



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Industrial

**CONSIDERACIONES TÉCNICAS PARA LA CREACIÓN E
IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE**

Roberto García López

Asesorado por el Ing. Hugo Humberto Rivera Pérez

Guatemala, septiembre de 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**CONSIDERACIONES TÉCNICAS PARA LA CREACIÓN E
IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

ROBERTO GARCÍA LÓPEZ

ASESORADO POR EL ING. HUGO HUMBERTO RIVERA PÉREZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO INDUSTRIAL

GUATEMALA, SEPTIEMBRE DE 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. César Ernesto Urquizú Rodas
EXAMINADOR	Ing. William Abel Aguilar Vásquez
EXAMINADOR	Ing. Víctor Hugo García Roque
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

CONSIDERACIONES TÉCNICAS PARA LA CREACIÓN E IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Industrial, con fecha octubre de 2008.



Roberto García López

Guatemala 25 de abril del 2011

Ingeniero

César Ernesto Urquizú Rodas

Director de Escuela, Ingeniería Mecánica Industrial

Universidad de San Carlos de Guatemala

Facultad de Ingeniería

Presente

Ingeniero Urquizú:

Cordialmente me dirijo a usted con el propósito de informarle que he asesorado y revisado el trabajo de graduación titulado "CONSIDERACIONES TÉCNICAS PARA LA CREACIÓN E IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE" elaborado por el estudiante Roberto García López.

Habiendo determinado que el presente, cumple con los lineamientos establecidos por la Facultad de Ingeniería y que el mismo es de utilidad, doy mi respectiva autorización, por lo que ruego a usted se sirva dar el visto bueno para que éste sea presentado ante las máximas autoridades de la Facultad de Ingeniería.

Sin otro particular, me suscribo de usted.

Atentamente,



Ing. Hugo Humberto Rivera Pérez

Asesor

Colegiado No. 7161

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERÍA

REF.REV.EMI.078.011

Como Catedrático Revisor del Trabajo de Graduación titulado **CONSIDERACIONES TÉCNICAS PARA LA CREACIÓN E IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE**, presentado por el estudiante universitario **Roberto García López**, apruebo el presente trabajo y recomiendo la autorización del mismo.

ID Y ENSEÑAD A TODOS

Victor Hugo Garcia Roque
INGENIERO INDUSTRIAL
Colegiado No. 5133

Ing. Victor Hugo Garcia Roque
Catedrático Revisor de Trabajos de Graduación
Escuela de Ingeniería Mecánica Industrial

Guatemala, mayo de 2011.

/mgp



REF.DIR.EMI.126.011

El Director de la Escuela de Ingeniería Mecánica Industrial de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el Visto Bueno del Revisor y la aprobación del Área de Lingüística del trabajo de graduación titulado **CONSIDERACIONES TÉCNICAS PARA LA CREACIÓN E IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE**, presentado por el estudiante universitario **Roberto García López**, aprueba el presente trabajo y solicita la autorización del mismo.

“ID Y ENSEÑAD A TODOS”


Ing. Cesar Ernesto Urquizú Rodas
DIRECTOR
Escuela de Ingeniería Mecánica Industrial



Guatemala, septiembre de 2011.

/mgp

Universidad de San Carlos
de Guatemala

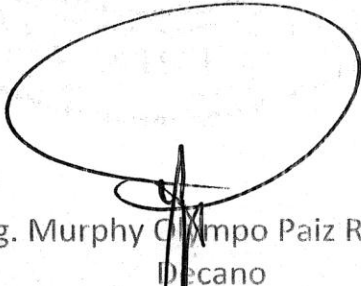


Facultad de Ingeniería
Decanato

DTG. 321.2011.

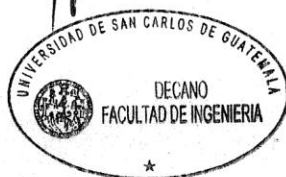
El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Industrial, al trabajo de graduación titulado: **CONSIDERACIONES TÉCNICAS PARA LA CREACIÓN E IMPLEMENTACIÓN DE UN LABORATORIO DE INFORMÁTICA FORENSE**, presentado por el estudiante universitario **Roberto García López**, autoriza la impresión del mismo.

IMPRÍMASE:


Ing. Murphy Olimpo Paiz Recinos
Decano

Guatemala, 2 de septiembre de 2011.

/gdech



ACTO QUE DEDICO A:

- Jesucristo** Mi abogado fiel, quien algún día, hará resplandecer la justicia como la luz del medio día.
- Mi esposa e hijas** Eleonora Escribá Mazariegos de García, por estar junto a mí, ser un soporte amoroso y motivacional. Además, gracias por realizar una revisión ortográfica del trabajo; Sara Marianne García Escribá y Ana Lucía García Escribá, hijitas preciosas, su apoyo y amor me han hecho reconocer que tengo un pedacito de cielo aquí en la Tierra.
- Mis padres** Salomón García Canizalez (q.e.p.d.) y Etelvina López Estrada. Gracias por el esfuerzo y sacrificios que realizaron por mí durante toda mi vida. Mamá, gracias por tu ejemplo y valentía.
- Mi abuelita** Vitalina Estrada Guevara (q.e.p.d.), por sus cuidados cuando fui niño.
- Mis suegros** Albin Ariel Escribá Vela (q.e.p.d.) y Margarita Mazariegos vda. de Escribá.
- Familia política** Alvin y Raquel Escribá López, Ángel y Alejandra Trinidad Escribá, Emilio y Melania Aguilar García, Rafael y Cristina Antillón, Roberto y Edith Turcios

Escribá, Lidia Marina Mazariegos, Iracema Mazariegos de Urizar, Rudy Mazariegos Enríquez, Julio Mazariegos Enríquez, Joaquín Enríquez (q.e.p.d.), Arturo Mazariegos, Juan José Celada Mazariegos, Rodrigo Celada Mazariegos, Melina Celada Mazariegos, Juan Carlos Turcios, Julio Roberto Turcios, Luz Vela vda. de Escribá. Por aceptarme como hijo, cuñado, sobrino, primo, nieto y tío.

Mis amigos

Gerardo Jerez, Melvin Fernández, Manuel Jiménez, Roberto Jiménez, Moisés Godínez, Eduardo Rivera, Edgar Figueroa, Rafael Patzán (q.e.p.d.), Carolina Godínez, Javier Cruz, Arturo Jiménez, Juan Fausto Girón, Carlos Carrera, Jaime Sevilla, Hugo Rivera y Anabella Córdova. La travesía de la vida ha sido mejor junto a ustedes – Hugo, sin tu ayuda y motivación no lo habría logrado -. Gracias.

Mi sobrino

César Adolfo García Morataya y familia, gracias por estar en los tiempos difíciles y por los consejos en la adolescencia.

A los señores

David y Miriam Hernández, Abraham y Zemira González, Pablito y Jean Sywulka, Julio y Enriqueta Godínez, Carlos y Karin Ramos, Víctor y Thelma Argueta, y Jorge y Lorena Galindo. Hermanos queridos, gracias por preocuparse por mi vida espiritual y la de mi familia.

Compañeros de trabajo Rony Galindo, Alfonso León, Eric García, Marcos García, Guillermo Álvarez, Giancarlo Tobar, Ruldin Ayala, Víctor Carranza, Danilo Ovalle y Luis Elías. Por todo lo que he aprendido de ustedes en todas las áreas.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	XI
LISTA DE SÍMBOLOS	XVII
GLOSARIO	XXI
RESUMEN	XLIII
OBJETIVOS.....	XLV
INTRODUCCIÓN	XLVII
1. INFORMACION PRELIMINAR	
1.1. Breve historia de la Informática Forense	1
1.1.1. La Informática Forense	3
1.2. El proceso de investigación forense	5
1.2.1. Identificación	6
1.2.2. Preservación	6
1.2.3. Recolección.....	6
1.2.4. Búsqueda y análisis	10
1.2.5. Presentación	11
1.2.6. Decisión	11
1.3. El Ministerio Público	12
1.3.1. Descripción, visión y misión, del Ministerio Público	12
1.3.2. Funciones del Ministerio Público, de acuerdo a la Constitución Política de la República y su Ley Orgánica	13
1.3.3. Organización	13
1.4. El Instituto Nacional de Ciencias Forenses (INACIF).....	14
1.4.1. Descripción general del INACIF	14

1.4.2.	Servicios ofrecidos.....	14
1.5.	La cadena de custodia	15
1.6.	Breve descripción de las áreas forenses	17
1.7.	Objetivos del laboratorio de Informática Forense	19
2.	PROCESOS REALIZADOS EN UN LABORATORIO DE INFORMÁTICA FORENSE	
2.1.	Normas y políticas a seguir para la realización de peritajes	21
2.2.	Descripción general de los procesos y procedimientos	26
2.2.1.	Diagramas de flujo	31
2.2.2.	Diagramas de proceso.....	32
2.3.	Descripción del proceso de solicitud del peritaje	57
2.3.1.	Sugerencias del embalaje.....	58
2.3.2.	Documentación obligatoria	58
2.4.	Documentación de los procesos.....	59
2.4.1.	Fotografías y videos	59
2.4.2.	Bitácora de actuaciones.....	59
2.4.3.	Sistema informático de seguimiento	60
2.5.	Elaboración de informes	60
2.5.1.	Asesoría legal	62
2.5.2.	Ratificación del peritaje informático ante tribunales	62
3.	INSTRUMENTOS, HERRAMIENTAS Y MATERIALES UTILIZADOS COMUNMENTE EN PERITAJES INFORMÁTICOS	
3.1.	Herramientas de mano	65
3.1.1.	Instrumentos de punta (llaves y destornilladores).....	66
3.1.2.	Instrumentos de palanca.....	67
3.1.3.	Instrumentos de corte y percusivos	68
3.2.	Instrumentos de medición.....	69

3.3.	Juego de lupas manuales y de montaje de pedestal	71
3.4.	Equipo de documentación	73
3.4.1.	Fotografías: cámara digital de alta resolución.....	73
3.4.2.	Videos: cámara de alta resolución y alto fps	73
3.5.	Convertidores	75
3.5.1.	Multiridrive (<i>SCSI, IDE, SATA, USB, FW, etc.</i>).....	76
3.5.2.	Lectores de tarjetas de memoria.....	77
3.5.3.	Sincronizadores (<i>celulares, palms, pocketPC, etc.</i>).....	78
3.5.4.	Cables y conectores.....	80
3.6.	Adaptadores de corriente/voltaje	81
3.7.	Dispositivos Lector/Escritor <i>CD/DVD/Blu-ray</i>	82
3.8.	<i>Software</i>	82
3.8.1.	Bloqueador de escrituras a disco (<i>write blockers</i>).....	83
3.8.2.	Herramientas de <i>Booting</i> o carga.....	84
3.8.2.1.	<i>OS CD</i>	85
3.8.2.2.	<i>OS USB</i>	85
3.8.3.	Herramientas de búsqueda y recuperación.....	85
3.8.3.1.	Texto – comparación/excepción.....	85
3.8.3.2.	Archivos escondidos	86
3.8.3.3.	Archivos eliminados	87
3.8.4.	Acceso a datos.....	88
3.8.4.1.	Recuperadores de contraseñas	88
3.8.4.2.	Descifradores (<i>Decrypters</i>).....	90
3.8.4.3.	Lector y analizador de celulares.....	90
3.8.5.	Creadores de imágenes y duplicación	93
3.8.6.	Editores hexadecimales	94
3.8.7.	Analizadores de datos.....	95
3.8.8.	Analizador de inventario de aplicaciones	95
3.9.	<i>Hardware</i>	96

3.9.1.	Bloqueador de escrituras a disco (<i>write blocker</i>)	96
3.9.2.	Duplicadores o clonadores de discos duros	97
3.9.3.	Dispositivos móviles de almacenamiento masivo	98
3.10.	Materiales	99
3.10.1.	Cintas adhesivas y aislantes.....	99
3.10.2.	Rotuladores	99
3.10.3.	Sujetadores y organizadores	100
3.10.4.	Pinza lagarto.....	101
3.10.5.	Lijas para metales.....	102
3.10.6.	Escobillas.....	102
3.11.	Costos aproximados	103
4.	MOBILIARIO Y EQUIPO	
4.1.	Estanterías, gabinetes y archivos.....	107
4.2.	Carretillas y equipos móviles.....	109
4.3.	Escritorios.....	110
4.4.	Equipo Informático de la estación de trabajo forense.....	112
4.4.1.	Requisitos mínimos de <i>hardware</i>	112
4.4.2.	Requisitos mínimos de <i>software</i>	115
4.4.3.	Costos aproximados	116
5.	DISEÑO DE LA ESTACION DE TRABAJO FORENSE	
5.1.	Diseño ergonómico del módulo	119
5.2.	Secciones de la estación de trabajo forense	130
5.3.	Iluminación.....	135
5.4.	Materiales y colores.....	136
5.5.	Tomacorrientes.....	137
5.6.	Conectores de red y telefonía.....	138
5.7.	Costo aproximado	139

6.	ASPECTOS IMPORTANTES A CONSIDERAR EN EL DISEÑO DEL LABORATORIO	
6.1.	Aspectos a considerar en el diseño del ambiente físico	142
6.1.1.	Requerimientos generales de la planta	142
6.1.1.1.	Puertas	142
6.1.1.2.	Ventanas	144
6.1.1.3.	Pasillos	146
6.1.1.4.	Entradas/salidas	146
6.1.1.5.	Comedor	146
6.1.1.6.	Sala de espera	147
6.1.1.7.	Administración	147
6.1.1.8.	Cuarto de evidencias	148
6.1.1.9.	Sala de reuniones/capacitación	149
6.1.1.10.	Clínica	149
6.1.1.11.	Área de servidores/Informática	150
6.1.1.12.	Bibliotecas	151
	6.1.1.12.1. Material de consulta y referencia	152
	6.1.1.12.2. Biblioteca de <i>software</i>	152
	6.1.1.12.2.1. Aseguramiento de licencias	152
	6.1.1.12.3. <i>Internet</i>	153
6.1.1.13.	Baños	153
6.1.1.14.	<i>Lockers</i>	154
6.1.2.	Seguridad	154
6.1.2.1.	Accesos restringidos	155
	6.1.2.1.1. Tarjetas de aproximación	156
	6.1.2.1.2. Biométricos	156
6.1.2.2.	Circuito cerrado de televisión – <i>CCTV</i>	157

6.1.2.3.	Detectores de metal.....	158
6.1.2.4.	<i>Staff</i> de seguridad.....	158
6.1.3.	Accesibilidad.....	160
6.1.3.1.	Entradas y salidas parqueos.....	160
6.1.3.2.	Entradas y salidas peatonales.....	162
6.1.4.	Acondicionamiento.....	162
6.1.4.1.	Energía eléctrica.....	162
6.1.4.1.1.	Drenaje a tierra.....	163
6.1.4.1.2.	Pararrayos.....	163
6.1.4.1.3.	Fuentes in-interrumpibles de energía.....	163
6.1.4.1.4.	Cajas de protección.....	164
6.1.4.2.	Iluminación por áreas.....	165
6.1.4.2.1.	Tipos de lámparas.....	167
6.1.4.2.2.	<i>Dimmers</i>	169
6.1.4.2.3.	Iluminación de emergencia.....	169
6.1.4.3.	Pisos, paredes y techos.....	170
6.1.4.3.1.	Materiales.....	173
6.1.4.3.2.	Pinturas.....	174
6.1.4.3.3.	Colores.....	175
6.1.4.4.	Aire acondicionado.....	175
6.1.4.5.	Sistemas de protección.....	177
6.1.4.5.1.	Alarmas y sensores.....	177
6.1.4.5.2.	Salidas de emergencia.....	177
6.1.4.5.3.	Extintores.....	178
6.2.	Nomenclatura de colores de las instalaciones.....	181
6.3.	Planta telefónica.....	182
6.4.	Plano de distribución de planta sugerido.....	184

7.	MANTENIMIENTO	
7.1.	Mantenimiento del laboratorio.....	188
7.1.1.	Programación de mantenimiento	188
7.1.1.1.	Estructura del edificio	189
7.1.1.2.	Instrumentos equipos y herramientas	189
7.1.1.3.	Sistemas eléctricos y de protección	190
7.1.1.4.	Equipo de protección personal	190
7.1.1.5.	Aire acondicionado.....	190
7.1.1.6.	Alarmas y sensores	191
7.1.1.7.	Abastecimientos	191
7.1.1.8.	Pago de servicios	192
7.2.	Acondicionamiento y aseguramiento de la bodega.....	193
7.3.	Evacuación de basura y desechos con contenido químico.....	197
7.4.	Importancia del programa continuo de aseguramiento de la calidad.....	201
7.5.	Importancia de las certificaciones	203
7.6.	Importancia de la capacitación continua	204
7.7.	Perfil profesional del perito	205
8.	FUENTES DE FINANCIAMIENTO	
8.1.	Proyección en el presupuesto anual de funcionamiento.....	209
8.2.	Convenios de cooperación financiera y de capacitación	209
8.2.1.	Inter-institucional	209
8.2.2.	Organismos internacionales y países amigos	210
8.2.3.	Universidades	211
8.3.	Donaciones.....	211
9.	CONTROL Y SEGUIMIENTO	
9.1.	Creación del comité de proyecto.....	214

9.1.1.	Definición del rol de jefe de proyecto	214
9.1.2.	Definición de las comisiones.....	215
9.1.2.1.	Obra física.....	215
9.1.2.2.	Adquisición de mobiliario, equipo y materiales	216
9.1.2.3.	Adquisición de dispositivos forenses	216
9.1.2.4.	Evaluación de procesos forenses	217
9.1.2.5.	Contratación de personal.....	217
9.1.2.6.	Comisión de compras	218
9.1.2.7.	Comisión de mantenimiento.....	218
9.1.2.8.	Comisión de finanzas.....	220
9.1.3.	Creación de instrumentos de control: <i>CPM</i> , formularios, cronogramas, encuestas de seguimiento, etc.....	221
9.2.	Revisión de las cartas de cooperación	222
9.2.1.	Términos e indicadores del programa de cooperación o donación	222
9.2.2.	Delimitación de la inversión	225
9.2.3.	Reajustes.....	226
9.2.4.	Ampliaciones (enmiendas).....	226
9.3.	Verificación de las instalaciones.....	227
9.3.1.	Inspecciones oculares	227
9.3.2.	Mediciones.....	227
9.3.3.	Comparación con estándares.....	228
9.3.4.	Correcciones o mejoras pertinentes	228
9.4.	Adquisición de mobiliario y equipo	229
9.4.1.	Verificación de propiedades y calidad de los bienes muebles	229
9.4.2.	Comparación con lo planificado.....	230
9.4.3.	Correcciones.....	230

9.5.	Adquisición de instrumentos, <i>hardware</i> , <i>software</i> , etc.	230
9.5.1.	Levantado de hojas de especificación	231
9.5.1.1.	Creación de las bases - productos y proveedores	231
9.5.2.	El proceso de licitación y compra.....	231
9.5.3.	Estudio de proveedores	232
9.5.3.1.	Productos, servicios, mantenimientos y reparaciones.....	232
9.5.3.2.	Calidad y conformación de normas	233
9.6.	Revisión de procesos y diagramas	234
9.6.1.	Definición de tareas	234
9.6.2.	Verificación de estándares y normas	234
9.6.3.	Examen de herramientas e instrumentos.....	235
9.7.	Reclutamiento	235
9.7.1.	Revisión, cambios y mejoras del perfil del perito	235
9.7.2.	Revisión de perfiles puestos administrativos.....	236
	CONCLUSIONES	237
	RECOMENDACIONES	239
	BIBLIOGRAFÍA	241

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Proceso de investigación forense de evidencia digital.....	5
2.	Adquisición, filtrado y análisis de data objetos para la obtención de evidencia.....	27
3.	Diagrama procesos 1 y 2.....	35
4.	Distintos tipos de tarjetas de almacenamiento.....	39
5.	Multi-lector y bloqueador de tarjetas.....	40
6.	Multi-lector y bloqueador de tarjetas, <i>USB</i> y conexiones <i>SATA</i> , <i>SCSI</i> e <i>IDE</i>	41
7.	Diagrama procesos 3 y 4.....	42
8.	Disco duro extraído.....	43
9.	Remoción conector propietario.....	43
10.	Adaptador datos/energía.....	43
11.	Conexión disco duro a bloqueador.....	44
12.	Conexión disco duro-bloqueador-computadora forense.....	44
13.	Diagrama proceso 5.....	48
14.	Set de cables de sincronización para <i>PDA</i> s y celulares.....	49

15.	Bolsa (<i>StrongHold</i>) y caja de protección contra señales de radio frecuencia.....	49
16.	Diagrama proceso 6.....	52
17.	Ejemplo 1 de exploración de herramienta de búsqueda (<i>Encase</i>)...	53
18.	Ejemplo 2 de exploración de herramienta de búsqueda (<i>Encase</i>)...	53
19.	Diagrama proceso 7.....	56
20.	Ejemplo de captura de datos de un celular (<i>UFED Cellebrite</i>).....	57
21.	Juego de destornilladores de precisión.....	66
22.	Formas comunes de cabezas de tornillos.....	67
23.	Herramientas de palanca.....	68
24.	Ejemplos de tijeras, martillo de desplazamiento, cortadora y espátula.....	69
25.	Ejemplo de <i>tester</i> digital (<i>FLUKE 287</i>).....	70
26.	Ejemplos de fotografía forense: (A) micro-cámara y (B) <i>microchip</i>	71
27.	<i>Vernier</i> o pie de rey digital.....	71
28.	Lupa de pedestal con brazo articulado extensible para ensamblar a escritorio.....	72
29.	Lectores multi-tarjeta.....	77
30.	Ejemplos de cables de sincronización de <i>PDA</i> s y celulares.....	78
31.	Ejemplo de cable coaxial.....	80
32.	Ejemplo de conectores <i>DB9</i>	81
33.	Adaptadores de corriente y voltaje.....	81

34.	Duplicador/Grabador de discos <i>CD/DVD/BLURAY</i>	82
35.	<i>Tableau TAC1441e</i>	89
36.	<i>UFED - Universal Forensic Extraction Device</i>	91
37.	<i>Device Seizure Field Kit y CSI Stick</i> (imagen ampliada).....	92
38.	Ejemplo de visualización de archivos con editor hexadecimal.....	94
39.	Duplicadores: <i>Tableau TD1</i> (A) y <i>Logicube Talon</i> (B).....	98
40.	Discos duros externos: (A) <i>Western Digital MyPassPort Studio</i> y (B) <i>Wiebetech ToughTech FS Mini</i>	99
41.	Muestra de rotulador (etiquetador).....	100
42.	Ejemplos de organizadores de cables de uso común.....	101
43.	Ejemplo de pinzas cocodrilo.....	101
44.	Set de escobilla antiestáticas de uso forense.....	102
45.	Estantería para almacén de evidencias.....	108
46.	Equipo de transporte: <i>troquet</i> plegable (A), carretilla contenedor (B)..	109
47.	Carretilla plegable con ruedas y brazo extensible.....	110
48.	Mueble modular con divisiones para delimitación del área de la estación de trabajo.....	111
49.	Diseño de silla ajustable (ergonómica).....	111
50.	Mostrador de recepción de indicios.....	112
51.	Estación forense <i>FRED</i>	114
52.	Estación forense <i>Forensic Tower III</i>	115
53.	Medidas antropométricas comunes para persona sentada.....	122

54.	Medidas antropométricas comunes para persona sentada (continuación).....	123
55.	Diseño ergonómico de la silla de la estación de trabajo (medidas en centímetros).....	125
56.	Indicación de las fuerzas de soporte que debe ejercer la silla en la región lumbar.....	126
57.	Silla ergonómica ajustable <i>AERON</i> de <i>Herman-Miller</i>	128
58.	Diseño básico del escritorio de la estación de trabajo (medidas en centímetros).....	129
59.	Armazón de escritorio de altura ajustable eléctricamente.....	129
60.	Croquis de las secciones de la estación de trabajo forense.....	134
61.	Croquis de la vista frontal de la estación de trabajo forense.....	134
62.	Puerta con mecanismo de apertura <i>slide-door</i>	143
63.	Puertas de vidrio para secciones internas del laboratorio.....	144
64.	Utilización de pantallas de bloqueo de rayos solares.....	145
65.	Utilización de ventanas amplias en los laboratorios.....	145
66.	Uso de paneles solares para iluminación de exteriores.....	161
67.	Ejemplo de caja eléctrica de seguridad.....	165
68.	Distribución típica de alumbrado general.....	166
69.	Distribución de alumbrado general localizado.....	166
70.	Ejemplo de utilización de vidrio en los laboratorios forenses.....	171
71.	Empotramiento de gabinetes contra incendios en paredes.....	180

72.	Distribución de la planta del laboratorio de Informática Forense.....	185
73.	Ejemplo de utilización de colores para los contenedores.....	198

TABLAS

I.	Descripción de las áreas de procesamiento de evidencia.....	30
II.	Simbología utilizada en los diagramas de flujo.....	31
III.	Velocidades de transmisión de diferentes buses.....	76
IV.	Precio de algunos productos para el laboratorio.....	104
V.	Costos básicos mobiliario y equipo.....	117
VI.	Dimensiones antropométricas humanas para el hombre.....	124
VII.	Precio de algunos productos para la estación de trabajo forense...	140
VIII.	Recomendaciones de iluminación para el laboratorio de Informática Forense.....	168
IX.	Tipos de fuego según la clasificación americana.....	178
X.	Nomenclatura de colores del laboratorio.....	181
XI.	Colores asociados para indicar el contenido de los contenedores para reciclaje.....	198
XII.	Programación de tiempos (recomendados) para el mantenimiento del laboratorio.....	200

LISTA DE SÍMBOLOS

Símbolo	Significado
CCTV	Circuito cerrado de televisión
CF	<i>Compact flash</i>
PC	Computadora personal
NOT	Conector lógico NO
OR	Conector lógico O
AND	Conector lógico Y
FPS	Cuadros por segundo
DBMS	<i>Data base management system</i>
DVD	<i>Digital versatile disc</i>
DMX	<i>Digital MultipleX</i>
CD	<i>Compact disk</i> (disco compacto)
HD	Disco duro
\$	Dólares americanos
G	Generación (en servicios móviles inalámbricos)
GPRS	<i>General packet radio service</i>
Gb	<i>Gigabyte</i>

GHz	<i>Gigahertz</i>
GPS	<i>Global positioning system</i>
°	Grados
GSM	<i>Groupe spécial mobile o global system for mobile communications</i>
Hz	<i>Hertz</i>
HDMI	<i>High definition multimedia interface</i>
IEEE	Instituto de ingenieros eléctricos y electrónicos
IDE	<i>Integrated drive electronics</i>
Mb	<i>Megabyte</i>
IM	Mensajería instantánea
MMC	<i>Multimedia card</i>
MMS	<i>Multimedia messaging system</i>
LCD	Pantalla de cristal líquido
PCI	<i>Peripheral component interconnect</i>
PDA	<i>Personal digital assistant</i>
PIN	<i>Personal information number</i>
PUK	<i>Personal unlocking key</i>
PVC	Policloruro de vinilo
%	Porcentaje
Q.	Quetzales

RF	Radiofrecuencia
RAM	<i>Random-access memory</i>
ROM	<i>Read only memory</i>
SD	<i>Secure digital</i>
S	Segundo
OS	Sistema operativo
SIM	<i>Subscriber identity module</i>
Tb	<i>Terabyte</i>
USB	<i>Universal serial bus</i>
VoIP	<i>Voice over IP</i>
WAP	<i>Wireless application protocol</i>

GLOSARIO

Antropometría	Estudio de las dimensiones, proporciones y características inherentes al cuerpo humano (análisis estructural) y la forma en que éste se mueve o ejerce fuerzas (análisis funcional).
Autenticar	Procedimiento por medio del cual se garantiza que una copia de un data-objeto es fiel y exacta al original, sin ningún tipo de alteración. Ver <i>Hash</i> .
Backup	Medida de precaución para el cuidado de nuestra información consistente en obtener una copia de los datos, configuraciones, ambiente, etc. de un sistema con la finalidad de enfrentar desastres o pérdidas por cualquier circunstancia.
BIOS	Código de computadora almacenado comúnmente en memoria <i>ROM</i> que realiza las tareas básicas de control, monitoreo y comprobación de los componentes: disco duro, teclado, memoria, etc., previo a delegarle las tareas más avanzadas al Sistema Operativo. (<i>Basic Input/Output System</i>).

- Bit** Dígito binario, componente de más bajo nivel de lenguaje de computadoras, el cual secuenciado, se constituye en señales, datos e información dentro de un sistema. (*Binary Digit*).
- Bluetooth** Especificación para redes inalámbricas de área personal (*WPANs*) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y globalmente libre.
- Booting** Expresión utilizada para referirse al proceso de carga, arranque o inicio del sistema operativo en memoria.
- Botnet** Término que hace referencia a un conjunto de *robots* informáticos (*software*) o *bots*, que buscan vulnerabilidades en los sistemas y se instalan en los mismos ejecutándose de manera autónoma y automática. El artífice del *botnet* puede controlar los computadores de forma remota con finalidades normalmente poco éticas (computadoras zombis).
- Bus** Medio físico de comunicación de datos interno utilizado por las computadoras. Estos buses, interconectan por ejemplo la placa madre (*motherboard*) con el microprocesador y los dispositivos periféricos como discos duros, *CD roms*; adaptadores gráficos, etc.
- Case** Caja que contiene los componentes de procesamiento de una computadora y las conexiones hacia otros dispositivos.

Clonar	Proceso por el que se consiguen copias idénticas de un medio de almacenamiento.
Cluster	Sistema de archivos en un disco duro, un <i>cluster</i> es un conjunto contiguo de sectores que componen la unidad más pequeña de almacenamiento. Los archivos se almacenan en uno o varios clústeres, dependiendo del tamaño que le haya sido asignado. Sin embargo, si el archivo es más pequeño que un clúster, éste lo ocupa completo.
Compact flash	Dispositivo de almacenamiento. Características: memoria no volátiles, bajo consumo de energía, resisten cambios drásticos de temperatura y funcionan a una velocidad de transferencia de datos muy buena. Actualmente, son muy utilizadas en aparatos electrónicos portátiles como cámaras digitales.
Cyberwarfare	Guerra cibernética, conocida por los economistas como el quinto dominio de guerra, luego de tierra, mar, aire y espacio. Ésta ha generado tal preocupación debido a la potencial inhabilitación de servicios esenciales o daños a los sistemas financieros. Por esta razón, el presidente de los Estados Unidos, Barack Obama declaró que la infraestructura digital de los Estados Unidos es un patrimonio nacional y en mayo del 2010 el Pentágono creó una nueva unidad denominada ciber comando o <i>Cybercom</i> .

- Data-objeto** Término utilizado para definir una porción de información almacenada en un sistema informático, constituidos por una secuencia de 0's y 1's lógicamente organizados y que constituyen datos o información en forma de imágenes, documentos, programas, música, etc. En este sentido, un data-objeto es una representación más exacta que el vocablo archivo, debido a que este último puede contener metadatos, o sea información de la información (v.g. nombre del autor o iniciales, nombre de la organización, comentarios, versión de la aplicación en que fue elaborado, etc.).
- Descifrar** Convertir un texto cifrado (o encriptado) a su forma original.
- Digital MultipleX*** Protocolo electrónico utilizado en luminotecnia para gestión y control de iluminación.
- Disco compacto** Soporte digital óptico utilizado para almacenar cualquier tipo de información (audio, imágenes, vídeo, documentos y otros datos). Actualmente es el medio físico más utilizado para la distribución de audio. (*CD, compact disc*)
- Diskette*** Medio de almacenamiento removible consistente en un disco de material magnético envuelto en una cubierta de plástico rígido. Hay de varios tamaños sin embargo, son considerados productos discontinuados debido a las nuevas tecnologías en almacenamiento.

Dongle	Dispositivo de <i>hardware</i> (comúnmente conectado a un puerto <i>USB</i>) utilizado como medida de seguridad para la ejecución de una determinada aplicación en un equipo informático. Utilizado comúnmente como método de licenciamiento para evitar las copias ilegales del software.
Driver	Programa informático que le permite al sistema operativo interactuar con un periférico (pantallas, impresoras, escáners, etc.) proporcionando una interfaz estandarizada para usarlo. Éste contiene las instrucciones que le indican al Sistema Operativo, cómo debe controlar y comunicarse con el dispositivo. El fabricante de dichos dispositivos comúnmente adjunta al producto estos drivers en un medio de almacenamiento.
DVD	Dispositivo de almacenamiento óptico similar al <i>CD</i> pero con mayor capacidad. (<i>DVD, Digital versatile disc</i>)
EDGE	Tecnología de telefonía móvil celular, considerada como una evolución del <i>GPRS</i> . (<i>EDGE, enhanced data rates for GSM of evolution</i>)
Editor Hexadecimal	Programa informático que permite a un usuario modificar archivos binarios almacenados en sectores de datos de disquetes o discos duros. Con éstos, el usuario puede ver o redactar el contenido intacto y exacto de un archivo. Ocurre lo contrario con otros programas de alto nivel que interpretan el mismo contenido del archivo de forma diferente.

Embalador	Encargado de empacar, marcar y registrar los indicios para ser remitidos al laboratorio.
Emplazamiento	Fijación de un plazo o término en el proceso penal durante el cual se intima a las partes o terceros vinculados (testigos o peritos) para que cumplan una actividad o formulen alguna manifestación de voluntad; en general, bajo apercibimiento de cargar con alguna consecuencia gravosa: rebeldía, sanción, tenerlo por no presentado, remoción de cargo, multa, etc.
Encriptar	Término utilizado para hacer referencia al uso de esquemas algorítmicos para hacer ilegible la información con fines de seguridad, especialmente en ambientes públicos como internet o redes corporativas. Utilizado también para el aseguramiento del traslado de información en caso de robo.
Escáner	Aparato utilizado para explorar un objeto con la finalidad de descubrir su interior o bien obtener una "imagen" del mismo. Existe una gran variedad de acuerdo a la aplicación particular, por ejemplo, escaners de código de barras, biométricos, rastreadores inalámbricos, médicos, etc.
Esteganografía	Disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

Ethernet	Estándar que define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos de una red de computadoras.
Evidencia	Indicio que luego del estudio pericial se establece que está íntimamente relacionado con el delito que se investiga y que puede utilizarse como prueba o en la reconstrucción del hecho.
Firewall	Mecanismo de seguridad basado en <i>software</i> y/o <i>hardware</i> que limita el acceso no autorizado a una red o una computadora.
Firewire	Puerto de comunicaciones de alta velocidad, reconocida con el estándar <i>IEEE</i> 1394. Es básicamente, una tecnología para la entrada/salida de datos en serie a alta velocidad y la conexión de dispositivos digitales como videocámaras, discos duros, dispositivos ópticos, etc. Llamado también, por algunos <i>iLink</i> .
Firmware	Bloque de instrucciones o programa con propósitos específicos, grabado en una memoria no volátil (v.g. <i>ROM</i>) que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Éste, al estar integrado en la electrónica de un dispositivo es en parte <i>hardware</i> , pero también es <i>software</i> , ya está basado en algún tipo de lenguaje de programación y por lo tanto proporciona lógica.

- Fuerza bruta** Forma de recuperar una clave o contraseña probando todas las combinaciones posibles hasta encontrar la que permite el acceso.
- G** Término para referirse a los cambios en conectividad móvil, llamados generaciones: 1G, basada en infraestructura análoga para la transmisión de voz. 2G, basada en tecnologías digitales, ofrecen mejor calidad y capacidad de voz que su predecesor, éstos soportan voz y servicios de datos transferidos por circuito y paquetes. *GSM*, *TDMA* son algunas de las tecnologías de segunda generación. 3G, tecnología de telecomunicaciones de tercera generación que cumple con los estándares de telefonía móvil dados por las especificaciones de la *International Mobile Telecommunications - 2000 (IMT-2000)*, las cuales proveen servicios inalámbricos de área amplia para voz, datos, video, televisión, etc. Actualmente, ya se están realizando pruebas y definiciones para la generación 4G.
- Gigabyte** Unidad de almacenamiento equivalente 1 024 *megabytes*.
- GigaHertz** Medida actual de la velocidad de un microprocesador; múltiplo de la unidad de medida de frecuencia *Hertz (Hz)* equivalente a 1 000 000 000 *Hz*. O sea un ciclo de 1 nanosegundo.

- GRPRS** Servicio general de paquetes vía radio es una extensión del sistema global para comunicaciones móviles (*GSM*) para la transmisión de datos no conmutada (o por paquetes). Este Servicio es similar al *GSM* pero a mayores velocidades y con forma de tarificación diferente. (*GPRS, general packet radio service*).
- GSM** Sistema estándar de telefonía móvil digital que permite conectarse a través entre otras cosas enviar y recibir mensajes por e-mail, faxes, navegar por Internet, acceder con seguridad a la red informática de una compañía, así como utilizar otras funciones digitales de transmisión de datos, incluyendo el Servicio de mensajes cortos (*SMS*) o mensajes de texto. (*GSM, groupe spécial mobile o global system for mobile communications*).
- Hacking** Llamase así a las actividades que incluyen el modificar el *hardware* o *software* de los sistemas informáticos para cumplir con algún fin particular.
- Hardware** Se le llama así, a todas las partes tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico.
- Hash** Función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., o bien para resumir o identificar probabilísticamente un gran conjunto de

información a través de un sólo dato. El *hash* es el resultado de dicha función o algoritmo.

HDMI

Norma de audio y vídeo digital cifrado sin compresión que provee una interfaz entre cualquier fuente de audio y vídeo digital y un monitor, televisor digital u otro artefacto que reciba señales de multimedia de alta definición. Éste también la transmisión de audio digital multicanal en un único cable. (*HDMI, high definition multimedia interface*)

Huevo de pascua

El huevo de pascua (virtual) o *Easter Egg*, es un mensaje o capacidad, aplicación o programa oculto contenido en *software*, películas, videojuegos, etc.

IDE

Interfaz de transmisión de datos en bus dentro de equipos informáticos. Este sistema hace que un disco lleve circuitería integrada una placa que controle las funciones del dispositivo. (*IDE, integrated drive electronics*).

IM

Mensajería instantánea: sistema de intercambio de mensajes escritos en tiempo real a través de una Red.

Imagen

Dispositivo de almacenamiento que contiene la réplica exacta de otro medio de almacenamiento, como un disco duro, un disquete o un disco óptico. Ésta usualmente se produce creando una copia completa (o *bit por bit*), del medio de origen y por lo tanto duplicando perfectamente la estructura y contenidos del dispositivo de almacenamiento original.

Incidente	Momento en el cual se cometió un delito.
Indexar	En informática, es la acción de elaboración de un índice que contenga de forma ordenada la información, con la finalidad de obtener resultados de forma sustancialmente más rápida y relevante al momento de realizar una búsqueda.
Indicio	Del latín <i>indictum</i> , que significa signo aparente y probable de que existe alguna cosa, sinónimo de señal, muestra o indicación. Un indicio es todo material significativo obtenido adecuadamente de una escena o de un allanamiento que tiene relación con un hecho delictuoso y que puede, luego del análisis pericial, convertirse en evidencia.
Ingeniería social	Actuaciones de manipulación de personas para que éstas realicen ciertos actos o divulguen algún tipo de información, comúnmente haciéndose pasar por una persona legítima o de alto rango utilizando la confianza o la intimidación.
Jamming	Acción de prevenir que un dispositivo, como un teléfono celular, reciba señales de estaciones base o antenas. Los dispositivos que realizan esta función son llamados <i>jammers</i> .
Jumper	Elemento para interconectar dos terminales de manera temporal sin tener que efectuar una operación que requiera herramienta adicional. Esta interconexión cierra el circuito eléctrico del que forma parte.

Kernel	Es el núcleo de un Sistema Operativo y el principal responsable de facilitar a los distintos programas el acceso seguro al <i>hardware</i> de la computadora y la gestión de los recursos del sistema.
Knowledge base	Base de datos de conocimientos: colección de información de experiencias, problemáticas, resultados y soluciones encontradas a lo largo del tiempo por una organización.
Laptop	Computadora personal de uso móvil.
Law Enforcement	Término colectivo utilizado para designar a aquellos profesionales que están dedicados a defender o reforzar las leyes y estatutos de un determinado marco o jurisdicción legal. Este "reforzamiento" persigue primero el prevenir la ocurrencia de crímenes que de alguna forma dañen a un ser humano o a la sociedad y segundo, que el criminal sea tratado de una manera acorde a las leyes locales.
LCD	Pantalla delgada y plana formada por un número de <i>píxeles</i> en color o monocromos colocados delante de una fuente de luz o reflectora. A menudo se utiliza en dispositivos electrónicos de pilas, ya que utiliza cantidades muy pequeñas de energía eléctrica. (<i>LCD, liquid crystal display</i>).
LED	Diodo emisor semiconductor que emite luz. (<i>LED, light emitting diode</i>).

Legacy	Sistema informático (equipos informáticos o aplicaciones), que ha quedado anticuado, o discontinuado, pero que sigue siendo utilizado debido al costo de actualización o porque no se puede reemplazar.
Log	Registro de eventos durante un rango de tiempo en particular.
Louver	Ventana especial con paletas horizontales colocadas en ángulo para admitir luz y aire y prevenir de alguna forma el ingreso de lluvia, luz solar o ruido.
Lux	Unidad derivada del Sistema Internacional de Unidades para la iluminancia o nivel de iluminación.
Malware	<i>Malware</i> (del inglés <i>malicious software</i>), <i>software</i> malicioso o malintencionado que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. En este sentido, es un <i>software</i> hostil, intrusivo o molesto.
Megabyte	Unidad de almacenamiento de información equivalente a 1 024 <i>kilobytes</i> .
Megapixel	Un millón de <i>pixeles</i> .
Metadata	Datos constituidos por la información de la información, por ejemplo, un archivo, independiente de su contenido posee metadata como la fecha de creación o modificación, nombre del autor, comentarios, versión de la aplicación, etc.

Microprocesador	Circuito integrado central y más complejo de una computadora, por analogía, el "cerebro" de un Sistema u ordenador.
MMC	Tarjeta de memoria. (<i>MMC, multimedia card</i>).
MMS	Sistema de mensajería de multimedia, estándar de mensajería permite a los teléfonos móviles enviar y recibir contenidos multimedia (sonido, video, fotos, etc.). (<i>MMS, multimedia messaging system</i>).
Motherboard	Placa de circuitería base, donde están impresos los circuitos donde van conectados todos los componentes de la computadora.
Multifuncional	Artefacto que se conecta a la computadora y que posee variadas funciones, por ejemplo, impresora, escáner de imágenes, fotocopidora, fax, etc.
Netbook	Computadora portátil de bajo costo y generalmente reducidas dimensiones, lo cual aporta una mayor movilidad y autonomía.
Partición	Nombre genérico que recibe cada división presente en una sola unidad física de almacenamiento de datos.
Password-crack	Dícese de todas las herramientas o metodologías disponibles para averiguar una contraseña o desbloquear el contenido de un archivo o data-objeto.

- PCI** Bus de un computador para conectar dispositivos periféricos directamente a su *motherboard*. (*PCI, peripheral component interconnect*).
- PDA** Computadora de bolsillo o de mano. (*PDA, personal digital assistant*).
- Pendrive** Dispositivo de almacenamiento que utiliza memoria *flash* para guardar la información y que comúnmente se conecta a un puerto *USB*, por lo cual se le denomina memoria *USB*.
- Phishing** Delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial (contraseña, números de cuenta bancaria, tarjetas de crédito, etc.) de forma fraudulenta. El estafador o *phisher*, se hace pasar o hace creer a las personas que las comunicaciones a un sitio, página de *internet* o las respuestas a un mensaje de correo provienen de una empresa segura o de confianza donde solicita dicha información.
- PIN** Número de identificación personal, código numérico usado en ciertos sistemas, como un teléfono móvil o un cajero automático, para obtener acceso a algo, o identificarse. En este sentido el *PIN* es un tipo de contraseña. (*PIN, personal identification number*).

- Pixel** La menor unidad homogénea en color que forma parte de una imagen digital, ya sea esta una fotografía, un fotograma de vídeo o un gráfico.
- Planimetrista** Encargado de realizar los croquis o dibujos con información relevante de una escena delictiva: medidas de habitaciones, distancia de objetos respecto referenciales, ubicaciones de los rótulos de los indicios, etc.
- Plug and Play** Conectar y listo: tecnología que permite a un dispositivo informático ser conectado a una computadora sin tener que configurar, mediante *jumpers* o software específico (*drivers*), proporcionado por el fabricante, ni proporcionar parámetros a sus controladores. Para que sea posible, el sistema operativo con el que funciona el ordenador debe tener soporte para dicho dispositivo.
- PUK** Clave Personal de Desbloqueo. Es el código normalmente usado en los sistemas de telefonía móvil que funciona como una clave o contraseña para desbloquear la tarjeta SIM del equipo móvil cuando se ha olvidado el *PIN*. (*PUK, personal unlocking key*).
- RAID** Sistema de almacenamiento que utiliza múltiples discos duros entre los que distribuyen o replican los datos. Éstos brindan los siguientes beneficios: mayor integridad, mayor tolerancia a fallos, mayor rendimiento y mayor capacidad. (*RAID, redundant array of independent disks*).

- RAM** Medio de almacenamiento donde se guarda toda la información, programas, datos, etc. con los que se está trabajando en una computadora en un momento determinado y que se mantiene y actualiza dinámicamente mientras el equipo es alimentado por energía. (*RAM, random-access memory*).
- Repositorio** Sitio centralizado donde se almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos.
- ROM** Medio de almacenamiento que solamente se puede leer y que guarda comúnmente instrucciones o programas que permiten arrancar un computador o efectuar diagnósticos. (*ROM, read only memory*).
- SATA** Interfaz de transferencia de datos entre la placa base y algunos dispositivos de almacenamiento (disco duro, lectores *CD/DVD*, unidades de estado sólido, etc.) que proporciona mayores velocidades, mejor aprovechamiento de varias unidades, mayor longitud del cable de transmisión de datos, capacidad para conectar unidades en caliente (es decir, insertar el dispositivo sin tener que apagar el ordenador), etc. (*SATA, serial advanced technology attachment*).
- SD** Formato de tarjeta de memoria utilizado en dispositivos portátiles tales como cámaras fotográficas digitales, *PDA*, teléfonos móviles, etc. (*SD, secure sigital*).

Sensor	Dispositivo capaz de detectar magnitudes físicas o químicas, llamadas variables de instrumentación (temperatura, intensidad lumínica, humedad, presión, etc.) y transformarlas en variables eléctricas capaces de ser manipuladas.
Shred	Proceso de borrado seguro, consistente en sobrescribir el archivo o archivos indicados varias veces con varios patrones de texto, trastornando el contenido del archivo original en información sin sentido.
Sincronizar	Proceso utilizado para mantener los contenidos o versiones iguales en dos dispositivos. Pasar información de un medio a otro en forma automática a fin de mantener la misma información.
Sistema de Archivos	Sistema para estructurar la forma de organizar, guardar, acceder y asegurar la información y su meta-datos en una unidad de almacenamiento (normalmente un disco duro). Los sistemas operativos utilizan un gestor para trabajar con estas estructuras (<i>FAT, NTFS, MVS, etc.</i>).
Sistema manejador de Bases de Datos	Conjunto de programas que se encargan de manejar la creación, accesos, seguridad, etc. a una base de datos. (<i>DBMS, Data Base Management System</i>)
Slack	Espacio existente entre el tamaño físico (o lógico), de un archivo y el final de su espacio o <i>cluster</i> asignado.

