04	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	7.05	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	7.05.02	C1002042514.		GUIDANCE SOFTWARE	06/04/2013	
QUICK VIEW PLUS	10.1.0			AVANTSTAR		
FTK IMAGER	3.1.1.8			ACCESDATA		

MANTENIMIENTOS								
FECHA			SOFTWARE	HARDWARE	PREV.	CORR.	PROCEDIMIENTO EFECTUADO	REALIZADO POR
DD	MM	AAAA						

EL usuario es responsable de la custodia del equipo y la confidencialidad de la información oficial contenida en los recursos informáticos que le han sido asignados por la Entidad

!IMPORTANTE! Recuerde que la clave es personal e intrasferible

Verificó que el equipo esta operando bien y tiene todos las aplicaciones y software requerido

FIRMA RESPONSABLE DEL EQUIPO: _____

NUMERO CEDULA: _____

NOMBRES Y APELLIDOS TECNICO:

FISCALIA GENERAL DE LA NACION	SUBPROCESO INFORMÁTICA Y TELEMÁTICA	Código: FGN-12000-F-18
	FORMATO HOJA VIDA COMPUTADORES Y RECIBIDO	Versión: 04 Pagina ___ de ___

FECHA : _____

IDENTIFICACION CPU				
No. HOJA VIDA	MARCA	TIPO	MODELO	SERIAL
LAB-DELINFO-03	Digital Intelligence		FREDDIE	E012C0357790
NOMBRE DEL EQUIPO		DIRECCION MAC		PLACA
ESTACION FORENSE III				SIN

CARACTERISTICAS TÉCNICAS				
ELEMENTOS	MARCA	TIPO	CANTIDAD	VELOCIDAD/CAPACIDAD
PROCESADOR	INTEL	CORE I7-3960X	1	3,3 GHZ
MEMORIA RAM	64 GB	DDR3-1600		
DISCO DURO INTERNO	D0:931,51 GB, D1:465,76 GB, D2: 931,51 GB.			
TARJETA DE VIDEO	NVIDIA	GT 630 4GB	1	
TARJETA DE RED		DUAL 10/100/1000 MBS	1	
TARJETA PARALELA	INCLUIDA			
OTRAS TARJETAS	ULTRABAY3	HARDWARE WRITE BLOCKER	1	
OBSERVACIONES				

PERIFERICOS				
COMPONENTES COMPUTADOR	MARCA	MODELO	SERIAL	PLACA
MONITOR	INTEGRADO		SIN	SIN
TECLADO	INTEGRADO		SIN	SIN
MOUSE	INTEGRADO		SIN	SIN
PARLANTES	INTEGRADO		SIN	SIN

RESPONSABLE DEL ACTIVO				
TIPO RESPONSABLE ACTIVO	NOMBRES Y APELLIDOS	CEDULA	FECHA ASIGNACION (DD/MM/AAAA)	TELEFONO
DELITOS INFORMATICOS	PABLO ANDRES GAVIRIA	5,204,498	17/05/2013	7215532

FUNCION PRINCIPAL	UBICACIÓN			
SECCIONAL	MUNICIPIO	AREA	DEPENDENCIA	DIRECCION FISICA
PASTO	PASTO	SECCION INVESTI.	DELITOS INFORMATICOS	CLLA 19 N. 21-10 QUINTO PISO

NUMERO CONTRATO	FECHA CONTRATO (DD/MM/AAAA)	CONTRATISTA/TELEFONO	INICIO GARANTIA (DD/MM/AAAA)	FIN GARANTIA (DD/MM/AAAA)

SOFTWARE INSTALADO						
NOMBRE SOFTWARE	VERSION	LICENCIA No.	ORIGEN LICENCIA	FABRICANTE	FECHA INSTALACION (DD/MM/AAAA)	REFERENCIA INVENTARIO LICENCIA
WINDOWS 7, WI 98 SE	2003 SP 2			MICROSOFT		
ENCASE	6.19.4	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	6.19.6	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	6.19.7	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	7.04	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	7.05	C1002042514.		GUIDANCE SOFTWARE		
ENCASE	7.05.02	C1002042514.		GUIDANCE SOFTWARE		
QUICK VIEW PLUS	10.1.0			AVANTSTAR		
FTK IMAGER	3.1.1.8			ACCESDATA		
FTK IMAGER	3,3			ACCESDATA		