Smartphone	Término comercial para denominar a un teléfono móvil que ofrece más funciones integradas (manejador de archivos, agendas, reproductores, conexión a internet, <i>GPS</i> , etc).
Socket	Punto de contacto para realizar conexiones. Existen <i>sockets</i> (o enchufes) de conexión física y <i>sockets</i> lógicos utilizados para la conexión de una computadora, dependiendo del protocolo de red, a un servicio en otra computadora.
Softphone	Programa especial de gestión de llamadas telefónicas que mediante la conexión y configuración específica en la planta telefónica hace que la computadora pueda ser utilizada como un teléfono.
Software	Equipamiento o soporte lógico de una computadora digital; comprende el conjunto de los componentes necesarios que hacen posible la realización de tareas específicas tales como el procesador de texto, hojas electrónicas, sistema operativo, etc.
String	Secuencia o hilera finita de símbolos elegidos de un conjunto o alfabeto (v.g. una palabra es considerada un <i>string</i> de caracteres).
Suite	Recopilación de programas o aplicaciones orientadas a un trabajo particular, por ejemplo, una <i>suite</i> de oficina incluiría procesadores de palabras, hojas electrónicas, presentador de diapositivas, etc., una <i>suite</i> de informática forense

incluiría bloqueadores, editores hexadecimales, rastreadores, descifradores, etc.

Tablet Computadora portátil con la que se puede interactuar a través de una pantalla táctil o multi-táctil. Comúnmente, el usuario puede utilizar los dedos para trabajar y dar instrucciones al equipo. Posee *hardware* para acceder a *Internet* o redes celulares y utilizar sus servicios.

Terabyte Unidad de almacenamiento de información cuyo símbolo es el *Tb*, y equivale a 10^{12} bytes, aproximadamente 10 000 *gigabytes*.

Troquet Carretilla consistente en dos ruedas y una plataforma que permite apilar objetos para transportarlos.

Unidad central de proceso Núcleo principal de una computadora, éste incluye el microprocesador, memorias de transacción, registros, buses de datos, etc. (*CPU, central process unit*)

USB Puerto serial muy versátil (o universal) utilizado para conectar periféricos o medios de almacenamiento a una computadora. (*USB, universal serial bus*).

VoIP Grupo de recursos que hacen posible la comunicación o transmisión de voz a través de Internet utilizando el protocolo *IP*, lo que significa que la voz se envía en forma digital y se transforma en paquetes de datos. (*VoIP, Voice over IP*).

- WAP** Estándar para realizar comunicaciones inalámbricas. Se trata de un conjunto de normas y especificaciones que regulan el modo en que los dispositivos inalámbricos se pueden comunicar y acceder a un aparato o una red. (*WAP, wireless application protocol*).
- Wipe** Conjunto de procedimientos para eliminar en forma segura de un computador los historiales, bitácoras, archivos, etc. a fin de evitar que sea visto el comportamiento de una computadora o sus archivos.
- Wireless** Se llama así a todas aquellas comunicaciones realizadas sin el uso de cables. Es aquella en la que extremos de la comunicación (emisor/receptor), no se encuentran unidos por un medio de propagación físico, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio.

RESUMEN

El documento contiene nueve capítulos, los cuales enfocan varios aspectos importantes para la instauración y establecimiento de un laboratorio de Informática Forense, desde el diseño de los procedimientos básicos hasta el establecimiento de las comisiones para control y seguimiento del proyecto.

El capítulo uno presenta una breve reseña de la evolución de lo que hoy se conoce como Informática Forense; observa las generalidades del proceso de investigación forense para la obtención de evidencia digital, describe brevemente qué es la cadena de custodia, el Ministerio Público y el INACIF.

Los capítulos dos y tres esbozan el núcleo central del trabajo: políticas y normas para la realización del trabajo forense, descripción básica de los procesos, recomendaciones de buenas prácticas, enumera y describe las herramientas, instrumentos y dispositivos utilizados en la realización de peritajes informáticos, etc.

Lo relacionado con el mobiliario y equipo para el área administrativa se encuentra en el capítulo cuatro, en éste, se brindan recomendaciones respecto a los materiales de los muebles, la adecuación de los equipos necesarios para realizar las labores diarias, la necesidad de contar con equipos telefónicos, multifuncionales, estanterías, etc.

El capítulo cinco trata con el diseño de la estación de trabajo forense y recalca la importancia que ésta esté acondicionada para las labores forenses, en el sentido de cuidados ergonómicos, para evitar lesiones por mala postura,

fatiga innecesaria, cansancio ocular, etc. Se presentan detalles fundamentales como dimensiones del módulo, instalación de iluminación apropiada, temperatura conveniente, etc.

El diseño del edificio aparece en el capítulo seis. En éste se indican aspectos importantes necesarios para un sitio de trabajo (v.g. baños, comedor, clínica médica, aire acondicionado, etc.), instalación de sistemas de protección (fusibles, reguladores de voltaje, extintores, etc.), que protejan y garanticen la inversión realizada, se consideran detalles de seguridad, etc.

El capítulo siete muestra el plan básico de mantenimiento. En éste se considera la importancia de la creación de planes de limpieza, manejo de la basura, cuidados de la bodega de indicios o evidencias, mantenimiento del aire acondicionado, etc. En este capítulo, también se menciona la importancia de la instauración de un programa continuo de aseguramiento de la calidad, las certificaciones y la capacitación.

El capítulo ocho refiere algunas formas de obtención de financiamiento interno y de Cooperación Internacional. Además, brinda algunas sugerencias respecto al uso de inversión mixta en las diferentes fases del proyecto (montaje de infraestructura, puesta en marcha, sostenibilidad, etc.).

El capítulo nueve propone la creación de las comisiones elementales que implica un proyecto (obra física, compras, finanzas, etc.), la generación de los instrumentos de control (cronogramas, formularios, CPM, etc.). La importancia de las inspecciones y mediciones durante la construcción y obra gris; y finalmente la adecuación y revisión de los perfiles de los profesionales y de los procesos, previo a la contratación de personal.

OBJETIVOS

General

Proveer las consideraciones técnicas necesarias para la creación e implementación de un laboratorio de Informática Forense con los respectivos requerimientos del edificio, puertas, mobiliario, equipo, etc., las herramientas e instrumentos forenses utilizados y los procedimientos básicos para la realización de peritajes o expertajes.

Específicos

1. Reconocer la importancia del trabajo cooperativo multidisciplinario del área forense en la reconstrucción de hechos delictivos en la persecución penal; recordando que la disciplina forense es la aplicación de conocimientos científicos para la resolución de problemas legales.
2. Esbozar los procesos básicos que permitan conocer de antemano cómo responder con éxito ante un incidente determinado, dónde comenzar, qué analizar, cómo buscar y cuándo requerir asesoría legal o asistencia externa.
3. Proveer el marco técnico para la realización de peritajes informáticos así como la lexicología apropiada.

4. Concientizar al perito respecto a la responsabilidad profesional, sus consecuencias y repercusiones al participar en casos legales.
5. Coadyuvar a la justicia en Guatemala: preparando parte de la infraestructura que apoye la investigación de este tipo de delitos.
6. Ampliar el campo de acción de la Ingeniería Forense en Guatemala.
7. Servir como base financiera inicial para el cálculo del costo del equipo, herramientas e instrumentos propios de la Informática Forense.

INTRODUCCIÓN

La utilización de la tecnología para usos delictivos ha propiciado la especialización de la investigación y persecución penal. Actualmente, las organizaciones encargadas de realizar estudios forenses, Instituto Nacional de Ciencias Forenses INACIF, y el de dirigir las investigaciones, Ministerio Público, aún no cuentan con una unidad formalmente definida que atienda exclusivamente este tipo de “delitos informáticos”. Esto, a pesar que el Ministerio Público ha realizado un buen trabajo al día de hoy con el personal de los Departamentos de Sicomp y Tecnología e Informática.

Tomando en consideración la inminente necesidad que nuestro país cuente con un laboratorio dedicado a la Informática Forense, se ha elaborado el presente trabajo con las consideraciones técnicas que permitan sentar las bases tanto de creación, como de implementación de un laboratorio dedicado a este tipo de labores.

El material incluido puede utilizarse para la creación de una unidad de Informática Forense en cualquiera de las organizaciones citadas previamente, o bien para la instauración de una independiente, razón por la cual se desarrollaron los temas del diseño físico de las instalaciones, mantenimiento, obtención de fuentes de financiamiento y el de creación de comisiones para el control y seguimiento del proyecto.

1. INFORMACIÓN PRELIMINAR

1.1. Breve historia de la Informática Forense

Los orígenes de la informática forense se remontan aproximadamente a un poco más de 35 años. Ésta, en gran parte se basó en principios generados en los Estados Unidos de América cuando las agencias militares y las organizaciones de reforzamiento de la ley (*Law Enforcement Agencies*) observaron que los criminales evolucionaron y se especializaron en su modo de operación, gracias al auge de la tecnología.

Por esta razón, las agencias gubernamentales estadounidenses formaron entidades especializadas dedicadas a la investigación de esta nueva modalidad en la comisión de delitos, por ejemplo, de sabotaje de servicios básicos, espionaje, robo de identidades, transferencias bancarias fraudulentas, invasión de la privacidad, etc. El objetivo de estas agencias no solo era investigar quién había violado la seguridad sino cómo lo había realizado, con el propósito de establecer políticas de prevención y generar los mecanismos de protección más adecuados ante dichas amenazas.

A mediados de la década de los ochenta, las tecnologías informáticas fueron más accesibles debido a la comercialización de computadoras, los servicios de telefonía, la computación móvil, las comunicaciones satelitales, el *Internet*, etc., esto facilitó la vida de las personas pero lamentablemente propició su uso para la comisión de delitos. Fue durante esta década que el tema de los delitos informáticos se hizo más plausible y se valoró a nivel legal, económico, financiero y político su repercusión.

Durante los años noventa hubo un apogeo en la aparición de empresas dedicadas completamente a la elaboración de *software* y *hardware* de prevención, en primera instancia aparecieron empresas con orientación a soluciones de antivirus que luego se generalizaron a ámbitos más globales como detección de intrusos, comunicaciones seguras, encriptación, *firewalls*, etc. Éstas, además de comercializar dichos productos, ofrecían consultorías en temas de seguridad informática, análisis de riesgo, respuesta a incidentes, recuperación de desastres, identificación de métodos de ingeniería social, etc.

Durante esta década e inicios del nuevo milenio aumentó significativamente el número de eventos delictivos informáticos lo cual motivó la aparición de expertos (v.g. Brian Carrier, Wietse Venema y Dan Farmer) y de empresas aún más especializadas en el desarrollo de herramientas informático-forenses, soluciones de seguridad, estudio de procesos y creación de normas o estándares. Por ejemplo, en la actualidad, tanto la *ISO (International Organization for Standardization)* como *NIST (National Institute of Standards and Technology)*, entidades conocidas a nivel mundial por el desarrollo, estudio y publicación de estándares, incluyen dentro de sus investigaciones estos temas.

Finalmente, la aparición de delitos informáticos ha promovido la creación de leyes, proyectos legislativos, instituciones y programas para el estudio e investigación de esta nueva disciplina en varios países¹, en las áreas de definición y taxonomía, estandarización de herramientas y procedimientos, establecimiento de buenas prácticas, creación de leyes conexas (v.g. protección de datos, telecomunicaciones y propiedad intelectual), etc.

¹ Ver, por ejemplo: *Computer Forensics Associates* (<http://www.computerforensicsassociates.com/>), *The Electronic Evidence Information Center* (<http://www.e-evidence.info/>), *International High Technology Crime Investigation Association* (<http://www.htcia.org/>), *The International Organization of Computer Evidence* (<http://www.ioce.org/>), *US-CERT* (<http://www.us-cert.gov/>), *Center for Computer Forensics* (<http://www.computer-forensics.net/>), *Australian High Tech Crime Centre* (<http://www.afp.gov.au/national/e-crime/ahtcc.html>) etc.

A partir de este momento, dentro del presente documento, cuando se refiera al término tecnología entiéndase cualquier producto de la tecnología Informática. En general, cualquier dispositivo físico y/o lógico, herramienta, sentencias o códigos que procesen información, la almacenen, la transfieran, le cambien formato, encripten o descifren, etc.

Esto comprende computadoras (o emulación por máquina virtual) y todos sus dispositivos periféricos, tanto de entrada como de salida, procesadores, medios de almacenamiento volátiles o no-volátiles, locales, remotos o extraíbles; equipos de manejo de transmisión, recepción o amplificación de frecuencias, transferencia de información (por ejemplo, texto, audio o video) sean estos análogos o digitales, de transferencia física o inalámbrica, de cualquier estándar, norma, método o protocolo, activos o pasivos; detectores y/o sensores de cualquier tipo, escaners, rastreadores, etc.

Se incluye también, cualquier *set* de instrucciones (*software, firmware, etc.*) almacenados en cualquier medio y a cualquier nivel, sean estos códigos fuente u objeto, entiéndase aplicaciones o programas comerciales, científicos, sistemas operativos, manejadores de base de datos, etc.

1.1.1. La Informática Forense

La Informática Forense es considerada una disciplina auxiliar de la Justicia que persigue a través de conocimientos técnicos y procedimientos formales demostrar que la tecnología fue empleada en los siguientes casos: como medio utilizado en la comisión de delitos; como objeto directo de acciones delincuenciales; y como referencia, respecto a otros medios, objetos o personas involucrados en hechos criminales.

- Tecnología utilizada como medio en la realización de delitos

La Informática Forense se aplica cuando es necesario investigar si la tecnología fue utilizada directamente en la comisión de un delito. Por ejemplo, al utilizar un objeto tecnológico (equipo sindicado) para la intrusión a una red empresarial, bancaria, estatal, personal, etc. con el fin de adulterar, robar, eliminar o cambiar datos o registros, secuestrar documentos privados, espiar y publicar información sensible, quebrantar sistemas de seguridad, interceptación de servicios de comunicación privada, utilización de redes inalámbricas sin autorización, etc.

- Tecnología como objeto de acciones delincuenciales

La Informática Forense es útil para investigar o demostrar si un objeto tecnológico (equipo agraviado) ha sido motivo de un delito, por ejemplo, haciendo que éste falle, funcione en forma inadecuada, se altere para cumplir objetivos delincuenciales, etc. Ejemplos típicos de esto son el sabotaje, las computadoras zombis, la interrupción de servicios automatizados (sistemas de transporte, semáforos, ascensores, radares, etc.), la destrucción física de equipos, etc.

- Tecnología utilizada como referencia

La Informática Forense es útil para obtener información de un objeto tecnológico (equipo testigo), que por su uso ha captado información en forma escrita, video, audio, o cualquier otro tipo de señal, frecuencia, etc. y cuyo registro puede ser utilizable para complementar un caso, o brindar elementos que están relacionados directa o indirectamente con el objeto de averiguación. Por ejemplo, cámaras de seguridad, información de

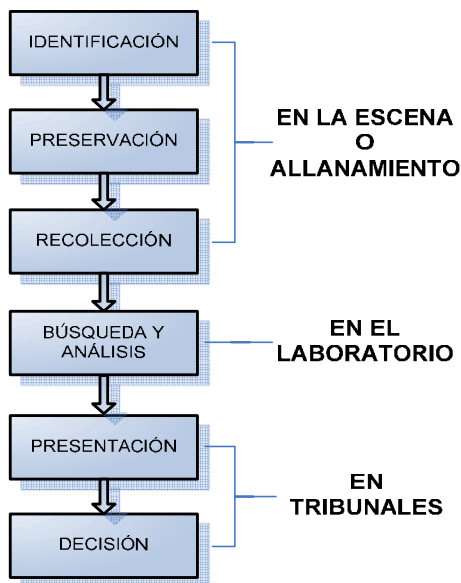
mensajes o llamadas en celulares, documentos escritos con nombres de personas involucradas, registros biométricos de entradas y salidas de oficinas o edificios, monitoreo por sistemas de posicionamiento global (GPS - *Global Positioning Systems*), etc.

1.2. El proceso de investigación forense

Este proceso desde el inicio hasta la conclusión en Tribunales debe incluir los siguientes pasos: identificación, preservación, recolección, búsqueda y análisis, presentación y decisión.

Las tres primeras se dan durante el curso del procesamiento de una escena o un allanamiento; la búsqueda y el análisis se llevan a cabo en el laboratorio y finalmente, la presentación y decisión se realizan en los Tribunales de Justicia.

Figura 1. **Proceso de investigación forense de evidencia digital**



Fuente: *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, p. 46

1.2.1. Identificación

Consiste en pura observación y comprensión de la forma en que fue cometido el delito. En primera instancia es la formulación de las hipótesis básicas y cómo han interactuado todos los objetos o las partes, es decir la contemplación de todas las piezas de un rompecabezas y la delimitación física de la escena, asignación de un identificador o número, la inspección y documentación del estado de los objetos (computadoras, teléfonos celulares, *smart-phones*, *tablets*, asistentes personales - *Personal Digital Assistants*, *PDA*s -, etc.). Esta documentación también debe incluir la toma de fotografías y video, la narración descriptiva del ambiente o escena, relato posible de los hechos, comportamiento de usuarios o testigos, olores, temperaturas, etc.

1.2.2. Preservación

En la identificación ya se realizó una delimitación física del área donde ocurrió el incidente. La preservación es el aislamiento de la escena y por lo tanto de todos los objetos informáticos a fin de conservar la integridad y de protegerlos contra cualquier tipo de contaminación, alteración, modificación, robo, etc. Por lo general tanto la identificación como la preservación se realizan en paralelo.

1.2.3. Recolección

Consiste en el empaquetamiento de todos los elementos o indicios encontrados en el paso de identificación. Este empaquetamiento o embalaje debe cumplir con varias normas que no pueden omitirse porque es aquí, donde inicia la cadena de custodia y por lo tanto debe estar correctamente individualizado y etiquetado, descrito fielmente; debe incluir además, el lugar,

circunstancia en que se obtuvo, la fecha y hora, nombre del embalador, marca de los equipos, modelos, números de serie, etc., y debe ser sellado y firmado por el agente fiscal a cargo de las diligencias; y aunque sobreentendido, debe etiquetarse externamente indicando que el contenido es frágil, sensible a la humedad, campos magnéticos intensos, etc.

Adicionalmente debe utilizarse el empaque apropiado a fin de evitar deterioro, corrosión, oxidación, etc. de los indicios y en el caso de sistemas informáticos, las conexiones de entrada/salida deben sellarse con cuidado. Si se utilizara cinta adhesiva debe considerarse no dañar ningún componente con el pegamento de ésta.

Si el equipo estuviera constituido por varias partes o conexiones, éstas deben ser rotuladas (es decir, rotular en una correspondencia uno a uno: cable "A" con *socket* "A", conexión "B" con toma "B"; etc.). Adicionalmente, las partes deben ser registradas y descritas en el embalaje respectivo y cuando sea posible, debe embalsarse junto con los equipos, los manuales de usuario, documentación de instalación, notas del fabricante, etc. Todo esto es útil para el ensamblaje posterior en los laboratorios y además, éstos pueden contener información valiosa para los peritos.

Los mismos cuidados de empaquetado se deben considerar al embalar medios de almacenamiento externos (tarjetas de memoria, discos duros, *pendrives*, etc.), celulares, reproductores (*portable digital media players* - MP3, MP4, MP5, *IPODs*, etc.), *tablets*, cámaras digitales, etc.

En general, para la recolección de equipos o dispositivos informáticos se recomienda lo siguiente.

- Si se tiene alguna duda respecto a la captura de dispositivos o equipos, siempre se pregunta al fiscal encargado respecto a la no violación de la cobertura del allanamiento en la orden del Juez emisor.
- Utilizar la indumentaria apropiada (v.g. guantes de *latex*).
- Colocar un rótulo de identificación sobre cada elemento que se considere un indicio (generalmente un plástico con un número o una letra).
- Siempre solicitar al técnico o administrador encargado de los equipos que esté presente durante toda la diligencia, quien debe mostrar el estado general del sistema (archivos abiertos, servicios o programas en ejecución, conexiones de red, etc.). Tomar el nombre y puesto de la persona para el levantado del acta respectiva, así como la hora de inicio y final del trabajo.
- Fotografiar y video-grabar el equipo en todas sus caras y su entorno (i.e. las conexiones traseras, laterales, dispositivos conectados, la oficina, etc.), y documentar todo el proceso de recolección. Cerciorarse que, tanto la cámara de video como la de fotografías presenten la fecha y hora actuales.
- Si el equipo está apagado, no debe encenderse.
- Para computadoras personales, si el equipo está encendido, tratar de obtener información relevante (v.g. contraseñas del Sistema Operativo, *BIOS - Basic Input Output System* -, archivos abiertos, estado de la memoria *RAM - Random Access Memory* -, etc.) y luego apagarlo de forma apropiada.

Si existiera la duda razonable de que el equipo está eliminando información (potencial evidencia), se debe detener el suministro eléctrico del equipo desenchufando los cables. Si el equipo es móvil, por ejemplo una laptop, se debe retirar la batería para evitar encendidos accidentales o retornos de estado de suspensión o hibernación.

En el caso de equipos centrales o servidores, el encargado o administrador del sistema tendrá que realizar la secuencia de apagado respectiva. Esto último es sumamente importante debido a que algunos sistemas operativos son más sensibles a corromperse en su núcleo central (*kernel*). La decisión de realizar el procedimiento correcto de apagado o el abrupto desenchufe de cables de energía depende de la directiva de preservación de la evidencia y/o la no destrucción de la misma; lo cual, dependerá en gran parte de la experiencia y pericia del técnico y el aval del fiscal a cargo.

- Se debe secuestrar también los manuales de los equipos, los dispositivos conectados al computador, por ejemplo discos externos; también si estuvieran presentes, *CDs (Compact Disks)*, *DVDs (Digital Versatile Disks)*, memorias flash, tarjetas *SD (Secure Digital Cards)*, *dongles*, etc.
- Previo al embalaje, se debe preguntar al administrador o encargado de los equipos acerca de los procedimientos de apagado/encendido y las contraseñas. Registrar y documentar con todo detalle dichos procedimientos.

En una escena o allanamiento está involucrado un equipo multidisciplinario de profesionales y técnicos: fiscales, auxiliares, planimetrías, embaladores, fotógrafos, policías, etc., trabajando bajo las directivas del agente fiscal del Ministerio Público, quien posee la investidura para dirigir las actividades

investigativas y es éste quien estará a cargo de velar porque todo el procedimiento sea realizado íntegramente.

1.2.4. Búsqueda y análisis

Los procesos de búsqueda y análisis son ejecutados en el laboratorio con las herramientas e instrumentos especializados bajo el marco del método científico. Para la realización de estos procesos se debe contar con las directrices de investigación brindadas por el agente fiscal, quien también debe brindar la asesoría legal respectiva, especialmente en tópicos como invasión a la privacidad o violación de garantías.

Esta etapa determina si los indicios pueden ser considerados como evidencias e incorporados como medios de prueba, por lo que cada análisis debe realizarse con el máximo cuidado posible. Esto incluye la elaboración de informes, reportes y dictámenes, los cuales deben ser redactados de una forma clara, explicando los tecnicismos de modo sencillo, de tal manera que tanto el fiscal como el juez puedan valorar la evidencia, así como los procedimientos utilizados para obtenerla.

Técnicamente, esta etapa está constituida por la buena práctica de obtención de una copia exacta de los medios de almacenamiento originales *bit* por *bit* de la media original junto a su respectiva firma digital, que garantice su autenticidad, el estudio del equipo (sistema operativo, aplicaciones, bitácoras – *logs* -, procesos, etc.), el análisis de la media (sistema de archivos, espacios no asignados en *clusters*, archivos temporales, etc.), la búsqueda de información (nombres, lugares, fechas, etc.) o patrones de data específicos, la recuperación de información eliminada o escondida y cuando es viable, el descifrado.

La descripción general de estos procedimientos se encuentra en el capítulo dos de este documento.

1.2.5. Presentación

Es la exposición de la evidencia como prueba en los Tribunales utilizando los medios audio-visuales necesarios para no omitir ningún detalle, tanto de su valor como del impacto que ésta pueda producir. Se incluyen aquí: los reportes, informes y dictámenes de los análisis realizados, así como la documentación de procedimientos, herramientas, técnicas, *software*, etc., utilizados en la obtención de los hallazgos. Esta documentación es relevante para dejar sentado que la evidencia se obtuvo por métodos legítimos (i.e. no fue obtenida mediante la violación de una garantía, el uso de procedimientos ilegales o no aprobados u ordenados por autoridad competente). En este sentido, la evidencia debe ser completa, confiable, admisible, auténtica y creíble.

La presentación incluye la preparación del testimonio, la hoja de vida y un resumen de la experiencia en materia forense de los peritos y/o los expertos, lo cual puede llegar a ser muy útil cuando se ataca la idoneidad o calidad del perito.

1.2.6. Decisión

La etapa de decisión es aquella donde se considera - por los tribunales - la admisibilidad de la evidencia y ésta se constituye como prueba dentro del caso particular. Esta es la etapa a la que se debe aspirar llegar, porque constituye la cúspide de todo el trabajo realizado por el laboratorio.

1.3. El Ministerio Público

1.3.1. Descripción, visión y misión del Ministerio Público

Descripción

El Ministerio Público fue creado con base en el artículo 251 de la Constitución Política de la República de Guatemala, el cual establece que el Ministerio Público es una institución auxiliar de la administración pública y de los tribunales, con funciones autónomas de rango constitucional, cuyo fin principal es velar por el estricto cumplimiento de las leyes del país. El Ministerio Público se rige por su Ley Orgánica, Decreto No. 40-94 del Congreso de la República y sus reformas.

Visión

“Ser una institución eficiente, eficaz y transparente, que con apego al principio de legalidad, contribuya a la consolidación del estado de derecho.”

Misión

“Promueve la persecución penal, dirige la investigación de los delitos de acción pública y vela por el estricto cumplimiento de las leyes del país.”

1.3.2. Funciones del Ministerio Público de acuerdo a la Constitución Política de la República y su Ley Orgánica

El artículo 2 de la Ley Orgánica del Ministerio Público asigna a la institución las siguientes funciones, sin perjuicio de las que le atribuyan otras leyes:

- Investigar los delitos de acción pública y promover la persecución penal ante los tribunales, según las facultades que le confieren la Constitución, las leyes de la República, y los Tratados y Convenios Internacionales.
- Ejercer la acción civil en los casos previstos por la ley y asesorar a quien pretenda querellarse por delitos de acción privada, de conformidad con lo que establece el Código Procesal Penal.
- Dirigir a la policía y demás cuerpos de seguridad del Estado en la investigación de hechos delictivos.
- Preservar el Estado de derecho y el respeto a los derechos humanos, efectuando las diligencias necesarias ante los tribunales de justicia.

1.3.3. Organización

El Ministerio Público para cumplir con las funciones asignadas, se encuentra estructurado de conformidad con lo establecido en la Ley Orgánica del Ministerio Público y los acuerdos que emita el Consejo del Ministerio Público y, el Fiscal General de la República, de acuerdo a las facultades que le confiere su propia Ley Orgánica.

La estructura organizacional de esta institución está conformada por tres áreas, siendo éstas: fiscalía, investigaciones y administración.

1.4. Instituto Nacional de Ciencias Forenses de Guatemala (INACIF)

1.4.1. Descripción general del INACIF

Es el Instituto Nacional de Ciencias Forenses de Guatemala creado de la necesidad de unificar los servicios forenses periciales, mediante el desarrollo científico del trabajo que realiza como institución autónoma, garantizando la imparcialidad y confiabilidad de la investigación técnica científica y contribuyendo a la determinación de la prueba científica.

Se crea el Instituto Nacional de Ciencias Forenses de Guatemala, bajo el Decreto número 32-2006 del Congreso de la República. Podrá denominarse INACIF, a la institución auxiliar de la administración de justicia, con autonomía funcional, personalidad jurídica y patrimonio propio. Tiene competencia a nivel nacional y la responsabilidad en materia de peritajes técnicos científicos de conformidad con la presente Ley.

El INACIF tiene como finalidad principal la prestación del servicio de investigación científica de forma independiente, emitiendo dictámenes técnicos científicos.

1.4.2. Servicios ofrecidos

El INACIF, como una entidad de apoyo al sector justicia del país, pone a disposición servicios para las áreas técnico-científico en las materias forenses siguientes.

- Clínica forense
- Odontología forense
- Patología forense
- Antropología forense
- Psiquiatría-Psicología forense
- Biología forense
- Dactiloscopia forense
- Físico-Química forense
- Sustancia controladas
- Toxicología forense
- Documentoscopia y grafotecnia forense
- Identificación y reidentificación de vehículos
- Balística forense

1.5. La cadena de custodia

Es una herramienta de aplicación obligatoria, utilizada para asegurar la identidad, inalterabilidad y la integridad de la evidencia en todo el proceso legal. Por esta razón, en otros países se le conoce como Garantía de Autenticidad y consiste en la documentación cronológica de todos los pasos (investigaciones, análisis, laboratorios, estudios, etc.) que ha atravesado la evidencia (o los indicios) desde la recolección realizada por el embalador hasta su incorporación como prueba ante los tribunales y su respectiva deposición o destrucción.

Dicha documentación incluye la descripción a detalle de la evidencia, el registro exacto de fechas y horas, los nombres de personas (con credenciales de identificación), tanto de quien entrega como de quien recibe, nombres de los cargos o puestos, lugares, procesos de almacenamiento, transporte, etc. En otras palabras, cada persona por cuyas manos pase el indicio o evidencia debe

convertirse en un eslabón comprobable y verificable a través de marcas, sellos u otros medios de autenticación dentro de toda la cadena de custodia.

En este sentido, la evidencia nunca debe permanecer sin una persona que la vigile y cuide (i.e. custodia) en cada punto dentro de todo el proceso legal.

Para preservar la integridad de la evidencia a fin que pueda ser utilizada como prueba en los Tribunales de Justicia, ésta debe ser manejada con responsabilidad y cuidado, siguiendo un procedimiento plenamente establecido por objeto según sea el caso, a fin de evitar alegaciones que la puedan comprometer o la desvirtúen como prueba en el caso.

Esto último, debido a que es común que la contraparte legal ataque tanto al perito como a la evidencia o los estudios realizados sobre la misma en el sentido de contaminación, mal manejo, implantación fraudulenta, etc. a fin de sembrar la duda o desconfianza desde su recolección, su análisis hasta la incorporación de la misma en los estrados judiciales.

Por la razón anterior, es importante que el perito trabaje muy de cerca con el fiscal encargado del caso y se asesore apropiadamente respecto al manejo de la cadena de custodia y así seguir un procedimiento apropiado y tomar en cuenta hasta los detalles más sencillos, por ejemplo, una práctica común en Guatemala y otros países, indica que el embalaje se debe abrir por el lado o área que no ha sido firmado y sellado.

Todos estos conocimientos los irá adquiriendo el perito, tanto por experiencia propia como a través de consejos, directrices, indicaciones, etc., de otras personas.

Es esencial reconocer que debe existir una especialidad de perito por objeto a ser sometido a estudio, conservando no sólo el conocimiento técnico, las buenas prácticas, sino también la formación del principio de objetividad, parcialidad, unidad, ética y transparencia en los peritajes que se realicen.

1.6. Breve descripción de las áreas forenses

Debido del amplio espectro de la Informática y los requerimientos legales expuestos por los jueces, en la actualidad, el grado de especialización ha sido tal, que de acuerdo al campo de acción, ya se habla de las siguientes áreas o especializaciones en Informática forense, entre otras.

- Informática forense de Redes (*Network Forensics*)

Investigación delictiva realizada en la relación a delitos realizados en o con plataformas cliente-servidor así como los medios de comunicación en una red de computadoras, esto incluye el estudio de *routers*, *switches*, *firewalls*, etc. Se incluye aquí, el análisis de tráfico, *logs*, estudio de rutas, protocolos, puertos, *Chat*, correo electrónico, detección de intrusos, etc. Esta rama evolucionó grandemente luego del aparecimiento de *malware*, correo no solicitado (*spam*), alteración de sitios *web*, *hacking*, explotación de agujeros de *software*, etc. Su enfoque básico es la seguridad y la protección de información corporativa, lo cual ha provocado también la creación del área llamada respuesta a incidentes (*First Responders*) para hacerle frente a este tipo de ataques.

- Informática forense de Internet (*Internet Forensics*)

Parecido al anterior solamente que a un ámbito mucho mayor, el *Internet*. El enfoque de la investigación gira en torno a suplantación de identidad, pornografía y explotación infantil, fraudes, *phishing*, piratería, etc.

- Telefonía Forense (*Telephony Forensics* y *Mobile Phone Forensics*)

Investigación y prevención de delitos a través del análisis de dispositivos de comunicación telefónica, *logs* llamadas realizadas, tarjetas de almacenamiento (v.g. *sim*s, *SD*, *micro SD*, etc.), bitácoras de antenas de los proveedores de servicios, ubicación por triangulación, interceptar o intervenir llamadas, etc.

Dichas áreas se dividen en dos grandes secciones, de acuerdo al estatus del equipo tecnológico y los exámenes forenses a realizar, estas son, análisis en vida (o tiempo real) y análisis *post-mortem*. Un análisis en vida es aquel que se realiza en los equipos en el momento que están siendo violentados, empleados en la comisión del delito o bien se encuentran en el estado en que fueron usados (i.e. no han sido apagados ni utilizados luego del evento); esto garantiza un gran nivel de integridad de la evidencia, debido a que se ha mantenido la información residente en memoria principal (i.e. archivos en uso, procesos en ejecución, conexiones o puertos abiertos, archivos temporales, etc.), así como el estado de los *caches* u otros medios de almacenamiento volátil al momento en que ocurrió el incidente.

Contrario a lo anterior, el análisis *post-mortem* es aquel que se realiza en equipos informáticos, especialmente los de tamaño considerable, obtenidos a través del procesamiento de alguna escena o allanamiento y que han sido

apagados, embalados y llevados posteriormente para su estudio y análisis a los laboratorios respectivos para la búsqueda de información que pueda ser utilizada como evidencia.

Se exceptúan, bajo duda razonable, los dispositivos portátiles (especialmente *smartphones* y *PDA*s) en el sentido que deben permanecer encendidos si se considera que están protegidos por contraseña, debido a que si se apaga o reinicia es posible que se bloquee e impida el acceso a la potencial evidencia. Por esta razón, se debiera contar con una variedad de conectores de alimentación (ver capítulo tres), sino hubiera en el momento, se debe tomar una decisión de acuerdo a la pericia del técnico y los lineamientos del fiscal encargado del caso.

Para delimitar, el presente documento se enmarcó dentro del contexto de un análisis *post-mortem*, y adicionalmente, los procedimientos mostrados en los capítulos dos y tres están basados en sistemas operativos *Microsoft Windows* de 32 *bits* o con *set* de instrucciones basados en arquitecturas x86, que actualmente son los más comunes en nuestro medio, esto no menoscaba que los mismos puedan generalizarse a otras plataformas tomando en cuenta las diferencias naturales existentes entre las mismas (v.g. el sistema de archivos, diferencias entre *kernels*, manejo de memoria, etc.).

1.7. Objetivos del laboratorio de Informática Forense

- Objetivo general

Realizar los estudios y análisis correspondientes a los equipos, medios o dispositivos tecnológicos remitidos por la Fiscalía a fin de encontrar información

que pueda ser empleada como evidencia en el esclarecimiento de un caso y tenga valor eficaz como elemento de prueba en los Tribunales de Justicia.

- Objetivos específicos
 - Realizar los procesos periciales con la ética y profesionalismo inherentes al sistema de Justicia.
 - Aplicar en cada caso, un manejo apropiado de los indicios y evidencias, el empleo de herramientas aprobadas, el uso de métodos acordes enmarcados en una cultura de buenas prácticas, y la atención en el detalle en la documentación, tanto de los procedimientos como de los análisis realizados.
 - Mantener una evolución continua a la par de los avances tecnológicos, promover la certificación de procesos y el control de calidad, estar al día respecto la publicación de leyes y estándares, sostener un adiestramiento y capacitación constante.
 - Realizar los informes y dictámenes basados en los principios de objetividad, imparcialidad y transparencia, y ratificar los mismos ante los tribunales, cuando sea requerido.

2. PROCESOS REALIZADOS EN UN LABORATORIO DE INFORMÁTICA FORENSE

2.1. Normas y políticas a seguir para la realización de peritajes informáticos

Normas inherentes a los peritos

Estas son las normas personales y laborales más importantes que deben poseer los técnicos en la realización de peritajes.

- **Integridad:** debe cumplir con rectitud los deberes de su cargo y estar comprometido con altos valores y principios, reconociendo que su trabajo ayudará a encontrar la verdad y por lo tanto no debe aceptar ningún tipo de presión que altere o produzca un sesgo en los resultados.
- **Confidencialidad:** se debe respetar la confidencialidad de los estudios y análisis que realice. Tanto los resultados como el descubrimiento de otro tipo de información, debe mantenerse en privado y ser conocida solamente por el fiscal del caso.
- **Imparcialidad:** el técnico no debe dejarse influenciar por sus sentimientos, hechos pasados, comentarios, etc., es decir debe ser objetivo.
- **Idoneidad:** debe poseer conocimientos y habilidades que garanticen la calidad del trabajo y debe mantener dicha capacidad con la formación

profesional continua correspondiente. Esto incluye poseer un acervo básico de tópicos legales relacionados con su trabajo (v.g. Propiedad intelectual, patentes, privacidad, perjurio, etc.).

- Independencia: el técnico no debe tener ninguna relación de afinidad con la institución o persona que se está investigando. Debe mantenerse fuera del caso y por consiguiente de todos los estudios y conclusiones de los análisis.
- Competencia: debe ser hábil dentro de los límites de su especialidad y por tanto, no deben aceptar trabajos que estén fuera de su área de competencia, especialmente si existen departamentos con especialistas o expertos en la materia en el laboratorio. Esto debido al manejo que se hace en tribunales respecto a las competencias de los peritos.

Normas inherentes a los procesos

Estas son las normas que deben cumplirse para la realización de los procesos, unas son de carácter legal y otras de carácter técnico.

- Documentación legal: el perito debe tener por lo menos una copia de los documentos que amparen la solicitud del trabajo que incluya la descripción de los equipos, marcas, modelos, números de serie, etc., fecha y hora; y el aval o el consentimiento de la autoridad correspondiente a fin de evitar violaciones de cualquier tipo.
- Documentación de caso: debido a que el contenido de los medios de almacenamiento puede ser abrumador, se debe proveer de ciertos elementos de búsqueda con la finalidad de disminuir los tiempos de

realización del análisis, esto especialmente en aquellos archivos que contengan caracteres (números, letras, símbolos, etc.) definidos, por ejemplo documentos elaborados con procesadores de palabras, editores, hojas electrónicas, etc. Datos como: nombres, apodos, direcciones, números de teléfonos, etc., pueden ser útiles.

En algunos casos, la descripción del uso del dispositivo también puede dar pautas para la búsqueda y descripción de procesos o *software* particular instalado en los equipos. Contar con herramientas de indexación también resulta útil para la realización de búsquedas rápidas.

- Buenas prácticas: se debe poseer el entrenamiento apropiado de los procedimientos de la cadena de custodia: el manejo de los sellos, la apertura del embalaje, etc., recordando que un mal procedimiento en el manejo de la misma provoca la invalidez de la evidencia.
- Plan de trabajo: Deben existir planes de trabajo para los equipos conocidos, así como crearse los respectivos ante el apareamiento de nuevas tecnologías.
- Vestimenta adecuada: siempre se debe utilizar la indumentaria apropiada antes de realizar el trabajo: guantes, gafas protectoras, batas, etc.
- Inalterabilidad de la evidencia: nunca debe alterarse el objeto (indicio) sobre el cual se realizarán los estudios. Especialmente, en el caso de los medios de almacenamiento, por esta razón, debe recurrirse a la realización de un bloqueo contra escritura del medio y luego debe realizarse una copia exacta (imagen *bit* por *bit*), autenticada por un procedimiento o algoritmo estándar (v.g. función *Hash*).

Esto último se ejecuta tanto en el original como en la copia y en ambos casos, el valor retornado por la función hash debe ser igual, lo que garantiza la copia como fiel.

La probabilidad que un valor *hash* sea igual con información diferente es muy pequeña y tiende a cero mientras más bits significativos se utilicen. Aunque las funciones *Hash* – especialmente *MD5* y *SHA-1* - se han utilizado desde hace mucho tiempo para identificar si un archivo ha sido modificado, existe el problema que éste, no nos dice en cuanto y si consideramos que los archivos están en medios magnéticos se vuelve un problema demostrar que un archivo no ha sido modificado por algún campo magnético cuando el *hash* ya no coincide.

Especialmente si el valor de un *bit* cambiado particular era de un espacio en blanco – es decir, no cambia el contenido del archivo -. De aquí la importancia de manejar los equipos (evidencia) en medios estériles y libres de contaminación de cualquier tipo, especialmente magnetismo. Si así no fuere el caso se debería utilizar otro medio de autenticación. Finalmente, debido a las colisiones previstas para el *SHA-1*, *NIST* recomienda la utilización de la familia del *Hash SHA-2* (*SHA-224/256/384/512*).

También deben considerarse los siguientes cuidados.

- De preferencia, no se debe iniciar (*booting*), el equipo considerado evidencia, desde el sistema operativo instalado en el aparato a investigar.

- Realizar un examen profundo de elementos indeseables o códigos maliciosos (*malware*), que puedan infectar los equipos forenses o disparar eventos destructivos como eliminación de información.
- En el caso de dispositivos portátiles: celulares, computadores de bolsillo, asistentes personales, cámaras digitales, *smart-phones*, *tablets*, y otros, si el aparato está apagado no debe encenderse hasta que se cuente con un medio de alimentación eléctrica; si el dispositivo está encendido, debe preservarse en ese estado debido a que si se apaga o reinicia es posible que se bloquee e impida el acceso a la potencial evidencia; la decisión de encender o apagar el aparato debe basarse en los conocimientos y experiencia del perito, debido a que existen dispositivos que preservan información en tanto haya energía en la batería del mismo.
- Si por alguna razón, se deba trasladar el contenido de un medio de almacenamiento, se debe considerar el riesgo que ésta pueda ser extraviada o robada, por lo tanto, como norma general, se debe obtener una copia de la misma y protegerla a través del uso de encriptación o cifrado con un método aprobado.
- Siempre se debe tener a mano los instrumentos de documentación respectivos (formularios, listas de chequeo, cronogramas, cámaras fotográficas, video-cámaras, etc.). Las fotografías y videos deben incluir dentro de los mismos objetos de referencia dimensionales. Para esto último comúnmente, se utilizan reglas o cintas métricas.
- Si el aparato (evidencia) es de reciente tecnología o si está protegido con algún artificio (contraseña o encriptación) que hace que éste sea imposible

de investigar utilizando los equipos actuales del laboratorio se debe solicitar ayuda o asesoría externa con la consiguiente certificación.

Nunca tratar a base de prueba y error con la evidencia. Esto mismo puede ser aplicable cuando la capacidad instalada del laboratorio ha sido superada por la demanda, en este tipo de casos, probablemente se tendrá que tomar en cuenta la colaboración de laboratorios foráneos.

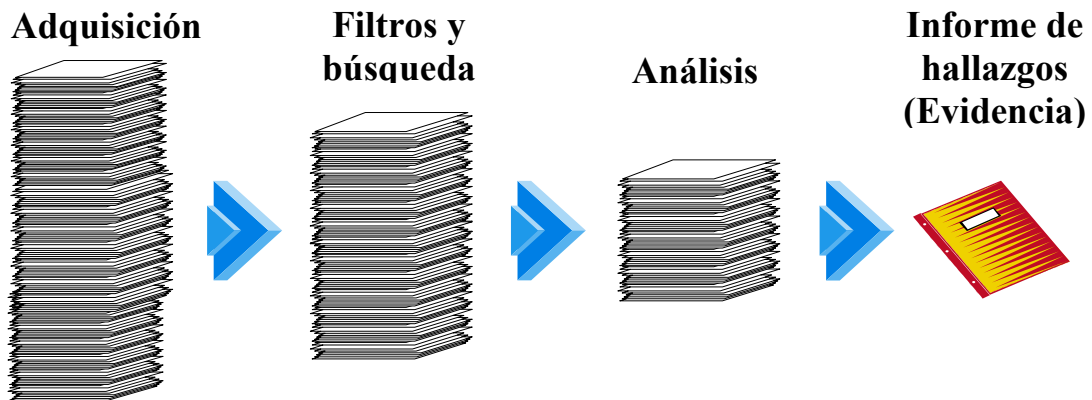
2.2. Descripción general de los procesos y procedimientos

El objetivo principal de los procesos forenses es encontrar evidencia que brinde los elementos necesarios para establecer un hecho o evento delictivo, en aras de producir un veredicto que conduzca a la ejecución efectiva de la justicia.

Dentro del proceso forense, luego de la identificación, preservación y recolección continúa la búsqueda y análisis. Esto se realiza dentro del laboratorio y es el tópico principal del presente capítulo.

La figura 2 muestra lo arduo que resulta la obtención de la evidencia, porque para descubrirla, previamente se ha pasado por un proceso de extracción de una cantidad exuberante de datos en forma de archivos, programas, bitácoras, configuraciones, recuperación de objetos eliminados y ocultos, etc., los cuales luego se deben filtrar a través de búsquedas de cadenas de texto, revisión de contenidos, exploración y escaneo de data-objetos, etc. a fin de obtener la valiosa evidencia.

Figura 2. **Adquisición, filtrado y análisis de data-objetos para la obtención de evidencia**



Fuente: basado en *Electronic crime scene investigation. National Institute of Justice* p. 22.

Por lo anteriormente descrito, es imperativo que el perito tenga una comunicación directa y constante con el fiscal de caso a fin de realizar el filtrado de una forma más eficiente y eficaz, esto permitirá plantear la hipótesis, que ofrecerá pautas adicionales de análisis y permitirá realizar la búsqueda de evidencia con más enfoque.

Todo peritaje forense contiene los siguientes elementos: los equipos o dispositivos digitales a investigar, los datos provistos por el fiscal (para la formulación de hipótesis y búsquedas), las herramientas forenses, el equipo de documentación, el conocimiento técnico de los peritos y la asesoría legal.

Los procesos mostrados utilizan dispositivos particulares y adecuados para la realización de cada tarea. Sin embargo, en los capítulos tres y cuatro se hace mención de la utilización de computadoras especializadas que tienen instalados de fábrica dichos dispositivos, por ejemplo, algunos equipos contienen bloqueadores de disco duro, lector multi-tarjetas, *USB*, *firewire*, etc.,

poseen adaptadores para diferentes tipos de conexiones y disponen del *software* pre-instalado apropiado para la obtención de imágenes y la realización del análisis. Estas estaciones, simplificarán el trabajo y requerirán de la adaptación de los procesos mostrados.

Los procesos contemplados consideran los siguientes aspectos:

- Análisis post-mortem: como se mencionó en el capítulo uno de este trabajo, todos los procesos están orientados al análisis *post-mortem* de los equipos y son una guía general (diagramas propuestos) para la realización de los mismos, debido a que cubrir cada caso sería prácticamente imposible por todas las variantes que existen y la actualización tanto de la tecnología como de las herramientas forenses.
- Indicios considerados: computadoras personales (*laptops, netbooks, desktops, tablets, etc.*), asistentes personales, celulares; dispositivos de almacenamiento: discos duros; tarjetas *SD, MMC, CF, USB flash, etc.*
- El presente documento, no es un manual paso a paso para la utilización de las tecnologías a las que se haga referencia dentro del mismo, ni es un manual de usuario de *software*. Es simplemente una guía de los procesos más comunes realizados en un laboratorio de Informática Forense.
- Se asume dentro de cada proceso que los indicios fueron llevados al almacén con la documentación respectiva (i.e. cadena de custodia, solicitud de peritaje, consentimientos, órdenes, etc.) y están a la espera de ser asignados a la unidad o perito para ser procesados o analizados.

- Los diagramas no contemplan los procesos realizados cuando los indicios son enviados a laboratorios externos o la intervención de consultores foráneos (cuando el laboratorio no pueda cubrir el estudio por nuevas tecnologías, indicios fuertemente encriptados, capacidad instalada, etc.).
- El laboratorio debe contar con un sistema informático de seguimiento de casos, el cual debe contener los registros de quién y qué pruebas, o análisis se han realizado en los indicios y las fechas en que se ha efectuado, debe permitir programar y asignar recursos de laboratorio y debe funcionar de tal manera que se conozca en qué etapa y en qué unidad se encuentra la evidencia en cualquier momento.
- En el caso de dispositivos de almacenamiento como: cintas magnéticas, cartuchos, arreglos de redundancia de discos independientes (*Redundant Array of Independent Disks – RAID*), dispositivos de registro de posicionamiento global (*Global Positioning System - GPS*), *Smartphones*, etc., éstos no están contemplados en el presente trabajo, sin embargo, algunos principios mostrados en los diagramas pueden ser aplicables. Inclusive, por abstracción puede ser adaptable a otras plataformas como *Linux, WinMobile, Symbian, Android, etc.*
- En algunos países se recurre a los laboratorios de Informática Forense para la obtención de información proveniente de dispositivos o medios de almacenamiento dañados o semi-destruidos, esto requiere de ciertas pericias y equipos que están fuera del ámbito de cobertura del presente trabajo.

Para la realización de los procesos, el laboratorio debe contar con las áreas mostradas en la tabla I.

Tabla I. Descripción de las áreas de procesamiento de evidencia del laboratorio

No.	Área	Descripción
1	Almacén de indicios/evidencias	<p>Área donde ingresan los indicios y la papelería legal, se asigna un código de seguimiento en el sistema informático y se almacenan apropiadamente, tanto los indicios como las imágenes ya analizadas que serán utilizadas por la parte solicitante (v.g. la fiscalía)</p>
2	Reconocimiento de indicios	<p>Área donde se clasifican los indicios de acuerdo a su tipo (<i>PCs</i>, celulares, <i>PDA</i>s, <i>tablets</i>, etc.) y se distribuyen a los diferentes peritos de acuerdo a la especialidad, experiencia, prioridad, etc. Esta área también realiza lo siguiente:</p> <ul style="list-style-type: none"> • Define los procedimientos y el cronograma a seguir • Solicita colaboración o asistencia foránea, cuando el caso lo amerita • Cancela el peritaje debido a incongruencias de papelería respecto a indicios, o bien cuando el laboratorio no cuenta con las herramientas y mecanismos necesarios para la búsqueda y el análisis de la evidencia y no se ha podido obtener asistencia externa
3	Laboratorio	<p>El laboratorio incluye las áreas de obtención de imágenes y el área de análisis. Los procesos que se realizan en éste son:</p> <ul style="list-style-type: none"> • Documentación de inventario de <i>Hardware</i> y obtención de imagen <i>bit por bit</i> • Documentación del inventario de <i>Software</i> del equipo (Sistema Operativo, <i>drivers</i>, aplicaciones, procesos, otros)

Continuación tabla I.




	<ul style="list-style-type: none"> • Análisis de arquitectura y estructura de los medios de almacenamiento (sistema de archivos, directorios, particiones, <i>slacks</i>, fragmentos, etc.) • Análisis de eventos (bitácoras e historiales) • Recuperación de objetos eliminados • Recuperación de data-objetos ocultos • Indexación, exploración y búsqueda de cadenas (<i>strings</i>) • Conversiones • Deposición y esterilización de medios • Elaboración de dictámenes e informes
--	--

Fuente: elaboración propia

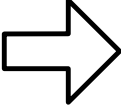
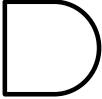
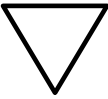
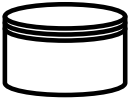

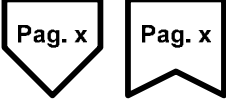
2.2.1. Diagramas de flujo

Para representar los procesos se recurre a la utilización de diagramas de flujo, los que muestran la secuencia de actividades que siguen los indicios para la obtención de la evidencia. La notación se muestra en la tabla II.

Tabla II. **Descripción de la simbología utilizada en los diagramas de flujo**

SÍMBOLO	NOMBRE	DESCRIPCIÓN
	Inicio y Final	Marca el comienzo o la finalización de los procedimientos.
	Documentación	Indica procedimientos de llenado de formularios, cadena de custodia, levantado de actas, etc.
	Operación	Es utilizado cuando se realiza algún proceso, actividad o análisis en el indicio o la evidencia

Continuación tabla II.

	Transporte	Se utiliza cuando el indicio o evidencia es trasladado (a laboratorio, almacén, externo, etc.).
	Demora	Indica cuando el indicio o evidencia debe esperar por una razón no planificada la continuación al siguiente proceso (v.g. espera de un dictamen o una aprobación).
	Almacenamiento	Se utiliza este símbolo cuando el indicio/evidencia es almacenado, archivado o protegido en un sitio.
	Sistema Informático	Indica el momento en que se ingresa información o se consulta la base de datos del sistema informático.
	Conector en página	Representa una conexión o enlace de una parte del diagrama de flujo con otra parte del mismo dentro de la misma página.
	Conector fuera de página	Estas figuras se utilizan para representar la continuación del diagrama de flujo en otra página. La primera figura indica que el diagrama continúa en la página x mientras que la segunda indica que viene de la página x.

Fuente: <http://www.eduteka.org>

2.2.2. Diagramas de proceso

A continuación se muestran los diagramas de los procesos básicos a realizar en el laboratorio de Informática Forense. Éstos deben contemplarse únicamente como modelos o plantillas para la elaboración posterior de diagramas más específicos de acuerdo a las necesidades particulares, reformas en las leyes, cambios en las metodologías aprobadas, actualizaciones en tecnologías, etc.

Proceso 1: entrada y registro de indicios

Descripción: Recepción de indicios y papelería respectiva. Llenado de formularios de seguimiento y cadena de custodia. Apertura del embalaje para corroboración del contenido con la documentación y la descripción de los objetos. Asignación del código de seguimiento en el sistema informático. Almacenamiento apropiado y asignación al laboratorio o técnico particular. Respecto a la existencia de incoherencia en la papelería, se debe rechazar el ingreso al almacén hasta que los errores sean corregidos.

Algunos autores no recomiendan la apertura de sellos en estas instancias (ingreso al almacén), sin embargo, la tendencia en seguridad antiterrorista actual (por explosivos, sustancias biológicas, agentes químicos, etc.) hace que esto sea necesario, considerando el gran daño que causaría una bomba dentro del almacén, en relación a la integridad de las personas y las evidencias almacenadas. El laboratorio tendrá que consensuar respecto a esta decisión. En el presente trabajo se ha optado por la seguridad al ingreso de los embalajes o contenedores.

Área encargada: Almacén de indicios/evidencias

Instrumentos, herramientas y materiales utilizados:

- Cuchillas, cortadoras, tenazas y tijeras
- Utensilios de oficina, formularios y papelería respectiva
- Guantes de látex, pulsera antiestática, gafas, bata, etc
- Lupas
- Carretillas

Proceso 2: identificación del indicio y asignación de laboratorio y perito

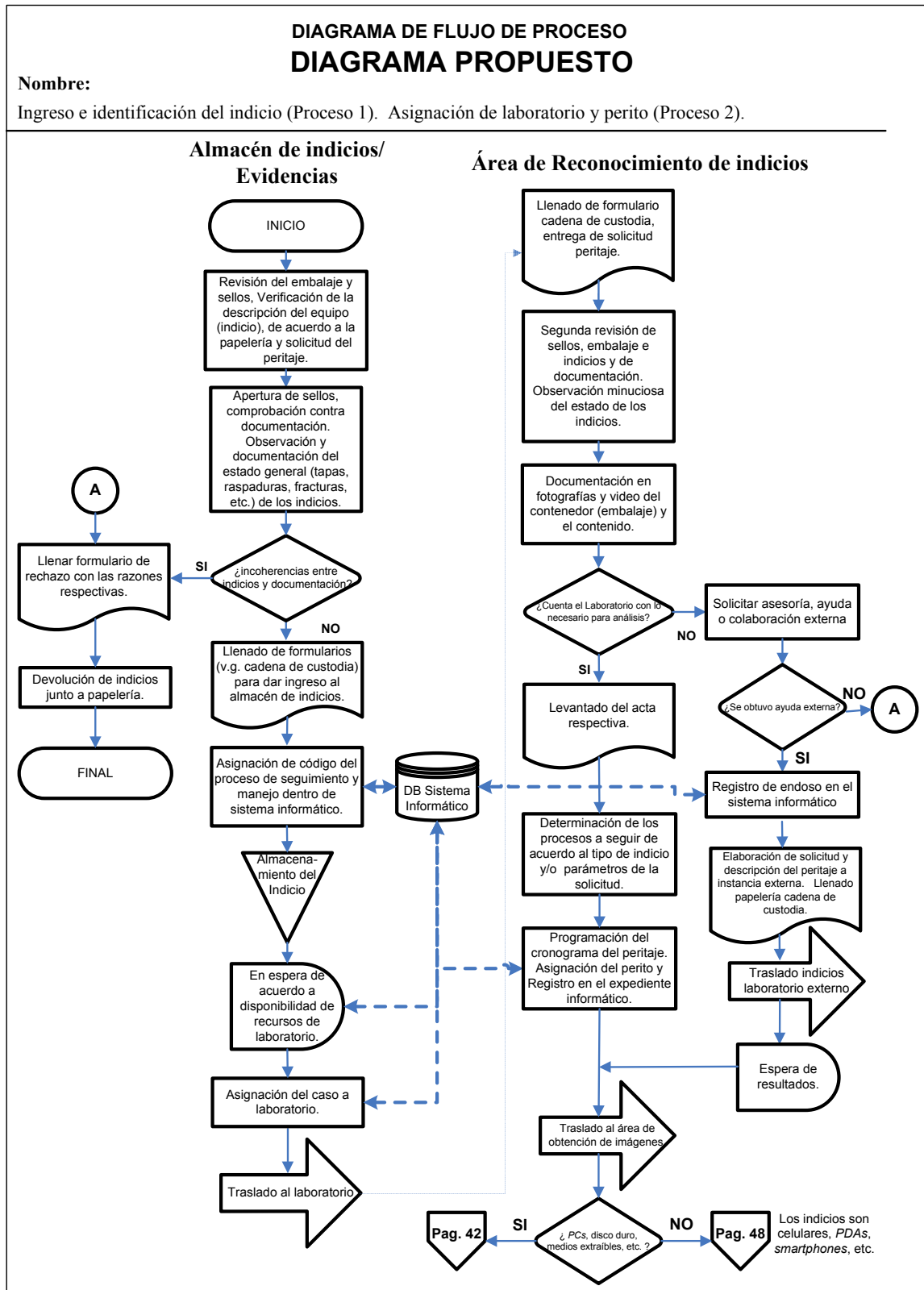
Descripción: determinación de los análisis a realizar sobre los indicios de acuerdo a su tipo (*PCs*, celulares, *PDA*s, *tablets*, dispositivos de almacenamiento, etc.). Comprobación de capacidad de respuesta del laboratorio respecto al caso específico y gestión de transferencia a entidades externas cuando no se tenga la facultad. Esto último cuando el objeto a analizar posee características complejas de analizar, por ejemplo, sistemas de protección por contraseña o encriptación, nuevas tecnologías, carencia de instrumentos apropiados (certificados), capacidad instalada, restricciones técnicas del *staff*, etc.

Área encargada: identificación del indicio

Instrumentos, herramientas y materiales utilizados:

- Cuchillas, cortadoras, tenazas y tijeras
- Utensilios de oficina, formularios y papelería respectiva
- Guantes de látex, pulsera antiestática, gafas, bata, etc
- Lupas
- Cámaras de video y fotografía
- Carretillas

Figura 3. Diagrama procesos 1 y 2



Proceso 3: Documentación del básica del *hardware* y obtención de imágenes de disco duro

Descripción: éste consiste en la elaboración de un informe general del *Hardware* del equipo a analizar, así como la obtención de una imagen exacta –en medios estériles - de los discos duros encontrados en los equipos y su autenticación respectiva. Esto garantizará la integridad del indicio y servirá para realizar los estudios, análisis y pruebas en el laboratorio. Este proceso continúa luego del reconocimiento de indicios y puede ser aplicable cuando en el embalaje vienen solamente los discos duros.

Esto incluye, la obtención de las imágenes de las siguientes áreas².

- El espacio no asignado (*Unallocated space*): espacio en un medio electrónico que en el momento no está siendo ocupado o utilizado por ningún archivo activo dentro del sistema de archivos. La revisión de esta área es muy útil, debido a que puede contener información remanente o residual de archivos que previamente ocupaban dicho espacio.
- *File Slack* (espacio de holgura o sobra): espacio comprendido entre el final lógico de un archivo y el final de la unidad de asignación (*cluster*) para dicho archivo. Éste al igual que el anterior, puede contener potencialmente información que residía en ese espacio y que fue eliminada o movida.
- Espacio no particionado: espacio vacío en un medio de almacenamiento que no es parte de ninguna partición, es decir, el área comprendida entre la suma de las áreas particionadas y el 100% de espacio del medio. Por ejemplo, en los discos *IDE* y *SATA* pueden existir áreas protegidas (*HPA*,

² Ver TANENBAUM, Andrew; WOODHULL, Albert. Sistemas Operativos, diseño e implementación.

Host Protected Area o *DCO, Device Configuration Overlay*) que se pueden utilizar para ocultar información del sistema operativo. La lectura de estas áreas, comúnmente, se realiza a través de aplicaciones especiales.

La esterilización de discos duros puede realizarse con variadas aplicaciones (v.g. *wipers, shredders, sanitizers*, etc.). Por ejemplo, recurriendo a productos como *Darik's Boot and Nuke* (<http://www.dban.org/>), *SecureErase* (<http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml>), *Active@KillDisk* (<http://www.killdisk.com/>), etc. Sin embargo, la administración del laboratorio puede generar las políticas adecuadas dependiendo del tiempo a invertir en la(s) esterilización(es) y su respectivo grado de confiabilidad, la cantidad de discos a utilizar, etc., de tal forma que se elija desde un simple formateo rápido hasta esterilización basada en estándares del Departamento de Defensa de Estados Unidos (*DOD Standards*).

Finalmente, la media original puede contener errores (v.g. sectores dañados) los que probablemente darán alguna falla al momento de obtener la imagen. Esto no es cubierto dentro del presente material y se sugiere la investigación respectiva.

Área encargada: Obtención de imágenes

Instrumentos, herramientas y materiales utilizados:

- Destornilladores y/o llaves de puntas (*Allen, Phillips*, hexagonales, etc.)
- Guantes de látex, pulsera antiestática, gafas, bata, etc
- Protector anti escritura de disco (*HD Write Blocker*)
- Medio de almacenamiento estéril (vacío o recién formateado)

- Computadora forense: la que se utiliza para realizar los procesos de investigación; contiene el *software* especial para el trabajo (creación de imágenes, indexadores, herramientas de búsqueda, etc.)

Aunque existen otros métodos y varios productos de diferentes marcas para la obtención de imágenes de disco (v.g. Protección de escritura por *software*), en el presente trabajo se ha optado por el más aceptado: la utilización del bloqueador de disco duro (*hard-disk write blocker*) y un producto de obtención de imágenes (por ejemplo, dependiendo del sistema operativo, *FTK, Forensic ToolKit; EnCase, ILook*, etc.)³. Debido a que estos productos vienen como una suite, incluyen otras bondades muy útiles, por ejemplo, reconocimiento de virus, ordenamiento de archivos por tipo, indexación y búsqueda.

Respecto la obtención de imágenes, existen productos que pueden trabajar con varios discos simultáneamente (ver <http://www.ics-iq.com/> y <http://www.diskology.com>), la elección de éstos dependerá, tanto de la carga del laboratorio como del presupuesto asignado. El presente documento muestra solamente el proceso para la obtención de una imagen a la vez.

³ Ver <http://www.accessdata.com/forensictoolkit.html>, <http://www.guidancesoftware.com/>, <http://www.perlusto.com/>.

Proceso 4: obtención de imágenes de medios de almacenamiento extraíbles

Descripción: éste se utilizará para la obtención de imágenes de media extraíble (por ejemplo, tarjetas *SD*, utilizadas en *PDA*s, *Memory Stick* usadas para guardar información proveniente de cámaras fotográficas o video, memorias *USB flash*, etc.). Este proceso se realiza luego del reconocimiento de indicios (Proceso 2).

Área encargada: obtención de imágenes

Instrumentos, herramientas y materiales utilizados:

- Computadora forense
- Aparato lector multi-tarjeta

Para la obtención de imágenes de medios extraíbles de almacenamiento (*SD*, *MMC*, *CF*, etc.), se debe utilizar un dispositivo lector multi-tarjeta considerando el bloqueo contra escritura de los mismos.

- Bloquearlos: utilizando el pestillo (si hubiera) para evitar la escritura en los mismos. La figura 4 muestra el lugar donde se encuentra este pestillo en las tarjetas *SD* (*Secure Digital*), *CF* (*Compact Flash*) y la *Memory Stick*.

Figura 4. Distintos tipos de tarjetas de almacenamiento



Fuente: <http://www.wikipedia.org>

- Recurrir a modificaciones del registro⁴ de la computadora forense, en caso de que esta sea *Windows*; esto funciona especialmente para conexiones lectores multi-tarjeta con conexión *USB*.
- Utilizando herramientas de *hardware* como la mostrada en la siguiente figura 5.

Figura 5. **Multi-lector y bloqueador de tarjetas**



Fuente: <http://www.tableau.com>

El Producto mostrado en la figura 5 (*Tableau, TDA8-M*), ofrece bloqueo para los medios: *CompactFlash I y II, SmartMedia, Memory Stick, Memory Stick PRO, Memory Stick DUO, Memory Stick PRO DUO, Micro Drive, Multimedia Card, SD, MINI SD, SDHC, y XD flash memory*. Las memorias *USB flash* también necesitan un producto similar como el *Tableau T3458is* (figura 6), que además de bloquear discos con conectores *SATA, SCSI e IDE*, también permite la protección contra escritura de memorias *USB*.

⁴ Ver http://www.accessdata.com/media/en_US/print/papers/wp.USB_Write_Protect.en_us.pdf

Figura 6. Lector y bloqueador de tarjetas conexiones **USB/SATA/SCSI/IDE**



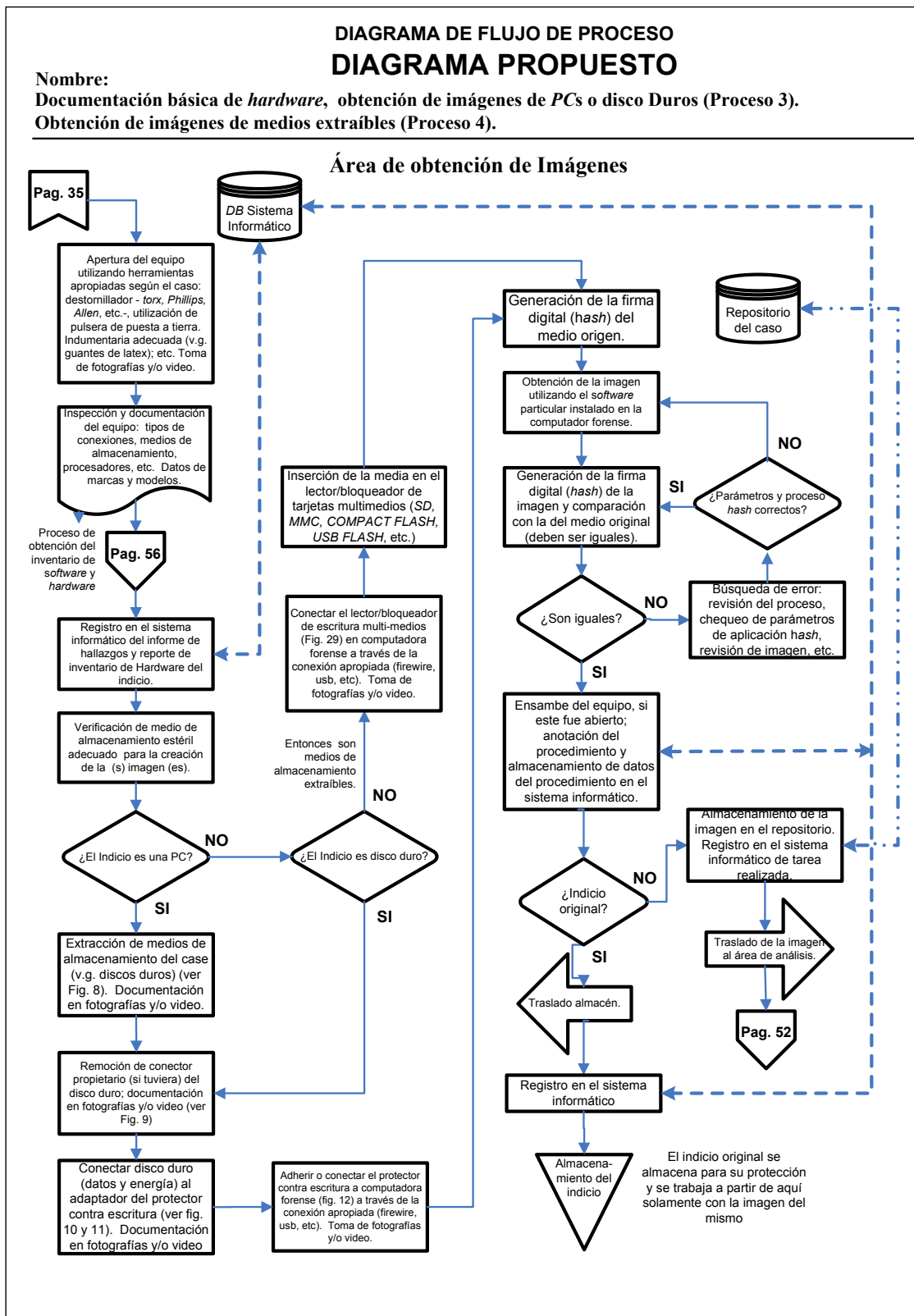
Fuente: <http://www.tableau.com>

Además de los productos *Tableau*, existen muchas otras empresas que ofrecen productos similares. Aquí se mencionaron éstos, simplemente porque son soluciones comunes en el ámbito forense.

Si se tuviera que extraer la imagen de medios de almacenamiento antiguos o *legacy* como *diskettes* (8,0, 5,25 o 3,5 pulgadas), cintas magnéticas, cartuchos, etc., se sugiere la investigación respectiva, tanto para el bloqueo como para la obtención de la imagen. En el presente trabajo solamente se ha tratado con los medios más comunes en la actualidad.

Finalmente, se debe obtener para cada original e imagen, una certificación que garantice la confiabilidad de autenticidad de la mismos (huella digital), para esto se recurrirá a la familia de funciones *hash*, tomando en cuenta que mientras mayor sea el nivel de confiabilidad (seguridad) requerido, mayor será el tiempo invertido. Así, se podría optar por el modesto pero rápido *MD* (*Message-Digest algorithm*, especialmente el *MD5*) o bien, aunque más lento, por el estándar promovido por *NIST* (*SHA*, especialmente el *SHA-2*).

Figura 7. Diagrama procesos 3 y 4



Fuente: elaboración propia.

Imágenes de referencia del proceso anterior:

Figura 8. **Disco duro extraído**



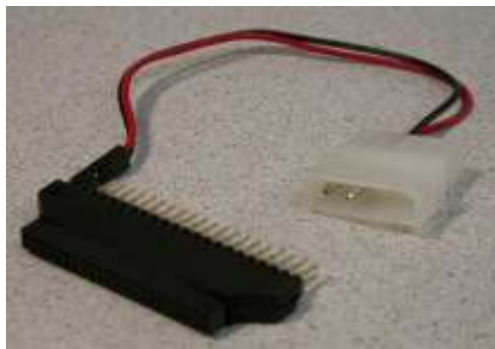
Fuente: <http://www.tableau.com>

Figura 9. **Remoción conector propietario**



Fuente: <http://www.tableau.com>

Figura 10. **Adaptador de datos y energía**



Fuente: <http://www.tableau.com>

Figura 11. **Conexión disco duro a bloqueador**



Fuente: <http://www.tableau.com>

Figura 12. **Conexión disco duro-bloqueador-computadora forense**



Fuente: <http://www.tableau.com>

Proceso 5: obtención de información de celulares y *PDA*s (*handhelds*)

Descripción: la obtención de información de celulares y *PDA*s es uno de los procesos más comunes realizados por los laboratorios de Informática Forense alrededor del Mundo, debido a la gran cantidad de usuarios que existen actualmente y por el constante atractivo que brinda su versatilidad. Existen ciertas similitudes entre los mismos, especialmente por la forma de sincronización con las computadoras, el manejo de archivos y los mecanismos agregados. Por ejemplo, éstas son algunas características, tanto de los aparatos como de los servicios ofrecidos por los proveedores.

- Incorporación de mecanismos: se han añadido a ambos productos cámaras fotográficas y de video, reproductores de audio/video, sintonizadores de radio, etc. Esta tendencia ha sido muy notoria al fusionar los celulares con los *PDA*s (teléfonos inteligentes o *smartphones*), produciendo así, que ahora éstos posean virtudes como administración de información personal (*PIM, Personal Information Management*), agendas, hojas electrónicas, procesadores de palabras, base de datos, etc.
- Incremento de capacidades: cada día los celulares cuentan con mayor memoria tanto interna como externa a través de ranuras de expansión, mayor resolución de captura de imágenes, habilidad de conexión a otras redes telefónicas o inalámbricas por medio de dispositivos infrarrojo, *bluetooth, WiFi*, etc.
- Aumento y mejora de servicios: actualmente es común encontrar los siguientes servicios para celulares: *SMS* (servicio de mensajes cortos, *Short Message Service*), *MMS* (servicio de mensajería multi-media, *Multi-Media Messaging Service*), correo electrónico, navegación en *Internet, IM*

(mensajería instantánea, *Instant Messaging*), conferencia, posicionamiento global (*GPS*), etc., incluyendo el mejoramiento en las tecnologías de velocidad de transferencia, por ejemplo, *GPRS (General Packet Radio System)*, *EDGE (Enhanced Data Rates for Global Evolution)* y todas las variantes (o generaciones) *G (1G, 3G, 4G, etc.)*, y muchas más.

Por todas estas razones, la cantidad de información contenida en estos dispositivos puede ser mayor de lo esperado y por lo tanto, para la obtención de información de celulares y/o *PDA*s se debe recurrir a un procedimiento especial y a la utilización de herramientas informáticas de *software* y *hardware* certificadas, que permitan conectarse a los equipos (sincronizadores) y obtener información de las diferentes memorias que éstos poseen (*RAM, ROM, FileStore* y tarjetas de memoria externa), para la búsqueda de evidencia (lista de contactos, bitácora de llamadas, archivos personales, etc.).

Adicionalmente, de acuerdo al estado en que se encuentre el dispositivo móvil se deben tomar en cuenta las siguientes indicaciones.

- Si el dispositivo está en el estado de nacimiento (*Nascent state*), como cuando se recibe de fábrica, se ejecuta un *hard reset* o el dispositivo se queda sin carga. Se debe analizar la media externa insertada, y si éstas no contienen nada se debe tratar de recuperar del formateo anterior.
- Si el dispositivo está en estado inactivo (*Quiescent state*), éste aún posee información en memoria activa que puede ser útil.
- El dispositivo puede pasar a un estado activo por la activación de algún evento, comúnmente provocado por aplicaciones relacionadas con el tiempo (alarmas, cuentas regresivas, calendarios, etc.). Esto provoca un

consumo de batería que puede resultar en agotamiento de la energía, especialmente si el evento hace utiliza la pantalla o el sistema de audio. Quedaría a discreción del perito dar prioridad a la desactivación de estas opciones con la aprobación legal respectiva.

Finalmente, si en un caso particular no se tienen los cables apropiados, se debe solicitar a la jefatura o gerencia del laboratorio para la adquisición respectiva. Sin embargo, si no se lograra conseguir se puede recurrir a métodos alternos (opciones inalámbricas o procedimientos manuales) con el aval de la asistencia legal correspondiente (fiscal, juez, asesoría técnica jurídica de laboratorio, etc.).

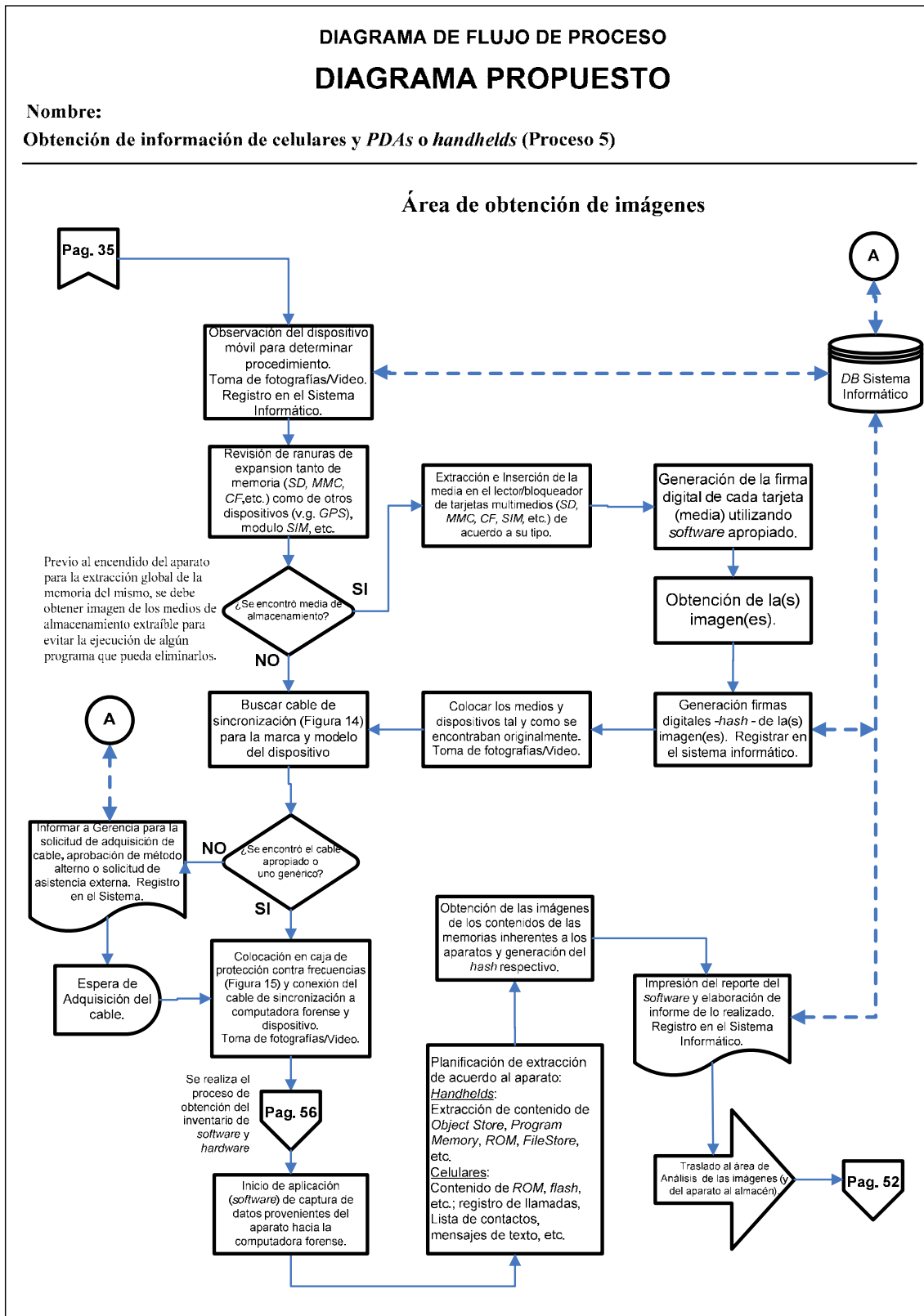
Como se mencionó previamente, el enfoque del trabajo es hacia equipos con plataformas *Windows* (*WinCE*, *PocketPc 200X*, *Windows SE* o *Windows Mobile X*) o dispositivos móviles (*PDA*s y celulares) que aunque estén basados en otros sistemas operativos se pueden analizar con herramientas de *software Win32*. Para sistemas operativos *Symbian*, *PalmOS*, *MacOS* (v.g. *iOS*), *Android*, etc., deben efectuarse los estudios particulares correspondientes.

Área encargada: Obtención de imágenes.

Instrumentos, herramientas y materiales utilizados:

- Cables de sincronización
- *Software/hardware* de captura de dispositivos móviles
- Computadora forense
- Bolsa bloqueadora de radio-frecuencias
- Dispositivo lector de tarjetas *SIM*

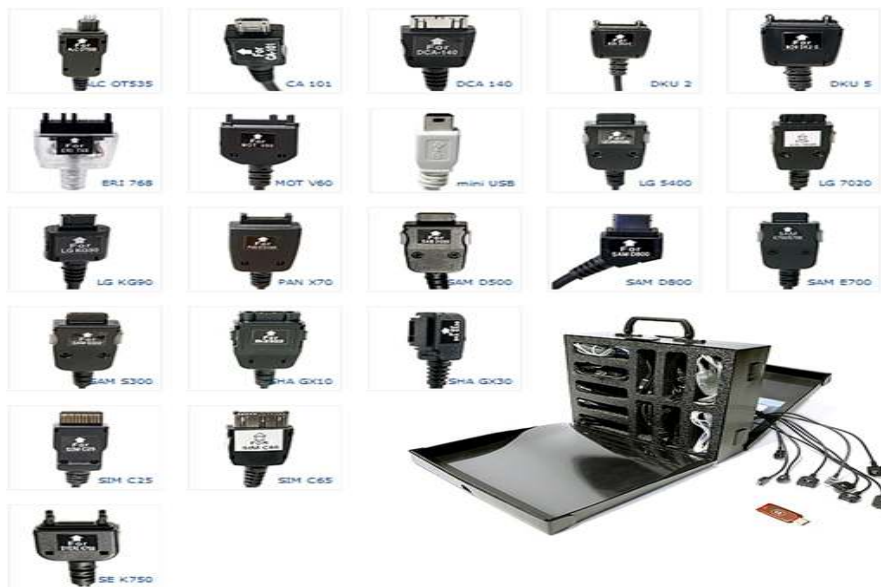
Figura 13. Diagrama proceso 5



Fuente: elaboración propia.

Figuras de referencia del diagrama de flujo anterior:

Figura 14. **Set de cables de sincronización para PDAs y celulares**



Fuente: <http://cellforensics.com>

Figura 15. **Bolsa (StrongHold), y caja de protección contra señales De radio frecuencia**



Fuente: <http://www.paraben-forensics.com>

Proceso 6: búsqueda y análisis de evidencia

Descripción: este proceso es el pináculo de las operaciones forenses. Todos los esfuerzos para extraer información y obtener imágenes de los medios se coronan aquí. El proceso en gran porcentaje consiste en la búsqueda de texto, *software*, data-objetos, etc., que se transforme en evidencia. Sea la obtención de el nombre de una persona dentro de un documento, la fecha de un archivo, el número telefónico de un sospechoso en el historial de llamadas de un celular, un video con detalles de un evento, etc.

Es importante destacar el trabajo conjunto con el fiscal encargado del caso para las directrices de búsqueda, y así determinar el qué, quién, cuándo, cómo, por qué y dónde de la evidencia encontrada.

Al finalizar la búsqueda y análisis, se debe enviar los reportes e informes junto con una copia (si es factible) de los data-objetos encontrados en forma cronológica y en un formato accesible. Esto último, debido a que en ocasiones, el archivo u objeto fue creado utilizando una aplicación propietaria poco común, que no puede ser leída o interpretada por la mayoría de equipos de la Fiscalía.

Por esta razón se debe realizar una conversión, tratando en la medida de lo posible que sea sin ningún tipo de pérdida o alteración. La descripción en orden cronológico de los hallazgos es importante, porque permite enmarcar en el tiempo los eventos y qué ha sucedido con el equipo y los data-objetos, por ejemplo: las fechas y horas de creación, modificación o eliminación de archivos, las bitácoras de navegación, recepción y envío de mensajes.

Lo anterior, implica un estudio minucioso de las fechas consignadas dentro del documento (escritas por el usuario, por ejemplo dentro de una carta), y su respectiva comparación con las fechas de la meta-data. No está demás enfatizar que el informe debe ser legible y comprensible.

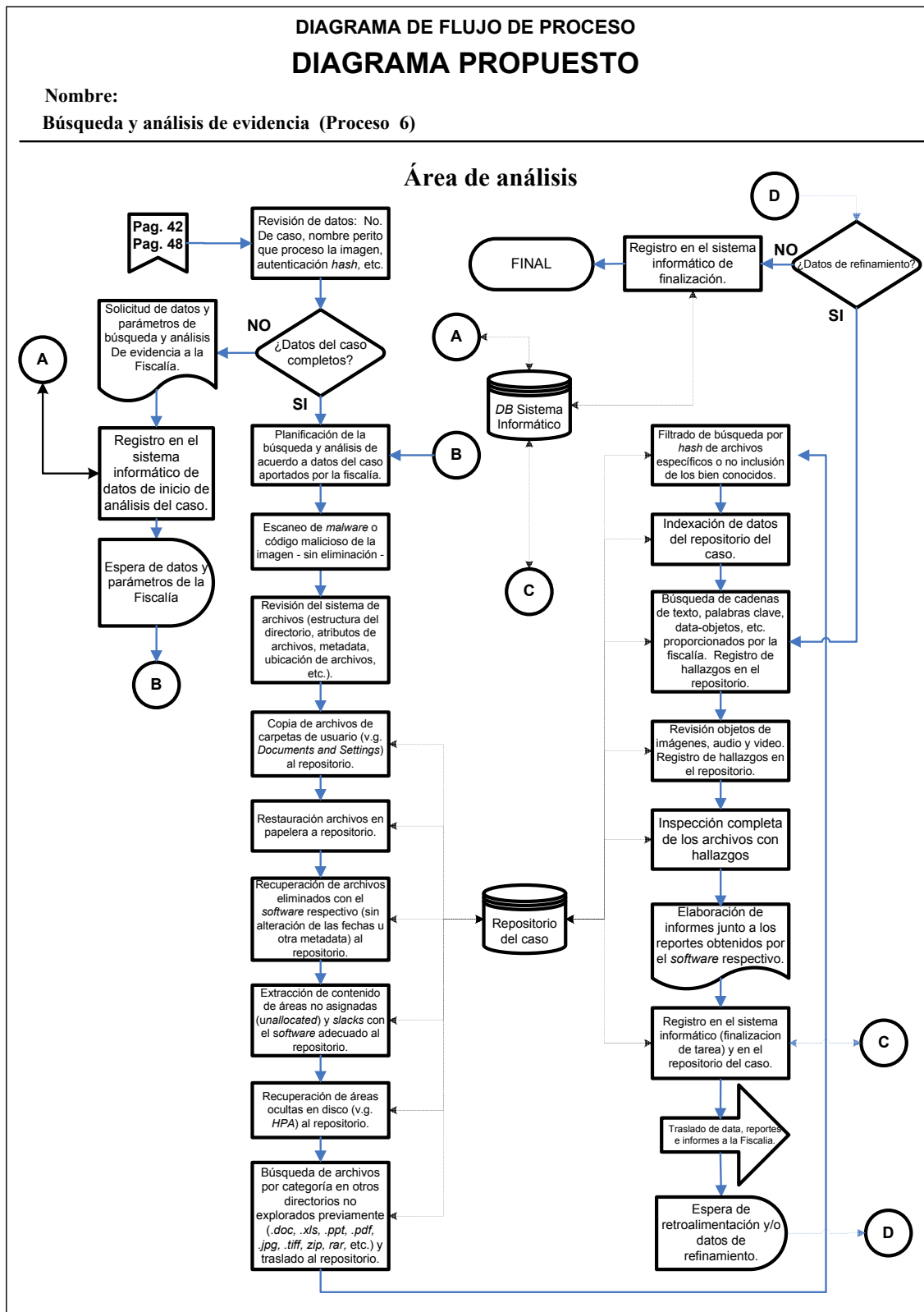
El perito posteriormente debe estar pendiente de la retroalimentación de la Fiscalía para afinar o establecer nuevos parámetros de búsqueda.

Área encargada: análisis

Instrumentos, herramientas y materiales utilizados:

- Imagen(es) de los medios obtenidas en los procesos 3, 4 y 5
- Computadora forense
- *Software* Antivirus
- *Software* de recuperación de archivos sin modificación de metadata
- *Software* de inspección de áreas ocultas
- *Software* de indexación, búsqueda avanzada (por contenido y por tipo) y comparación
- Editor Hexadecimal
- Base de datos de *hashes*. Ésta es muy útil para descartar los archivos bien conocidos o comunes al sistema operativo, Parámetros de configuración de instalación, etc. Muy útil cuando se analiza o busca evidencia de archivos cuyo contenido se ha disfrazado
- Repositorio del caso: es un espacio de disco duro en la computadora forense, un servidor u otro medio seguramente protegido. Este repositorio almacenará todos los datos recabados en los procesos de filtrado para posteriormente, ser analizados en búsqueda de la evidencia

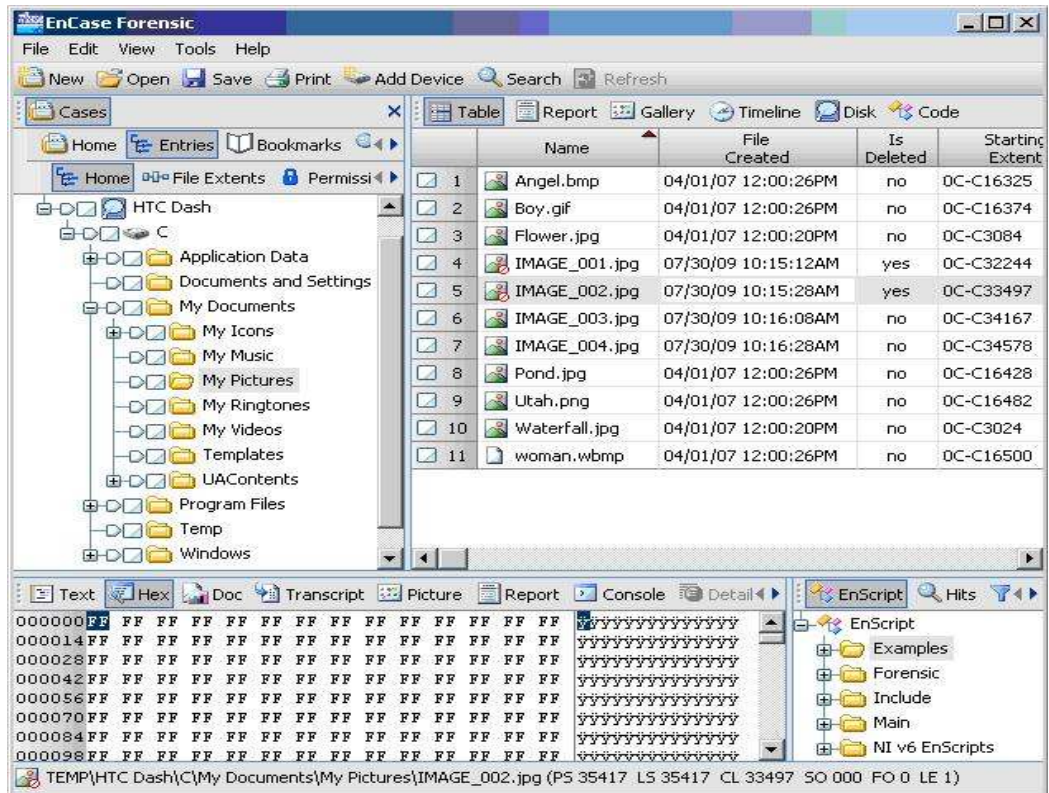
Figura 16. Diagrama proceso 6



Fuente: elaboración propia

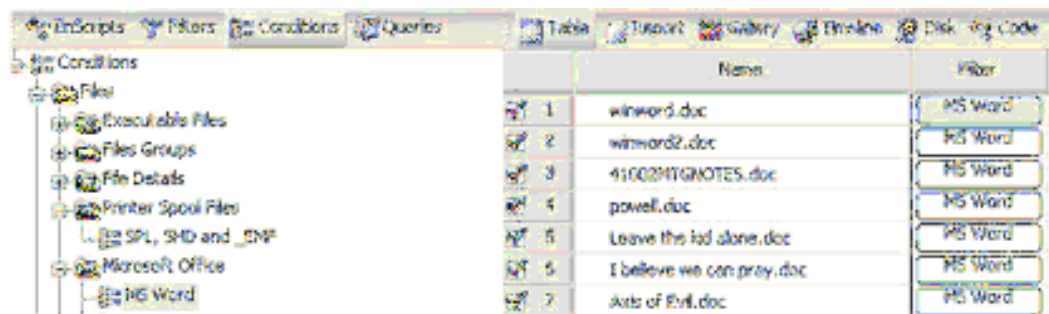
Figuras de referencia del proceso anterior:

Figura 17. Ejemplo 1 de exploración de herramienta de búsqueda (*Encase*)



Fuente: <http://blogs.sans.org/computer-forensics>

Figura 18. Ejemplo 2 de exploración de herramienta de búsqueda (*Encase*)



Fuente: <http://blogs.sans.org/computer-forensics>

Proceso 7: obtención del inventario *hardware/software* del indicio

Descripción: este consiste en la elaboración de un informe general del *software* o los programas que se ejecutaban en el dispositivo a analizar. Este proceso es importante, porque al realizarlo se descubre qué características especiales posee el indicio y para qué era utilizado. Para lograr esto, se utiliza *Software* especial dedicado a la obtención de información del dispositivo particular (*PDA*, celular, computador, etc). Para el caso de discos duros puede recurrirse a una aplicación forense para extracción de data de las áreas *hive* del mismo. Por supuesto, para la adquisición de datos de *PDA*s y celulares (o *smartphones*), se requiere nuevamente, de los cables de sincronización respectivos. En términos generales, este proceso persigue elaborar reportes de la información siguiente.