MANTENIMIENTOS								
FECHA			SOFTWARE	HARDWARE	PREV.	CORR.	PROCEDIMIENTO EFECTUADO	REALIZADO POR
DD	MM	AAAA						

EL usuario es responsable de la custodia del equipo y la confidencialidad de la información oficial contenida en los recursos informáticos que le han sido asignados por la Entidad

!IMPORTANTE! Recuerde que la clave es personal e intrasferible

Verificó que el equipo esta operando bien y tiene todos las aplicaciones y software requerido

FIRMA RESPONSABLE DEL EQUIPO: _____ _____

NUMERO CEDULA: _____

NOMBRES Y APELLIDOS TECNICO:

FISCALIA GENERAL DE LA NACION	SUBPROCESO INFORMÁTICA Y TELEMÁTICA	Código: FGN-12000-F-18
	FORMATO HOJA VIDA COMPUTADORES Y RECIBIDO	Versión: 04 Pagina ___ de ___

FECHA : _____

IDENTIFICACION CPU				
No. HOJA VIDA	MARCA	TIPO	MODELO	SERIAL
LAB-DELINFO-06	CelleBrite		UFED PHYSICAL PRO	5528040
NOMBRE DEL EQUIPO		DIRECCION MAC		PLACA
UFED		00:16:00:00:6D:88		SIN

CARACTERISTICAS TÉCNICAS				
ELEMENTOS	MARCA	TIPO	CANTIDAD	VELOCIDAD/CAPACIDAD
PROCESADOR				
MEMORIA RAM				
DISCO DURO INTERNO				
TARJETA DE VIDEO				
TARJETA DE RED				
TARJETA PARALELA				
OTRAS TARJETAS				
OBSERVACIONES				

PERIFERICOS				
COMPONENTES COMPUTADOR	MARCA	MODELO	SERIAL	PLACA
MONITOR	INTEGRADO		SIN	SIN
TECLADO	INTEGRADO		SIN	SIN
MOUSE	INTEGRADO		SIN	SIN
PARLANTES	INTEGRADO		SIN	SIN

RESPONSABLE DEL ACTIVO				
TIPO RESPONSABLE ACTIVO	NOMBRES Y APELLIDOS	CEDULA	FECHA ASIGNACION (DD/MM/AAAA)	TELEFONO
DELITOS INFORMATICOS	PABLO ANDRES GAVIRIA	5,204,498	17/05/2013	7215532

FUNCION PRINCIPAL	UBICACIÓN			
SECCIONAL	MUNICIPIO	AREA	DEPENDENCIA	DIRECCION FISICA
PASTO	PASTO	SECCION INVESTI.	DELITOS INFORMATICOS	CLLA 19 N. 21-10 QUINTO PISO

NUMERO CONTRATO	FECHA CONTRATO (DD/MM/AAAA)	CONTRATISTA/TELEFONO	INICIO GARANTIA (DD/MM/AAAA)	FIN GARANTIA (DD/MM/AAAA)

SOFTWARE INSTALADO						
NOMBRE SOFTWARE	VERSION	LICENCIA No.	ORIGEN LICENCIA	FABRICANTE	FECHA INSTALACION (DD/MM/AAAA)	REFERENCIA INVENTARIO LICENCIA
UFED	1.9.00	1670612200		CELLEBRITE		

MANTENIMIENTOS								
FECHA			SOFTWARE	HARDWARE	PREV.	CORR.	PROCEDIMIENTO EFECTUADO	REALIZADO POR
DD	MM	AAAA						

EL usuario es responsable de la custodia del equipo y la confidencialidad de la información oficial contenida en los recursos informáticos que le han sido asignados por la Entidad