- Marca, modelo, número de serie, etc. del equipo;
- Qué aplicaciones, programas o procesos se ejecutaban en el equipo.
- Qué dispositivos de *hardware* se conectaban al mismo (de acuerdo a los *drivers* instalados);
- Los detalles del almacenamiento del equipo (capacidad del disco duro, sistema de archivos, memoria interna, tamaño de las memorias *RAM*, *ROM*, *filestore*, etc.);
- Nombres de usuarios registrados en las licencias;
- Nombre del equipo y configuraciones generales, con qué *hosts* se sincronizaba, detalles de las conexiones (*IP*, *DNS*, *WAP*, etc.);
- Códigos o nombres de las empresas que le brindaban algún tipo de servicio (v.g. telefonía, *Internet*, etc.);
- Cantidad de puertos o *slots* de ampliación (para otros dispositivos, tarjetas de memoria, etc.);

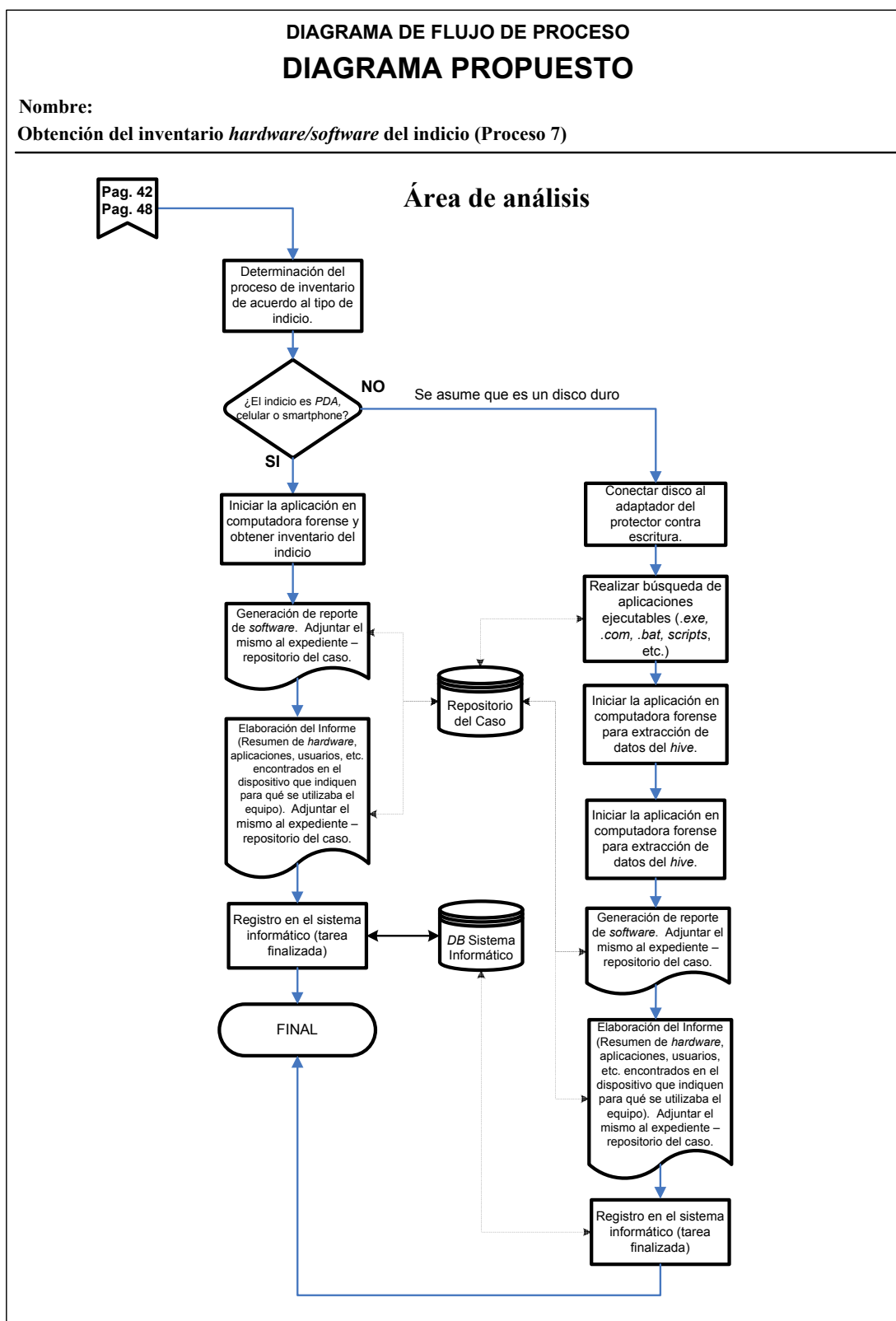
- Marca y tipo de microprocesador;
- Sistema operativo del equipo;
- Propiedades del audio y/o video; etc.

Área encargada: análisis

Instrumentos, herramientas y materiales utilizados:

- Computadora forense
- Aplicación especial para la obtención de inventario *software/hardware* de acuerdo al tipo de indicio (i.e. celulares o *smart-phones*, *PDA*s y discos duros)
- Visualizadores de archivo: para poder ver el contenido sin necesidad de recurrir a la aplicación madre con que se creó el archivo
- Cables de sincronización
- Bloqueador contra escritura de discos duros
- Repositorio de almacenamiento del caso

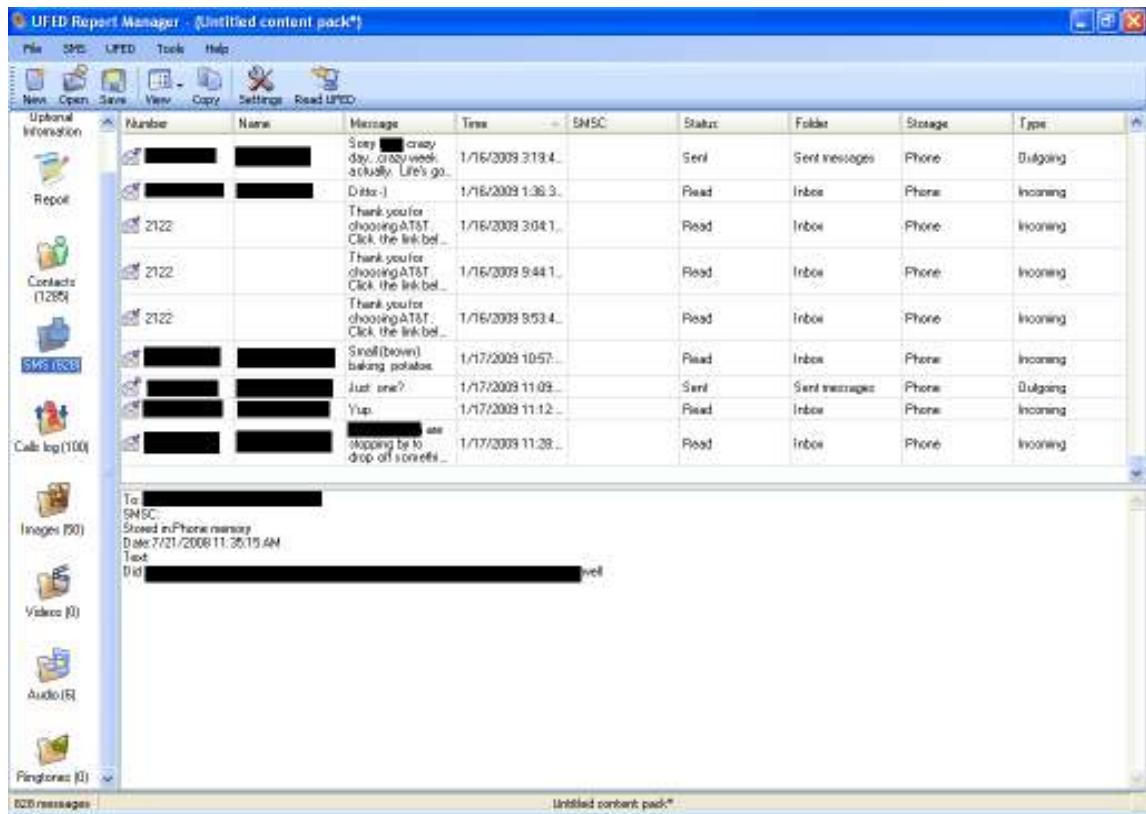
Figura 19. Diagrama proceso 7



Fuente: elaboración propia

Figuras de referencia del proceso anterior:

Figura 20. Ejemplo de captura de datos de un celular (*UFED Cellebrite*)



Fuente: <http://viaforensics.com>

2.3. Descripción del proceso de solicitud del peritaje

La solicitud del peritaje es muy importante, debido a que puede tener implicaciones legales posteriores críticas. Por lo tanto, debe llenar todas las formalidades de ley, debe incluir la fecha de solicitud, nombre del agente fiscal (solicitante), nombre de la fiscalía y agencia respectiva, detalle completo del indicio, etc.

2.3.1. Sugerencias del embalaje

Para recibir los indicios, éstos deben llegar al laboratorio con las siguientes características de embalaje:

- El contenedor debe estar completamente cerrado y sellado, de preferencia en un empaque de acuerdo al tipo de indicio.
- Debe incluir la documentación de la cadena de custodia respectiva. Nombre del embalador, fecha y hora de inicio de la cadena, nombre del agente fiscal a cargo de la investigación, descripción exacta del contenido (tipo de aparato, modelo, número de serie, etc.)
- Dentro del paquete debe estar incluido todo lo indicado en la documentación (dispositivos, memorias, cables, etc.).
- Si los dispositivos del paquete estuvieran protegidos por contraseña, ésta debe incluirse, de preferencia en un sobre cerrado dentro del contenedor; o bien, debe ser incluida en la solicitud adjunta del peritaje.
- Si los indicios estuvieran impregnados de algún tipo de sustancia (lodo, sangre, polvo, químicos, etc.) se debe especificar claramente en la carátula del contenedor. Esto para proteger al perito de algún tipo de contaminación.

2.3.2. Documentación obligatoria

Junto con los equipos o dispositivos a analizar, debe incluirse la siguiente documentación de carácter obligatorio.

- Memorial o documento de solicitud del fiscal: éste debe incluir la requisición formal del trabajo técnico-científico, la descripción completa y detallada de los equipos (indicios), narración de lo que se investiga o indicaciones particulares del peritaje (v.g. obtención del listado de llamadas telefónicas de un celular), etc. y finalmente, la solicitud debe ir firmada y sellada por el fiscal.
- La nota de asignación del trabajo: este nombramiento o asignación debe realizarse por escrito y debe ser emitido por la autoridad correspondiente o jefe del laboratorio de Informática Forense.

2.4. Documentación de los procesos

2.4.1. Fotografías y videos

Las fotografías y los videos son dos herramientas valiosas para el perito, cuando se trata de demostrar el trabajo realizado y sobre todo, que éste se ha realizado bajo las normas legales y siguiendo las buenas prácticas.

2.4.2. Bitácora de actuaciones

Adicional al registro en video y fotografía se debe llevar un libro con la bitácora de cada actividad realizada. Ésta debe incluir: la fecha y hora en que se practicaron, los nombres de las herramientas utilizadas (especialmente del *Hardware* y *Software*), las notas y observaciones de la asesoría externa, tanto técnica como legal, y los nombres de las personas o instituciones a las que se les requirió (si fue necesario).

2.4.3. Sistema informático de seguimiento

Este sistema es importante para la coordinación de los recursos de laboratorio: qué perito lleva un caso determinado, qué procesos se han realizado, qué equipo forense está disponible, etc., esto permitirá distribuir uniformemente el trabajo y manejar el cronograma de cada caso. Y en la toma de decisiones, puede utilizarse para justificar cambios de ampliación en la capacidad instalada del laboratorio.

2.5. Elaboración de informes

Otro punto crucial del peritaje es la elaboración de los informes y reportes de hallazgos encontrados. Este debe seguir un formato preestablecido o estándar, de tal manera que, ante cualquier lectura de los mismos, se reconozca fácilmente dónde se debe leer la información importante.

Los informes deben incluir un sumario de todos los pasos que se realizaron, las conclusiones a las que se llegó en la investigación, nombres de los participantes (peritos y/o laboratorios foráneos, etc.).

La adición de las pruebas realizadas documentadas apropiadamente con bosquejos, fotografías y/o videos, etc., hace que el informe luzca legalmente aceptable y más asimilable.

La información que debe incluirse es la siguiente:

- Identificación del laboratorio (nombre, dirección, teléfono, etc.), junto con las certificaciones respectivas (si existieran).

- Número del caso (de la Fiscalía).
- La cadena de custodia respectiva.
- Nombre completo del agente fiscal encargado.
- Nombre completo del perito o los peritos que realizaron la investigación, con sus respectivas firmas y sellos.
- Nombre del remitente, en caso sea persona diferente de los mencionados en la línea anterior; firmado y sellado.
- Fechas y horas: de ingreso de los indicios al almacén, de asignación del trabajo al perito (o laboratorio específico), de realización de los reportes e informes, de finalización del trabajo y de entrega a la Fiscalía, etc.
- Descripción general de los *ítems* (marca, modelo, número de serie, etc.) tanto de los examinados, como de aquellos que por alguna razón no se pudo realizar la investigación.
- Descripción general de los equipos o dispositivos utilizados (marcas, modelos, versiones, etc.), incluyendo el *software* empleado para las tareas forenses. Una nota de la certificación de dichos equipos resulta fundamental, si existiera.
- La bitácora de actuaciones: incluyendo las fotografías y/o videos de los procesos realizados, *print-screens* de las pantallas de recuperación de archivos eliminados, búsquedas de *strings*, exploración del contenido de archivos, etc.

- Se debe incluir las ayudas utilizadas, asesorías requeridas, referencias bibliográficas, técnicas utilizadas (descifrado, esteganografía, *password-cracking*, etc.)
- Conclusiones de la investigación.

2.5.1. Asesoría legal

En muchas ocasiones, el informe deberá incluir ciertas resoluciones legales obtenidas, a partir de la solicitud de colaboración del perito al departamento de Asesoría Jurídica del laboratorio. Éstas, pueden incluirse para el enriquecimiento del expediente

2.5.2. Ratificación del peritaje informático ante tribunales

El perito debe estar preparado ante cualquier citación que se le requiera para ratificar el peritaje realizado. Esta ratificación es la culminación de todo el proceso, debido a que es aquí cuando la evidencia encontrada se transforma en prueba indubitable de la comisión de un delito. Por esta razón, se enumeran las siguientes sugerencias.

- Tener copia de los informes realizados (hallazgos, bitácoras, asesorías solicitadas, documentación de solicitud del peritaje, etc.).
- Poseer una hoja de vida actualizada como profesional en Informática Forense. Ésta debe incluir, tanto las certificaciones de los estudios realizados, como la experiencia y logros obtenidos en materia forense.

- Llevar por si se requiriera y si no estuviera incluido en los informes, una copia de las fotografías y videos del proceso forense realizado.
- Estar preparado para guardar la calma en todo momento, debido a que probablemente se pondrá en tela de duda la calidad y capacidad del perito, así como de los procesos e informes obtenidos.
- Debido a la popularidad de programas de televisión con temas forenses (v.g *C.S.I, Crime Scene Investigation*), actualmente existe la tendencia a pensar que todo lo observado en dichos programas es realizable o que es tecnología accesible y de uso general. A esto se le conoce como el “síndrome del *CSI*”. El técnico debe estar en la capacidad de reconocer el potencial de los recursos con los que se cuenta en el laboratorio o en Guatemala, así como estar al día respecto a los avances en Informática Forense, a fin de aclarar el punto ante el fiscal con el objeto de delimitar entre la realidad y la ficción.

3. INSTRUMENTOS, HERRAMIENTAS Y MATERIALES UTILIZADOS COMUNMENTE EN PERITAJES INFORMÁTICOS

Para la realización exitosa de los peritajes forenses es necesario contar con un conjunto de instrumentos y herramientas especializadas, tanto de utilización manual (destornilladores, alicates, pinzas, etc.), como herramientas informáticas de *Hardware* y *Software*. Éstas ayudan a que el perito cuente con todos los elementos necesarios para que su trabajo sea más eficiente, bien sea la utilización de una lupa para la lectura del número de serie de un celular, o la utilización de un organizador de cables para mantener el orden en la estación de trabajo.

Algunas de estas herramientas y materiales podrían ser consideradas por algunos como superfluas, pero su carencia puede resultar en una pérdida de tiempo valioso para un caso; por ejemplo, en lo oportuno que puede resultar tener un destornillador *torx* en un momento determinado para la apertura del *case* de un dispositivo.

3.1. Herramientas de mano

Las herramientas de mano son utensilios, generalmente metálicos (o de aleaciones), con mangos de plástico y/o goma utilizados para realizar, de forma más eficiente (con el menor consumo de energía), y con la adecuación antropológica adecuada, tareas de construcción, montajes, reparación, etc., con determinado grado de dificultad que sería difícil de realizar, si no se contara con ellas.

En la actualidad estas herramientas pueden obtenerse en presentaciones multifuncionales (i.e. un instrumento con varios acoples o puntas intercambiables). Comúnmente, para los trabajos forenses se necesita de este tipo de utensilios llamados herramientas de precisión, por la forma en que se ejerce el movimiento sobre el eje y por el tamaño de las puntas, que van desde un milímetro hasta un centímetro.

Figura 21. **Juego de destornilladores de precisión**



Fuente: <http://www.thephoneshop.es>

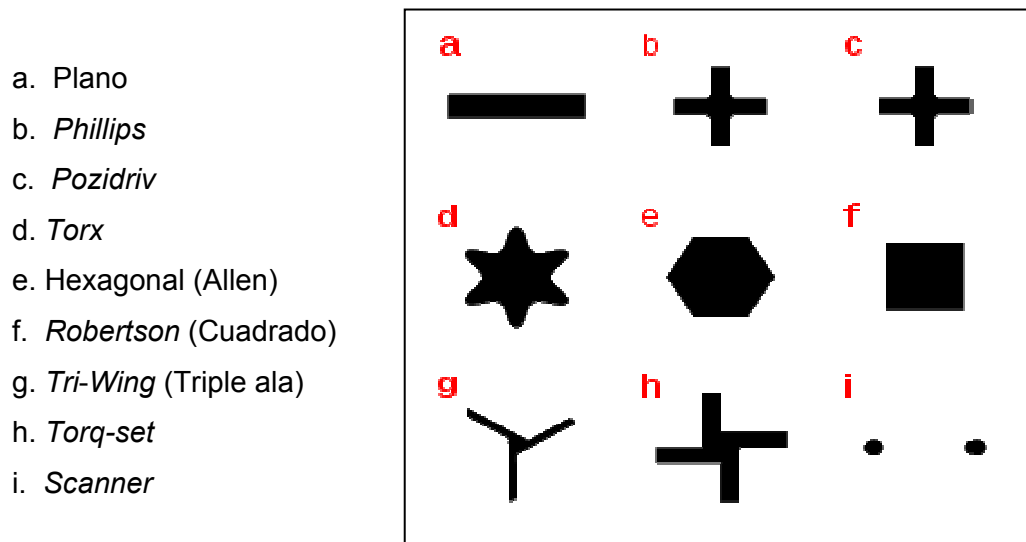
La clasificación de estos utensilios se basa en el tipo de trabajo que realizan y la forma en que se ejercen las fuerzas (torques y palancas) sobre los mismos.

3.1.1. Instrumentos de punta (llaves y destornilladores)

Se utilizan para fijar, sujetar o inmovilizar piezas, comúnmente se clasifican por la forma de acoplamiento de la punta o la cabeza del tornillo. Estas formas pueden ser de cruz, hexagonales, estrella, etc. Algunos de estos acoplamientos son de uso frecuente en otros países, otros en cambio, tienen

cierta orientación de ingeniería, como es el caso de los tornillos Bristol utilizados en aviónica o los *Torx* utilizados en *PDA*s. La figura 22 muestra los acoplamientos más comunes.

Figura 22. **Formas comunes de cabezas de tornillos**



Fuente: <http://wikipedia.org/>

3.1.2. Instrumentos de palanca

Estas herramientas están basadas en las palancas de primera clase, es decir, aquellas en las que el fulcro se encuentra situado entre la potencia y la resistencia y se utilizan para extraer o sujetar piezas. Algunas de éstas incluyen cortadores de cables. Las herramientas que pertenecen a este grupo son: las pinzas, alicates, extractores, cigüeñas, etc. Algunos ejemplos de éstos aparecen en la figura 23.

Figura 23. **Herramientas de palanca**



Fuente: <http://wikipedia.org>

3.1.3. Instrumentos de corte y percusivos

Dentro de los instrumentos de corte se pueden mencionar todos los que son utilizados para cortar, escariar y raspar. En esta clasificación están las cuchillas, las tijeras y las espátulillas. Éstas son útiles, especialmente para la apertura del embalaje de los indicios.

Dentro de esta categoría se encuentran las brocas, las herramientas para mandrinar y los buriles, que a pesar de no ser muy utilizados en la Informática Forense podrían llegar a serlo en algún caso. Por otra parte, dentro de los instrumentos percusivos el más útil es el martillo, no con fines de deformación, sino de pequeños desplazamientos. Por esta última razón, se prefieren aquellos martillitos con cabezas de madera o plástico.

Figura 24. **Ejemplos de tijeras, martillo de desplazamiento, cortadora y espátula**



Fuentes: <http://wikipedia.org>, <http://www.nautilus21.com>, <http://www.ferreteriachile.cl>

3.2. Instrumentos de medición

Esta categoría de instrumentos incluyen a todos los aparatos que se utilizan para comparar magnitudes físicas, mediante un proceso de medición. Esta comparación se realiza contra otros objetos, estándares preestablecidos, patrones, etc. De la medición resulta un número (comúnmente una diferencia o una relación), entre el objeto que se estudia y la unidad de referencia. Las magnitudes físicas pueden ser peso, masa, presión, longitud, etc.

Para la Informática Forense, éstos deben poseer dos características importantes, a decir, sensibilidad y precisión (una confiabilidad muy alta). De preferencia, cuando sea posible, deben estar dentro de los requerimientos de certificación de las instituciones dedicadas a los estándares.

Figura 25. Ejemplo de *tester* digital (*FLUKE 287*)

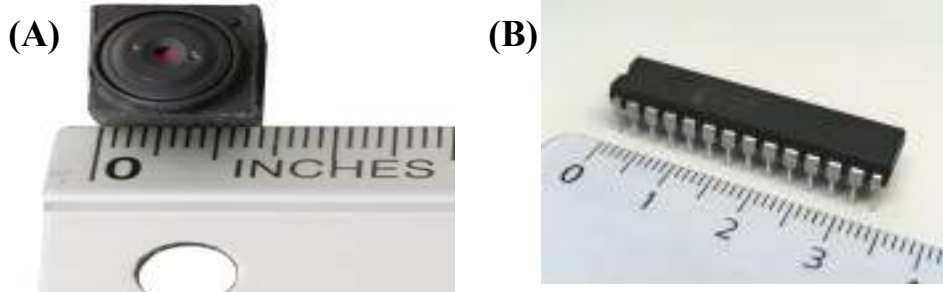


Fuente <http://www.myflukestore.com>

Un instrumento de medición común en los laboratorios, es el multímetro, llamado también *tester* o polímetro. Éste es utilizado para medir diferentes magnitudes como: temperatura, voltaje, corriente, etc., se prefieren los digitales (figura 25) a los análogos y que adicionalmente posean memorias.

Por otra parte, las reglas y las cintas métricas, son muy útiles no solamente para medir los objetos sino también se incluyen como norma en las fotografías forenses para mostrar un referencial del tamaño de los objetos. Actualmente, existen cintas métricas adheribles muy útiles para fijar a escritorios o lugares donde sería difícil colocar un medio de referencia dentro de las fotografías (paredes, interiores de *cases*, *CPUs*, etc.).

Figura 26. Ejemplos de fotografía forense: (A) micro-cámara y (B) *microchip*



Fuentes: (A) <http://www.supercircuits.com>; (B) <http://en.wikipedia.org>

Otro instrumento muy útil es el *Vernier* digital, utilizado para medir el calibre o la distancia lineal externa o interna entre dos puntos de un objeto.

Figura 27. *Vernier* o pie de rey digital



Fuente: <http://www.saferwholesale.com>

3.3. Juego de lupas manuales y de montaje de pedestal

Éstas son particularmente útiles, especialmente para la lectura de números de registro, la verificación de pequeñas conexiones, revisión de soldaduras, etc. Existen manuales (o portables) y de pedestal, las cuales, se pueden fijar a un escritorio.

Éstas últimas, generalmente poseen un brazo extensible con articulaciones que permiten moverla en varias direcciones y adicionalmente, incluyen una lámpara, con lo que se mejora significativamente la visión.

Actualmente existen en el mercado lupas electrónicas, muy utilizadas en la industria textil, numismática y por dentistas; sin embargo, el uso de éstas lo determinará la frecuencia de la necesidad de la analizar detalles realmente pequeños.

Figura 28. **Lupa de pedestal con brazo articulado extensible para ensamblar a escritorio**



Fuente: www.directindustry.es

3.4. Equipo de documentación

Los dispositivos más comunes para la documentación de los procesos forenses en el laboratorio son las cámaras de video y las de fotografía. Éstas son el complemento ideal para llevar una bitácora completa de todo lo que se ha realizado en cada proceso y permite, cuando sea requerido, mostrar visualmente la correcta realización del trabajo y la observancia de las buenas prácticas.

3.4.1. Fotografías: cámara digital de alta resolución

Hasta hace algún tiempo, solamente se admitía en los laboratorios el *film* o película en la fotografía, ahora se utiliza también la fotografía digital de alta resolución, especialmente porque esto permite tratar las imágenes como archivos y así incorporarlas al expediente sin problema alguno, mejorando el tiempo de montaje o diagramación del informe final y también son más fáciles de almacenar. Deben ser de una resolución tal que, cuando se amplíen las fotografías conserven todos los detalles.

La gerencia del laboratorio siempre estará al tanto de las recomendaciones de los tribunales de Guatemala, respecto al uso de películas fotográficas (*film*) o el uso de cámaras digitales. Esto debido al argumento que la fotografía digital es más fácil de manipular o alterar.

3.4.2. Videos: cámara de alta resolución y alto *fps* (cuadros por segundo)

En muchas ocasiones se necesita documentar un evento en el que se requiere no dejar lugar a dudas respecto la continuidad del mismo. Para este tipo de casos se utiliza una cámara de video que para usos forenses, deben ser

de alta resolución y que permita captar el evento con la mayor cantidad de cuadros por segundo (*fps*, *frames per second*). Esto debido a que el detalle es un punto esencial en todos los casos penales, y con cámaras de estas características, sería asequible realizar énfasis (congelamiento de imagen) en un momento particular del video, sin pérdida de calidad.

Muchas cámaras modernas permiten realizar ambas tareas con una excelente calidad y con prestaciones adicionales como: abundante memoria interna, ranuras de expansión para almacenamiento externo, conexiones *USB* y *firewire*, capacidad de acercamientos (macro o “*close-ups*”), captación de video en alta definición, etc.

En resumen, se sugiere obtener una cámara digital con las siguientes características mínimas:

- Alta definición de captación fotográfica, por lo menos 12 *megapixeles*.
- Primordialmente, que pueda grabar formatos de imagen *TIFF* (*Tagged Image File Format*) y *RAW*. Adicionalmente la compresión común *JPEG* (*Joint Photographic Experts Group*).
- Con ranuras de expansión *SD*, *Compact Flash*, *Memory Stick*, etc.
- Con una velocidad de obturación elevada (v.g. 1 / 8 000 segundos).
- Captación de video con resolución *HDTV* (*High Definition Television*), o bien con manejo de estándares de *codecs* avanzados de alta definición como *AVCHD* (*Advanced Video Codec High Definition*).

- Capaz de realizar acercamientos sin pérdida de enfoque.
- De preferencia con tecnología *DSLR (Digital Single-Lens Reflex camera)*.
- Con pantalla *LCD (Liquid Cristal Display)*.
- Con interfaces de conexión como *RCA* compuesto, *firewire* y/o *HDMI (High-Definition Multi-media Interface)*.

Finalmente, se debe recordar que dentro del marco del trabajo actual, las cámaras son utilizadas solamente con motivos de documentación de los procesos y no son utilizadas para obtener información de documentos alterados, prendas con químicos particulares, detección de huellas, etc. en cuyo caso se utilizan otro tipo de cámaras que realicen ese tipo de exploración (v.g. filtración de frecuencias ultravioleta o infrarroja). Adicionalmente, las cámaras actuales poseen otro tipo de características que están más allá del ámbito de cobertura, por ejemplo, el interlineado de la señal, el escaneo progresivo, las conversiones de formato de video, etc.).

3.5. Convertidores

Los convertidores o adaptadores son elementos que permiten leer o escribir en dispositivos de almacenamiento cuando no se cuenta con el adecuado. Estos elementos se adecuan, tanto a la forma de transmisión de datos, como a la forma de alimentación eléctrica. Los más comunes son aquellos que permiten obtener información de dispositivos discontinuados o que ya no son utilizados por los fabricantes para la producción de los equipos informáticos. Los más comunes son los convertidores de interfaces (conexiones) de bus de discos duros.

3.5.1. Convertidores *Multi-drive*

Actualmente se comercializan convertidores adaptables a diferentes interfaces como: *SCSI (Small Computer System Interface)*, *IDE (Integrated Drive Electronics)*, o *ATA (Advance Technology Attachment)*, *SATA (Serial ATA)*, *PATA (Parallel ATA)*, *PCMCIA (Personal Computer Memory Card International Association)*, o los más antiguos *ISA (Industry Standard Architecture)*, e *EISA (Extended ISA)*. El equipo forense debe contener conexiones o adaptadores para todos estos interfaces y éstos deben estar conectados a la bahía de mayor velocidad de transferencia. Por ejemplo, si tuviera conexiones *SATA*, debería la computadora forense poseer convertidores *SATA-SCSI*, *SATA-IDE*, etc. A continuación se muestra una tabla comparativa de los interfaces más comunes y su velocidad de transmisión:

Tabla III. **Velocidades de transmisión de diferentes buses**

Tipo de Interface	Velocidades de transmisión (Mb/s)
ISA	De 1,2 a 5,3
EISA	Hasta 32
IDE/ATA	De 66 a 100
SCSI	De 5 a 160
PATA	De 100 a 133
SATA	De 150 a 600

Fuente: <http://wikipedia.org>

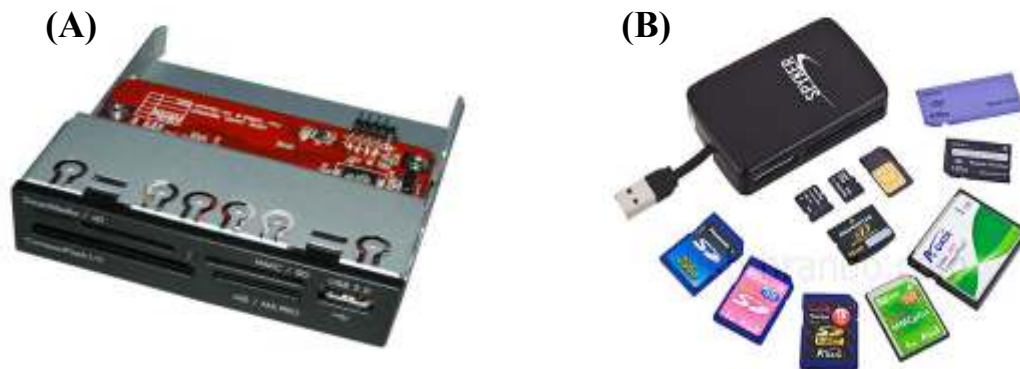
El equipo forense también debe poseer otras conexiones comunes utilizadas para conectar periféricos a la computadora como *USB (Universal Serial Bus)* y el *FW (FireWire)*. Con las normas actuales que van para *USB 2,0* de 16 a 60 *Mb/s.* y *USB 3,0* con velocidades de transferencia de hasta 600

Mb/s. Respecto a las conexiones *FireWire*, conocidas también como *iLink*, éstas comúnmente son utilizadas para conectar dispositivos digitales como cámaras o video-cámaras. Con la gran ventaja que la versión más comercial obtiene velocidades que van de los 1,6 *Gb/s*. Hasta los 3,2 *Gb/s*.

3.5.2. Lectores de tarjetas de memoria

Con la proliferación de dispositivos portables (*PDA*s, celulares, cámaras, *tablets*, reproductores de audio/video, etc.), también se ha popularizado la utilización de medios de almacenamiento de tamaño compacto (aproximadamente oscilan de 0,5 a 2,0 centímetros). Entre estos medios o tarjetas de almacenamiento están la *SD* (*Secure Digital*), *CompactFlash*, *Memory Stick*, etc. Por esta razón, el laboratorio debe contar con los dispositivos que permitan leer este tipo de tarjeta. Actualmente, existen lectores que permiten la lectura de varios tipos de tarjetas como los mostrados en la figura 29, donde la imagen (A) corresponde a un lector multi-tarjeta interno y (B) a uno externo, el cual puede conectarse a la estación forense a través de un puerto *USB*.

Figura 29. Lectores multi-tarjeta



Fuente: <http://www.geeks.com>

3.5.3. Sincronizadores

Comúnmente, los dispositivos como celulares y asistentes personales (*PDA*s), necesitan mantener una comunicación con uno o varios equipos anfitriones, o computadoras, a través de la cual se puedan instalar aplicaciones o trasladar información (contactos, correos electrónicos, agenda de actividades, archivos, etc.).

Este vínculo con el equipo anfitrión, permite que dichos datos puedan ser actualizados constantemente al realizarse la conexión o bien simplemente trasladarlos a manera de una copia de respaldo (*backup*). Esto es lo que realizan los sincronizadores, que en realidad constan de un cable especial y una aplicación (*software*) de sincronización que puede ser de terceros o incluirse dentro de los sistemas operativos con las opciones de conectar y listo (*plug and play*).

Figura 30. Ejemplos de cables de sincronización de *PDA*s y celulares



Fuente: <http://palmfreeware.info>

Debido a la gran variedad modelos y marcas de celulares, *PDA*s y *smartphones*, se vuelve apremiante que el laboratorio cuente con un juego extenso de cables de sincronización que permitan extraer información de la mayoría de los mismos.

Por otra parte, es normal que los cables tengan una conexión *USB* en el otro extremo lo cual es útil, debido a que si el aparato está diseñado para recibir alimentación eléctrica a través de este tipo de conexión, esto garantizaría que el dispositivo se mantenga cargado, lo que es conveniente para el examinador forense debido a que una falla en la energía puede conducir a la pérdida de información o la activación de bloqueos por contraseña, *PIN* (*personal identity number*) o *PUK* (*personal unblocking key*). Por lo general, si un suscriptor ingresa el *PIN* equivocado tres veces seguidas, un celular se bloquea hasta que se ingresa el *PUK*.

Finalmente, a pesar que existen otros medios y productos para acceder al contenido de estos aparatos utilizando medios inalámbricos (*bluetooth* o *WiFi*), el método preferido y más confiable es el físico (i.e. utilizando un cable).

Lo anterior, también conduce a la necesidad de que el área de laboratorio dedicada a trabajar con celulares cuente con un recubrimiento en los techos y paredes que bloquee las señales de radio frecuencia o bien utilizar cajas o bolsas especiales (v.g. *StrongHold*⁵ esta construída de níquel, cobre, plata y nylon), a fin de aislar el dispositivo y así evitar el acceso al mismo en forma remota con el objetivo de impedir la activación de alguna secuencia de borrado, congestiónamiento de mensajes (*jamming*, con el objetivo de ir borrando los mensajes más antiguos en la cola), alteración de la información o la marcación accidental de un número desde el teléfono investigado.

⁵ Ver <http://www.paraben-forensics.com>

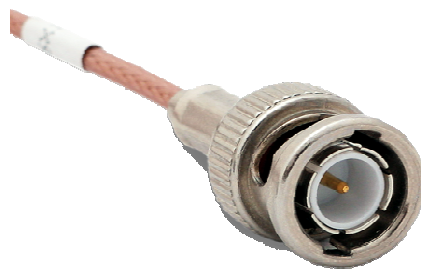
3.5.4. Cables y conectores

Debido a la existencia de la gran variedad de conexiones en el mundo informático, también resulta necesario contar con un *set* de cables que puedan acoplarse al equipo-indicio, especialmente si éste es de tecnología antigua. Esto es particularmente aplicable cuando se requiere conectar un teclado, un dispositivo apuntador o un monitor a un *CPU* que posee conexiones descontinuadas o en desuso.

También se deberá contemplar la existencia de conectores o convertidores del tipo *DIN*, *BNC*, *DB*, *HD*, *ARJ*, etc., así como la existencia de cables *USB*, *UTP*, coaxiales, etc. o bien las herramientas que permitan realizarlos.

Lo anterior también es aplicable a dispositivos singulares como cartuchos, cintas magnéticas, dispositivos de lectura, etc. de generaciones anteriores y que aún son utilizados por algunas empresas en Guatemala.

Figura 31. **Ejemplo de cable coaxial**



Fuente: <http://www.saftehnika.com>

Figura 32. Ejemplo de conectores **DB9**



Fuente: <http://www.computercableinc.com>

3.6. Adaptadores de corriente/voltaje

El laboratorio debe contar con gran cantidad de estos adaptadores así como de diferentes *plugs* (enchufes de conexión), que puedan en la mayoría de casos poder adecuarse a los diferentes indicios que ingresen al laboratorio (esto porque frecuentemente los indicios llegan sin éstos). Otro cuidado que se debe observar es respecto a la polaridad del indicio, es decir, positivo dentro y negativo fuera o viceversa.

Figura 33. Adaptadores de corriente y voltaje



Fuente: <http://www.ebest24.com>

3.7. Dispositivos lector/escritor CD/DVD/Blu-ray

El laboratorio debe contar con un conjunto de grabadores o duplicadores (*burners*), de CDs, DVDs y *Blu-ray* de alta velocidad, que serán utilizados para hacer respaldos o copias de seguridad (*backups*), de todo lo relacionado con los casos (v.g. evidencia).

Estos dispositivos de preferencia deben poseer memoria, *buffer* y disco duro, para minimizar el tiempo de quemado.

Figura 34. Duplicador/Grabador de discos CD/DVD/BLURAY



Fuente: <http://www4.shopping.com>

3.8. Software

El uso de *software* junto con las herramientas de *hardware* es el *sine qua non* de la Informática Forense. Una ventaja especial de las soluciones de *software* es que en la actualidad se incluyen varias aplicaciones en el mismo producto, como el *Forensic Toolkit* de la empresa *AccessData Corp* tiene

incluido recuperación de contraseñas, descifrado de archivos (*decrypt*), indexación y búsqueda de expresiones, etc.

También existen en el *Internet* aplicaciones gratuitas a través de licencias *GNU – Open Source*, que incluyen una gran variedad de aplicaciones forenses; sin embargo, éstas generalmente no cuentan con un soporte especializado o una garantía de funcionamiento y por lo tanto no están certificadas.

3.8.1. Bloqueador de escrituras a disco (*write blockers*)

Estas aplicaciones son las que bloquean el disco duro para evitar que se realicen escrituras al mismo. También existe su homólogo en *hardware*. Estas son las características de este *software*:

- No es necesario abrir el *case* de la computadora.
- Posee elementos de valor agregado, por ejemplo, herramientas para la obtención de la imagen, generación del *hash*, editor de contenidos, etc.
- Es más lento que las herramientas de *Hardware*.

En el capítulo dos del presente documento, el diseño de los procesos contempló la utilización de herramientas de bloqueo de escritura basadas en *hardware*; sin embargo, la elección de una o de otra dependerá de la evaluación del desempeño necesitado, del precio y el apego a las normas.

En este último sentido deberán preferirse aquellas que estén acreditadas o avaladas por las instituciones de estándares, las agencias de reforzamiento de la ley o los Tribunales de Justicia⁶.

Estos son algunos de los productos más populares de esta categoría:

- *SAFE (System Acquisition Forensic Environment)* de la empresa *ForensicSoft* (<http://www.forensicsoft.com>)
- *EnCase Physical Disk Emulator* de la empresa *GuidanceSoftware* (<http://www.guidancesoftware.com>)
- *Paraben's Forensic Replicator* de la empresa *Paraben Forensic Tools* (<http://www.paraben-forensics.com>)

3.8.2. Herramientas de *Booting* o carga

Estos productos son muy útiles cuando por alguna razón se requiere ingresar a la computadora investigada sin utilizar sus recursos. Estas herramientas consisten en una modificación del núcleo de un sistema operativo con la inclusión de utilerías forenses. La ventaja radica en que el inicio del sistema se puede realizar desde un *CD* o una memoria *USB*. Esta opción de carga (*booting*), es una de las características que viene incluida generalmente en muchas de las soluciones de *software*.

⁶ Ver <http://dereknewton.com/2010/05/write-blockers-hardware-vs-software/>
http://www.cfft.nist.gov/hardware_write_block.htm,
http://www.cfft.nist.gov/software_write_block.htm.

3.8.2.1. OS CD

Un *OS CD* (*Operating System Compact Disk*), es un disco compacto que incluye el sistema de carga y las herramientas forenses. Ejemplo: *SAFE* de *ForensicSoft*.

También se les conoce con el nombre de *Live CDs*. Especialmente en el ambiente *Unix/Linux* debido a que son modificaciones de las diferentes distribuciones. Estas soluciones pueden ser útiles porque permiten montar y bloquear los volúmenes de *Windows* y realizar la exploración forense con productos gratuitos.

3.8.2.2. OS USB

Realizan el mismo trabajo que los *OS CD*, solamente que éstos vienen contenidos en una memoria *USB* y pueden ejecutarse desde dicha bahía. Por su característica de fácil transportabilidad, a este tipo de aplicaciones se les denomina portables. Ejemplo: *EnCase Portable Kit* de *GuidanceSoftware*.

3.8.3. Herramientas de búsqueda y recuperación

Éstas permiten realizar tres de las tareas relevantes del trabajo forense: buscar información (evidencia), recuperar data-objetos eliminados y encontrar archivos ocultos.

3.8.3.1. Texto – comparación/excepción

Regularmente, lo más buscado en un medio de almacenamiento es texto (nombres, números, fechas, hileras de caracteres, etc.). Y, por lo tanto, la

aplicación que realiza, debe ser capaz de trabajar con operadores lógicos (*AND*, *OR* & *NOT*) y caracteres comodines. Adicionalmente, debe poseer escaneo interno para buscar expresiones dentro de los data-objetos y poder realizar indexaciones para hacer más eficiente el rastreo de expresiones. La indexación tomará tiempo, pero valdrá la pena si el caso requiere múltiples búsquedas.

Por otra parte, estas herramientas pueden poseer características avanzadas de búsqueda como escaneo de áreas no particionadas o no asignadas, *slacks*, encabezados de archivos, o la más reciente técnica forense de *data-carving*. Ejemplos de estas *Suites* que permiten realizar búsquedas se enumeran a continuación.

- *Paraben's Text Searcher* (<http://www.paraben-forensics.com>)
- *ForensicToolkit* (<http://www.accessdata.com>)
- *DtSearch* (<http://www.dtsearch.com>)
- *DataLifter.Net* (<http://www.datalifter.com>)
- *TextSearch PLUS* (<http://www.forensics-intl.com>)

3.8.3.2. Archivos escondidos

Existen varias formas de ocultar los archivos o data-objetos, a través de colocarlos en áreas no particionadas u ocultas al sistema operativo (como se mencionó en el capítulo dos de este trabajo), o bien ubicándolos dentro de las áreas válidas, debido a que los sistemas de archivo (*FAT/NTFS*), permiten realizar esto simplemente al cambiar el atributo de visibilidad del archivo.

Por lo tanto, estas herramientas tendrían que realizar la búsqueda a lo largo de todo el medio de almacenamiento, sea en áreas no particionadas o en el directorio de archivos no importando su atributo de visibilidad o el artificio utilizado para ocultar el archivo o data-objeto.

3.8.3.3. Archivos eliminados

Éstas son aplicaciones que rescatan los archivos que han sido borrados de un medio de almacenamiento. Existen muchos productos en el mercado, sin embargo, se recomienda que la aplicación posea la certificación correspondiente, o en su defecto, que sea utilizada o recomendada por una gran cantidad laboratorios o agencias forenses⁷.

Un programa que realice recuperación de archivos eliminados por lo menos debe cumplir requisitos siguientes.

- Recuperación de formateos previos en varios sistemas de archivo y medios de almacenamiento fijos y extraíbles (discos duros, tarjetas de memoria, *USB flash*, etc.).
- Escaneo de alta velocidad para búsqueda de archivos eliminados.
- Recuperación sin modificación de metadata, especialmente de fechas de eliminación los archivos.

Estas son algunas aplicaciones que permiten la recuperación de archivos eliminados:

⁷ Ver <http://www.computerforensicsworld.com>;
<http://www.forensicfocus.com>,
<http://www.computer-forensics.co.uk>.

- *DataLifter® - File Extractor Pro* (<http://www.datalifter.com>)
- *Paraben's Sorter* (<http://www.paraben-forensics.com>)
- *Encase Forensics* (<http://www.guidancesoftware.com>)
- *ForensicToolkit* (<http://www.accessdata.com>)

3.8.4. Acceso a datos

Luego de encontrar los archivos ocultos y aquéllos que han sido eliminados, está la interrogante si éstos están protegidos por contraseña, o bien si han sido cifrados. Estas herramientas tratan de romper el código que las bloquea a fin de acceder los mismos y así poder investigar su contenido.

3.8.4.1. Recuperadores de contraseñas

Estas aplicaciones utilizan variados métodos como: fuerza bruta, ataque a diccionario, *rainbowcrack*, etc., para tratar de encontrar o romper la contraseña contenida en un data-objeto y así, poder analizar el contenido del mismo. Estas aplicaciones funcionan utilizando, por lo general, los mismos algoritmos, sin embargo, su desempeño puede variar.

Se recomienda seleccionar aquellas que incluyan la mayor cantidad de formatos de archivos (*.doc*, *.xls*, *.dbf*, *.zip*, *.rar*, *.arj*, etc.) y que posean tecnologías recientes como las solución *Software/Hardware* de alto potencial de cálculo denominada ataque por red distribuida (*DNA*, *Distributed Network Attack*), consistente en la utilización de varios procesadores.

Empresas que ofrecen aplicaciones para recuperación de contraseñas.

- *AccessData* (<http://www.accessdata.com>)
- *EIComSoft* (<http://www.elcomsoft.com>)

También existen soluciones de *hardware*, con la ventaja que algunas de éstas complementan al *software* (*Tableau TACC1441* y el *AccessData DNA*) y le brindan a éste, una aceleración significativa (hasta en un 60%). Productos tales como el TAC1441 de la empresa *Tableau*, mostrado en la figura siguiente posee características especiales como: varios procesadores simultáneos trabajando en paralelo, múltiples formatos (*WinZip*, *WinRAR*, *PGP*, etc.), y cifrados (v.g. *AES 256*, *RSA*, *CAST*, *SHA-1*, etc.).

Figura 35. **Tableau TAC1441e**



Fuente: <http://www.tableau.com>

3.8.4.2. Descifradores (*Decrypters*)

Hoy en día, ya es rutinario que las personas encripten o cifren sus archivos privados. Para ello, utilizan productos basados en varios algoritmos algunos de los cuales son tan fuertes, que resultan casi imposible descrifrarlos debido al tiempo que implicaría esta tarea⁸. Muchas de esas aplicaciones para cifrar son gratuitas, lo que hace que esto esté al alcance de la mano. Sin embargo, en el mercado existen algunos productos que tratan de descifrar estos archivos utilizando técnicas avanzadas como las mencionadas en la sección de recuperación de contraseñas (ver inciso 3.8.4.1. del presente capítulo).

Suites para descifrado:

- *ForensicToolkit* (<http://www.accessdata.com>)
- *Decryption Collection Enterprise* (<http://www.paraben-forensics.com>)
- *Encase Forensics* (<http://www.guidancesoftware.com>)

3.8.4.3. Lector y analizador de información de celulares

Estos productos permiten al profesional forense obtener información de celulares (lista de contactos, registro de llamadas, fotografías, etc.). Este tipo de herramientas consta de dos componentes:

⁸ Se calcula que utilizando un ataque de fuerza bruta contra un mensaje cifrado en *AES (Advanced Encryption Standard)* requeriría el uso de aproximadamente 11×10^{77} combinaciones. *NIST* estima que esto representaría, utilizando computadoras actuales (año 2009), casi 149 trillones de años! (Fuente: <http://research.sun.com/features/encryption/>).

- *Software* de administración: controla que la estación forense realice la conexión al celular, protege contra escritura al dispositivo, extrae la información y la deposita en un lugar predeterminado y realiza los reportes en forma legible de la data encontrada.
- Medios de conexión: usualmente son cables de conexión especiales (figuras 14 y 30) o bien, medios de conexión inalámbrica (*bluetooth*, *WiFi* o *IR*). Se prefiere la conexión física (cable) por ser más confiable y estable.

Estos productos trabajan con varias tecnologías de celulares (*GSM*, *CDMA*, *3G*, etc.). Varios de éstos poseen un dispositivo intermediario (v.g. *UFED - Universal Forensic Extraction Device* de la empresa *Cellebrite*), con conexiones *USB/Firewire/ARJ*, memoria, lectores de tarjetas *SIM/SD*, extracción de información eliminada u oculta, etc. Otros por su parte son portables y tienen el tamaño de una memoria *USB* (*CSI Stick* de *Paraben*), o traen incluido lectores de tarjetas y bolsas para bloqueo de radio frecuencias (*Seizure field kit* de *Paraben*). Adicionalmente, éstos traen predefinida una gran base de datos de marcas y modelos de celulares y *smart-phones* junto con los cables de conexión respectivos y la opción de descarga de actualizaciones del *Internet*.

Figura 36. ***UFED - Universal Forensic Extraction Device***



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

Figura 37. **Device Seizure Field Kit y CSI Stick (imagen ampliada)**



Fuente: <http://www.paraben-forensics.com>

Debido a la forma de funcionamiento, algunos productos como los anteriores, también son utilizados con fines forenses para explorar una gran variedad de *PDA*s.

Otras aplicaciones con funcionalidad similar son las siguientes.

- *Paraben's Cell Seizure Toolbox* (<http://www.paraben-forensics.com>)
- *Paraben's PDA Seizure Toolbox* (<http://www.paraben-forensics.com>)
- *Cell Phone Analyzer* (<http://www.bkforensics.com>)
- *EnCase Neutrino* (<http://www.guidancesoftware.com>)
- *FTK Mobile Phone Examiner* (<http://www.accessdata.com>)

Para la utilización de estos productos se debe considerar los siguientes aspectos:

- Verificar la carga eléctrica de la batería antes de proceder con la extracción.
- El dispositivo debe estar aislado de cualquier red durante todo el análisis y extracción de información a través de mecanismos seguros como bolsas, jaulas de *Faraday* o cualquier bloqueador de radio frecuencias.
- La extracción de información en estos casos también debe ser autenticada.

3.8.5. Creadores de imágenes y duplicación

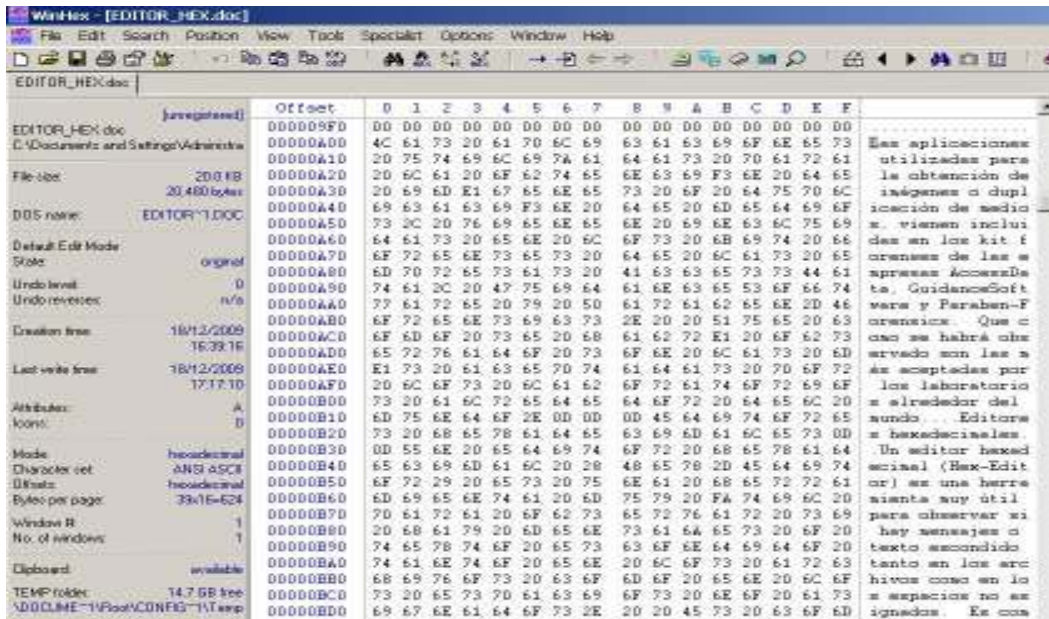
Éstos, generalmente, vienen junto a los bloqueadores de escritura y se consideran complementarios, debido a que luego de aplicar uno continúa el otro. La elección de las opciones de *software* o *hardware* depende básicamente de la velocidad de trabajo y las prestaciones adicionales que puedan incluirse, por ejemplo, la autenticación de las copias y el manejo de múltiples formatos (v.g. .E01, .L01, .AD1, *ISO*, etc.).

Las aplicaciones utilizadas para la obtención de imágenes o duplicación de medios, vienen incluidas en los *kit* forenses de las empresas *AccessData*, *GuidanceSoftware* y *Paraben-Forensics*; ya que son las más aceptadas por los laboratorios alrededor del mundo.

3.8.6. Editores hexadecimales

Un editor hexadecimal, *Hex-editor*, es una herramienta utilizada para visualizar el contenido de los archivos y los espacios no asignados en la memoria. Con éstos, se puede observar el texto crudo (en forma hexadecimal), del medio de almacenamiento, en este sentido es una aplicación de procesamiento de datos de bajo nivel, opuesto a la forma en que se verían los archivos en su aplicación nativa, lo cual resulta eficaz para observar algún código desconocido, texto o mensaje dentro del data-objeto particular.

Figura 38. Ejemplo de visualización de archivos con editor hexadecimal



Fuente: imagen obtenida utilizando *WinHex* en el archivo que contenía el presente documento; elaboración propia.

Existen muchos editores hexadecimales, inclusive algunos gratuitos; sin embargo, uno de los más aceptados es la suite *WinHex* de la empresa *X-Ways Forensics* (<http://www.x-ways.net>), que incluye muchas otras herramientas para análisis forense.

3.8.7. Analizadores de datos

Son una familia de aplicaciones que tratan a través de algoritmos avanzados, detectar si los archivos incluyen algo adicional a su contenido propio. Básicamente, intentan detectar la utilización de técnicas para ocultar mensajes dentro de los archivos, que no necesariamente implica ilegibilidad del objeto portador, en este caso el archivo contenedor pareciera normal. El texto oculto puede ir embebido dentro de una imagen (estenografía), un programa compilado o ejecutable, un código disparable al presionar una secuencia de teclas (v.g. huevos de pascua), etc.

Empresas que ofrecen soluciones forenses a esta problemática son:

- *WetStone Technologies* (<http://www.wetstonetech.com>)
- *Outguess* (<http://www.outguess.org>)

3.8.8. Analizador de inventario de aplicaciones

Estas son útiles para obtener el listado de programas y servicios que están instalados en un equipo. Esto permitirá el análisis de para qué se utilizaba la computadora, qué dispositivos se conectaban a ella, si fue utilizada para robo de contraseñas (a través de *keyloggers* o *spyware*), etc. Para los celulares y las PDAs también existen productos para realizar esta tarea.

Estas son algunas aplicaciones para realizar esta tarea.

- *Application Inventory* (<http://www.funduc.com>)
- *SmartInventory* (<http://www.softwaremetering.com>)
- *Paraben's Cell Seizure Toolbox* (<http://www.paraben-forensics.com>)
- *EnCase Neutrino* (<http://www.guidancesoftware.com>)
- *Aida32* (<http://www.softspecialist.com>); este proyecto fue cerrado pero aún se puede encontrar la aplicación gratuita en *Internet*.

3.9. Hardware

3.9.1. Bloqueador de escrituras a disco (*hard disk write-blocker*)

Un bloqueador de disco duro es un dispositivo que no permite realizar escrituras en el mismo. Como se describió previamente, la utilización de estos dispositivos constituye una de las normas de buenas prácticas del manejo de los indicios, por lo tanto, su utilización en un laboratorio es imprescindible.

Existe en el mercado gran cantidad de productos que realizan esta importante tarea; sin embargo, debe haber una inclinación a elegir aquéllos que hayan sido probados y certificados por la *ISO* o por *NIST*, o en su defecto, sean de aceptación general por los laboratorios informático-forenses o agencias de reforzamiento de ley (*taskforce agencies*) alrededor del mundo.

3.9.2. Duplicadores o clonadores de discos duros

Estos dispositivos de *hardware* son de los más utilizados en los laboratorios de Informática Forense, por lo tanto, se debe contar con una buena cantidad. Además, debido a que la duplicación y obtención de imágenes son tareas críticas, se recomienda que éstos posean las siguientes características básicas:

- Alto desempeño. Alta velocidad de adquisición de la imagen.
- De trabajo intenso pesado (*Heavy-duty*). Se utilizaran cotidianamente.
- Producto certificado o probado en otros laboratorios con experiencia.
- Poseer interfaces de conexión *IDE/SATA/SCSI/USB/FIREWIRE*.
- Poseer de preferencia algún algoritmo para la generación de autenticación (por ejemplo, *MD5* o *SHA*) sobre la marcha.
- Detección de *HPA/DCO*⁹.
- Sin dispositivos de procesamiento o conversión intermedios.

⁹ Ver http://en.wikipedia.org/wiki/Host_protected_area;
http://en.wikipedia.org/wiki/Device_configuration_overlay; y
http://www.wiebetech.com/hpa_dco.php.

Figura 39. Duplicadores: *Tableau TD1 (A)* y *Logicube Talon (B)*



Fuentes: (A) <http://www.tableau.com>; (B) <http://logicubeforensics.com>

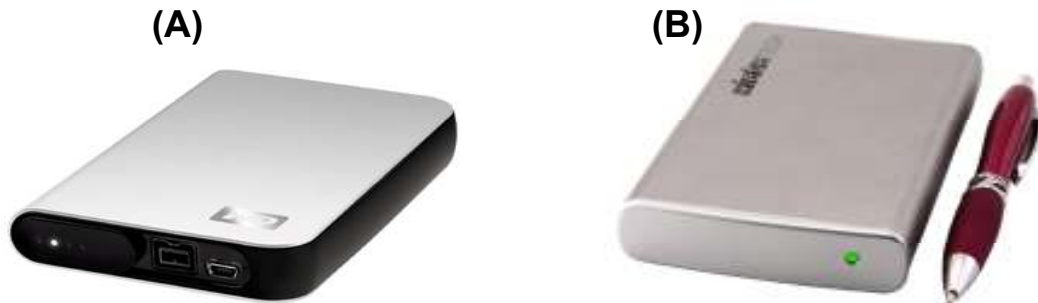
Si la carga de trabajo en este aspecto fuera abrumadora, se puede optar por duplicadores de múltiples discos por ejemplo, los productos ofrecidos por <http://diskology.com> los cuales pueden trabajar con varios discos simultáneamente.

3.9.3. Dispositivos móviles de almacenamiento masivo

Generalmente, el perito tendrá que copiar grandes cantidades de información por diversos motivos, por ejemplo, para trasladar la información a tribunales, para realizar procesos paralelos, para poseer un respaldo contra pérdidas, etc. En este tipo de situaciones es necesario contar con medios de almacenamiento masivo externos. Actualmente, existen productos que poseen un almacenamiento que va, desde 500 *gigabytes* (como los mostrados en la figura 40), hasta 3 *terabytes*¹⁰.

¹⁰ Ver <http://www.wiebetech.com>.

Figura 40. **Discos duros externos: (A) Western Digital MyPassPort Studio y (B) Wiebetech ToughTech FS Mini**



Fuentes: (A) <http://www.wdc.com>; (B) <http://www.wiebetech.com.com>

3.10. Materiales

A continuación se describen algunos materiales útiles; sin embargo, otros no contemplados en el presente trabajo también pueden resultar necesarios, por ejemplo, soldadoras y aspiradoras.

3.10.1. Cintas adhesivas y aislantes

Las cintas adhesivas y aislantes tienen muchos usos, desde el aislamiento de conductores de electricidad hasta para la fijación temporal de componentes o conexiones para evitar los enredos de los cables.

3.10.2. Rotuladores

Las etiquetas adhesibles o *stickers* son muy importantes, debido a que permiten rotular dispositivos, cables, *sockets*, etc. para ordenar el trabajo realizado, especialmente aquéllos con múltiples elementos. Este etiquetado puede realizarse en forma legible y sencilla utilizando rotuladores, los cuales

vienen en diferentes formas, tamaños y capacidades. Actualmente se han comercializado los digitales con teclado y memorias. Éstos son un complemento ideal para la documentación del proceso al permitir la colocación de etiquetas con observaciones, fechas, números, etc. a color dentro de las fotografías o vídeos.

Figura 41. **Muestra de rotulador (etiquetador)**

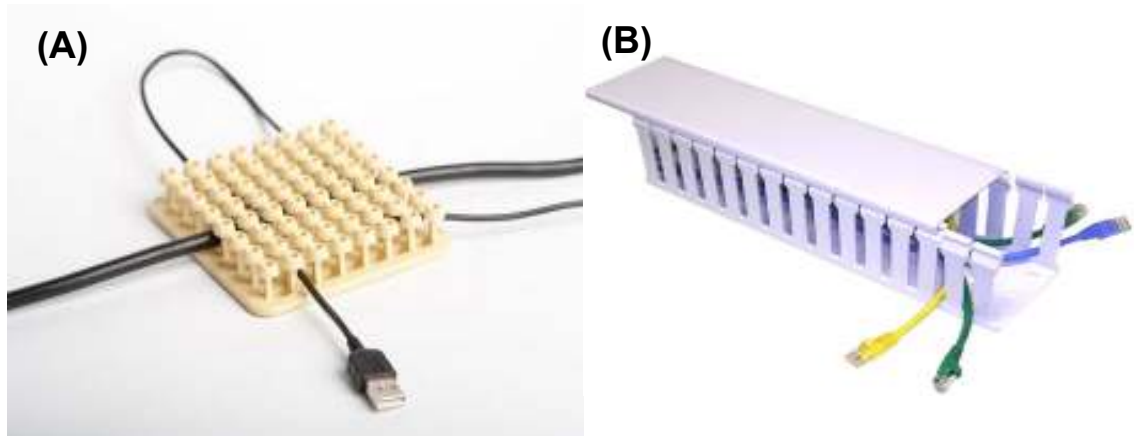


Fuente: <http://www.brother-usa.com>

3.10.3. Sujetadores y organizadores

Para mantener la estación de trabajo con el mayor orden posible se requiere de sujetadores y organizadores de cables, baterías, herramientas manuales (destornilladores, alicates, pinzas, etc.), de tal forma que cada cosa tenga su lugar. Esto es especialmente necesario con los cables de datos y energía en el sentido que una desconexión accidental puede producir pérdida de información o del trabajo realizado.

Figura 42. **Ejemplos de organizadores de cables de uso común**



Fuentes: (A) <http://tec.nologia.com>; (B) <http://cableorganizer.com>

3.10.4. **Pinza lagarto**

A pesar que el nombre es un poco coloquial, es con el que se le conoce a estas pinzas en Guatemala. Éstas son muy útiles para realizar conexiones eléctricas temporales y puentes de prueba utilizados para verificar conexiones, previo a soldar o empalmar.

Figura 43. **Ejemplo de pinzas cocodrilo**



Fuente: <http://www.virtualvillage.es>

3.10.5. Lijas para metales

Estos abrasivos se utilizan para afinar o suavizar las superficies y para limpieza mediante frotamiento de algún tipo de corrosión u óxido o para remover pinturas o barnices donde no se puede utilizar productos químicos que pueden dañar el dispositivo. Muy útiles, por ejemplo: para ver números de serie, modelo, versión, detalle de placas, etc., cuando por alguna razón éstos tienen suciedad u otro tipo herrumbre.

En electrónica e informática, las más utilizadas son las de óxido de aluminio y carburo de silicio sobre tela y grano medio-fino (i.e. 100 - 180).

3.10.6. Escobillas

Éstas son indispensables para limpiar superficies difíciles de alcanzar, por ejemplo, aquellos espacios en la circuitería dentro de un dispositivo electrónico. Existen algunos productos en el mercado consistentes en escobillas con boquillas especiales que pueden conectarse a aspiradoras a fin de eliminar la mota o el polvo que se desprende al realizar la limpieza. El laboratorio deberá contar con un conjunto de escobillas de variados tamaños con cerdas de material antiestático.

Figura 44. **Set de escobillas antiestáticas de uso forense**



Fuente: <http://www.ashbrush.com/>

3.10. Costos aproximados

Los productos y los precios mostrados a continuación fueron obtenidos a través de su búsqueda en *Internet* en diciembre de 2010 y constituyen solamente una guía o base de cálculo. La mayoría de productos tienen un precio indicado en dólares; por lo tanto fue necesario realizar la conversión a quetzales que a la fecha es aproximadamente de Q. 8,50 por cada dólar. Adicionalmente, se tomó un enfoque pesimista, ya que se redondeó al número entero siguiente. Por ejemplo, si el producto tenía un precio de \$ 993,50, el precio mostrado en la tabla sería Q. 8 449,00 (994,00 x 8,50); cabe mencionar, que los precios mostrados, no incluyen el manejo, envío, impuestos, seguros, etc.

Por supuesto, la tecnología y los precios variarán con el tiempo y por lo tanto se sugiere la actualización y adecuación de los productos y sus precios a las necesidades particulares. La investigación de mercado en el futuro puede brindar agradables noticias, especialmente por la tendencia del *software* gratuito y las exoneraciones para algunas instituciones de gobierno mediante ley interna expresa o solicitud ante la Superintendencia de Administración Tributaria (SAT). De preferencia, se sugiere considerar aquellas soluciones globalizadas (o *suites*), que cubran gran parte de los procesos informático-forenses.

Al momento no existe una herramienta de *software* que pueda realizar todas las tareas. Por lo tanto, se deben someter a evaluación por parte de la gerencia del laboratorio (o del proyecto). Sin embargo, las soluciones más aceptadas por las instituciones forenses y laboratorios provienen de las siguientes empresas:

- *GuidanceSoftware*
- *AccessData*
- *Paraben*
- *Maresware Computer Forensics Software*

La tabla IV muestra algunos de los precios de los productos listados en el presente capítulo.

Tabla IV. Precio de productos para el laboratorio

No.	Producto	Precio (en Quetzales)	Descripción
1	Tester digital	3 952,50	Tester Fluke 287
2	SAFE CD BOOT	10 200,00	SAFE Enterprise edition - MS-WIN / INTEL. Capacidad de obtener <i>hash</i> , preparación de disco destino (formateo y limpieza - <i>sanitazion</i> , soporte básico de búsqueda, puede reiniciar máquina indicio y bloquear el disco duro, etc.
3	SAFE HARD DISK BLOCKER (Software)	1 870,00	SAFE HDB MS-WIN/INTEL
4	Hardware para obtención de imágenes	10 115,00	TABLEAU TD1, soporte para SATA e IDE, velocidad de transferencia de hasta 6GB/min. Soporte de <i>Hash</i> (md5 y sha1), preparación de disco destino, soporte de imagen de disco a disco (directo), etc.
5	Logicube talon	15 300,00	Logicube talon, soporte para IDE/UDMA/SATA, captura de discos SCSI via cable USB, autenticación MD5 y SHA-256, capacidad de seleccionar distintos para CD y DVD.
6	Duplicador de alto rendimiento	50 872,50	Image MASter 4008i; para varios discos duros.

Continuación tabla IV.

7	Disco externo de alta transferencia <i>Western Digital.</i>	1 827,50	<i>Western Digital.</i> Velocidad de transferencia por bus serie (1394b)800 Mb/s (Máx)
8	Recuperación de archivos	425,00	<i>Quetek File Recovery.</i> Recuperación de nombre original, contenido, rutas y fechas para sistemas <i>NTFS, FAT 32/16/12, etc.</i>
9	Búsqueda de texto	1 105,00	<i>Paraben text search</i>
10	Copiador de alto desempeño de CDs, DVDs y discos <i>Bluray</i>	11 475,00	<i>VinPower BD-LG-3.</i> Buffer de 64 MB, 60 CD/hora, 30 DVD/hora, HD de 160 GB, 52X
11	<i>Forensic toolkit</i>	19 040,00	<i>AccessData toolkit ftk3</i>
12	Paraben Bundle	33 957,50	<i>Paraben P3 Command kit</i>
13	<i>Encase Forensics (Law Enforcement)</i>	25 500,00	<i>Guidance Software Encase Forensics</i>
14	<i>Password Cracker</i>	36 082,50	<i>Tableau TACC 1441e</i>
15	<i>Decryption tool</i>	12 707,50	<i>AccessData DNA</i>
16	<i>Paraben CSI Stick</i>	2 550,00	Analizador y extractor de información de celulares (portable)
17	<i>Device Seizure Command Kit</i>	15 929,00	Analizador y extractor de información de celulares (kit standard)
18	Rotulador (etiquetador)	306,00	<i>Brother PT-80 P-touch Electronic Labeling System</i>
19	Bolsa bloqueadora de radio frecuencias	255,00	<i>Paraben RF blocker bag (Stronghold)</i>
20	Caja bloqueadora de radio frecuencias	12 707,50	<i>Paraben RF blocker box</i>
21	Cellebrite Universal Forensic Extraction Device	35 700,00	<i>Cellebrite UFED</i>
22	Set de destornilladores de precisión	1 020,00	Allen, hex, torx, etc

Continuación tabla IV.

23	Set de alicates para electrónica	722,50	Set de 6 alicates/cortadora
24	Tijeras y cuchillas	255,00	Set de 2 tijeras y 2 cortadoras
25	Martillo	115,00	Martillito de mazo plástico
26	Espatulillas	85,00	Set de dos espatulillas
27	Reglas forenses	382,50	Set de reglas para fotografía forense
28	Pie de rey	255,00	Versión electrónica con lector digital
29	Lupas	387,00	Set de 6 lupas
30	Lámpara con Lupa de pedestal	2 380,00	Para ensamble en escritorio
31	Cámara fotográfica	50 065,00	Nikon D2X
32	Convertidores disco duro	382,50	IDE SATA
33	Lector bloqueador multitarjeta	425,00	Tableau TDA8-M Media Reader
34	Juego de sincronizadores	7 650,00	Set de 50 cables para PDAs y Celulares varias marcas y modelos
35	Adaptador genérico de energía	935,00	Adaptador con puntas adaptables al conector

Fuente: elaboración propia

4. MOBILIARIO Y EQUIPO

Este capítulo describe someramente, el mobiliario y equipo apropiado, tanto para el personal administrativo, como para el de almacén de evidencias. Algunas consideraciones son básicas pero útiles para la protección de los indicios y para el desempeño óptimo de las labores propias del laboratorio.

4.1. Estanterías, gabinetes y archivos

Las estanterías son muebles que se utilizarán para almacenar los indicios, las herramientas, algunos dispositivos forenses y los materiales utilizados. Deben estar construidas de acero inoxidable con paños cubiertos de plástico (v.g. polipropileno), con mecanismos de aseguramiento que eviten que los objetos caigan con facilidad. La utilización de cubiertas o chapas plásticas es importante porque: son de mantenimiento y limpieza sencillos; tienen bajo peso; pueden ser antideslizantes y resistir fuertes impactos; ofrecen alto aislamiento térmico, eléctrico y a la corrosión; y, existe gran variedad de colores. Dichas estanterías pueden poseer componentes de movimiento: rodos, montaje sobre carrileras u otra forma de desplazamiento, y de fijación al suelo.

Finalmente, las estanterías deben organizarse de tal forma que sean:

- Accesibles, tanto horizontal como verticalmente, es decir, que exista espacio suficiente para el movimiento de escalerillas y el tránsito con carretillas; éstas adicionalmente, no deben ser tan altas que pongan en riesgo, tanto los indicios como al personal.

- Reconocibles a través de la utilización de códigos y colores que permitan encontrar el indicio fácilmente. Esta característica puede resultar útil como dato para el programa informático de seguimiento de casos.
- Seguras y manejables: deben soportar el peso de los indicios y protegerlos con un alto grado de confiabilidad contra accidentes o temblores, especialmente al momento de darles mantenimiento.

Figura 45. **Estantería para almacén de evidencias**



Fuente: <http://www.manutan.es>

Los gabinetes deben construirse de acero inoxidable y plástico de alta resistencia, de preferencia en colores claros. Éstos pueden situarse en variados espacios, por ejemplo, en el área administrativa para guardar los materiales de oficina, en el laboratorio para utilizarse como botiquín de primeros auxilios, etc., la ventaja de éstos, es que pueden colocarse en el piso o en las paredes.

Los archivos son muy útiles para el almacenamiento y clasificación de papelería y por lo tanto su uso es general, tanto para las áreas administrativas como las de laboratorio. Éstos deben ser de acero inoxidable con gavetas y cerraduras individuales.

Por supuesto, no deben faltar los equipos telefónicos y de comunicación interna (v.g. el sistema de voceo general para emergencias). Entre otros deben considerarse los siguientes: destructoras de papel, multi-funcionales (impresora, escáner, fotocopidora, etc), proyectores, entre otros.

4.2. Carretillas y equipos móviles

Éstos se utilizan básicamente para el transporte de los indicios (evidencias), dentro del edificio. Desde el ingreso y traslado al almacén y su posterior movimiento a las diferentes áreas del laboratorio. Se incluyen los *troquets*, carretones, carretillas con mesetas elevadoras, etc.

Figura 46. **Troquet plegable (A); carretilla contenedor (B)**



Fuente: <http://www.manutan.es>

Algunos equipos de transporte pueden utilizarse para el traslado de las evidencias a los tribunales, como la carretilla plegable mostrada en la figura 47.

Figura 47. **Carretilla plegable con ruedas y brazo extensible**



Fuente: <http://www.manutan.es>

4.3. Escritorios

Los escritorios del personal administrativo deben estar en ambientes modulares que permitan el ordenamiento del espacio en forma arquitectónica, de material anti-reflejante y anti-acústico. Los escritorios y los paneles de los módulos deben contar con ductos ocultos prediseñados para acoplar fácilmente las tomas de energía eléctrica, red informática y telefónica; los escritorios, deben poseer sus respectivas gavetas y espacios de almacenamiento de utensilios o papelería.

Figura 48. **Modular con divisiones para las áreas de trabajo**



Fuente: <http://www.manutan.es>

El diseño de las sillas debe ser ergonómico (con buen apoyo lumbar y ajustables, tanto en altura como en ángulo de inclinación/reclinación), giratorias, con rodamientos, y de preferencia, de estructura de PVC de alto impacto.

Figura 49. **Diseño de silla ajustable (ergonómica)**



Fuente: <http://www.simply-ergonomic.co.uk>

En el área de ingreso de indicios deben colocarse mostradores de acero inoxidable con recubrimiento plástico en color claro; éstos deben poseer anaqueles graduables en altura para facilitar la recepción de los indicios de diferentes tamaños y pesos, con almohadillas antideslizantes en la superficie.

Figura 50. **Mostrador de recepción de indicios**



Fuente: <http://www.indimob.net>

La sala de espera puede tener sillas estáticas de pvc con estructura metálica, anti-deslizantes y separadas entre sí, por un espacio considerable para el acomodamiento de las personas y de los indicios.

4.4. Equipo Informático de la estación de trabajo forense

4.4.1. Requisitos mínimos de *hardware*

El equipo informático para el análisis forense debe poseer características mucho más avanzadas que las computadoras tradicionales utilizadas en Guatemala, en este sentido debe poseer:

- Un procesador basado en arquitecturas x86, de alto desempeño relativo (mayor o igual 2,66 GHz), de alto rendimiento, sin calentamiento crítico, con memorias caches de buen tamaño y velocidad (al menos 8Gb a 2,66GHz), etc. Puede ser un procesador Intel o AMD de 64 bits (Pentium D o AMD64) ; esto permitirá anticiparse o estar preparado al cambio natural de 32 a 64 bits, lo que facultará el direccionamiento a un tamaño mayor de memoria y brindará un mejor desempeño.
- Un tamaño de memoria RAM de por lo menos 6 Gb.
- Por lo menos 1 Tb y 7 200 rpm en disco duro.
- Por lo menos con 6 puertos para controladores SATA/IDE y 2 puertos con soporte SCSI.
- Con 2 o más puertos FireWire IEEE 1394b.
- Como mínimo 6 conexiones USB.
- Slot para conexión de soporte de disco de 3,5".
- Dos o más canales para controladores PCIe.
- CD/DVD/Bluray Drive.
- Todas las demás conexiones tradicionales (DB-9, DB-15, DB-25, Din/PS2, Ethernet LAN, Jacks de audio, etc.).

- Se recomienda el uso de dos monitores de por lo menos 48,26 cm (19 pulgadas). Esto amplía el espacio del escritorio de trabajo (pantalla), debido a que muchas veces se necesita más espacio para organizar ventanas, facilitar la realización de varias tareas a la vez, comparación de documentos, etc.

Debido a que ensamblar, configurar y afinar (*tunning*), un equipo con los requerimientos mostrados no es sencillo, comúnmente, los laboratorios de informática forense optan por opciones de fábrica como las ofrecidas por las empresas *Digital Intelligence* (www.digitalintelligence.com) y *Forensic Computers Inc.* (<http://www.forensic-computers.com>).

Figura 51. **Estación *FRED***



Fuente: <http://www.digitalintelligence.com>

Figura 52. **Estación *Forensic Tower III***



Fuente: <http://www.forensic-computers.com>

Los equipos mostrados en las figuras anteriores son soluciones intermedias, debido a que ambas empresas también comercializan equipos más poderosos y brindan por un costo adicional la instalación o ensamble de bloqueadores de disco duro, soporte para *RAID*, almacenamiento en cinta magnética, etc.

4.4.2. Requisitos mínimos de *software*

Entre los requisitos mínimos de *software* (aplicaciones de 64 *bits* de preferencia) de la estación forense se encuentran:

- *Windows XP 64* pre-instalado y configurado con soporte de arranque para otras plataformas (*MS-DOS, Linux, etc.*).

- Antivirus (v.g. *Nod32*) con protección contra intrusos, *firewall* y licencia de actualización diaria.
- Cualquiera de las *suites* siguientes (en orden de aceptación por los laboratorios).
 - *Encase 64*
 - *Forensic Toolkit*
 - *Paraben Bundle Solution*

4.5. Costos aproximados

Estos costos son solo una guía para la consideración de adquisición de mobiliario y equipo para una sola estación, es decir, un mueble de recepción de indicios, una estantería, una estación forense, etc. Por lo tanto, esto, se tendrá que adecuar luego de hacer un cálculo del número de trabajadores, la cantidad de unidades de proceso, la demanda de peritajes forenses, etc.

Los productos y los precios mostrados en la tabla V fueron obtenidos a través de su búsqueda en *Internet* en el 2010. Los productos tienen un precio indicado en dólares (y euros en algunos casos), por lo tanto fue necesario realizar la conversión a quetzales, que a la fecha es de aproximadamente Q. 8,50 por cada dólar. Adicionalmente, se tomó un enfoque pesimista, ya que se redondeó al número entero siguiente. Por ejemplo, si el producto tenía un precio de \$ 993,50, el precio mostrado en la tabla sería Q. 8 449,00 (\$ 994,00 x Q 8,50 / \$ 1,00); los precios mostrados, no incluyen el manejo, envío, impuestos, seguros, etc.

Tabla V. **Costos básicos mobiliario y equipo**

No.	Producto	Precio (en Quetzales)	Descripción
1	Mueble modular	5 300,00	Modular para delimitación de la estación forense: escritorio, computadora, área de trabajo, etc.
2	<i>Troquet</i> plegable	2 590,00	Traslado de equipos (indicios) de 80 libras o más.
3	Carretilla-contenedor	5 958,50	Traslado de equipos (indicios) para pesos menores de 30 libras.
4	Estantería (unidad)	2 220,00	3 áreas verticales con 5 entrepaños.
5	Caja plegable - carrito	630,00	Para transporte de objetos dentro del laboratorio o al exterior. Soporte de aproximadamente 50 libras.
6	Mostrador	13 800,00	Para el área de recepción de indicios en la sección del almacén.
7	Estación forense <i>FRED DX</i>	67 991,50	Computadora para el trabajo forense.
8	Estación forense <i>Forensic Tower III</i>	94 520,00	Computadora para el trabajo forense
9	Silla Ergonómica de escritorio <i>ergohuman chair</i>	3 400,00	Para oficinas y muebles del área administrativa.

Fuente: elaboración propia

5. DISEÑO DE LA ESTACIÓN DE TRABAJO FORENSE

Debido a la gran cantidad de tiempo invertido por un perito en su estación de trabajo, es necesario que ésta se ajuste a su antropometría estructural y funcional, de tal forma que la interacción con los muebles, herramientas y dispositivos de trabajo sea lo más eficiente posible y así se eviten problemas de aumento de fatiga innecesaria, enfermedades o lesiones por mala postura (neuropatía del túnel carpiano, tendinitis, lumbago, etc.), accidentes, tensión nerviosa, entre otras. Adicionalmente se deben considerar factores como ventilación, temperatura, iluminación, aislamiento de ruido y vibración; además de las consideraciones ergonómicas, el sitio de trabajo también debe incluir los servicios de electricidad, red informática y telefónica.

5.1. Diseño ergonómico del módulo

Todas las empresas encargadas de diseñar y desarrollar productos para ser utilizados por personas (escritorios, automóviles, herramientas, etc.), consideran los factores antropométricos del mercado (i.e. usuarios), y los criterios ergonómicos que deben cumplir dichos productos. Para esto utilizan tablas antropométricas estratificadas por género, edad, región, etc. que están disponibles en muchos países (v.g. Japón, Hong Kong, Estados Unidos, Finlandia, etc.); lamentablemente, este tipo de información al día de hoy no está disponible¹¹ en la mayoría de países latinoamericanos (exceptuando México y Colombia). Por lo tanto, para el diseño de la estación se han tomado datos

¹¹ La Universidad de San Carlos guarda un registro general de datos de sus egresados (altura, peso, masa muscular, etc.) y algunos hospitales tienen información solamente de niños. Sin embargo, para el diseño se deben contemplar otros datos como longitud de brazos, piernas, caderas, etc.

antropométricos de México como base. Debido a la variabilidad de las medidas y proporciones humanas respecto de las medias¹², los productos deben incluir mecanismos de adaptación o graduación.

Aunque para realizar el diseño y construcción de un puesto de trabajo se deben considerar las posiciones: parado y sentado. Aquí se realizará el estudio solamente con base en la segunda, debido a que ésta es la posición más frecuente de trabajo.

Tomando en cuenta lo anterior, los datos antropométricos más significativos para el modelado de la estación de trabajo son los siguientes.

- A. Altura poplítea: distancia vertical desde el suelo hasta el punto más alto de la depresión poplítea, estando la persona sentada con ambos pies apoyados en forma plana sobre el suelo y el borde del asiento no ejerciendo presión en la cara posterior del muslo derecho; los muslos deben estar en posición horizontal formando un ángulo de 90 grados con el tronco y las piernas.
- B. Distancia sacro-poplítea: distancia horizontal medida desde el punto correspondiente a la depresión poplítea de la pierna, hasta el plano vertical situado en la espalda del individuo, cuando tiene el muslo en posición horizontal y formando un ángulo de 90 grados con las piernas y el tronco.

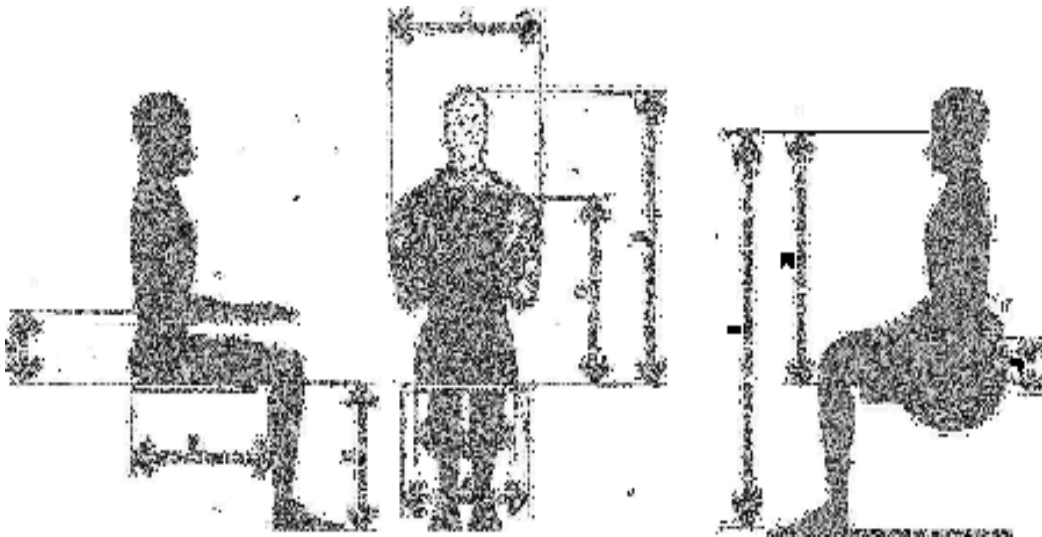
¹² “En un estudio antropométrico de la *AirForce (USA)*, se comprobó que de 4,000 personas investigadas, ninguna se encontraba en el intervalo del 30% de la media en una serie de 10 mediciones. Se ha generalizado en exceso el concepto de la persona estándar, hasta tal punto que hay autores, que a partir de la estatura de la persona son capaces de determinar todas las demás dimensiones del cuerpo; como puede comprenderse, esto es una ficción, que conduce inevitablemente a diseños erróneos.” (Publicaciones de Ingeniería de Sistemas, la Ergonomía en la Ingeniería de Sistemas, MONDELO, Pedro R.; TORADA Enrique Gregori. p. 33.)

- C. Altura codo-asiento: distancia desde el plano del asiento hasta la depresión del codo, cuando el sujeto tiene su brazo paralelo a la línea media del tronco y el antebrazo forma un ángulo de 90 grados.
- D. Altura hombro-asiento: distancia vertical desde el plano del asiento hasta el borde superior del hombro en posición de descanso.
- E. Distancia coronilla-asiento: distancia vertical desde el plano del asiento hasta el borde superior de la coronilla.
- F. Anchura codo-codo: distancia horizontal entre los codos con la persona sentada y los brazos colgando libremente, los antebrazos doblados y las manos sobre las piernas.
- G. Anchura de caderas sentado: distancia horizontal que existe entre las caderas, encontrándose el sujeto sentado con el tórax erguido y perpendicular al plano del asiento.
- H. Anchura hombro-hombro: distancia máxima que separa los músculos deltoides.
- I. Altura ojos-suelo: distancia vertical medida desde el eje horizontal que pasa por el centro de la pupila del ojo derecho hasta la superficie del suelo, cuando el sujeto está sentado y el tórax forma un ángulo de 90 grados con el asiento.
- J. Altura muslo-asiento: distancia vertical desde el punto más alto del muslo derecho a nivel inguinal, tomando como referencia el pliegue cutáneo que se forma entre el muslo y la cintura pélvica, y el plano horizontal del asiento al

estar el sujeto sentado, con un ángulo de 90 grados entre el tórax y el muslo.

- K. Altura ojos-asiento: distancia vertical medida desde el eje horizontal que pasa por el centro de la pupila del ojo derecho hasta la superficie del asiento, cuando el sujeto está sentado y el tórax forma un ángulo de 90 grados con el asiento.

Figura 53. Medidas antropométricas comunes para persona sentada

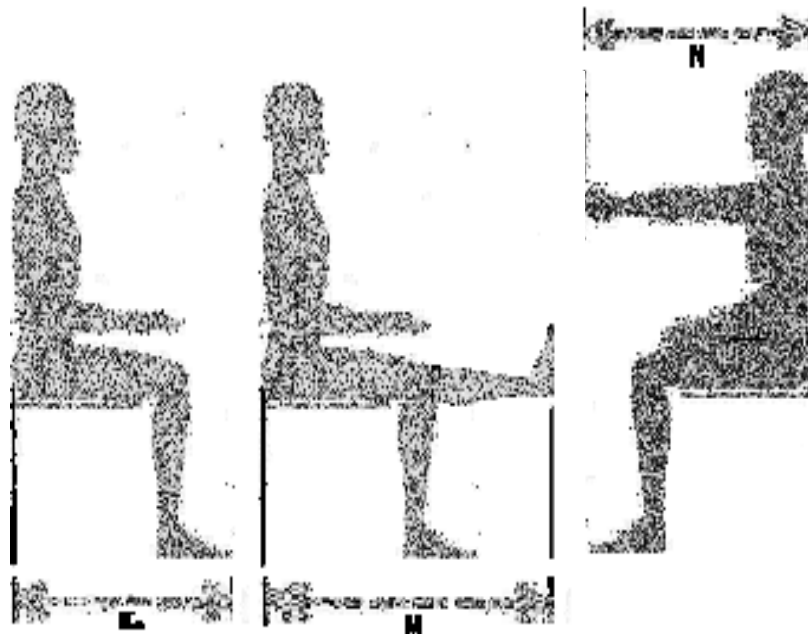


Fuente: PANERO, Julius. Las dimensiones humanas en los espacios interiores.p. 61

- L. Distancia nalga-punta del pie: distancia horizontal desde el punto de intersección de 90 grados con la vertical del respaldo a la punta del pie en ángulo cuadrado con el muslo.
- M. Distancia nalga-talón: distancia horizontal desde el punto de intersección de 90 grados con la vertical del respaldo al talón del pie en ángulo cuadrado con el muslo.

N. Alcance máximo del brazo: es la distancia horizontal medida desde la espalda hasta el eje vertical imaginario que se produce en la mano con el puño cerrado, cuando la persona está sentada con la espalda vertical en el respaldo y tiene el brazo extendido al máximo y perpendicular al eje del torso.

Figura 54. **Medidas antropométricas comunes para persona sentada (continuación)**



Fuente: PANERO, Julius. Las dimensiones humanas en los espacios interiores. p. 75-82, 100.

Considerando que la mayoría de técnicos de Informática-forense son hombres comprendidos entre los 20 y 50 años, se toman los datos estadísticos de la tabla VI para las medidas antropométricas previamente enumeradas.

Tabla VI. Dimensiones antropométricas humanas para el hombre¹³

Item	Nombre de la dimensión	Distancia media (centímetros) X	Desviación estándar (centímetros) σ	Adicionar aproximadamente por ropa ligera (centímetros) h
A.	Altura poplítea	43,69	2,49	3,81
B.	Distancia sacro-poplítea	48,77	2,51	1,27
C.	Altura codo-asiento	23,11	2,64	1,27
D.	Altura hombro-asiento	62,48	3,18	2,54
E.	Distancia coronilla-asiento	90,68	3,66	8,89
F.	Anchura codo-codo	38,72	4,26	2,54
G.	Anchura de caderas sentado	34,04	2,39	2,54
H.	Anchura hombro-hombro	45,47	2,54	2,54
I.	Altura ojos-suelo	127,51	3,58	2,54
J.	Altura muslo-asiento	12,45	No Disponible	1,27
K.	Altura ojos-asiento	78,74	3,58	2,54
L.	Distancia nalga-punta del pie	75,44	4,88	2,54
M.	Distancia nalga-talón	102,88	3,68	3,81
N.	Alcance máximo del brazo	68,64	4,92	No disponible
	Peso (en libras)	156,10	16,60	

Fuente: Morelos Laboratorio de Producción. Antropometría; Instituto Tecnológico y de Estudios Superiores de Monterrey Campus. Enero 2007.

Estas medidas son utilizadas para realizar el diseño, tanto de las sillas como del escritorio que formarán parte de la estación de trabajo.

Para el acotamiento de los requerimientos de la silla se recurre principio del diseño para un intervalo ajustable mencionado por Pedro R. Mondelo¹⁴, éste

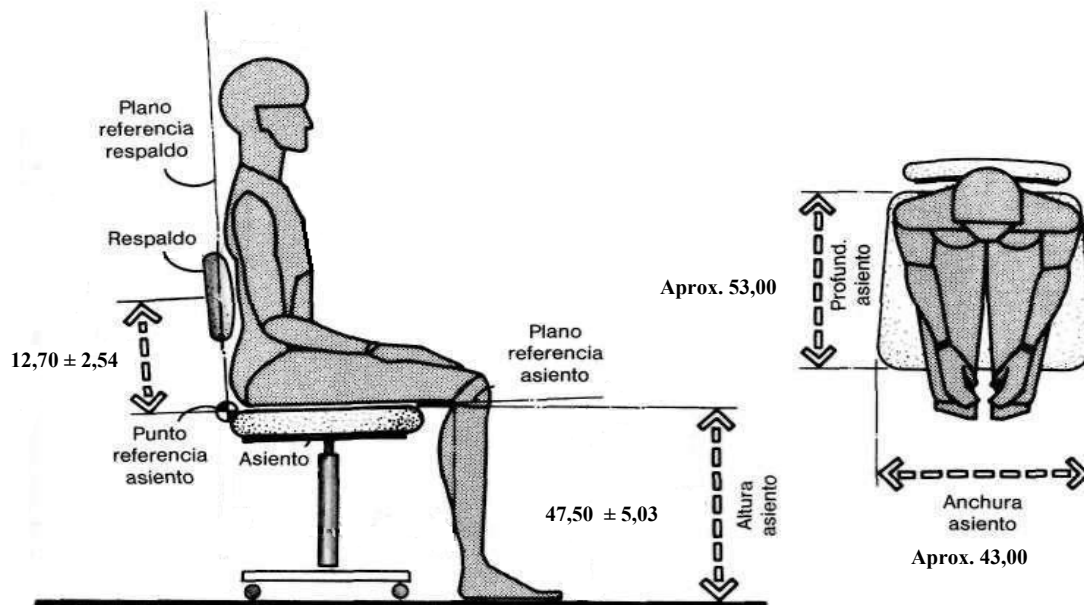
¹³ De la tabla fuente original, solamente se consideraron los datos del percentil 50 para personas sentadas con una holgura de vestimenta ligera y se adaptaron a los nombres antropométricos dados dentro del presente documento.

¹⁴ MONDELO, Pedro R. et al. Diseño de puestos de trabajo (Ergonomía 3), p. 54.

al contrario de los diseños fijos, introduce mecanismos de ajuste dentro de los márgenes establecidos como normales, lo que permite a la persona adecuar la silla a sus características corporales. Por esta razón, este diseño resulta caro. Actualmente, muchas empresas incluyen en el diseño de sillas estos mecanismos de graduación. (Ver figuras 49 y 57).

De acuerdo a lo anterior y tomando en consideración los datos antropométricos de la tabla VI, los requerimientos de la silla son los siguientes¹⁵.

Figura 55. **Diseño ergonómico de la silla de la estación de trabajo (medidas en centímetros)**



Fuente: PANERO, Julius. Las dimensiones humanas en los espacios interiores. p. 127.

¹⁵ Para las dimensiones centrales y el ajuste se tomó la media más la holgura por indumentaria ligera (i.e. $X+h \pm \sigma$). Adicionalmente, para el asiento se tomaron las medidas máximas debido a que comúnmente no se encuentran mecanismos de graduación para éstas y finalmente, no se muestran los radios de las curvaturas. Las medidas mostradas "cubren" una dispersión de 1σ , ésta podría ampliarse para incluir más elementos de la población, pero afectaría la factibilidad de colocación de los ajustes o graduaciones.

Dicha silla de trabajo debe soportar por lo menos 400 libras. El margen aquí se aumentó, debido a que comúnmente los trabajadores sedentarios tienden a pesar mucho más que el promedio.

El soporte a las 5 vértebras lumbares debe ser el apropiado, debido a que éstas soportan gran parte del peso del tronco¹⁶. La tabla VI, no contiene información de la longitud lumbar, ni de la altura asiento al punto central lumbar, debido a que esa región varía significativamente de una persona a otra¹⁷ (10,16 a 15,24 cm.). Sin embargo, para el diseño mostrado se considerará un soporte curvo-suavizado de aproximadamente 12,70 cm., con graduación de $\pm 2,54$ cm.

Figura 56. **Fuerzas de soporte que debe ejercer la silla en región lumbar**



Fuente: PANERO, Julius. Las dimensiones humanas en los espacios interiores. p. 65.