!IMPORTANTE! Recuerde que la clave es personal e intrasferible

Verificó que el equipo esta operando bien y tiene todos las aplicaciones y software requerido

FIRMA RESPONSABLE DEL EQUIPO: _____

NUMERO CEDULA: _____

NOMBRES Y APELLIDOS TECNICO: _____

FISCALIA GENERAL DE LA NACION	SUBPROCESO INFORMÁTICA Y TELEMÁTICA	Código: FGN-12000-F-18
	FORMATO HOJA VIDA COMPUTADORES Y RECIBIDO	Versión: 04
		Pagina ___ de ___

FECHA : _____

IDENTIFICACION CPU				
No. HOJA VIDA	MARCA	TIPO	MODELO	SERIAL
LAB-DELINFO-05	HEWLETT PACKARD	LAPTOP	PROBOOK 4420S	CNF0508W3G
NOMBRE DEL EQUIPO		DIRECCION MAC		PLACA
ESTACION FORENSE PC UFED				SIN

CARACTERISTICAS TÉCNICAS				
ELEMENTOS	MARCA	TIPO	CANTIDAD	VELOCIDAD/CAPACIDAD
PROCESADOR	INTEL	CORE I5-M460	1	2,53 GHZ
MEMORIA RAM	4 GB	DDR3	2	
DISCO DURO INTERNO	D0: 465,76 G.B.			
TARJETA DE VIDEO	INTEGRADA			
TARJETA DE RED	INTEGRADA		1	
TARJETA PARALELA	INTEGRADA			
OTRAS TARJETAS				
OBSERVACIONES				

PERIFERICOS				
COMPONENTES COMPUTADOR	MARCA	MODELO	SERIAL	PLACA
MONITOR	INTEGRADO		SIN	SIN
TECLADO	INTEGRADO		SIN	SIN
MOUSE	INTEGRADO		SIN	SIN
PARLANTES	INTEGRADO		SIN	SIN

RESPONSABLE DEL ACTIVO				
TIPO RESPONSABLE ACTIVO	NOMBRES Y APELLIDOS	CEDULA	FECHA ASIGNACION (DD/MM/AAAA)	TELEFONO
DELITOS INFORMATICOS	PABLO ANDRES GAVIRIA	5,204,498	17/05/2013	7215532

FUNCION PRINCIPAL	UBICACIÓN			
SECCIONAL	MUNICIPIO	AREA	DEPENDENCIA	DIRECCION FISICA
PASTO	PASTO	SECCION INVESTI.	DELITOS INFORMATICOS	CLLA 19 N. 21-10 QUINTO PISO

NUMERO CONTRATO	FECHA CONTRATO (DD/MM/AAAA)	CONTRATISTA/TELEFONO	INICIO GARANTIA (DD/MM/AAAA)	FIN GARANTIA (DD/MM/AAAA)

SOFTWARE INSTALADO						
NOMBRE SOFTWARE	VERSION	LICENCIA No.	ORIGEN LICENCIA	FABRICANTE	FECHA INSTALACION (DD/MM/AAAA)	REFERENCIA INVENTARIO LICENCIA
WINDOWS 7	2003 SP 2			MICROSOFT		

MANTENIMIENTOS								
FECHA			SOFTWARE	HARDWARE	PREV.	CORR.	PROCEDIMIENTO EFECTUADO	REALIZADO POR
DD	MM	AAAA						
30	5	2013	windows 7				MANTENIMIENTO PREVENTIVO	PABLO A. GAVIRIA

EL usuario es responsable de la custodia del equipo y la confidencialidad de la información oficial contenida en los recursos informáticos que le han sido asignados por la Entidad

!IMPORTANTE! Recuerde que la clave es personal e intrasferible

Verificó que el equipo esta operando bien y tiene todos las aplicaciones y software requerido

FIRMA RESPONSABLE DEL EQUIPO: _____

NUMERO CEDULA: _____

NOMBRES Y APELLIDOS TECNICO: _____