¹⁶ Ver <http://www.nlm.nih.gov/medlineplus/spanish/ency/article/000442.htm>; "La mayoría de las hernias se presentan en la parte inferior de la espalda o área lumbar de la columna. La hernia discal lumbar se presenta 15 veces más frecuentemente que la hernia discal cervical (del cuello) y es una de las causas más comunes de lumbago. Por su parte, los discos cervicales resultan afectados en un 8% de los casos, mientras que los discos de la espalda alta y media (torácicos) en sólo el 1 al 2%."

¹⁷ HERMANMILLER (<http://www.hermanmiller.com>). "Ergonomic criteria for the design of the Aeron chair", *The antropometrics of Fit*, Bill Stumpf, Don Chadwick, and Bill Dowell, p. 3; *Importance of Chair Designs That Support the Lower Back*, CEU (Continuing Education Unit), p. 4.

Adicionalmente, la silla debe poseer las siguientes características:

- Suave curvatura en cascada el borde de la silla: para aliviar la presión sobre los vasos sanguíneos de los muslos y prevenir el entumecimiento de las piernas, los pies fríos y las venas varicosas. Este borde debe inclinarse suavemente hacia abajo y no debe presionar el muslo.
- No exageradamente acolchada: esto a la larga puede promover la mala postura de la espalda, debido a que el acolchado tomará la forma del cuerpo. Adicionalmente, el acolchado puede provocar calor desagradable.
- Movilidad: la silla debe poder deslizarse sin esfuerzo para permitirle al cuerpo hacer movimientos o trasladarse sin dificultades.
- Apoya brazos: para que la silla soporte el peso de los brazos mientras trabaja (y no la parte superior de la espalda).
- Profundidad: la silla debe ser adecuada en profundidad, de tal manera que cuando la persona está sentada con la espalda bien apoyada, esto no debe molestar el doble natural de la rodilla.
- Altura: la silla debe ser suficientemente alta para que los muslos formen un ángulo de 90 grados con el piso.
- Apoya pies: este es un buen complemento para una silla, porque le permite a la persona ajustarse al respaldo y eventualmente cambiar la posición de los pies y las piernas para descanso.

Figura 57. **Silla ergonómica ajustable *AERON* de *HermanMiller***

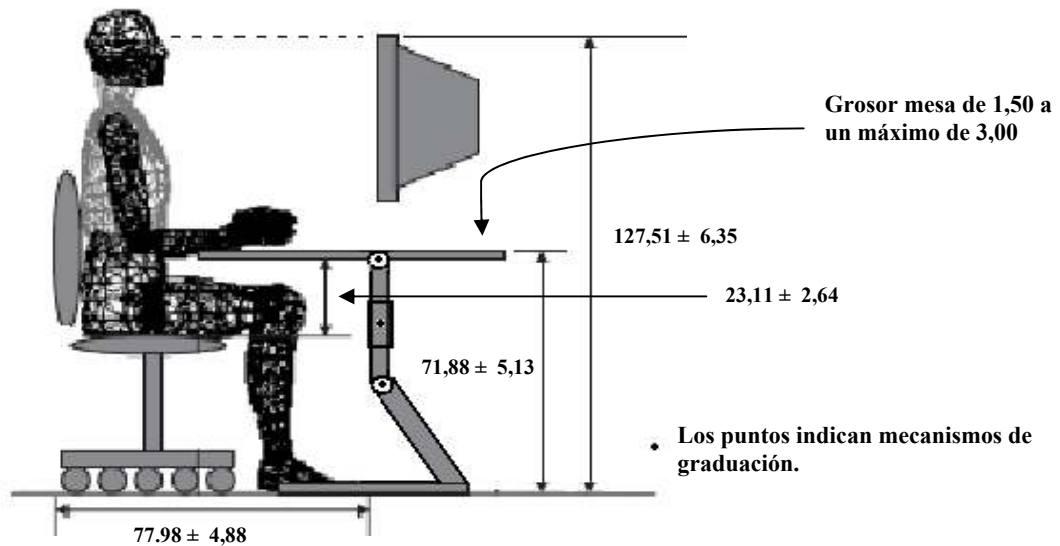


Fuente: <http://www.hermanmiller.com>

Para el diseño del escritorio de trabajo se deben tomar en cuenta el radio del alcance máximo funcional de los brazos en ángulos de 180 grados en el plano horizontal y 90 grados en el vertical, la distancia nalga-punta del pie, la altura codo-asiento, la altura poplítea, la altura ojos-suelo y se debe considerar una holgura aceptable para los movimientos de relajación de las piernas, comprendida comúnmente entre 90 y 110 centímetros desde el borde exterior de la mesa. De preferencia el mueble debe poseer mecanismos de graduación angular y desplazamiento vertical, de acuerdo a los índices o desviaciones de los promedios.

El diseño *grosso* del escritorio con las medidas centrales y los ajustes tomados de la tabla VI, se observa en la figura 58.

Figura 58. **Diseño básico del escritorio de la estación de trabajo (medidas en centímetros)**



Fuente: Adaptación basada en ATTWOOD, Dennis. *Ergonomic Solutions for the Process Industries, Specifications for a seated workstation*, p. 248. et. al.

En la actualidad existen empresas dedicadas a realizar este tipo de muebles con mecanismos de graduación como el mostrado en la figura 59.

Figura 59. **Armazón de escritorio de altura ajustable eléctricamente**



Fuente: <http://www.simply-ergonomic.co.uk>

5.2. Secciones de la estación de trabajo forense

Previo a la delimitación de las secciones de la estación de trabajo forense, se debe tomar en consideración las siguientes recomendaciones de espacio¹⁸:

- De preferencia, debe tener forma de U o bien cuadrada con un lado abierto y una distancia lineal mínima de 7,62 metros.
- La sección donde se ubica, tanto la computadora como el *hardware* forense (área de imágenes y análisis), por lo menos debe medir 1,53 metros. En esta sección deben colocarse en los paneles frontales las herramientas de mano de uso frecuente, los cables de sincronización, instrumentos de medición, etc. De acuerdo al presupuesto por estación, también puede considerarse algún traslape de áreas entre estaciones, especialmente en aquellos casos en que los peritos se comparten herramientas y *hardware*. Esto último es muy común debido a lo caro de las herramientas forenses.
- Se recomienda que el área para obtención de imágenes o duplicación, cuente con una longitud de 1,53 metros. Optativamente, de preferencia, separada del área de análisis, especialmente en aquellos casos de demanda alta de peritajes, debido a que se invierte gran cantidad de tiempo en la generación de imágenes. Por simplicidad, en la figura 60 se colocaron las áreas de obtención de imágenes y análisis en la misma estación de trabajo)

¹⁸ Medidas tomadas del borrador de anteproyecto "A Guide for Planning and Implementing a Computer Forensics Unit"; National Center for Forensic Science, The National Institute of Justice (NIJ). Revisado en febrero del 2008.

- El área administrativa de la estación de trabajo (donde se escriben los informes, se llenan formularios o investiga en libros, se prepara el testimonio, etc.), por lo menos debe medir 2,44 metros.
- La estación de trabajo debe contar con un área de almacenamiento temporal, de por lo menos 6,10 metros cuadrados con su propia área de energía eléctrica. Esto generalmente se logra con separadores horizontales o anaqueles empotrados en la pared para el ahorro de espacio.
- El área administrativa debe contar con gabinetes para el almacenamiento de material de escritorio (papel, lapiceros, engrapadoras, cuadernos, etc.), y archivos con llave para guardar informes, reportes y dictámenes de casos. Éstos deben ser de por lo menos 40 x 60 x 70 centímetros por lado. Esta área debe contar con anaqueles para almacenar libros, manuales de usuario, guías, referencias, etc. Además, debe incluir todo lo necesario para la conexión de impresoras y/o *scanners*.

También se recomienda que la estación forense cuente con:

- Dos monitores para la ampliación del escritorio (pantalla) de trabajo. Esto será muy útil para visualizar varios procesos -para no cerrar o minimizar ventanas-, comparar documentos o archivos en forma paralela, mantener en una pantalla diversos borradores y en otra la compilación de extractos, etc.

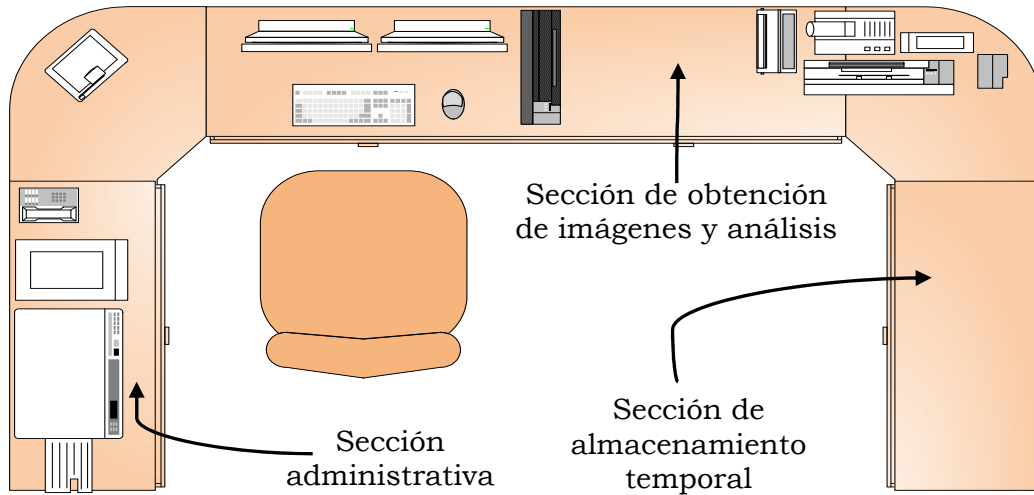
- Servicios necesarios: energía eléctrica, red, telefonía e *Internet*. En el caso de la energía eléctrica, ésta debe proveerse en varias tomas y reguladas. La estación debe poseer una fuente in-interrumpible de energía (*UPS*).
- De acuerdo al presupuesto, también puede utilizarse una computadora adicional para la sección administrativa. Para ahorrar espacio se puede utilizar un dispositivo llamado *KVM (Keyboard-Video-Mouse)* que permite “manejar” dos o más computadores utilizando solamente un monitor, un teclado y un ratón. Ésta contará con los servicios de red (programa de seguimiento de casos, red interna, *Internet*, etc.), y la otra (la estación forense) exclusivamente para el trabajo de análisis. Esto se acostumbra en algunos laboratorios por seguridad debido a que mantiene la evidencia aislada de cualquier potencial contaminación por cualquier ataque, intrusión, virus, etc.
- Se deben generar las políticas para restringir el acceso a personal no autorizado al área del laboratorio y las estaciones deben bloquearse automáticamente si no hay actividad en un tiempo determinado por la gerencia. Las pantallas de preferencia deben colocarse fuera de la vista si existieran ventanas.
- El área de almacenamiento temporal puede incluir, tanto los indicios como todos los medios de almacenamiento utilizados para las imágenes.
- Todo el cableado propio de la estación debe estar oculto en los ductos del modular para evitar que queden cables en el suelo susceptibles de arrastrarse con las piernas, los pies, escobas, etc.

El módulo de la estación de trabajo está dividido en tres secciones:

- Administrativa.
- Obtención de imágenes y análisis.
- Almacenamiento temporal.

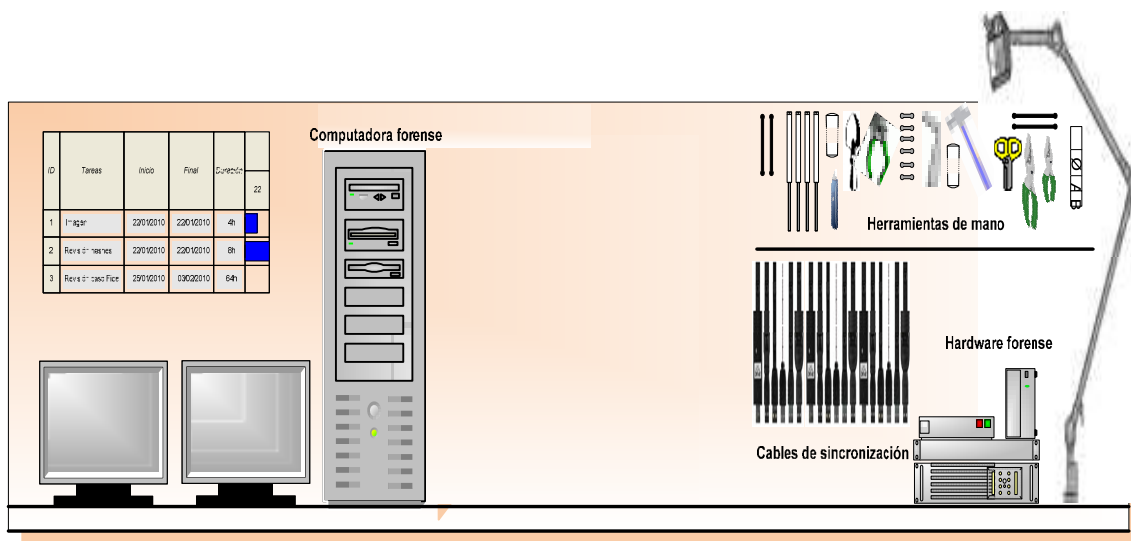
La distribución de estas áreas se observa en la figura 60 y 61, en la página siguiente.

Figura 60. Croquis de las secciones de la estación de trabajo forense



Fuente: elaboración propia

Figura 61. Croquis de la vista frontal de la estación de trabajo forense



Fuente: Elaboración propia

5.3. Iluminación

La estación de trabajo debe estar en un ambiente donde la iluminación sea la apropiada, especialmente por la gran cantidad de tiempo invertida en cada uno de los procesos y el nivel de minuciosidad requerido. La iluminación debe cumplir con los siguientes aspectos:

- Ser adecuada: la iluminancia recomendada para el ambiente de la estación de trabajo es la misma que la utilizada para exigencias visuales altas y muy altas para oficinas e inspecciones textiles, emitidas por *CENTC169*¹⁹, es decir, de los 750 a los 1 500 *luxes*. Sin embargo, para la lámpara-lupa del escritorio se recomienda una iluminancia equivalente en rango entre los 1 500 y los 2 000 *luxes*.
- Balancearse con luz natural: se recomienda el uso de ventanas con los mecanismos de atenuación respectivos (para graduación entre los 200 y 500 *luxes*). Las ventanas son muy útiles porque proveen un ambiente más natural y son valiosas para descansar la vista en objetos lejanos, aunque se recomienda que no estén expuestas a la luz directa del sol.
- Ser uniforme: la iluminación en toda el área de trabajo debe ser igual en cada sección. Esto se puede lograr con difusores, los que a su vez hacen que la iluminación sea suave y un tanto difusa. Se recomienda que se logre una difusión tal que no llegue a eliminar las sombras. Las luminarias deben situarse de tal manera que la luz llegue al trabajador lateralmente y por ambos lados para evitar las sombras de ambas manos.

¹⁹ Comité Técnico 169 del Comité Europeo Normalizador (*CENTC 169*). Iluminación en función de tareas.

- Evitar el deslumbramiento: la luz directa y la reflejada debe permitir que los ojos se adapten fácilmente, especialmente en el cambio visual entre secciones o áreas de trabajo. El deslumbramiento reduce la agudeza visual, provoca fatiga ocular y puede producir dolores de cabeza y afecciones mayores con el tiempo. Para evitar esto, se debe evitar las superficies muy blancas o pulidas y los altos contrastes en muebles, paneles, paredes, techos, etc.
- Evitar la producción de calor excesivo: deben preferirse aquellas luminarias que generen menos cantidad de calor.

Adicionalmente, debido a que seguramente muchos trabajos se realizarán por la noche., se debe considerar como complemento la iluminación de emergencia que facilite una evacuación pronta en caso de cualquier desastre o incidente, Por supuesto con el uso de luminarias de señalización alimentadas por una fuente autónoma de energía.

5.4. Materiales y colores

Características de los materiales de la estación de trabajo forense:

- Impermeables y resistentes a la corrosión
- Material aislante
- Que no conduzcan el calor
- Materiales no brillantes (i.e. maderas barnizadas, metales pulidos, vidrios, etc.)

- Si tiene chapas, éstas deben ser de color de tono claro de baja reflectancia, de color uniforme, sin pigmentaciones, líneas, betas, etc.
- La estructura de los muebles debe ser de metal de alta resistencia, de preferencia acero inoxidable

5.5. Tomacorrientes

La estación debe contar con dos tipos de energía en los tomacorrientes:

- Energía normal (110 / 220 voltios a 60 *hertz*), para el uso de las lámparas, trituradoras de papel, cargadores de baterías, etc.
- Energía regulada. En nuestro país, debido a las grandes variaciones existentes en la distribución de electricidad, es necesario contar con dispositivos que acondicionen la misma, especialmente en el aspecto de la suavización de picos o las bajadas y subidas de tensión en las líneas. Esto protegerá de daños eléctricos a los equipos, alargará su vida útil y cumplirá con los requerimientos para el reclamo de garantías.

Por esta razón, el uso de energía regulada, constituye la *conditio sine qua non* de alimentación eléctrica para dispositivos de alta sensibilidad y de precio elevado. Este circuito de energía regulada de preferencia debe estar conectado a una fuente de emergencia a través de un *bypass* electrónico, que permita brindar un tiempo prudencial al perito para guardar y proteger la información que esté siendo procesada. Por lo menos debe brindar un soporte eléctrico mínimo para no interrumpir aquellos procesos que consumen mucho tiempo (v.g. duplicación o clonación de discos, indexación y búsqueda, etc.).

En ambos casos, los tomacorrientes deben estar plenamente identificados por colores. Finalmente, el edificio debe contar con un adecuado drenaje de electricidad a través de un pozo de tierra física; deben considerarse también en el proyecto, las fuentes in-interrumpibles de poder (especialmente para cubrir el tiempo de reacción de la planta de emergencia), los fusibles, los supresores de transientes, etc.

La determinación de las especificaciones tanto de los equipos de protección como el de la planta de energía de emergencia dependerán de un estudio técnico de acuerdo a la demanda (o consumo) proyectada o la capacidad instalada del laboratorio.

La estación de trabajo debe contar por lo menos con 4 *sockets* de energía no regulada y por lo menos con 12 *sockets* de energía regulada, independiente de los utilizados por la computadora forense, éstos para la conexión de los diversos equipos de análisis y para los alimentar los indicios cuando son examinados.

5.6. Conectores de red y telefonía

El mueble de la estación forense debe contar por lo menos con tres conexiones de red:

- Red interna del edificio, esta brindará acceso a los servicios de *Internet*, correo electrónico, la aplicación forense de seguimiento de casos, etc.
- Red de almacenamiento de información casos, básicamente para guardar las imágenes, los informes, los datos analizados, etc.

- Una conexión de acceso telefónico.

Como norma de buenas prácticas de seguridad, nunca se debe almacenar información de casos en equipos que estén expuestos o que puedan ser conectados de alguna manera a redes externas (v.g. *Internet*).

Respecto a las conexiones telefónicas, por lo menos se debe contar con una en la estación forense, sin embargo, si se contara con el presupuesto para la adquisición de una planta telefónica *IP*, este *socket* puede obviarse.

Tanto el cableado de red como el de telefonía (si hubiera) debe instalarse en el mueble de manera oculta y los *sockets* deben estar colocados de tal manera, que el perito pueda realizar las conexiones sin estorbos o problemas.

5.7. Costo aproximado

Los productos y los precios mostrados en la tabla VII fueron obtenidos a través de su búsqueda en *Internet* en el 2010 y constituyen solamente una guía o base de cálculo.

Estos precios variarán con el tiempo y por tanto se deben actualizar y adecuar, contemplando el análisis de las exoneraciones para algunas instituciones de gobierno, mediante ley interna expresa o solicitud ante la Superintendencia de Administración Tributaria (SAT).

Tabla VII. Precio de productos para la estación forense de trabajo

No.	Producto	Precio (en Quetzales)	Descripción
1	Silla ergonómica <i>Aeron</i>	7 225,00	Para estación de trabajo forense
2	Mueble modular ajustable en altura con ductos ocultos para cableado estructurado, <i>sockets</i> pre-instalados, sección de 3 gavetas.	14 500,00	Para sección frontal estación de trabajo forense
3	Mueble modular con ductos ocultos para cableado estructurado, <i>sockets</i> pre-instalados, sección de 3 gavetas.	8 500,00	Para estación de trabajo forense - sección administrativa
4	Mueble modular con espacio de almacenamiento con entrepaños y sección de 3 gavetas.	4 000,00	Para estación de trabajo forense – sección de almacenamiento temporal

Fuente: elaboración propia

6. ASPECTOS IMPORTANTES A CONSIDERAR EN EL DISEÑO DEL LABORATORIO

Esta sección describe los aspectos ideales que deben considerarse al momento de la construcción del inmueble que albergará el laboratorio de Informática-forense: las diferentes áreas que debe contener (clínica, biblioteca, administración, etc.), las características físicas básicas de los diferentes elementos del edificio (ventanas, puertas, entradas, pasillos, etc.), el acondicionamiento, dispositivos esenciales de seguridad física (instalaciones), sistemas de protección, etc.

Se sugiere al momento de realizar los diseños y planos del edificio que la gerencia de proyecto indague y realice los estudios correspondientes a las tendencias estructurales, de desempeño, automatización y eficiencia de las construcciones modernas propias de los edificios inteligentes. Todos estos elementos deben estar enmarcados en los avances tecnológicos del momento y las consideraciones ambientales, tanto éticas como legales (v.g. emisiones, tratamiento de desechos, uso eficiente de la energía, etc.).

Este capítulo constituye solamente una guía de ayuda respecto de los elementos que deben tomarse en cuenta para una planificación y diseño de instalaciones más concienzudo y minucioso. Para delimitar y simplificar se ha considerado una construcción de un sólo nivel; si se desea implementar un laboratorio con más niveles, han de considerarse aspectos no incluidos en el presente trabajo, por ejemplo, escaleras, ascensores, escalerillas externas de emergencia, etc.

6.1. Aspectos a considerar en el diseño del ambiente físico

A continuación se enumeran algunos componentes fijos que debe poseer la construcción del inmueble. Para simplificar la descripción, se debe tomar en cuenta básicamente dos espacios de flujo:

- El área administrativa, aquella por donde transitarán personas solamente (ésta incluye la recepción, los espacios secretariales, la biblioteca, etc.).
- El laboratorio *per se*, donde circularán personas y evidencias. Implica consideraciones generales para el tránsito de carretillas o medios de transporte de equipos, herramientas y evidencias entre otros. Éste incluirá el espacio dedicado al almacén.

En aquellos espacios de conexión entre un área administrativa y una de laboratorio, deben aplicarse las consideraciones generales de este último.

Actualmente existe la tendencia de diseño de proveer la máxima sección posible de visualización, esto brinda una muy buena iluminación y la eliminación de la sensación de túnel.

6.1.1. Requerimientos generales de la planta

6.1.1.1. Puertas

Las puertas que dan al exterior tanto de las áreas administrativas como del laboratorio estarán compuestas por dos paneles; las interiores se prefieren de una sola hoja o panel. Para el laboratorio es una regla (debido al movimiento de equipos y transporte de las evidencias) que sean de paneles dobles con una

sección visual amplia de vidrio templado de alta resistencia a los impactos y que permita ver hacia el otro lado. Esto se aplica no solamente al laboratorio en sí sino también a todo el camino por donde pase la evidencia.

En ambientes con ventilación natural, algunas puertas pueden poseer rendijas que permitan el intercambio de aire, lo cual no es aplicable a en secciones con aire acondicionado.

La utilización de muelles, dispositivos de cierre hidráulico, sensores de movimiento o la utilización rieles (*slide doors*) para la apertura de puertas depende tanto del diseño final como de su justificación, debido a que éstas representan costos de instalación y mantenimiento extras. Sin embargo, debe invertirse en un mecanismo automático cuando el personal lleva cargas pesadas o mantiene ambas manos ocupadas al trasladar evidencias o equipos, actualmente, se ha convertido en algo normal la utilización de muelles.

Figura 62. **Puerta con mecanismo de apertura *slide-door***



Fuente: http://www.zedautomation.ie/automatic_sliding_door_automatic_biparting_door.htm

Figura 63. **Puertas de vidrio para secciones internas del laboratorio**

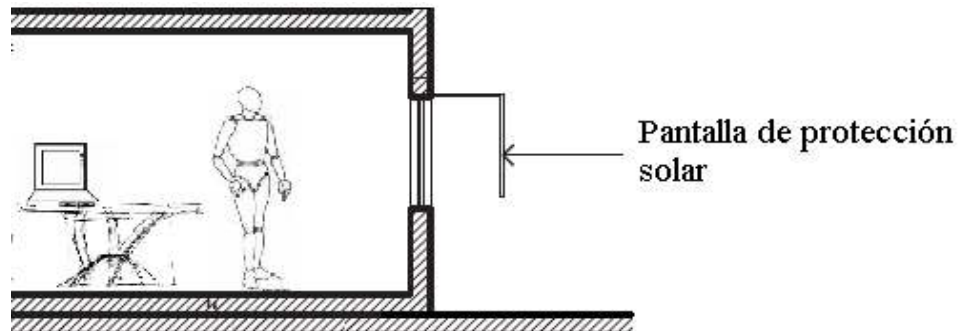


Fuente: <http://www.clearsphere.ie>

6.1.1.2. Ventanas

Las ventanas interiores tienen que ser amplias (inclusive cubriendo casi toda la pared en forma horizontal, como la mostrada en la figura 65), con marcos de aluminio o PVC y vidrio templado. Las ventanas exteriores adicionalmente, si estuvieran en contacto directo con la luz solar de preferencia deben ser protegidas por una pantalla de vidrio (ver figura 64), esto con la finalidad mantener la ventana libre de sobre calentamiento, lo que resulta en un ambiente interno más fresco y un uso más eficiente del aire acondicionado.

Figura 64. **Utilización de pantallas de bloqueo de rayos solares**



Fuente: GRIFFIN, Brian. *Laboratory design guide, 3rd. Edition.* p 29.

Respecto a los colores y las texturas, las ventanas interiores deben ser de preferencia transparentes; sin embargo, pueden considerarse algunas excepciones en oficinas por cuestiones de privacidad. Las exteriores deben ser polarizadas para evitar el deslumbramiento; la utilización de ventanales externos con persianas, mecanismos de difusión luminosa, *louvers*, etc. pueden resultar muy útiles, especialmente cuando falla la energía eléctrica y no existe iluminación o aire acondicionado.

Figura 65. **Utilización de ventanas amplias en los laboratorios**



Fuente: <http://ajniclean.tradeindia.com>

La existencia de ventanas exteriores debe estar enmarcada dentro de las consideraciones de las políticas de seguridad para el personal, la evidencia, la instrumentación y los procesos. Bajo ninguna circunstancia se recomienda su implementación si éstas representan algún riesgo.

6.1.1.3. Pasillos

Los pasillos de interconexión entre áreas (administración, almacén de evidencias, laboratorio, etc.), deben ser amplios (por lo menos del tamaño designado para las puertas con paneles dobles). Para las secciones interiores, se sugiere un mínimo de 2,5 metros. Algunos diseñadores utilizan medidas más pequeñas en los pasillos de paso entre áreas debido a que cuando es amplio se tiene la tendencia a amontonar cosas en los mismos “temporalmente”.

6.1.1.4. Entradas/salidas

Las áreas, tanto para el ingreso como el egreso de personal, se recomienda que sean de por lo menos tres metros, si se utiliza la misma sección como entrada y salida; considerando la potencial instalación de dispositivos de marcaje y ordenadores de colas. Para el ingreso de personas ajenas a la institución se recomienda un ancho menor (aproximadamente 1,5 metros), con finalidades de control y se sugiere que la salida y la entrada sean independientes. Las entradas deben contemplar un área para la colocación de un módulo de seguridad y la instalación de detectores de metal.

6.1.1.5. Comedor

El comedor es el área exclusiva para la ingesta de alimentos. Éste debe construirse en una esquina del edificio, tanto por cuestiones de ventilación como de instalación de ventanas que brinden un ambiente de quietud y tranquilidad,

las vistas a un jardín o áreas verdes son recomendables. Las dimensiones del mismo dependen del número de personas que laboran en el edificio, aunque se recomienda que el mínimo por persona sea de 1,20 metros cuadrados, debe incluirse un área de paso de por lo menos 1,5 metros.

La sección del comedor debe incluir servicios sanitarios accesibles o cercanos, la existencia de dispensadores de agua pura, instalaciones eléctricas para la instalación de hornos de microondas, etc.

Finalmente, la altura del techo debe ser tal que permita el flujo de los olores hacia el exterior del edificio utilizando algún mecanismo de extracción, el mínimo recomendado es de cuatro metros.

Si las dimensiones del comedor no cubrieran la demanda, se tendría que proponer una ampliación del área o bien el establecimiento de horarios.

6.1.1.6. Sala de espera

La sala de espera es la sección donde las personas aguardan a ser atendidas. Esta sección debe contemplar espacios para sillas; nuevamente, el área dependerá de la demanda de los servicios. Sin embargo, un área de 6 x 10 metros en la entrada de la recepción del área administrativa es una medida común. Esta sección, no debe tener contacto visual directo con los pasillos, las oficinas administrativas o el laboratorio.

6.1.1.7. Administración

Después del laboratorio, la administración es el área más grande debido a que es aquí donde se realizan todos los trámites propios de la organización.

Esta sección debe contemplar todos los departamentos necesarios para el buen funcionamiento de la institución: Recursos Humanos, Financiero/Tesorería, Gerencia/Planificación, Soporte *I.T.*/Informática, Compras/Inventarios, Servicios Generales, etc. El cálculo de las dimensiones dependerá de la carga de trabajo de acuerdo al total de trabajadores, aunque se considera un área cómoda de trabajo tres metros cuadrados por persona.

La Gerencia/Planificación puede incluir una sala privada para la atención de comitivas, donantes, personalidades del ámbito forense, sesiones con las diferentes jefaturas, etc.

6.1.1.8. Cuarto de evidencias

El cuarto o almacén de evidencias es el sitio donde se resguardarán todos los indicios a ser analizados posterior a su ingreso al recinto y su respectiva codificación. Las dimensiones de este espacio deben ser de tal forma que permitan tanto el almacenaje como el transporte hacia las diferentes unidades de laboratorio. Los pasillos deben estar identificados de preferencia por colores y de acuerdo a la clasificación realizada según al tipo de indicio o de exámenes a realizar. La distancia entre anaqueles o estanterías debe ser de por lo menos dos metros.

Esta es una de las secciones que debe poseer todos los elementos de protección, tanto ambientales como de seguridad ante intrusiones, y por lo tanto, debe poseer cámaras, alarmas, sensores de temperatura y humo, poseer paredes y techos de materiales aislantes, etc.

A diferencia de otras áreas, la colocación de ventanas se debe realizar analizando los peligros que éstas pueden representar por intrusiones, ladrones,

etc.; sin embargo, si se colocaran, debe contemplarse la seguridad. Por otra parte, la instalación de tragaluces reforzados puede resultar muy útil para complementar la iluminación artificial.

Los pisos deben ser reforzados, lisos y nivelados, de tal manera que provean una superficie adecuada para el desplazamiento de carretillas y el movimiento de las estanterías a la hora del mantenimiento o para la evacuación eficaz de las evidencias al momento de un siniestro o accidente.

6.1.1.9. Sala de reuniones/capacitación

Esta sala será la encargada de albergar al personal para la realización tanto de reuniones como de capacitaciones. Ésta, debe poseer algunas comodidades básicas, por ejemplo, un baño y una cocineta. Las dimensiones de la misma dependen del número de personas del *staff* del laboratorio como del número de reuniones y capacitaciones planificadas.

Se recomienda, adicionalmente, que esta área cuente con una pizarra fija, pantallas *LCD* o plasma con su respectivo anclaje (*bracket*), un sistema de audio, sistema de persianas e iluminación ajustable (*dimmers*), toma corrientes y conexiones de red, tanto en la pared como ocultos en el piso en el área frontal, para la colocación tanto de proyectores como la conexión de computadores; etc.

6.1.1.10. Clínica

Es el sitio donde se atenderá o remitirá a un centro asistencial al personal por dolencias o enfermedades. Esta es la sección donde se encontrará el personal, los equipos y los materiales o medicinas para brindar una atención primaria. Por lo tanto, debe poseer un cuarto con camillas, baños con duchas,

vestidores, etc. Adicionalmente, debe poseer la infraestructura eléctrica requerida por los equipos médicos.

De preferencia, la clínica debe poseer una sala de estar con vista a un jardín y situarse en un lugar que tenga acceso externo directo a la calle para el ingreso de paramédicos y ambulancias.

Aunque se optara por el *outsourcing* de servicios médicos, a través de contratos con hospitales o empresas de seguros, se recomienda que exista un sitio con la descripción anterior que cuente con botiquines. Esto requerirá el adiestramiento o capacitación del personal respecto a lectura de signos, atención en primeros auxilios y la elaboración de procedimientos de emergencias.

6.1.1.11. Área de servidores/informática

Este es el recinto donde se encuentran todos los servidores que proveen de servicios o albergan los datos y la información con que trabaja el área administrativa y el laboratorio. Esta área debe poseer todas las condiciones para mantener los equipos en perfecto funcionamiento: aire acondicionado, energía regulada con sus respectivas cajas, tomas a fuentes in-interrumpibles de poder, conexiones de red, etc. Por su naturaleza, este sitio es un lugar restringido y por lo tanto debe contemplarse la infraestructura de seguridad (accesos y vigilancia), y debe construirse en un área que no colinde directamente con el perímetro del edificio.

Se aconseja que el cuarto de servidores posea su propio sistema regulación de temperatura y que utilice el del edificio cuando el primero falle o se realicen reparaciones o mantenimientos.

6.1.1.12. Bibliotecas

Es el lugar donde se encuentran todos los materiales útiles para el estudio de casos, búsqueda de información, consultas a bibliografía especializada, tanto de carácter legal como del ámbito informático.

La biblioteca debe cumplir con las normas inherentes, es decir, un sitio silencioso, con iluminación adecuada, temperatura regulada, etc. que permita la lectura y la investigación en un ambiente confortable. La sección de consulta puede estar ubicada en un ambiente pequeño (10 X 10 metros), debido a que es un área de estancia temporal y por lo tanto, deben generarse las políticas de estancia por persona respectivas.

Las medidas de la sección de estanterías (librería, videoteca, etc.), dependen, tanto de la cantidad de materiales como del período de renovación de los mismos, aunque un área inicial aproximada de 12,40 X 4,80 metros puede alojar cuatro estanterías de 5,00 X 0,60 metros con entrepaños ajustables, dejando un pasillo de aproximadamente 1,20 metros entre estanterías utilizables en ambos lados.

Si hubiese una demanda de espacio mayor se puede contemplar la solución de estanterías móviles (comúnmente utilizadas en archivos de gran volumen); estas se pueden mover fácilmente utilizando un mecanismo para desplazar los anaqueles sobre carrileras (e.g. <http://www.movableshelvingusa.com>)

6.1.1.12.1. Material escrito de consulta y referencia

La biblioteca poseerá el material y la documentación (libros, videos, base de datos de conocimientos - *knowledge base* -, etc.), que le brinden al perito información pertinente a los procedimientos de investigación y actuación de otros profesionales, así como el acceso a los informes respectivos, fundamentos legales, etc. de casos previos y que estén disponibles.

6.1.1.12.2. Biblioteca de software

Esta es una sección importante de la biblioteca debido a que ahí se guardará copia del *software* forense utilizado en el laboratorio. Los originales (junto con sus licencias), se sugiere sean almacenados en un área protegida. La gerencia determinará si es almacenado en el cuarto de servidores, el departamento de *IT (Information Technologies)*, la biblioteca u otro lugar.

6.1.1.12.2.1. Aseguramiento de licencias

El *software* original junto con las licencias respectivas deben almacenarse en un lugar seguro, comúnmente llamado caja fuerte o *strong-box*; la cual puede ser literalmente una caja con blindaje o bien un sitio protegido bajo llave.

La existencia de cajas fuertes también implica o puede incluir el manejo de contraseñas en sobres cerrados o bien la utilización de una caja fuerte virtual (v.g. *Minitrezor*, <http://minitrezor.softonic.com/>).

6.1.1.12.3. Internet

Otro de los servicios disponibles dentro de la biblioteca será el servicio de *Internet*, para lo cual debe preverse la instalación de módulos que cuenten, tanto con conexiones eléctricas como con conexiones de red; la determinación de *internet* inalámbrico dependerá del estudio de seguridad efectuado por la gerencia.

6.1.1.13. Baños

Estos son parte integral de los servicios básicos que debe poseer cualquier edificio; sin embargo, actualmente, se han de contemplar más factores, tales como:

- Mejoramiento del diseño ergonómico para personas con discapacidades, lesiones, movilidad limitada o enfermedades²⁰;
- El uso eficiente de los recursos (agua, papel, energía eléctrica, etc.).
- Poseer un diseño arquitectónico moderno.

Por lo tanto, el gerente de proyecto debe contemplar dentro de los costos de la edificación lo referente a la accesibilidad de los servicios para todas las personas²¹ y considerar la utilización barras de apoyo, secadores de manos de alta presión, sensores en fluxómetros y puertas (para encendido y apagado de luces), etc. Estos últimos reducen el costo global operativo de los baños por

²⁰ Ver Instituto del Seguro Social Mexicano – IMSS. Lectura de las normas para la accesibilidad de las personas con discapacidad (<http://www.scribd.com/doc/21990677/Normas-Del-IMSS-Para-Discapacitados>)

²¹ Estas consideraciones deben reflejarse en todo el espíritu del diseño de la construcción junto con los conceptos ecológicos correspondientes a los edificios “verdes”.

utilización de agua, energía eléctrica en iluminación, mantenimiento y limpieza (no hay que retirar constantemente los botes con toallas de papel de los lavabos); adicionalmente, reducen significativamente la obstrucción de lavabos, mingitorios y ductos debido a la reducción del uso del papel; finalmente, proveen de una vista más agradable e higiénica.

Estas consideraciones deben reflejarse en todo el espíritu del diseño de la construcción junto con los conceptos ecológicos correspondientes a los edificios “verdes”.

6.1.1.14. Lockers

Debe contemplarse dentro de la construcción una sección para almacenamiento de objetos personales (ropa, bolsas, utensilios de limpieza, etc.). Especialmente para uso exclusivo de los trabajadores del laboratorio que hacen turnos o que deben pasar mayor tiempo dentro de las instalaciones.

Comúnmente se utilizan los llamados *lockers* o gabinetes metálicos de cerradura basada en candado con llave o combinación. Éstos, se ubican dentro del área de los baños utilizados por el *staff*.

6.1.2. Seguridad

La seguridad consiste en la generación y aplicación de políticas, normas, procedimientos y mecanismos que reduzcan a un nivel ínfimo los peligros o daños que corren las personas en el desempeño de sus labores o la protección de los procesos, máquinas, equipos o materiales utilizados en las actividades.

Parte de ésta, corresponde al área de Seguridad Industrial; sin embargo, dentro del presente trabajo, se ha considerado solamente la prevención de riesgos provenientes de factores humanos como ladrones, intrusos, fisgones, etc., razón por la cual se recomienda que el espacio dedicado al laboratorio y sus entradas sea construido en un área donde no haya tránsito de personas ajenas ni personal de administración. Por eso mismo, no debe haber puertas y ventanas hacia el exterior o en contacto directo con predios privados o públicos; debe considerarse muros perimetrales altos con mecanismos de prevención y detección de intrusos.

De preferencia debe existir una única entrada al laboratorio, exceptuando por supuesto una de uso exclusivo de emergencia o de carga, esto facilitará, tanto el control como el monitoreo; es aconsejable también, la eliminación de cualquier tipo de cielo falso y la existencia de azoteas accesibles desde el exterior. Todo esto, para la protección y seguridad del personal, los equipos forenses y fundamentalmente la evidencia.

6.1.2.1. Accesos restringidos

Hace años la medida tradicional para autorizar el ingreso a un recinto era a través de la verificación ocular realizada por el *staff* de seguridad de la empresa. Éste se encargaba de solicitar el documento de identificación o el gafete emitido por la empresa y verificar las fotografías o comparar los datos con un listado; sin embargo, ahora se utilizan otros mecanismos o dispositivos en conjunto con el anterior o en forma independiente. Básicamente, existen tres formas de realizar esta verificación:

- Utilizando tarjetas de aproximación, códigos o contraseñas digitadas.
- Uso de Biométricos.
- Métodos híbridos (combinación).

La gerencia del laboratorio deberá estudiar y seleccionar, de acuerdo a las circunstancias particulares, el mejor de los sistemas anteriormente expuesto.

6.1.2.1.1. Tarjetas de aproximación, códigos y contraseñas digitadas

Éstas son muy populares debido al bajo costo de los lectores como la asequibilidad de las tarjetas. Esta opción es comúnmente utilizada para el control horarios de entradas y salidas, debido a que incluye un módulo de *software* que captura la fecha y hora de marcaje. Adicionalmente, puede realizar cálculos de llegadas tarde y los reportes respectivos. También pueden instalarse dispositivos que permitan el acceso utilizando un teclado para el ingreso de contraseñas o códigos, el principal inconveniente de estos mecanismos es que pueden ser utilizados o transferidos a otras personas.

6.1.2.1.2. Biométricos

Los biométricos son dispositivos utilizados para el reconocimiento humano basado en las características únicas de los seres humanos. Los más comunes son los lectores de huellas dactilares, iris, patrones faciales, geometría de la palma de la mano, etc. éstas son consideradas características físicas-estáticas, mientras que la voz y la firma son reconocidas como características físicas-dinámicas.

Estos mecanismos son más recomendables, debido a que el reconocimiento se realiza con base en uno o más rasgos físicos intrínsecos únicos de las personas. Los lectores de este tipo generalmente, también leen tarjetas de aproximación y por lo tanto, pueden instalarse en los ingresos al edificio designados para el *staff*, tanto peatonal como accesos a parqueos, y en los ingresos a áreas restringidas.

6.1.2.2. Circuito cerrado de televisión – CCTV

El circuito cerrado de televisión (*Closed Circuit Television*), es otra forma de proveer seguridad, monitoreo y reconstrucción de eventos (robos, intrusiones, incendios, etc.). La seguridad del *CCTV* está basada en la percepción emocional de estar siendo vigilado, razón por la cual en muchas ocasiones algunas empresas utilizan una mezcla de cámaras señuelo – expuestas- y cámaras ocultas.

Otras ventajas ofrecidas por estos sistemas es la de grabación continua o por sensores de movimiento, visualización remota a través del cableado de red o *internet*, vigilancia nocturna (percepción infrarroja), control remoto de cámaras, etc., éstas pueden controlarse desde una sala de control remoto, donde se puede configurar su panorámica, enfoque, inclinación y acercamiento.

Para el diseño del sistema de monitoreo por *CCTV* para el laboratorio, se recomienda consultar con un especialista, el cual determinará los tipos de cámara a utilizar en los distintos ambientes, tanto internos como externos, la posición de las mismas, las graduaciones de enfoque/acercamiento, el mantenimiento, el *software* de monitoreo, los cálculos de espacio es los servidores de video, la capacitación de uso, las políticas de respaldo (*backup*), etc. En la actualidad, debido a la capacidad de manejo de los archivos en las

computadoras, se prefiere el uso de grabadores de video digitales (*digital video recorders - DVRs*) a su contra parte análoga.

6.1.2.3. Detectores de metal

Su finalidad es la de revelar si alguna persona desea ingresar a las instalaciones del edificio con alguna arma. Razón por la cual, éstos deben colocarse al ingreso a las instalaciones. La norma general adoptada no solamente por los laboratorios, sino por todas las instituciones privadas y estatales es la de garantizar el orden y la seguridad dentro de las instalaciones, razón por la cual, no debe ingresar nadie armado al edificio, sea ajeno o miembro del personal. Por este motivo, debe estimarse dentro del espacio planificado para el ingreso/egreso del edificio en una sección para guardar las armas junto con un método de registro (bitácora), del portador de la misma.

Debido al cambio de actitud ante los aspectos de seguridad a partir de los eventos del 9-11 en Estados Unidos, los gobiernos, las instituciones, los aeropuertos, etc. han optado por detectores más efectivos, los cuales no solamente detectan metal sino que ven en el interior de las personas, de tal manera que pueden descubrir si una persona lleva consigo algún objeto extraño (explosivos plásticos, cerámicos, armas, etc.), que pueda considerarse peligroso. El uso de este tipo de detectores u otros medios de detección como escaners de alta frecuencia o rayos X dependerá del estudio de seguridad, costo y presupuesto del proyecto.

6.1.2.4. Staff de seguridad

Muchas empresas han optado por la subcontratación o *outsourcing* del personal de protección y seguridad, por lo que la gerencia del laboratorio tendrá que evaluar, tanto los beneficios y los riesgos de ésta como de la opción de

contar con personal de seguridad propio. Ambas posturas tienen sus pros y sus contras. Sin embargo, debido al carácter del trabajo desarrollado en el laboratorio, se sugiere que éste cuente con personal de seguridad propio.

Ventajas:

- Son personas que han sido directamente investigadas por el departamento de Recursos Humanos del laboratorio y por lo tanto, se ha realizado un estudio laboral concienzudo (investigación del pasado, entrevistas, evaluación de la experiencia, exámenes psicológicos, poligráficos, etc.).
- Son personas con las cuales se tiene un vínculo contractual de requerimientos, obligaciones, derechos, etc. logrado por acuerdo, a través de un documento legal, lo cual permite una supervisión más efectiva.
- Es personal de seguridad llega a ser reconocible por todos (*staff* administrativo, de laboratorio, mantenimiento, etc.), generando un ambiente de confianza. Contrario a las empresas de seguridad que generalmente rotan a su personal.

Contras:

- Inversión en uniformes, armas, municiones, capacitación, etc.
- Se debe contemplar recursos e infraestructura para el personal de seguridad (baños, dormitorios, cocinetas, etc.).
- Se deben planificar los pasivos laborales, seguros, beneficios laborales, etc., al igual que para todo el personal del laboratorio.

6.1.3. Accesibilidad

El edificio debe poseer accesos que brinden las facilidades para el ingreso y egreso de personas, equipos o instrumentos, evidencias, deposición de basura, etc. En este sentido, deben preverse los espacios necesarios y de holgura que permitan el manejo adecuado de todo lo que entra y sale de las instalaciones.

6.1.3.1. Entradas y salidas parqueos

Idealmente, si el terreno y el presupuesto lo permite, el edificio debe poseer por lo menos tres entradas/salidas vehiculares, a saber:

- Personal de la institución
- Visitantes
- Evidencias y materiales.

Estos espacios de tránsito vehicular, como de parqueo, serán utilizados exclusivamente por el personal para el cual fue designado. Su manejo, mantenimiento y políticas de uso tendrán que ser desarrolladas y publicadas por la gerencia del laboratorio.

Estas áreas deben monitorearse por cámaras, poseer automatización de ingreso y egreso a través de talanqueras con tarjetas de aproximación, y ser vigiladas por el personal de seguridad, razón por la cual, deben incluirse garitas con sus servicios respectivos.

Figura 66. **Uso de paneles solares para iluminación de exteriores**



Fuente: <http://www.iluminacionsolar.com.mx>

Para la iluminación, de acuerdo al estudio respectivo (análisis costo-beneficio, tiempo de recuperación de la inversión, porcentaje de ahorro, etc.), pueden utilizarse fuentes de energía alternas²² (solar o eólica), con activación a través de foto-sensores conmutada a energía eléctrica convencional redundante cuando sea requerido.

El ingreso/egreso de materiales y evidencias debe estar separado de las dos anteriores por seguridad. Esta sección puede utilizarse también como área de descarga de equipos o de abastecimiento de insumos para el laboratorio por parte de los proveedores.

²² Ver Proyectos tecno-ecológicos de “energía limpia” y utilización de *leds* para iluminación interna y externa.

<http://www.amdee.org/>,

<http://www.anes.org>,

<http://www.iluminet.com.mx/>

6.1.3.2. Entradas y salidas peatonales

Al igual que en el caso de los accesos vehiculares, la entradas/salidas peatonales del personal y de los visitantes deben estar separadas – de preferencia en alas opuestas, y cumplir con los requerimientos de seguridad mencionados previamente (v.g. cámaras de seguridad, detectores, vigilancia por *staff*, etc.).

6.1.4. Acondicionamiento

Todos los elementos del edificio deben cumplir con sus funciones e interactuar como un sistema de engranajes a fin de realizar o cumplir su objetivo. Sean éstos estáticos: pisos, paredes, techos, etc.; dinámicos o movibles: puertas, cámaras, mecanismos con *relays*, etc.; de servicio: energía eléctrica, aire acondicionado, aguas servidas, etc.; de protección: fusibles, alarmas, extintores, etc.

Tanto la eficacia como eficiencia de todos los elementos del edificio dependen de un plan de mantenimiento y verificación continuo a fin de garantizar en todo momento un ambiente agradable y seguro para las personas, los procesos y los equipos forenses.

6.1.4.1. Energía eléctrica

Uno de los elementos más importantes del edificio es el servicio de energía eléctrica debido a que sin éste, no se podría realizar el trabajo forense, por lo tanto, la gerencia tiene que realizar las gestiones necesarias, no solamente para brindar un servicio in-interrumpible de energía, sino también que ésta esté acondicionada para no dañar los aparatos utilizados, esto último contribuirá a

alargar la vida útil de los equipos, protegerá la inversión y permitirá cumplir con los requerimientos de instalación y garantía solicitados por los proveedores o las empresas.

Existen muchos mecanismos y formas, tanto para ofrecer un servicio continuo de energía como de protección. En este apartado se describen los más básicos.

6.1.4.1.1. Drenaje a tierra

El edificio debe estar preparado con un sistema de protección de sobretensiones, tanto externas como internas, de tal forma que éstas no afecten a las personas o los equipos electrónicos. Las dimensiones y capacidades de este drenaje, así como la instalación de tierras unificadas o independientes y otros tópicos dependerán del estudio de cargas, seguridad y protección realizado por la empresa que se contrate para este propósito.

6.1.4.1.2. Pararrayos

Un rayo constituye un potencial peligro tanto para las personas como para los equipos, debido a la gran cantidad de energía abrupta que se genera. Razón por la cual, el edificio deberá contar con los mecanismos, tanto de protección como de drenaje de dicha energía, a través de un pararrayos.

6.1.4.1.3. Fuentes in-interrumpibles de energía

Las fuentes in-interrumpibles de poder o *UPS (uninterruptible power supply)*, son dispositivos que protegen y proveen energía temporal ante las fallas eléctricas. El uso de los mismos es ineludible, debido a que un corte en

la electricidad puede representar la pérdida de información, trabajo realizado, interrupción de los procesos, daño a la evidencia, etc.

Los *UPS* actuales tienen otras ventajas como la de monitoreo continuo, la protección a sobre voltaje y la regulación de picos. La adquisición de estos, dependerá de tres factores primordiales:

- La carga que se necesite soportar ante las fallas, medido comúnmente en KVA o Kilo voltio amperio.
- El tiempo de reacción o latencia máximo permitido para que entre en funcionamiento la planta eléctrica de emergencia o para guardar la data y apagar los equipos en forma apropiada. Este *run-time* es medido en minutos.
- La administración de configuración, manejo de agenda (v.g. apagado y encendido), diagnóstico, monitoreo, etc.

6.1.4.1.4. Cajas de protección

Las cajas de protección o seguridad, eléctrica son dispositivos que realizan las siguientes tareas:

- Delimitan o aíslan circuitos eléctricos; en este sentido también separa la propiedad y responsabilidad entre la empresa distribuidora de electricidad y el cliente. A estas cajas se les llama principales o de acometida.
- Facilita la distribución y delimitación de las cargas y conexiones internas por ambiente.

- Proveen protección ya que dentro de las mismas es donde comúnmente se instalan los fusibles y las conexiones a tierra.

Figura 67. **Ejemplo de caja eléctrica de seguridad**



Fuente: <http://www.directindustry.es>

La determinación de los tipos de cajas y los armarios, su aislamiento y las normas de instalación en otros, las brindará el estudio técnico eléctrico respectivo gestionado por el gerente de proyecto.

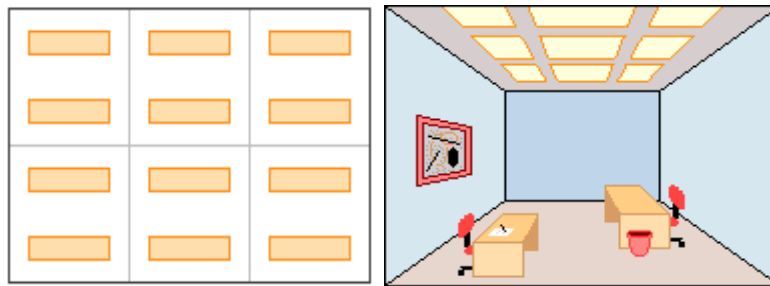
6.1.4.2. Iluminación por áreas

El tipo de iluminación dependerá básicamente del ambiente (oficinas, pasillos, parqueos, etc.), del requerimiento visual del trabajo realizado en los mismos y de la vista arquitectónica. En la medida de lo posible, la iluminación artificial debe balancearse con la natural.

Existen tres métodos que indican la forma de distribución de la luz:

- Alumbrado general: proporciona una iluminación uniforme sobre toda el área iluminada. Es un método de iluminación muy utilizado en oficinas, centros de enseñanza, fábricas, etc. Se consigue distribuyendo las luminarias de forma regular por todo el techo.

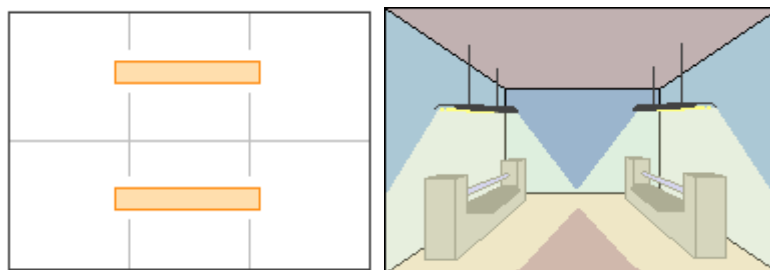
Figura 68. **Distribución típica de alumbrado general**



Fuente: <http://edison.upc.edu>

- Alumbrado general localizado: proporciona una distribución no uniforme de la luz, de manera que ésta se concentra sobre las áreas de trabajo. Así, se consigue cierto ahorro energético, puesto que la luz se concentra donde hace falta. Este método presenta algunos inconvenientes respecto al alumbrado general, especialmente si la diferencia de luminancias entre las zonas de trabajo es muy grande, debido a que puede producir algún grado de deslumbramiento.

Figura 69. **Distribución de alumbrado general localizado**



Fuente: <http://edison.upc.edu>

- Alumbrado localizado: éste es un método de iluminación suplementaria utilizado para realizar trabajos de precisión donde se requiere un excelente nivel de iluminación (v.g. 750 luxes o más). Resulta apropiado también en condiciones donde existen obstáculos que tapan la luz proveniente del alumbrado general o cuando es requerido, debido a la necesidad de personas con problemas visuales.

Este método también puede producir deslumbramiento por la diferencia entre las luminancias del área de trabajo y el alumbrado general. Esta iluminación se logra con lámparas de mesa, pedestal, rodamientos, etc. como las mostradas en las figuras 28 y 61.

6.1.4.2.1. Tipos de lámparas

La selección de los tipos de lámparas y la cantidad a instalar de las mismas, dependerá no solamente del ambiente interior o exterior, dimensiones (ancho, largo y altura de los lugares) y nivel visual requerido, sino también de sus características fotométricas, cromáticas, consumo energético, economía de instalación y mantenimiento.

La tabla VIII muestra los métodos e iluminancia recomendados para varios ambientes del laboratorio.

Tabla VIII. **Recomendaciones de iluminación para el laboratorio de Informática Forense**

Ambiente	Método(s) de iluminación aconsejado(s)	Iluminancia recomendada (Luxes)
Laboratorio	General / Localizado	500 / 750+
Oficinas administrativas	General	500
Almacén de evidencias	General localizado	500
Parqueos (noche)	General localizado	350
Pasillos interiores	General	450
Pasillos exteriores (noche)	General localizado	400
Biblioteca	General	500
Comedor	General	450
Sala de espera	General	450
Sala de reuniones / capacitación	General / localizado	500 / 750+
Clínicas	General / General localizado	500 / 600
Área de Informática	General	500
Baños	General	450
Ingresos/egresos vehiculares	General localizado	600
Ingresos/egresos peatonales	General localizado	550

Fuentes: <http://www.construnario.com/diccionario/swf/27506/Nivelesdeiluminacion.pdf>;
http://www.elprisma.com/apuntes/ingenieria_electrica_y_electronica/luminotecniaailuminacion;
<http://edison.upc.edu>

Los valores anteriores se tendrán que readecuar a las necesidades al finalizar la obra gris y pintura de ambientes, es recomendable el uso de tragaluces y ventanas para la eficiente iluminación natural, por ejemplo: de 7:00 a 17:00 horas o utilizar sensores que enciendan y apaguen luces.

6.1.4.2.2. Dimmers

Los *dimmers* son dispositivos utilizados para regular el voltaje de un sistema de luces con la finalidad de controlar su nivel de iluminación. Estos pueden graduarse manualmente o a través de protocolos especiales, por ejemplo el *digital multiplex, DMX* utilizado en gestión y control de iluminación. Por esta razón, éstos serán útiles en las salas de reuniones/capacitación, el laboratorio y cualquier otro recinto donde se necesite regular la iluminación.

6.1.4.2.3. Iluminación de emergencia

Como su nombre lo indica, este tipo de iluminación es el que se activará automáticamente en el momento que haya una falla de energía eléctrica. Esto será especialmente útil en aquellas áreas que tienen iluminación natural nula y/o por las noches. La iluminación de emergencia es necesaria porque puede salvar las vidas del personal al momento que suceda un evento catastrófico (sismos o terremotos), que corte el fluido eléctrico para que el personal pueda salir del edificio.

Por esta razón, la iluminación de emergencia debe instalarse estratégicamente en todas las unidades de trabajo y en los pasillos que conducen a las salidas de emergencia. Complementario a esto, en el recorrido de dichas salidas de emergencia se deben colocar pequeñas luces estroboscópicas que indiquen la ruta de evacuación; esto último debe contemplarse en el manual de contingencias y desastres del laboratorio.

6.1.4.3. Pisos, paredes y techos

A continuación algunas características generales respecto a pisos, paredes y techos para el laboratorio.

- Pisos: el tipo de piso, pavimento, revestimiento, etc. a colocar será de acuerdo al peso de los objetos y el movimiento que se tendrá en cada uno de los ambientes; sin embargo, en términos generales se recomienda que los pisos estén nivelados, de tal manera que permitan la fácil movilización de equipos (por desplazamiento o rodamiento), especialmente para los pasillos donde transitarán carretillas, el almacén de evidencias y el laboratorio. En cada caso se recomienda realizar un estudio de cargas (vivas y muertas), y resistencia de los materiales a fin de instalar el piso y el reforzamiento adecuado para cada ambiente.

Respecto a los colores, se prefieren los claros sin decoraciones, dibujos o detalles. Esto a lo largo de todo el camino de la evidencia para mantener la uniformidad, de tal manera que si una pieza pequeña cae al piso sea fácil de encontrar. Sin embargo, en las áreas administrativas y/o de gerencia puede colocarse un piso o recubrimiento ligeramente diferente, de tal forma que no haya un contraste brusco; adicionalmente, el nivel de reflexión del piso debe ser bajo, para que no moleste la vista y su acabado no debe ser tan pulido que pueda ocasionar algún accidente.

Algunos pisos de áreas particulares (v.g. baños), pueden incluir un pequeño drenaje con su respectivo sifón y tapa, para facilitar la limpieza y el lavado.

Para las áreas externas al edificio (banquetas, parqueos, accesos peatonales, etc.), también debe realizarse un análisis de cargas para determinar los materiales a utilizar (por ejemplo, concreto con barras o mallas metálicas u hormigón armado).

- Paredes: el material de las paredes de un edificio puede ser variado: concreto, tabla-yeso, block, etc.; sin embargo, la tendencia de utilizar vidrio de alta resistencia al impacto, plexiglass, policarbonato u otros similares, en lugar de las tradicionales paredes (ver figura 70), la finalidad es que además de proveer un diseño arquitectónico agradable, provea ambientes bien iluminados naturalmente y pueda observarse fácilmente cualquier incidente o accidente en los ambientes.

Figura 70. **Ejemplo de utilización de vidrio en los laboratorios forenses**



Fuente: *Tucson Police Department Crime Laboratory*

Sea cual fuere el material de las paredes seleccionado por la gerencia del proyecto, deben preferirse los materiales no inflamables, de buen aislamiento acústico y térmico. Las molduras, salva-juntas, zócalos, etc. deben ser además de ornamentales, resistentes a la humedad y la dilatación por temperatura (*MDF - Medium Density Fiberboard* - es una buena opción).

Los colores deben ser claros y uniformes con acabados o recubrimientos de preferencia en mate, de textura simple que no distraiga la mirada o provoque deslumbramiento por reflejo.

- Techos: los techos del edificio de Informática Forense estarán constituidos de losas de concreto armado con tragaluces estratégicamente ubicados, que puedan proveer de iluminación natural a algunas áreas (v.g. pasillos). La altura efectiva recomendada mínima (piso-techo) es de 2,60 metros. El uso de cielo falso o modular, por cuestiones estéticas, es recomendable sólo en el área administrativa, y si se decide por éste, debe contemplarse una altura mayor para las losas y que el material de cielo falso resista la humedad, sea incombustible, tenga resistencia a golpes, no desprenda partículas de polvo y no emita gases tóxicos al momento de haber un incendio.

Otras secciones del laboratorio, como paqueos a la intemperie, jardines, áreas de estar, pasillos, entre otros, pueden utilizar techos de duralita sobre armazones metálicas.

6.1.4.3.1. Materiales

La determinación de los materiales más apropiados se obtendrá a través de la asesoría que la gerencia gestione en el momento de la planificación de la construcción, esto debido a que una de las variables a considerar será el lugar donde se construya el laboratorio. Por ejemplo, se debe considerar el clima de la región y sus factores, temperatura, nivel de precipitación pluvial, grado de salinidad del ambiente, etc.

Algunas recomendaciones, que en general, deben poseer los materiales constitutivos del edificio, los materiales son:

- Resistentes a la corrosión: para minimizar los gastos en mantenimiento por oxidación u otro ataque electroquímico provocado por el contacto con el aire, los vapores, el agua u otros agentes ambientales.
- Aislantes acústicos: que garanticen un trabajo sin ruidos externos o provenientes de otros ambientes.
- Aislantes térmicos: para proveer ambiente agradable de trabajo y que minimice los costos por aire acondicionado.
- No contaminantes: que no desprendan polvos o vapores en reacción con el calor, contacto con agentes químicos o al final de su vida útil.
- No inflamables o de alta resistencia al fuego: es recomendable la planificación ante siniestros a fin de salvar vidas o minimizar los daños por expansión que causan los incendios. Actualmente, ya se utilizan armazones metálicas con recubrimiento de vermiculita

(<http://www.vermiizol.uz/vkes.htm>), éste, además de ofrecer toda una gama de bondades, es un estupendo aislante al fuego (punto de fusión aproximado de 1 250 °C), por esta misma razón, la vermiculita, también puede ser utilizada en ladrillos, tableros, losas, etc.

6.1.4.3.2. Pinturas

Para el exterior y a la intemperie, se recomienda pinturas con recubrimientos que repelan la lluvia y la humedad, con acabados en mate y de preferencia microbicidas (v.g. pinturas con silicatos). Para los techos, no es necesario aplicar una pintura, pero si considerar la aplicación regular de impermeabilizante.

Los interiores, dependiendo de los materiales utilizados en la construcción al término de la obra gris, muy probablemente tendrán que ser cubiertos con un fondo fijador para sellar los poros en las paredes, previo a la aplicación de las pinturas. Éstas se recomienda que sean en colores claros y acabados mate, emulsionadas en agua con pigmentos de origen mineral con un aglutinante de bajo nivel de combustión. Las pinturas adicionalmente deben poseer un alto grado de impermeabilidad, buena consistencia, inertes (que no desprenda gases en reacción a la temperatura), resistencia a la abrasión, lavabilidad y durabilidad.

Para las señales horizontales en el almacén, pasillos, parqueos y otros, debe utilizarse pinturas termoplásticas, debido a su durabilidad; las tuberías metálicas en exteriores deben colorearse con pinturas resistentes a la corrosión u oxidación. Para las que están enterradas o en contacto directo y permanente con líquidos, se debe utilizar pinturas bituminosas.

Finalmente, para los baños debe aplicarse pinturas resistentes a las condensaciones del vapor de agua, con esmalte sintético e impermeables.

6.1.4.3.3. Colores

De preferencia debe predominar la selección de colores claros y acabados en mate para todo el edificio; sin embargo, se pueden exceptuar aquellos casos donde se requiera llamar la atención por potenciales peligros en cuyo caso se puede complementar con colores satinados.

6.1.4.4. Aire acondicionado

El aire acondicionado es un tema relevante, debido al gran gasto que éste implica y por lo tanto, necesita de un estudio profundo para que el servicio sea eficiente y brinde las condiciones ambientales apropiadas para personal y los equipos informáticos. En los costos, se ha determinado empíricamente que aproximadamente por cada grado de enfriamiento en la temperatura, el consumo aumenta entre un 5% y un 7%.

Adicionalmente, debe contemplarse el aislamiento de los ambientes que permanecen expuestos al sol, mediante la utilización de pantallas (figura 64), toldos, cierre hermético de puertas, polarizado o colocación de películas reflectoras lo que puede lograr un ahorro significativo de un 20% hasta un 30% en el consumo de energía eléctrica en este rubro.

A continuación se describen algunas consideraciones importantes respecto al aire acondicionado.

- Debe contar con sistemas de regulación bien afinados a fin de mantener la temperatura y la humedad relativa satisfactorias en cualquier momento del día. De preferencia estos sistemas (v.g. termostatos), deben instalarse lo más lejos posible de las fuentes de calor. Actualmente, existen sistemas de *hardware/software* que permite realizar la programación del funcionamiento del aire acondicionado en forma eficiente utilizando sensores de temperatura y termostatos digitales estratégicamente localizados, lo que puede permitir un ahorro de hasta un 30%.
- La calidad del aire interior debe cumplir con las normas de seguridad o los estándares de ambientes de trabajo adecuados emitidos por el Ministerio de Salud Pública y Asistencia Social u otras organizaciones²³, a fin de evitar el síndrome del edificio enfermo. Por esta razón se debe diseñar un plan de mantenimiento de compresores, ventiladores, condensadores, sistemas de purificación del aire, *dampers*, limpieza de ductos, etc. así como el aislamiento de ambientes, la utilización de sistemas *multi-split*, etc.
- La gerencia del laboratorio generará las políticas que debe seguir el personal encargado de la limpieza, respecto la utilización de productos químicos en los ambientes. Debe analizarse, por ejemplo, el uso de aerosoles o aromatizadores en lata, el uso de *toner* o tintas secas, utilizados en los procesos de fotocopiado, la utilización de pesticidas o ciclos de fumigación, el empleo de productos químicos de limpieza con cloro o amoníaco, la prohibición explícita de fumar, la vaporización

²³ Por ejemplo, la *American Society of Heating, Refrigerating and Air-Conditioning Engineers* (<http://www.ashrae.org/>).

proveniente de hornos de microondas o cocinetas, ya que éstos pueden provocar malos olores y causar a la larga la proliferación de moho y hongos en los ductos, etc.

6.1.4.5. Sistemas de protección

Los sistemas de protección se utilizan para alertar de eventos que pongan en riesgo al personal y los equipos. Estos pueden emitir señales auditivas o visuales, las cuales deben ser reconocidas por las personas o los mecanismos de emergencia, de tal manera que se abran todas las puertas de un recinto, se activen los sistemas de irrigación, se señale una vía de evacuación, se llame a la policía, etc.

6.1.4.5.1. Alarmas y sensores

El edificio debe contar con una red de sensores distribuidos en ámbitos de cobertura (oficina, pasillos, bodegas, etc.). Éstos deben estar conectados o centralizados en una unidad de control (*hardware/software*) la cual será la encargada de activar todos los mecanismos de emergencia respectivos, enviar mensajes de advertencia, emitir mensajes de mantenimiento por correo electrónico, mensajes a celulares, etc.

En esta categoría se encuentran los detectores de humo, dióxido de carbono (si se utilizará gas en las cocinetas), sensores de movimiento, etc.

6.1.4.5.2. Salidas de emergencia

Éstas permitirán la rápida evacuación del personal al momento de ocurrir un incidente como: terremoto, incendio, desórdenes públicos, etc. Estas salidas

deben colocarse, de tal forma que sean convergentes a los ambientes del laboratorio y deben existir, por lo menos una en ambas alas de la construcción con salidas a la calle o los parqueos. Éstas deben estar correctamente señalizadas y deben poseer un rótulo luminoso alimentado por baterías activadas por el sistema de emergencia respectivo.

6.1.4.5.3. Extintores

Los extintores son equipos contenedores que portan en su interior un agente (espumas, agua, polvos, etc.), utilizado para combatir el fuego cuando éste recién comienza (foco incendiario), y no cuando éste ha crecido mucho o se ha descontrolado.

Los extintores se clasifican dependiendo de la materia en combustión o el tipo de fuego que combaten. La tabla IX describe la clasificación americana.

Tabla IX. Tipos de fuego según la clasificación americana

Tipo de Fuego	Materia en combustión	Notación
"A"	Combustibles sólidos (madera, papel, trapos, cartón, algodón, formica, cueros, plásticos, etc.)	Se representa con la letra "A" dentro de un triángulo color verde
"B"	Líquidos inflamables y combustibles por la mezcla de vapores (gases) y aire (derivados del petróleo, aceites, gasolina, kerosén, pinturas, Acetona, etc.)	Se representa con la letra "B" dentro de un cuadrado color rojo
"C"	Aparatos o equipos eléctricos y electrónicos (Televisores, radios, computadoras, etc.)	Se representa con la letra "C" dentro de un círculo color azul

Continuación tabla IX.

"D"	Metales combustibles o reactivos (aluminio, magnesio, sodio, potasio, cobre, etc.), estos metales arden a altas temperaturas, y exhalan suficiente oxígeno para mantener la combustión. Pueden reaccionar violentamente con el agua u otros químicos y deben ser manejados con cautela	Se representa con la letra "D" dentro de una estrella de 5 puntas color amarillo
"K"	Grasas y componentes combustibles para cocinar o acumulados en extractores y filtros de campanas	Su símbolo es un cuadrado o hexágono de color negro con una K de color blanco en su interior

Fuente: http://en.wikipedia.org/wiki/Fire_classes

Hace algunos años existía un extintor para cada tipo de fuego; sin embargo, actualmente existen dispositivos que combaten varios tipos, por ejemplo, el extintor, cuyo agente contiene polvos químicos mezclados (bicarbonato sódico, bicarbonato de potasio, cloruro potásico, mono fosfato de amonio, etc.), espumas AFFF, dióxido de carbono (CO₂), etc., pueden utilizarse para los fuegos A y B o para A, B y C, dependiendo del contenido del extintor.

De acuerdo a lo anterior, dentro de las instalaciones del laboratorio, se deben situar estratégicamente extintores ABC, debido a su versatilidad y por la conveniencia para la persona que lo utilice, especialmente si ésta no ha sido capacitada (en una emergencia, no hay tiempo de leer las instrucciones).

A continuación se detallan algunas recomendaciones respecto al uso, colocación y mantenimiento de los extintores.

- Estarán situados próximos a los sitios donde se estime mayor probabilidad de iniciarse un incendio (entradas a bodegas, oficinas, laboratorios, etc.), de ser posible, próximos a las salidas de evacuación, a una distancia razonable, fácilmente accesibles dentro de un gabinete color rojo, con

puerta de vidrio empotrado en la pared a una altura aceptable, convenientemente rotulado y a la par de una alarma manual de incendios.

Existen algunos sitios por suscripción que brindan normas para la prevención y la seguridad contra incendios (v.g. *National Fire Protection Association* - <http://www.nfpa.org>), éstos tratan temas respecto a los códigos y estándares para la colocación de mangueras, extintores, detección de incendios, señalización, mantenimiento de equipos, etc.

Figura 71. **Empotramiento de gabinetes contra incendios en paredes**



Fuente: <http://www.mailxmail.com/curso-control-extincion-fuego>

- Deben estar contemplados dentro del plan de mantenimiento general. El cual debe incluir la revisión de estado de la carga (peso y presión), del extintor, el estado de las partes mecánicas (boquilla, válvulas, manguera, etc.), poseer la etiqueta de mantenimiento respectiva, etc.

- La forma de uso y cuidados de los extintores deben contemplarse dentro de los planes de emergencia y la simulación de desastres.

6.2. Nomenclatura de colores de las instalaciones

La aplicación de los mismos será útil para:

- Conocer la ubicación de sitios o dispositivos
- El reconocimiento de riesgos
- Diferenciar los materiales y sus características (químicas y físicas); etc.

Por estas razones éstos se aplicarán a paredes, pisos, contenedores, etc., para indicar la ubicación de objetos o áreas de peligro (v.g. tuberías, dispositivos de seguridad, zonas prohibidas, etc.).

La tabla X muestra el uso recomendado de algunos colores.

Tabla X. **Nomenclatura de colores del laboratorio**

Color	Utilización
Verde	Para identificar donde se encuentran productos medicinales o de primeros auxilios (v.g. botiquines), dispositivos de protección personal (gafas, guantes, batas, etc.). Puertas de acceso a clínica médica de personal, ubicación de tanques de oxígeno y máscaras de protección respiratorio, etc. Utilizar también para indicar tuberías que conduzcan agua potable
Rojo	Identificación de áreas de extintores, mangueras y alarmas de activación manual contra incendios (botones o palancas), contenedores con arena, etc.

Continuación tabla X.

Amarillo	Para indicar precaución o prevenir al personal de potencial riesgo físico por equipos en movimiento. Útil para marcar las áreas de paso de carretillas o transporte de evidencias, entrada/salidas al almacén, etc. Comúnmente se utiliza en franjas alternadas con franjas negras o sin color e inclinadas respecto la horizontal
Naranja	Interior de cajas de instrumentos eléctricos, cajas de llaves, fusibles, conexiones eléctricas u otras que deban mantenerse cerradas por razones de seguridad
Gris	Tuberías de aguas negras y pluviales
Blanco	Entrada/Salida de corrientes de ventilación y aire acondicionado

Fuente: <http://es.wikipedia.org/wiki/Extintor>

El complemento necesario al uso de colores para identificar peligros y objetos es la utilización de rótulos con simbología universal, letras legibles en alto contraste en idioma Español, flechas indicando rutas o ubicaciones y la utilización de Braille. Existen otros temas importantes que no se cubren en el presente trabajo pero se recomienda profundizar para poder elaborar un compendio de Seguridad Industrial completo para el laboratorio de Informática Forense.

6.3. Planta telefónica

Éste será de los servicios más importantes del laboratorio, porque permitirá mantener la comunicación entre todas las unidades del laboratorio y la comunicación externa. Actualmente, existen dos tipos de telefonía: análoga y digital.

Sin embargo, debido a la tendencia moderna en el desarrollo de las redes de comunicación, la facilidad de integración tecnológica (*Internet*, videoconferencia, transmisión simultánea de voz y datos, etc.), hacen que la adopción de plantas telefónicas digitales sea recomendable.

La ventaja de contar con telefonía IP (*VoIP*), es que ésta puede trabajar en la misma infraestructura del cableado de red (computadoras), y que la gestión de llamadas hacia otros servidores con este tipo de telefonía es mucho más barato. Sin embargo, se debe contar con aparatos telefónicos y dispositivos activos de comunicación especiales (*switches* o conmutadores), que soporten o permitan priorizar la voz.

Para un mejor manejo y control de la telefonía se debe tomar en cuenta las siguientes recomendaciones:

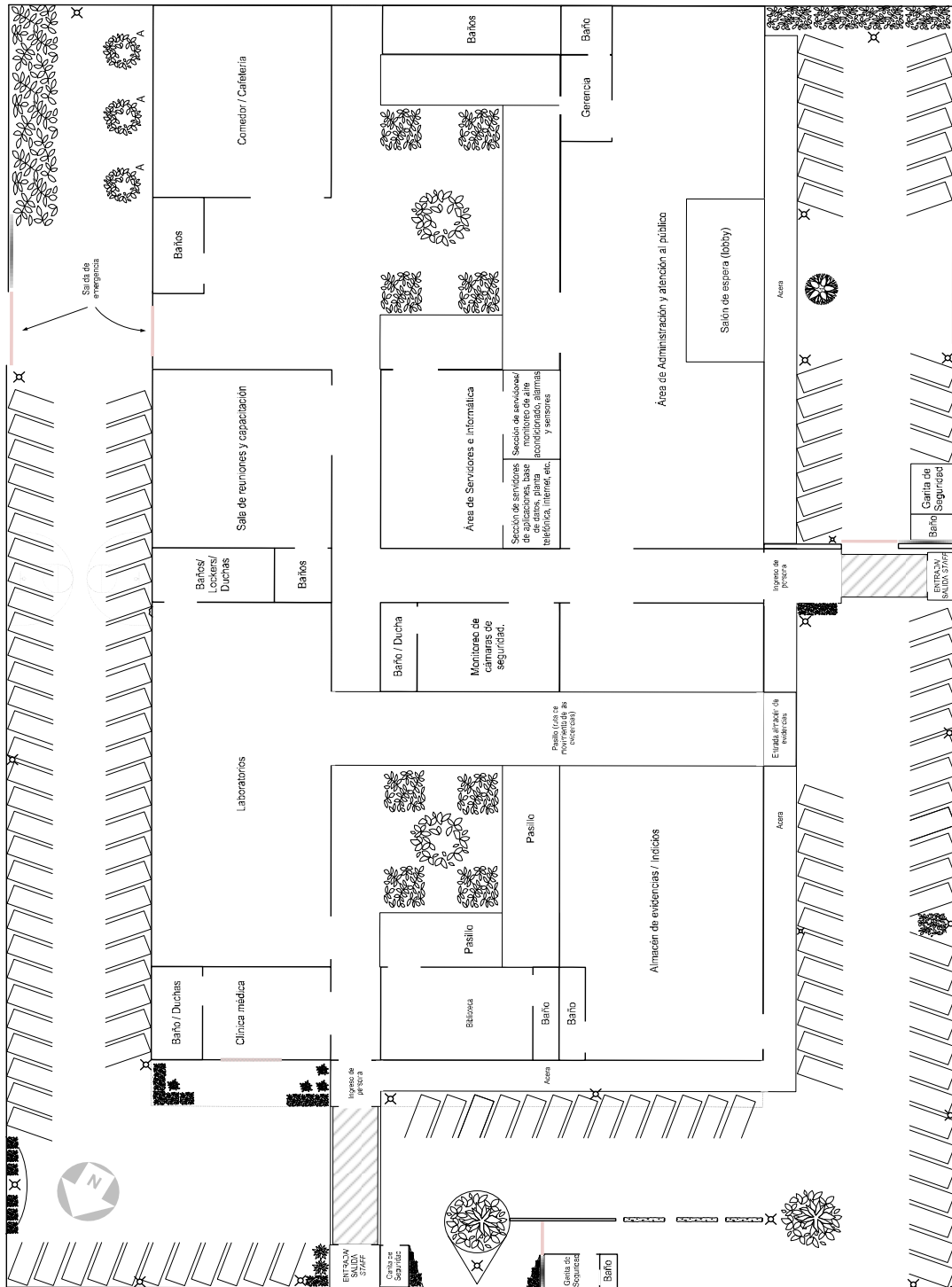
- Generar las políticas de uso del teléfono con la finalidad de minimizar los costos y evitar comunicaciones ociosas. Estas políticas incluyen la restricción de llamadas por categoría, tiempo, por código, etc.
- Uso de *software* de tarificación para el monitoreo del consumo, tanto general como de unidades administrativas, así como el mantenimiento de un registro de todas las llamadas entrantes y salientes, así como su duración.
- Utilización de *softphones* para bajar los costos en la compra de los aparatos telefónicos.

- Implementar los buzones de voz para mejorar la comunicación fuera de línea.
- Integrar (cuando fuere posible), los servicios voz-video-datos para mejorar el nivel de cooperación entre peritos, técnicos y capacitadores (locales o internacionales).

6.4. Plano de distribución de planta sugerido

En la figura 72 se muestra la distribución de planta de las áreas sugeridas en el presente documento. Para simplificar el diseño, ésta consta de un sólo nivel, no se ha contemplado las puertas, ventanas, áreas de expansión, sección de soporte de planta eléctrica de emergencia y otros detalles. Tomar en consideración que el diagrama es solamente una guía y no está a escala.

Figura 72. Distribución en planta del laboratorio de Informática Forense



Fuente: elaboración propia, basado en datos de JONES, Andy; VALLI, Craig. *Building a digital forensic laboratory*, p. 204-212; y NATIONAL INSTITUTE OF JUSTICE. *Forensic Laboratories: Handbook for facility, planning, design, construction and moving*, p 43.

7. MANTENIMIENTO DEL LABORATORIO

Una consecuencia natural del uso (o desuso), de los objetos es el deterioro. Por lo tanto, se deben crear los planes de mantenimiento para cada uno de los elementos del laboratorio (edificio, herramientas, equipos, etc.), de tal forma que:

- Se mantenga el nivel óptimo de funcionamiento del laboratorio.
- Se garantice un ambiente adecuado de trabajo (limpio y que minimice los riesgos a enfermedades o accidentes).
- Se brinde una alerta temprana ante eventualidades como incendios o riesgos de intoxicación.
- Se alargue la vida útil y se mantenga la confiabilidad de los dispositivos y aparatos utilizados como herramientas de trabajo.
- Se minimicen los costos por reparaciones mayores o de gran escala. En este caso, el mantenimiento puede considerarse una inversión.

El mantenimiento incluye la creación de los planes de mantenimiento preventivo y correctivo correspondientes a cada *ítem* del laboratorio así como los planes de contingencia respectivos. Actualmente, muchos sistemas están basados en *software* de monitoreo lo que facilita la planificación del mantenimiento, debido a que éste muestra la bitácora de los eventos sucedidos (fallas o advertencias), de los distintos elementos de un edificio (v.g. puertas

abiertas, sensores, termostatos, etc.), y avisa por celular o correo electrónico al encargado de los mismos.

Adicionalmente debe llevarse un registro contable del dinero invertido en el mantenimiento (limpieza, reparaciones, ajustes, etc.), de tal manera que pueda proyectarse este rubro en los gastos de operación del laboratorio en los presupuestos anuales.

El mantenimiento también puede considerar la capacitación del *staff* de peritos a fin de obtener las certificaciones correspondientes que avalen o acrediten el trabajo forense realizado por ellos antes las instancias judiciales o los tribunales.

7.1. Mantenimiento del laboratorio

El plan básico de mantenimiento está constituido por la limpieza y el orden de todas las áreas y búsqueda de fallas incipientes (grietas, fugas, descascaramientos, etc.); para esto último, es necesario realizar la programación de las inspecciones, tanto de los equipos encargados, como de las rutas a seguir.

7.1.1. Programación de mantenimiento

Para todas las programaciones de mantenimiento de todos los *ítems* del edificio se debe considerar el uso del *software* apropiado para el mismo, en éste se debe registrar todas las actividades realizadas, los incidentes (v.g. fallas en tuberías), los accidentes, etc., así como la bitácora de reparaciones o ajustes realizados; de preferencia el *software* debe mostrar al administrador del edificio

con antelación el calendario de mantenimiento o la programación de dichas actividades.

La periodicidad dependerá de los trabajos realizados en cada área, los materiales utilizados en la construcción (por ejemplo, los acabados en madera requieren mantenimiento frecuente), las solicitudes específicas, etc.

7.1.1.1. Estructura del edificio

Durante la limpieza diaria de pisos, paredes y puertas, también se pueden realizar inspecciones y cambios en lámparas, bisagras, muelles, rieles, etc., y brindarles los ajustes correspondientes a los mecanismos o aceitarlos apropiadamente. Estos eventos deben registrarse en el *software* respectivo.

Respecto a los techos se debe programar, por lo menos una vez al año, la impermeabilización de los mismos, así como la revisión de los desagües pluviales.

7.1.1.2. Instrumentos, equipos y herramientas

La gerencia debe invertir en un plan adecuado de mantenimiento para los equipos forenses (instrumentos, herramientas y dispositivos), utilizados en el laboratorio. Este mantenimiento debe ser específico para cada uno de los *items* y debe realizarlo personal capacitado (o el proveedor, de acuerdo a un contrato), tomando en consideración el tiempo que el equipo está fuera de servicio para que no afecte la programación de los peritajes.

Debido a que estos dispositivos están relacionados directamente con la finalidad de la institución, hay que considerar, por lo menos una limpieza de los

mismos, una vez al mes y el mantenimiento mayor correspondiente una vez trimestralmente o una frecuencia determinada por la cantidad de equipos, el tiempo de mantenimiento, la programación de trabajos, la solicitud de los usuarios (peritos), la potencial falla en el tiempo de entrega, etc.

7.1.1.3. Sistemas eléctricos y de protección

La administración del laboratorio debe desarrollar la planificación del mantenimiento de los sistemas de protección eléctrica, especialmente en el área de sobrecargas y regulación a fin de evitar daño los equipos. Junto a lo anterior, se debe establecer un programa de revisión y llenado de extintores, verificación de los sistemas contra incendio, etc.

7.1.1.4. Equipo de protección personal

Éstos deben revisarse diariamente, especialmente a aquellos utilizados por los laboratoristas y el personal de limpieza. Debe vigilarse porque las gafas, batas, guantes, etc. estén en perfecto estado.

7.1.1.5. Aire acondicionado

El aire acondicionado es uno de los servicios más importantes, debido a que satisface dos requerimientos esenciales: provee de un ambiente de trabajo adecuado para el personal; y, protege los equipos electrónicos del recalentamiento.

El mantenimiento de preferencia debe programarse desde la firma del contrato con la empresa proveedora del mismo. Comúnmente, los proveedores ofrecen este tipo de servicios agregados, los cuales incluyen revisiones

periódicas de termostatos, filtros, condensadores, etc. En este sentido y tomando en cuenta lo esencial del aire acondicionado, por lo menos debe programarse una visita mensual del personal de la empresa proveedora para darle mantenimiento.

7.1.1.6. Alarmas y sensores

La planificación del mantenimiento en este rubro debe considerar todos los dispositivos instalados que posean la capacidad de avisar de situaciones que puedan provocar algún tipo de desbalance, pérdida, avería, daño, etc., tanto de los elementos como el ambiente del edificio, las personas y los instrumentos o equipos forenses. Es decir, los sensores de movimiento, humo y gas, las cámaras del circuito cerrado de televisión (CCTV), internas y externas, los dispositivos emisores de alarmas visuales y auditivas, etc.

Debe planearse la revisión de las bitácoras de mensajes enviados por estos elementos, una vez cada quince días, así como planificar el resguardo de la información provista por los mismos, a fin de utilizarse para las estadísticas de servicio, planificación de cambios o reemplazos, solicitudes de garantías, etc. Esto incluye, el almacenamiento o conservación de los archivos de video provenientes del CCTV.

7.1.1.7. Abastecimientos

Para esto, lo mejor es crear un equipo que lleve los controles de consumo, así como las solicitudes emitidas por las diferentes unidades organizacionales del laboratorio. Esto con el propósito de elaborar un estudio del comportamiento del consumo y la obtención de los indicadores o niveles de agotamiento, similar al proceso de rotación de inventarios de una empresa.

Estos indicadores tendrán una relación proporcional directa con el tipo y número de casos llevado en el laboratorio, la cantidad de trabajadores, los horarios de trabajo, etc.

Los controles permitirán realizar con anticipación, los requerimientos correspondientes de suministros de oficina, papelería, materiales de limpieza, etc.; permitirá auditar los desperdicios o el mal uso de los mismos y finalmente, hará un buen empleo de los espacios o bodegas dedicados a los abastecimientos.

7.1.1.8. Pago de servicios

Otra parte de los gastos de funcionamiento lo constituyen los servicios de agua potable, energía eléctrica, telefonía, enlaces de datos, *Internet*, etc., necesarios para que el laboratorio opere eficientemente. Por lo tanto, debe existir una unidad organizacional que vele por la verificación de las facturas y el pago de las mismas a los proveedores, para no caer en mora, evitando el pago de intereses, y en grado extremo el corte de los servicios.

Actualmente, debido a la importancia de los servicios de enlaces de datos inter-institucionales e *Internet*, es recomendable que se cuente con las redundancias respectivas (de proveedores diferentes o independientes, de preferencia), para que cuando falle la conexión primaria, se pueda derivar el servicio al servicio secundario o de soporte. Tanto la forma de operación o conmutación entre servicios es tarea que planeará el Departamento de Tecnología (*IT* o Informática) del laboratorio.

7.2. Acondicionamiento y aseguramiento de la bodega

Básicamente existirán dos bodegas en el edificio, la descrita en el inciso 7.1.1.7., respecto a los suministros o abastecimientos utilizados en las labores diarias y la bodega o almacén de evidencias. Ambas requieren un tratamiento similar respecto a la protección, es decir la instalación de detectores de humo, cámaras, extintores, alarmas, etc. Sin embargo, el acondicionamiento y la seguridad del almacén de evidencias requiere del establecimiento de políticas y procedimientos adecuados, haciendo énfasis en la manipulación cuidadosa debido a las repercusiones legales respecto al mal manejo de las evidencias. A continuación algunas recomendaciones referentes.

Acondicionamiento

- Limpieza diaria con los productos apropiados (i.e. no con componentes que pongan en riesgo la evidencia).
- Los techos, pisos, tragaluces, ventanas, etc. deben ser revisados, por lo menos una vez cada seis meses o cuando la situación lo amerite.
- Tanto la limpieza profunda como las fumigaciones deben ser programadas, por lo menos dos meses antes para la planificación respectiva.
- Atención diaria de anaqueles, pasillos, entradas y salidas del almacén para el control de objetos mal colocados, gavetas abiertas, piezas tiradas, etc.
- Limpieza quincenal y verificación del funcionamiento de cámaras y sensores.

- Revisión periódica (de acuerdo a los proveedores), de los niveles de los extintores.

Aseguramiento

El aseguramiento se relaciona con la forma apropiada y los cuidados del trato de la evidencia en su ingreso, resguardo y salida, así como la observancia de las buenas prácticas. Esto incluye, la implementación de una codificación que indique en qué ambiente, pasillo, anaquel, entrepaño y caja se ubica un determinado objeto, así como la utilización meticulosa del sistema informático de seguimiento. De tal forma de registrar todos los datos y detalles pertinentes proceso que la evidencia siga.

Cuidados generales

Estos son algunos cuidados básicos que se deben tener respecto el aseguramiento de los materiales probatorios. La gerencia tendrá que realizar los estudios respectivos y generar los perfiles y procedimientos que deban seguir cada uno de los trabajadores del almacén, los formularios internos, los puntos de control, etc., así como los manuales de contingencia respectivos.

- El receptor de un elemento material probatorio o evidencia física, antes de hacerlo, verifica el recipiente que lo contiene y deja constancia del estado en que se encuentre, en el formato de registro de cadena de custodia adoptado, o aceptado en Guatemala.

- La gerencia del laboratorio elegirá, de acuerdo a la ley y los parámetros de seguridad, entre dos procedimientos:
 - Basado en la regla común, el embalaje sólo se abre por el perito designado para su estudio o análisis; y
 - Basado en la seguridad anti-terrorista o anti-narcótica, cuando hayan motivos razonables o se tenga duda respecto al contenido.

De acuerdo a esta última, el contenedor se abriría con la ayuda del personal capacitado y conocedor del manejo de explosivos, elementos dañinos, sustancias controladas, químicos precursores, etc. Luego deberá dejarse adjunto al registro de continuidad de la cadena, un informe suscrito de quienes intervinieron, indicando las razones que motivaron este proceder y el detalle de las condiciones en que se encontró y dejó el embalaje.

Sería catastrófico ingresar un embalaje con algún explosivo dentro debido a la potencial pérdida de vidas y la destrucción de otras evidencias dentro del almacén; por esta misma razón, algunos laboratorios forenses invierten en *scanners* en el área de ingreso de evidencias. Igual cuidado se debe mostrar ante el potencial contenido de sustancias controladas o narcóticos dentro de los elementos embalados o los *cases* de los equipos a analizar.

- La apertura del contenedor se hace por el lado diferente a donde se encuentra el sello inicial.
- Luego de la inspección, el elemento se introduce preferiblemente en el embalaje inicial, si las condiciones del mismo lo permiten, en caso de utilizarse un nuevo embalaje se conserva el rótulo y cinta de sello inicial.

Para sellar el embalaje se procede a imprimir la firma y número de documento de identificación del encargado de la recepción del elemento en la parte de su cierre y sobre ésta se coloca el sello.

- Debe considerarse como norma procedimental la toma de fotografías y videos de cada tarea realizada con embalaje y su contenido.
- No se recibirá ningún elemento, materia de prueba o evidencia física que no esté embalado, sellado, rotulado y con registro de cadena de custodia de conformidad con los establecidos oficialmente.
- Respecto a personal no autorizado; es prohibido el acceso a las áreas de almacén de personas diferentes a las asignadas. Ésta será una responsabilidad del encargado o jefe de almacén y el agente de seguridad designado.
- El jefe de almacén debe hacer una revisión diaria de las bitácoras de vigilancia realizada con las cámaras (ubicadas de preferencia, una en cada pasillo), los sensores de movimiento, el registro de ingreso del personal de acuerdo al sistema de seguridad empleado (tarjeta/biométrico).
- El jefe de almacén debe realizar periódicamente un inventario físico de los elementos resguardados o bien un muestreo de cotejación con el encontrado en el sistema informático de seguimiento de casos.
- El material probatorio, que ya ha sido analizado, y está a la espera que sea recogido o despachado, debe de preferencia ocupar el mismo lugar que le fue asignado desde un inicio.

- Las salidas de los materiales probatorios deben incluir una autorización donde se indique el nombre de la persona (v.g. fiscal), identificación, razón de la salida, etc., y debe registrarse en la cadena de custodia y el sistema informático de seguimiento.

Es importante y por lo tanto debe recalcar que el personal del laboratorio debe estar al tanto de los protocolos o las leyes referentes a la cadena de custodia y conexas. Las consideraciones mostradas en el presente documento pueden ser adoptadas si y solamente si, están de acuerdo a las leyes o protocolos aprobados en Guatemala.

7.3. Evacuación de basura y desechos con contenido químico

Esta debe realizarse en un espacio alejado de las labores diarias para evitar la infiltración de malos olores y en un espacio accesible tanto para la limpieza como para el ingreso de los camiones. Este lugar debe tratarse por lo menos una vez a la semana para evitar la proliferación de cualquier tipo de plaga y en las condiciones sanitarias adecuadas.

La basura de preferencia debe clasificarse de acuerdo a la materia y composición o reacción química, esto debe realizarse desde las mismas unidades organizacionales.

De acuerdo a lo anterior se deben generar los procedimientos y fomentar los hábitos ecológicos de cultura de reciclaje. Comúnmente, para realizar la tarea de clasificación de los desechos de acuerdo al tipo de material (orgánicos, plásticos, vidrios, papel, etc.), se requiere de la adopción de la nomenclatura (simbología), apropiada y la codificación en colores respectiva para los contenedores.

Tabla XI. **Colores asociados para indicar el contenido de los contenedores para reciclaje**

Tipo de material	Color del contenedor
Orgánicos (restos de comida, cáscaras de frutas, etc.)	Verde
Plásticos	Azul
Papel y cartón (periódicos, bolsas, cajas, etc.)	Amarillo
Vidrio y cristal (focos, lámparas, tazas, etc.)	Blanco
Metales (latas, envases, tubos, etc.)	Gris
Desechos sanitarios, peligrosos o no reciclables	Rojo
Otros desperdicios reciclables	Negro

Fuente: <http://www.economiadelaenergia.com/reciclaje/>

Figura 73. **Ejemplo de utilización de colores para los contenedores**



Fuente: <http://www.economiadelaenergia.com/reciclaje/>

La anterior es sólo una guía, debido a que existen otro tipo de materiales (textiles, maderas, lubricantes o aceites), etc., para los cuales, si el laboratorio los utilizara para alguna razón, se debiera investigar y crear los procedimientos para su adecuada evacuación o uso alterno.

En el caso de los materiales conocidos como *technotrash* o desechos provenientes de la tecnología (*DVDs*, computadoras, cartuchos, baterías, etc.), se requiere de la investigación local o regional de un proveedor que cumpla con las normas de responsabilidad ambiental, que posea procedimientos bien definidos de reciclaje y auditoría de la basura²⁴.

Si el laboratorio contratara una empresa con la descripción anterior, habría que solicitar el servicio de eliminación de la data (evidencia), es decir, que la información contenida en los discos duros, *CDs*, *DVDs*, etc., sea completamente destruida y no vaya inocentemente a la basura, donde posteriormente pueda ser mal usada. Esto es igualmente aplicable a la papelería o cualquier medio que contenga información. Han habido casos donde los intrusos (*dumpster divers* o "buceadores de contenedores ") encuentran tesoros en la basura para iniciar un proceso de ingeniería social, robo de información, usurpación de identidad, etc.

Si lo anterior no se puede garantizar, entonces, el laboratorio tendrá que contar con un servicio de destrucción de dicha información, la cual puede realizarse por *software*, destrucción física, usando fuerza bruta (por ejemplo, taladrando varias veces el disco duro o utilizando un esmeril en el caso de *CDs* o *DVDs*) o un equipo de emisión intensa de campos magnéticos²⁵. Posteriormente, se tendría que estudiar su deposición o el uso alternativo de los materiales (v.g. policarbonato de los *DVDs*).

²⁴ En Guatemala existen algunas iniciativas, tanto particulares como empresariales en cuanto a reciclaje, sin embargo, no existe aún una que se dedique específicamente a la basura tecnológica que brinde la cobertura o cubra el espectro de la misma como algunas de otros países (v.g. *GreenDisk* - <http://www.greendisk.com>).

²⁵ Estos dispositivos (de origen militar) han sido utilizados para borrar contenidos de discos duros, *VHS*, *DAT* y *ZIP drives*. Uno de los más famosos es el *GuardDog*, pese a su elevado precio, posee la ventaja de poder destruir la información de varios discos a la vez en segundos (ver <http://gtresearchnews.gatech.edu/newsrelease/erase.htm>; y http://www.technologyreview.com/read_article.aspx?id=17007&ch=infotech).

Seguramente en el futuro se crearán leyes concernientes al tratamiento de este tipo de basura, y por lo tanto la gerencia del laboratorio debe estar pendiente de la publicación de dichas leyes, así como de los adelantos tecnológicos en cuanto al cuidado del medio ambiente en este respecto.

En resumen, se sugiere que la gerencia plantee un programa de mantenimiento continuo de cada elemento del laboratorio de acuerdo a las necesidades particulares. A continuación se presenta una tabla-guía con los tiempos recomendados por cada elemento del laboratorio visto previamente.

Tabla XII. **Programación de tiempos (recomendados) para el mantenimiento del laboratorio**

Inciso	Elemento		Frecuencia
7.1.1.1	Estructura del edificio	Pisos, paredes, puertas, etc.	Diario
		Impermeabilización de techos	Una vez al año
		Revisión desagüe pluvial	Una vez al mes; en invierno aumentar a dos veces.
7.1.1.2	Instrumentos, equipos y herramientas	Limpieza y mantenimiento preventivo de los equipos forenses	Limpieza, por lo menos una vez al mes. Verificación de piezas, mecanismos, circuitería, etc. por lo menos una vez trimestralmente o a una frecuencia determinada por el proveedor (por contrato), la solicitud de los usuarios (peritos), disponibilidad de los equipos para las labores, etc.
7.1.1.3	Sistemas eléctricos y de protección	Revisión de circuitos de protección eléctrica (fusibles, extintores, UPS, etc.)	Por lo menos una vez al mes e inmediatamente después de eventos como apagones, sobrecargas, tormentas eléctricas, etc.
		Extintores y equipos contra incendio	De acuerdo a los tiempos brindados o especificados por los proveedores o la bitácora de fallas dadas por el <i>software</i> de monitoreo

Continuación tabla XII.

7.1.1.4	Equipo de protección personal	Gafas, batas, guantes, etc.	Diario
7.1.1.5	Aire acondicionado	Revisión y verificación de filtros, condensadores, termostatos, <i>dampers</i> , etc.	Una vez al mes (o de acuerdo a especificaciones del proveedor)
7.1.1.6	Alarmas y sensores	Alarmas contra incendios, sensores de humo, etc.	De acuerdo a los tiempos brindados o especificados por los proveedores o la bitácora de fallas dadas por el <i>software</i> de monitoreo
7.2	Almacén (bodega) de evidencias	Limpieza de anaqueles, pasillos, entradas y salidas, mecanismos movibles, etc.	Diario
		Tragaluces, ventanas, techos, etc.	Por lo menos una vez semestral
		Cámaras y sensores	Por lo menos cada quince días
		Extintores (o sistemas de extinción de fuegos)	De acuerdo a especificaciones del proveedor o luego de activación de alarmas en bitácora de monitoreo de sensores
7.3	Disposición de basura	Botes y contenedores (de reciclaje)	Diario
		Tratamiento de sitios (plagas y malos olores)	Una vez a la semana o la que designe la gerencia luego de la puesta en marcha o de acuerdo a las necesidades

Fuente: elaboración propia

7.4. Importancia del programa continuo de aseguramiento de la calidad

Las exigencias actuales de un servicio acorde a los requerimientos legales, tanto en el producto/servicio (el peritaje, los informes, la ratificación, etc.), como en el tiempo de entrega, hacen que el enfoque en la calidad sea muy

importante. Cada año aumentan los casos de solicitudes de análisis forenses en Informática por parte de la Fiscalía y por lo tanto, el laboratorio debe contar no solamente con la capacidad instalada para hacer frente a dicha demanda, sino también debe contar con un programa continuo de aseguramiento de la calidad.

Este programa de acciones planificadas y sistemáticas debe incluir un estudio de satisfacción respecto a las siguientes dimensiones.

- Dimensión técnica: estar en la capacidad de resolver todos los casos que lleguen al laboratorio que involucren tecnología, esto implica estar a la vanguardia, tanto en equipos, dispositivos y herramientas forenses, así como poseer la experticia de utilizarlos en forma eficaz y eficiente.
- Dimensión legal: el personal debe estar al día en cualquier cambio: ampliación, complemento o derogación de leyes referentes al trabajo forense realizado (v.g. cadena de custodia), de tal manera de ofrecer un producto completo, confiable, admisible, auténtico, creíble y útil como evidencia para el Ministerio Público y los Tribunales.
- Dimensión temporal: realizar el trabajo y entregarlo a tiempo, tomando en consideración los plazos (o normativas internas), o bien, que el Ministerio Público tiene la facultad de realizar emplazamientos. El tratamiento general de los trabajos es que el primero que entra es el primero que sale; sin embargo, habrán casos en los cuales se deberá priorizar el tiempo de entrega, por lo mencionado anteriormente u otras razones.
- Dimensión económica: en el contexto de minimización de los costos por caso, esto incluye por supuesto, los costos generados en la administración.

- Dimensión humana: la calidad en las relaciones entre personal del laboratorio y del Ministerio Público, confianza, veracidad, eficacia, etc.

La garantía o el nivel de satisfacción estarán relacionados íntimamente con la conformación a las normas, las buenas prácticas, las certificaciones (de los productos de *software/hardware*, del laboratorio y del *staff*), la pertenencia a asociaciones forenses mundiales, etc.

7.5. Importancia de las certificaciones

Actualmente muchas empresas realizan los trámites para obtener el aval de instituciones que demuestren que las personas, los procesos y los productos utilizados cumplen con los estándares de calidad, experiencia y competencia técnica respectivas o preestablecidas.

En Guatemala desde hace algunos años, los peritajes informáticos se han realizado con los escasos recursos disponibles, con instrumentos no avalados; sin embargo, se prevé que en un futuro cercano dichos trabajos periciales deban estar respaldados por una certificación o acreditación, que garantice y satisfaga los requerimientos en cuanto a certeza y buenas prácticas formulados por los tribunales o bien cumpla con normas emitidas por instituciones reconocidas (v.g. *ISO*, *NIST*, *NATA/AUSCERT*, entidades de metrología regionales, etc.) referentes a calidad, exactitud, confiabilidad, calibración, inspección, impacto ambiental, entre otros.

Los términos acreditación y certificación se han considerado como sinónimos, sin embargo, dentro del presente trabajo se les considera de la siguiente manera:

- **Acreditación:** procedimiento mediante el cual un organismo autorizado reconoce formalmente que una organización es competente para la realización de una determinada actividad.
- **Certificación:** es el proceso por el que una entidad independiente evalúa una organización, producto, proceso, servicio, persona, emitiendo posteriormente una declaración en la que quede de manifiesto la conformidad del evaluado con respecto a los requisitos de una norma o especificación técnica.

Este proceso de validación (obtención de la acreditación) que garantiza la calidad y la experticia o *know-how* del laboratorio, inicia con un análisis exhaustivo de los procedimientos, equipos y personal, el establecimiento de protocolos de trabajo, controles y programas de aseguramiento de la calidad. Y finalmente, la elaboración de la solicitud y la realización del examen por parte de la entidad correspondiente con autoridad de emisión para llegar al otorgamiento respectivo.

Debido a que estas acreditaciones y certificaciones garantizan la calidad y reconocen formalmente que el laboratorio es competente para la realización de sus actividades, la gerencia debe promover, persistir y gestionar la inversión financiera en la obtención de las mismas.

7.6. Importancia de la capacitación continua

La capacitación continua es importante por dos razones:

- Brinda una alta posibilidad de obtener certificaciones y acreditaciones.

- Permite estar actualizado y por lo tanto, estar en la capacidad de atender todos los casos en forma pronta, eficiente y eficaz.

Por estas razones, el laboratorio debe contar con un equipo que periódicamente estudie el mercado y vea las tendencias, tanto en tecnología como en productos informático-forenses y elaborar mesas de trabajo con la gerencia, para la planificación y análisis de compra de dichos productos y la justificación de la necesidad de capacitar al personal del laboratorio.

Debe considerarse, de preferencia, el estudio de los productos de uso masivo (por ejemplo, los *smart-phones*) debido a que habría que determinar si valdría la pena la inversión en un equipo que se utilice solamente en algunos casos.

Finalmente, la gerencia debe tratar de gestionar, en la medida de lo posible, acuerdos de valor agregado con los proveedores del equipo forense, de tal manera que la adquisición de los mismos, contemple también la capacitación de su uso.

7.7. Perfil profesional del perito

Al año 2010, aún no existe en Guatemala una carrera que explícitamente cubra los requerimientos de un profesional para la Informática Forense; sin embargo, las licenciaturas e ingenierías de carreras afines en sistemas, computación, informática, etc., tienen una base recomendable, especialmente aquéllas que incluyen en su *pensa*, temas centrales de sistemas operativos (*Windows, Linux, MacOS, Android*, etc.), diseño de sistemas, manejo de almacenamiento, bases de datos, arquitectura de computadores, redes,

comunicaciones (tecnologías, *internet*, correo electrónico, seguridad, etc.), desarrollo de aplicaciones, entre otros.

Por el carácter del tipo de trabajo a desarrollar, el perito adicionalmente debe poseer aptitudes psicomotrices finas, agudeza o visión sin problemas graves, carente de problemas de espalda (columna vertebral), que puedan acentuarse por el tipo de trabajo, etc.

Adicionalmente se considera que el profesional debe poseer otros conocimientos o habilidades, por ejemplo, manejo del idioma inglés, electrónica y electricidad, debe ser orientado a objetivos, poseer buena ortografía y redacción, etc.

La base técnica y de aptitud descrita previamente, puede ser complementada con otras carreras en Ciencias Criminalistas, Auditoría de Sistemas, Legislación de delitos informáticos, etc., y especializaciones en el campo forense particular, por ejemplo, *email forensics* (estudio forense del correo electrónico, protocolos, estructuras de almacenamiento, rastreo de *IPs*, *logs*, etc.), *file system forensic analysis* (análisis forense de sistemas de archivo, estudio de la forma en que los diversos sistemas operativos, almacenan, organizan, aseguran y manipulan los archivos y la data en un sistema), *cyberwarfare* (guerra cibernética), *cybercrime* (crímenes en el ciberespacio, investigación de delitos cometidos utilizando el *Internet*, robo o interceptación de información, sabotaje de redes de computadoras corporativas o gubernativas, pornografía infantil, etc.).

8. FUENTES DE FINANCIAMIENTO

Todo lo mencionado en los capítulos previos sería prácticamente irrealizable si no se dispusiera con los recursos económicos, tanto para la creación como para el funcionamiento y mantenimiento posteriores. Por supuesto, para poder llevarlo a cabo, se tiene que realizar el estudio del proyecto respectivo (i.e. factibilidad), tomando en consideración que éste tendrá un alto impacto social, debido al beneficio que las pruebas o evidencias representan para la ejecución penal efectiva.

Un proyecto como éste tiene que pasar por varias etapas, no solamente económicas y financieras, sino legales, por ejemplo, la creación de esta entidad (laboratorio de Informática Forense), debe realizarse y definirse a través de un Decreto del Congreso de la República de Guatemala para la elaboración de su Ley Orgánica, a no ser que sea contemplado administrativa y económicamente como parte de alguna institución existente²⁶ que ya cuente con instalaciones, patrimonio propio, personalidad jurídica, fuentes de cooperación, etc.

De acuerdo a lo anterior, la institución que adopte la creación del Laboratorio de Informática Forense requerirá realizar las proyecciones financieras correspondientes dentro del presupuesto asignado por el gobierno de Guatemala; sin embargo, también se pueden considerar otras fuentes internas, externas o una combinación de ambas; en resumen, las tres grandes

²⁶ Actualmente el INACIF no contempla este tipo de experticia forense y aunque el Ministerio Público cuenta con un departamento de Tecnología e Informática, que al día de hoy ha realizado un buen trabajo en este tipo de labores, aún no existe dentro del mismo, una unidad específica para este tipo de casos; sin embargo, debido a que en Guatemala existe un Instituto Nacional de Ciencias Forenses – INACIF - y considerando el nivel de imparcialidad requerido por la Ley, se recomienda que el laboratorio sea absorbido por éste.

fuentes de financiamiento a las que recurren las instituciones de Justicia para la creación de este tipo de instituciones son:

- Fuentes propias del Gobierno de Guatemala: las aprobadas dentro de un presupuesto anual de funcionamiento o la ampliación de uno ya existente (v.g. INACIF).
- Fuentes externas: la República de Guatemala ha recibido grandes aportes financieros de la Comunidad Internacional, especialmente en el sector Justicia. Instituciones como PNUD (Programa de las Naciones Unidas para el Desarrollo), OEA (Organización de Estados Americanos), Unión Europea, AECID (Agencia Española de Cooperación Internacional para el Desarrollo, etc.), han brindado ayuda, tanto en la creación de instituciones como en la puesta en marcha de las mismas, a través de acuerdos de cooperación internacional.

Este apoyo, puede ser muy útil para lograr la cobertura financiera en el montaje de la infraestructura inicial (mobiliario, equipo, instrumentos, herramientas, contratación de personal, etc.). Este apoyo no solamente puede constituirse en dinero sino también en capacitación, asesorías, donaciones, etc.

- Fuentes mixtas: este tipo de financiamiento consiste en la cobertura parcial de ciertos aspectos, tanto por el gobierno de Guatemala como de fuentes exógenas de acuerdo a los términos de cooperación preestablecidos y el manejo de contra partidas.

Éste puede ser muy útil a considerar para la capacitación de personal, obtención de las certificaciones, compra o renovación de equipos, adquisición de *software* y *hardware*, etc.

8.1. Proyección en el presupuesto anual de funcionamiento

Para poder realizar un presupuesto eficiente que contemple en forma realista todos los gastos, la gerencia o jefatura debe utilizar información estadística (si estuviera disponible) de egresos por renglón presupuestario, efectuados durante un periodo o ejercicio fiscal determinado de instituciones similares, por supuesto esto solamente a nivel de salarios, papelería, útiles de escritorio, etc.

Para el caso de las herramientas forenses (dispositivos, *software* y *hardware*), capacitación, servicios varios (energía, enlaces, *internet*, etc.) se deben realizar varios estudios, por ejemplo análisis de mercado, cotizaciones o licitaciones con proveedores, proyección del número esperado o demanda de casos a atender, fluctuación de la moneda, etc., a fin de realizar un buen cálculo de los márgenes o techos financieros; finalmente, adicional al precio de los dispositivos, deben considerarse los costos de operación y mantenimiento respectivos.

8.2. Convenios de cooperación financiera y de capacitación

8.2.1. Inter-institucional

Debido a que la creación de un laboratorio de este tipo repercutiría en beneficio de la Justicia en Guatemala, las instituciones pueden potencialmente colaborar, no sólo monetariamente sino aportando la experiencia del personal

en el área. Actualmente, el Organismo Judicial, Ministerio Público, Policía Nacional, entre otros, han tenido contacto con la Informática Forense, sea que se trate del análisis de contenido de computadoras, extracción de información de celulares, lectura de bitácoras de *GPS*, etc. Los convenios de cooperación interinstitucional pueden incluir, la transmisión de experiencia o capacitación, apoyo en equipos, recursos financieros, terrenos o edificios, etc.

8.2.2. Organismos internacionales y países amigos

Además de las organizaciones de cooperación previamente mencionadas, existen muchos otros países y organismos dispuestos a ayudar a las naciones en el combate a la delincuencia y el fortalecimiento de la Ley. Países como Canadá, Estados Unidos de América, Francia, España, etc., han apoyado en forma directa o a través de organismos ejecutores a la región centroamericana en temas como investigación, combate a la corrupción, lavado de dinero, crimen organizado, trata de personas, narcotráfico, etc. Este tipo de ayuda puede materializarse en dinero, capacitaciones (debido al gran avance que estos países tienen en el campo criminalista y en Informática Forense), pasantías en los laboratorios, asesorías técnicas, material bibliográfico, adquisición de herramientas informáticas tanto de *hardware* como de *software*, etc.

Respecto a los convenios de cooperación, la gerencia o jefatura del laboratorio debe elaborar con sumo cuidado el proyecto de solicitud ante los oferentes, indicando los términos de referencia y compromiso, los beneficios, los efectos y repercusiones, la descripción específica de los bienes tangibles o intangibles y su monto, la forma de evaluación o monitoreo de la ejecución o uso de los recursos, la sostenibilidad, impacto, etc.

8.2.3. Universidades

En el aspecto de universidades nacionales, éstas pueden brindar un gran apoyo al contemplar dentro de las carreras afines a la informática la *addenda* en forensia y criminalística; impulsando la investigación en buenas prácticas y procedimientos, promoviendo ante las instancias pertinentes la necesidad de marcos legales o leyes específicas, etc.

Respecto a universidades extranjeras, se puede llegar a acuerdos de intercambio, aprovechando que muchas de éstas incluyen en su *pensa*, carreras o diplomados afines, brindan cursos, talleres, seminarios, etc.

8.3. Donaciones

Una de las formas de cooperación que los organismos internacionales o los países utilizan es la donación. Esta comúnmente se brinda sin contrapartida y de mutuo acuerdo entre las dos partes. Aunque al realizarla es de carácter obligatorio elaborar la documentación legal respectiva, ésta tiene ciertas ventajas a nivel de impuestos y/o potenciales exoneraciones preestablecidas o a través de un Decreto del Congreso de la República.

9. CONTROL Y SEGUIMIENTO

El proyecto, al igual que otros, debe pasar por varias facetas: desde la aprobación de la puesta en marcha, la obtención de fondos (esto incluye la revisión de techos financieros y el ajuste del presupuesto asignado), hasta la revisión de los procesos y readecuación de los mismos, a nivel legal y tecnológico. El control y el seguimiento se ejecutarán basándose en los requerimientos y especificaciones, así como en el cronograma. Para poder realizarlo se deben planificar las inspecciones y mediciones respectivas a lo largo de la obra gris, haciendo las observaciones pertinentes y las presiones o negociaciones contractuales con la empresa constructora o los proveedores; esto con el fin de realizar ajustes, tanto físicos como cronológicos respectivos.

En el caso de la verificación de procesos (tiempos, recursos necesarios, capacitación, etc.), se recurrirá al levantado de encuestas y el registro de formularios, esto para medir la eficacia de las herramientas y dispositivos forenses, así como el tiempo aproximado utilizado por el *staff* del laboratorio en la realización de cada tarea.

Parte del seguimiento de la creación del laboratorio, es la definición del rol de jefe de proyecto y las comisiones de seguimiento, los que velaran por la adecuación del proceso de contratación del personal de las jefaturas de las distintas áreas, esto incluye el establecimiento de salarios y los perfiles de los profesionales; desarrollo de la obra física, control del correcto uso del presupuesto asignado, así como la gestión de cooperación (en el caso de financiamiento externo o mixto), investigación de productos forenses y proveedores, etc.

Dentro del presente trabajo, solamente se brinda una guía de lo que deben realizar las comisiones, debido a que el número de éstas en la vida real es mucho más grande y la definición de sus actividades es larga y compleja, por lo que se sugiere la lectura de material especializado.

9.1. Creación del comité de proyecto

Este comité es el grupo gestor y supervisor del proyecto y por lo tanto, es el encargado de cuidar porque se cumplan todas las fases del proyecto, los tiempos estipulados, o bien la realización de los ajustes, revisión de la obra, compras, etc. Éste se debe crear a través de la contratación de personas y/o ajustando personal calificado para realizar dichas labores provenientes del INACIF o el Ministerio Público. Este grupo de personas debe ser el idóneo de tal manera que utilice bien el empoderamiento (*empowerment*) que se le concederá.

9.1.1. Definición del rol de jefe de proyecto

Será el encargado de velar porque todas las comisiones trabajen y entreguen los resultados de acuerdo al establecimiento de los tiempos definidos, es la persona que dirigirá las convocatorias del comité en la toma de decisiones ante cualquier imprevisto. El jefe de proyecto debe poseer varias características, entre ellas están las siguientes:

- Habilidad de negociación: excelente comunicador y diestro en el manejo de la información.

- Liderazgo y pro actividad: consecuente y orientado con los objetivos, responsable, centrado en las personas y la sinergia, visión, buen manejo de los conflictos y la presión, etc.
- Experiencia y conocimiento: conoce el trabajo, cómo realizarlo y cómo enfrentar las contrariedades y los atrasos, experiencia en distribución de recursos de acuerdo a prioridades.

9.1.2. Definición de las comisiones

Las comisiones serán grupos pequeños de personas que se encargarán de la realización de ciertas actividades. Éstas serán elegidas por el jefe de proyecto, reconociendo la capacidad y experiencia de las personas y durarán hasta la conclusión de las actividades o la finalización del proyecto.

Estas comisiones realizarán cada tarea que les corresponda y generarán los instrumentos de evaluación respectivo del progreso de las mismas (v.g. formularios, especificaciones, perfiles profesionales, *tests*, calendarios (*a priori*) y ajustes dentro del cronograma general (*a posteriori*)).

9.1.2.1. Obra física

Será la encargada de las licencias de construcción respectivas, la revisión periódica del avance de la obra, verificará la calidad de los materiales y que se cumpla con las especificaciones de arquitectura e ingeniería, atenderá las necesidades, las contingencias (v.g. accidentes, falta de materiales, condiciones climáticas, etc.), realizará los ajustes en los tiempos para notificar y coordinar con otras comisiones en el caso de las actividades dependientes, por ejemplo, la comisión de mobiliario y equipo no podría iniciar el proceso de adquisición de los

mismos hasta no conocer exactamente las áreas donde estos se instalarán y su respectivo el tiempo de entrega.

9.1.2.2. Adquisición de mobiliario, equipo y materiales

Comisión encargada de elaborar las especificaciones del mobiliario y equipos de las áreas administrativas y laboratorio, debe realizar el estudio de mercado de proveedores, evaluar el presupuesto asignado y diseñar el proceso de cotización o licitación correspondiente, elaborar las bases de compra (garantías, formas de pago, tiempos de entrega y armado, etc.). Al momento de la entrega, esta unidad se encargará de vigilar por las especificaciones y detalles, la correcta instalación, los reclamos y las solicitudes de cambio.

9.1.2.3. Adquisición de Instrumentos, herramientas y dispositivos forenses

Junto con la comisión de evaluación de procesos forenses, esta comisión será la encargada de adoptar los estándares respectivos necesarios para el laboratorio en materia de *hardware* y *software* que cumpla con las necesidades proyectadas de trabajo y que haya pasado las pruebas de aprobación guatemaltecas (si existieran), o certificadas por instituciones reconocidas a nivel mundial en materia forense.

Esta comisión deberá estudiar las opciones ofrecidas por los proveedores, evaluar el presupuesto estipulado para este rubro (de acuerdo a la capacidad instalada proyectada de inicio de operaciones), realizar las bases de compra respectivas, negociar el mantenimiento y capacitación del uso de los mismos y velar por la observancia de las licencias concernientes, así como de las garantías.

9.1.2.4. Evaluación de procesos forenses

Esta es la comisión que velará por el estudio de las normas, especialmente las legales, a fin de evitar que algún procedimiento, aunque eficiente, contenga alguna incompatibilidad con los protocolos o las leyes establecidas en Guatemala.

9.1.2.5. Contratación de personal

La comisión de contratación de personal es la unidad de proyecto encargada de generar los procedimientos y evaluaciones a fin de encontrar los candidatos idóneos para cada área, valuando el potencial técnico del profesional, así como otras aptitudes, tanto físicas como mentales de los solicitantes, basándose en la serie de exámenes respectivos, como entrevistas, hojas de vida, experiencia, pruebas psicométricas, exámenes médicos, etc. También, esta comisión deberá levantar la base de datos respectiva a fin de iniciar adecuadamente el sistema de Recursos Humanos y el proceso de inducción respectivo.

Si no se pudiera establecer la comisión de contratación de personal, actualmente existen otras opciones que podrían considerarse como las agencias de colocación; las cuales de acuerdo a los perfiles enviados previamente, se encargarían de todo el proceso de evaluación e investigación o de antecedentes de los candidatos.

9.1.2.6. Comisión de compras

La comisión de compras será la encargada de realizar el inventario de ofrecimientos de los cooperantes (si los hubiera), así como de la forma de su aportación (completa, mixta, contra partida, donaciones, etc.); también deberá elaborar un inventario de los requerimientos de todo lo necesario para equipar el laboratorio (productos y servicios), para que pueda iniciar labores, esto incluye, la adquisición de los muebles, el servicio de electricidad, el servicio telefónico, los automóviles, etc. La determinación o definición de dichos requerimientos incluye la determinación de las cantidades, calidades, costos, etc., apropiados, así como la disposición de la forma de pago y del tiempo y lugar de entrega o de instalación; se incluye la forma de evaluación o ponderación de los proveedores, es decir, debe implementarse un mecanismo de decisión.

Dependiendo del monto, lo anterior debe enmarcarse dentro de la Ley de Compras y Contrataciones del Estado, por lo tanto, deben realizarse las bases respectivas y debe efectuarse su publicación en Guate-compras a fin de realizar la licitación o cotizaciones de los bienes o servicios.

9.1.2.7. Comisión de mantenimiento

La comisión de mantenimiento será la encargada de la planificación de todas las acciones que tienen como objetivo mantener, en sus primeras instancias, un laboratorio en buenas condiciones funcionales. Una vez, se termine el proyecto de construcción del edificio, generará las políticas y planes para mantenerlo funcionando de una forma eficiente. Esto involucra, la contratación o subcontratación del personal de limpieza, así como del *staff* pertinente que vigile el desempeño de talanqueras, puertas, grifos, ductos, etc.

En general, éstas son algunas funciones de la comisión de mantenimiento:

- Verificar que el contratista cumpla con los requerimiento de la obra (planos de construcción, eléctricos, pluvial, red, etc.), así como el acondicionamiento de los ambientes (luces, pintura, cerraduras, etc.); esto incluye la revisión exterior de techos, parqueos, áreas verdes, etc.
- Supervisar que el trabajo del contratista, se realice cumpliendo el cronograma, o bien se realicen los ajustes respectivos por cualquier inconveniente.
- Elaborar el primer programa de mantenimiento preventivo y correctivo de las instalaciones.
- Preparar los reportes ante el jefe de proyecto. Esto incluye información de avances, ajustes, costos, etc.
- Al finalizar, velar por finiquitar los contratos y cierres administrativos de las obras contratadas.

Al igual que otras comisiones, por lo general, al finalizar el proyecto de puesta en marcha, parte del personal involucrado en las comisiones, pasa a ser parte de la estructura organizacional de la entidad, en este caso por ejemplo, el director de la comisión puede desempeñar el rol de administrador del edificio del laboratorio.

9.1.2.8. Comisión de finanzas

El objetivo principal de la comisión de finanzas es controlar la ejecución de los recursos financieros y económicos del laboratorio, por lo tanto deberá contabilizar y auditar los movimientos de efectivo durante la fase inicial, construcción y puesta en marcha del laboratorio.

Funciones primarias de esta comisión son:

- Asesorar al jefe de proyecto en cualquier aspecto de índole financiero-contable, velando por el cumplimiento de las disposiciones legales vigentes en Guatemala en esta materia (administración e inversión de los recursos económicos asignados).
- Proponer normas y procedimientos, con el fin de lograr una adecuada gestión financiera del laboratorio, tanto de los fondos propios (o nacionales), como los provenientes de fuentes externas u obtenidos por cooperación internacional.
- Llevar los registros respectivos (balances, informes mensuales, movimientos de cajas, etc.), informando al jefe de proyecto del avance de ejecución presupuestaria, con la finalidad de proporcionar información para toma de decisiones.
- Exigir y controlar (en materia financiera) a todas las comisiones respecto al uso o inversiones de los recursos.
- Participar en el proceso de elaboración del presupuesto.

- Firmar los documentos de respaldo emitidos (v.g. cheques), por las diferentes contabilidades, en su condición de cuentadante.
- Presentar para la aprobación del señor director, toda la documentación relacionada con la administración financiera del Departamento Finanzas.
- Intervenir en el proceso de compras o adquisiciones que el laboratorio efectúe, avalando con la firma del encargado de comisión, las órdenes de compra dentro del proceso de cotizaciones, licitaciones, adjudicaciones y demás disposiciones legales.

9.1.3. Creación instrumentos de control: CPM, cronogramas, formularios, encuestas de seguimiento, etc.

Para poder efectuar un efectivo control y seguimiento del proyecto, se deben elaborar varios instrumentos, entre ellos: el cronograma – *Gantt* - con las fechas previstas de comienzo y final de cada actividad; los diagramas de Ruta Crítica – *CPMs*- los formularios de revisión e inspección de cada *ítem* de la construcción (losas, pisos, infraestructura eléctrica, etc.). Durante el inicio de actividades se deben realizar las encuestas de satisfacción, problemas encontrados, funcionamiento del edificio, operación de las herramientas forenses, etc.

Los objetivos para la realización de los instrumentos de control son:

- Mantener el ritmo de trabajo, así como la documentación de constatación de cada paso realizado.

- Obtener una idea general de la envergadura del proyecto y de los recursos a invertir (materiales, tiempos, humanos, etc.)
- Mostrar la importancia crítica de las actividades dependientes o secuenciales.
- Planificar las visitas de revisión, llamadas a los proveedores, entregas de materiales, etc.
- Realizar los ajustes en los calendarios o anticiparse a las contingencias.

9.2. Revisión de las cartas de cooperación

Una carta de cooperación es un documento donde se establecen los considerandos, acuerdos, cláusulas de compromiso, vigencias, formas de evaluación, nombres de representantes de los gobiernos o instituciones, etc. entre un país y otro o una organización y otra, para lograr la firma o mutuo acuerdo de convenios, pactos, colaboraciones, alianzas, etc. con el objetivo de obtener algún tipo de beneficio o alcance (mutuo, regional, humanitario, legal, etc.), a través de un conjunto de acciones, políticas, donaciones, asesorías, aportaciones financieras, etc. o por medio de la instauración de alguna institución en los países.

9.2.1. Términos e indicadores del programa de cooperación o donación

Existen muchos instrumentos para la medición de proyectos, tanto matemático-financieros, como temporales y de control (medir el avance). Por lo tanto, la gerencia debe predefinir qué instrumentos utilizar y qué comisiones

deben desarrollarlos. Por otra parte, debido al carácter y el ámbito de cobertura del laboratorio, debe considerarse una medición (preferiblemente estadística), del impacto social que éste tendrá en la República de Guatemala.

Debe considerarse también, la generación de instrumentos financieros que muestren la transparencia de la utilización de los fondos recaudados a través de cooperación internacional, lamentablemente un tema muy sensible, especialmente en los países de Latinoamérica).

Por lo anterior y con el fin de aclarar o justificar el proyecto ante los cooperantes o donantes, se deben establecer los términos y los índices del programa de cooperación. En el caso de los términos, éstos deben incluir todas las especificaciones técnicas, objetivos específicos del laboratorio, formas de ejecución presupuestaria, estudios de impacto social, proyección de resultados, los hitos del proyecto, etc.

Estos términos deben incluir entre otros:

- Visión, objetivos, alcance y resultados (qué debe ser alcanzado).
- Componentes, roles y responsabilidades (quién tomará parte en ello).
- Recursos, finanzas y planificación de calidad (cómo será alcanzado).
- Desglose del trabajo y calendarización (cuándo será alcanzado).
- Factores de éxito/riesgos y restricciones.

Los términos de referencia conforman una especie de mapa; dan un camino claro para el progreso, especificando qué necesita ser alcanzado, por quién y cuándo. Debe ser, entonces, una lista de resultados que concuerden con los requerimientos, alcance y limitaciones existentes.

Por otra parte, los indicadores son medidas resumen, de preferencia de índole estadística, referentes a la cantidad o magnitud de un conjunto de parámetros o atributos de una sociedad que permite clasificar las unidades de análisis (por ejemplo: personas afectadas por delitos informáticos). Para definir claramente los indicadores, éstos deben mostrar tanto la situación previa (a priori) antes de la implementación del laboratorio y los resultados esperados, o bien los datos obtenidos en un lapso de tiempo luego de la puesta en marcha (a posteriori); en este caso se persigue determinar el impacto social del proyecto.

Estos indicadores, por ejemplo, podrían ser el nivel de satisfacción de la necesidad, la disminución de delitos de índole informática, debido a las herramientas de apoyo a la persecución penal, la generación de iniciativas de ley más rígidas y específicas en esta materia, el número de casos llevados a tribunales con algún tipo de condena, etc.

Para elaborar los indicadores deben considerarse los siguientes requisitos.

- Validez: significa que los indicadores deben reflejar los impactos buscados, de tal manera que éstos se puedan comprobar.
- Confiabilidad: en el sentido que si las mediciones son realizadas por diferentes personas, los resultados deben ser similares o dentro del margen de tolerancia aceptable.

- Efecto demostrativo: deben darse evidencias de muestras concretas de los cambios.

Para esto pueden utilizarse cifras absolutas, porcentajes, promedios (u otras medidas estadísticas), escalas, etc. lo que se persigue es presentar ante las instituciones colaboradoras (cooperantes), el impacto positivo del proyecto apoyado por ellos, el buen uso de los recursos y el beneficio social alcanzado.

9.2.2. Delimitación de la inversión

Para poder iniciar el proyecto es necesario establecer el monto total de la inversión con una holgura considerable para cubrir las fluctuaciones normales de precios, los imprevistos, tanto internos como externos (de carácter político, cambios gubernamentales, desastres naturales, etc.).

La mejor estrategia es dividir el proyecto en fases y lograr la participación de la cooperación internacional, especialmente de aquellos países o entidades con orientación y experiencia en el sector justicia (v.g. Bélgica, Canadá, PNUD, AECID, etc.). Dicha ayuda es necesaria especialmente para la obtención de fondos para infraestructura de inicio de labores, tomando en consideración un auto-sostenimiento posterior a través del Presupuesto General de la Nación.

Esta infraestructura de lanzamiento del proyecto incluye, por ejemplo, la adquisición de los equipos, dispositivos y herramientas forenses, capacitación del personal, adquisición de mobiliario y equipo, vehículos, etc. Esto puede obtenerse a través de varios mecanismos como donaciones, firma de convenios o acuerdos, establecimiento de programas, etc.

9.2.3. Reajustes

En todo proyecto se deben realizar los ajustes necesarios, tanto en recursos materiales como humanos y temporales, aunque éstos deben estar plenamente justificados antes las entidades o los representantes de entidades cooperantes. Este tema debe tratarse con más delicadeza debido a que puede resultar exasperante para la cooperación internacional re-calcular o realizar los trámites de recaudación de fondos en cada entidad o país. De preferencia, los reajustes debieran cubrirse con financiamiento guatemalteco.

Sin embargo, si no se lograra la cobertura del proyecto con las finanzas nacionales, se puede recurrir a un estudio de lo que falta para la conclusión de los planes de implementación del laboratorio, a fin de proveer los datos para la solicitud de colaboración a través de un único reajuste. Éste debiera preverse con suficiente tiempo de anticipación y no en el momento de la carencia, y por tanto, a lo largo de la puesta en marcha deben existir diversos puntos de control financiero, de tal manera que se pueda identificar discrepancias entre lo proyectado y lo realizado mucho antes de llegar a la medianía del proyecto.

9.2.4. Ampliaciones (enmiendas)

Como se indicó previamente, debiera haber solamente un reajuste para la solicitud de una ampliación de fondos; sin embargo, se puede llegar a negociar a-priori los considerandos dentro de los convenios, a fin de contemplar las enmiendas durante las distintas fases del proyecto por cualquier circunstancia, especialmente las financieras y las relativas a los tiempos de avance del proyecto. Estas enmiendas debieran incluir ampliaciones (aumentos), ajuste de los tiempos de control o evaluación, traslados de fondos entre rubros (con el fundamento y el establecimiento de prioridades respectivo), etc.

Estas prioridades deben ser levantadas y ordenadas por la gerencia del proyecto y reevaluadas al momento de detectarse en la proyección de gastos, la carencia de los fondos a fin de determinar los *items* a sacrificar o modificar.

9.3. Verificación de las instalaciones

Para poder verificar el avance y los requerimientos en tiempo y calidad de la obra física es necesario la elaboración y llenado de formularios, tanto para la verificación del trabajo realizado (en tiempo y calidad), como para la evaluación de ajustes y supervisión del contratista.

9.3.1. Inspecciones oculares

Las inspecciones deben llevarse a cabo de acuerdo a la programación del cronograma, de preferencia deben ser realizadas por un equipo multidisciplinario (ingenieros civiles, arquitectos, jefe de proyecto, etc.).

Éstas deben documentarse con fotografías, toma de videos y notas, especialmente de aquellas actividades que habiendo sido calendarizadas no se han concluido o no se han realizado de acuerdo a las especificaciones planificadas.

9.3.2. Mediciones

Debido a que la inspección ocular es simplemente una observación somera de la estructura y partes constitutivas del edificio, es necesario realizar diversos tipos de mediciones (dimensiones, alturas, áreas, etc.), muestreo de tomacorrientes (corriente y voltaje), tanto las líneas reguladas como las estándares; revisión de interruptores, *relays*, sistemas de emergencia, etc. Por

esta razón, el equipo que realiza las inspecciones debe contar con los instrumentos necesarios para esta tarea.

Las mediciones deben documentarse apropiadamente para realizar las observaciones pertinentes y deben realizarse varias veces para asegurar la calidad, porque se han dado casos donde la medición eléctrica de un circuito en una fecha determinada cumple con los requerimientos, sin embargo, luego de la terminación de los otros circuitos, ya no satisface las especificaciones debido a errores, derivaciones secundarias, etc.

9.3.3. Comparación con estándares

Las mediciones realizadas deben compararse con un patrón o estándar pre-establecido. Éstos deben definirse antes del inicio de los trabajos a fin de que los cálculos financieros esperados para la construcción no se vean afectados durante la misma. Los estándares estarán enfocados en la calidad, durabilidad, márgenes de tolerancia, etc.

9.3.4. Correcciones o mejoras pertinentes

Generalmente, durante la construcción existen factores que hacen que lo planificado no pueda cumplirse (fallas con los proveedores de materiales, atrasos, cambios climáticos, fluctuaciones económicas fuera de control, etc.). Por lo tanto, debe esperarse que haya algún tipo de corrección que deba efectuarse sobre la marcha, o bien, también cabe la posibilidad que se implante alguna mejora (no contemplada en los planos), debido a muchas razones (v.g. cambios en las áreas, expansiones, más puntos de red informática, instalación de otros servicios, etc.).

Estas correcciones o mejoras, comúnmente traerán repercusiones económicas y financieras para el proyecto y por lo tanto, en la medida de lo posible deben tratar de preverse de tal forma que se realicen sin necesidad de botar o destruir lo ya edificado, es decir, tratando que no haya desperdicio.

9.4. Adquisición de mobiliario y equipo

Posterior a la construcción y los acabados del edificio, debe continuarse con la adquisición de todo el mobiliario y equipo de las diferentes áreas. Esta actividad debe realizarla la comisión correspondiente junto con la comisión de compras y finanzas de acuerdo a lo preestablecido en el proyecto y los planos, tomando en consideración los cambios, mejoras o ampliaciones de construcción.

Debiera existir desde el inicio del proyecto, un plano de ubicación de toda la mueblería del laboratorio (capacidad instalada prevista); sin embargo, la adquisición debe planearse desde que los ambientes están delimitados en la obra gris (i.e. cuando están todas las paredes), debido a que la negociación de compra toma tiempo y muchas veces el proveedor tiene que realizar las importaciones respectivas.

9.4.1. Verificación de propiedades y calidad de los bienes muebles

La comisión responsable mencionada en el inciso 9.1.2.2 debe velar porque, previo a la gestión de compra, se investigue acerca de los proveedores, calidad de sus productos, nivel de responsabilidad, experiencia, etc. y que los muebles cumplan con los requerimientos por áreas previstos en los capítulos cuatro, cinco y seis del presente documento.

9.4.2. Comparación con lo planificado

La gerencia siempre debe permanecer atenta a cualquier cambio surgido durante la construcción del inmueble a fin de establecer con certeza la cantidad, tamaño y especificaciones de los muebles de todas las áreas. Por lo tanto, debe poseer, no solamente los planos con indicaciones de ubicación de los muebles, sino también reacomodar los datos con el fin de que no haya sobrantes o faltantes. Se excluyen aquellos casos a futuro, cuando sea necesario adquirir más muebles debido a la expansión por motivos de demanda de servicios.

9.4.3. Correcciones

Como producto de inciso anterior, se tendrán que realizar las correcciones necesarias en los movimientos financieros del proyecto, tanto para cubrir o dejar en reserva el dinero respectivo, a fin de cuadrar las finanzas proyectadas con lo ejecutado en el aspecto de adquisición de mobiliario y equipo.

9.5. Adquisición de instrumentos, *hardware*, *software*, etc.

La compra de los instrumentos o dispositivos forenses, es tarea de la comisión respectiva, la cual a este punto ya tendrá todas las especificaciones y los estudios de mercado de proveedores para trasladarlo a la comisión de compras, para que ésta inicie el procedimiento respectivo, el cual de preferencia debe ser posterior al término de la construcción, la adecuación de ambientes, con el mobiliario y equipo, electricidad, iluminación, etc., y la contratación del personal de laboratorio, de tal forma que los equipos se puedan ser probados y no pase tiempo para reclamos, garantías, capacitaciones, etc.

9.5.1. Levantado de hojas de especificación

Para realizar un evento de cotización o licitación²⁷ deben realizarse las hojas de especificaciones o las bases de los productos de que se desean adquirir, éstas son importantes para comparar precios de productos idénticos (y no similares), calidades, soporte, garantías, etc. es decir, estas hojas definirán lo que el laboratorio como comprador quiere adquirir y que el proveedor debe proporcionar.

Estas bases también establecen los requisitos que deben cumplir los proveedores (declaraciones de impuestos, capacidades, experiencia, etc.) para que puedan participar. Dentro de las mismas se asientan los puntos de entrega, las fechas de recepción, cantidades, etc., de los productos o servicios a adquirir.

9.5.1.1. Creación de las bases - productos y proveedores

Luego de generar las especificaciones a detalle, se debe realizar la creación de las bases, donde además de mostrar los aspectos técnicos de los productos, se enlistan los requerimientos legales que los proveedores deben cumplir (patentes de comercio, fianzas, declaraciones juradas, etc.).

9.5.2. El proceso de licitación y compra

Luego de la detección de las necesidades, el levantado de las hojas de especificación, la creación de las bases y la publicación, debe integrarse una junta de cotización o licitación (de acuerdo al monto), cuyos miembros no deben

²⁷ Ver Ley de Compras y Contrataciones del Estado de Guatemala.

tener ningún impedimento o recusación. Esta junta tendrá competencia para recibir, calificar y adjudicar, tomando en consideración los requerimientos legales, las características de los bienes o servicios, precios, etc., ésta tomará la decisión pertinente y adjudicará o declinará el evento de acuerdo a las circunstancias particulares, dejando constancia de lo actuado en una acta.

Tomar en consideración que se debe conocer completamente la ley a fin de dominar el tema del proceso de cotización y licitación, para evitar problemas legales que pueden tener repercusiones muy serias. Para realizar estas tareas la gerencia deberá auxiliarse del departamento o área técnica-jurídica del laboratorio.

9.5.3. Estudio de proveedores

Parte del proceso de cotización o licitación es el estudio de los proveedores, especialmente en el caso de adquisición de los equipos forenses, considerando la importancia de estos en el laboratorio y el precio elevado de los mismos. Los proveedores, en este sentido deben poseer respaldo técnico acreditado, basado en normas y estándares, experiencia comprobada, etc. Por esta razón, previo a la compra, debe realizarse la investigación respectiva.

9.5.3.1. Productos, servicios, mantenimientos y reparaciones

Debido a la diversidad de productos con funciones similares, se debe solicitar todas las características técnicas de los mismos a cada uno de los proveedores, los cuales previo al evento deben haber sido revisadas y tabuladas de acuerdo a las especificaciones o necesidades del laboratorio. Estas actividades las realizará la comisión de adquisición de equipos forenses (ver

9.1.2.3.), no escatimando el costo, siempre y cuando no sobrepase el valor estimado mostrado en la tabla IV o el presupuesto asignado. A productos técnicamente iguales o similares deben analizarse otros aspectos para la elección como: el precio, el soporte técnico certificado, la capacitación (si la incluyera), la asistencia ante fallas, etc.

Debe considerarse, dentro de la compra de productos, las opciones tanto del mantenimiento de los equipos, como de las reparaciones, agregando las respectivas cláusulas de utilización prepago o alquiler de dispositivos forenses al momento de las reparaciones, esto para evitar el atraso en el trabajo del laboratorio.

Respecto a los mantenimiento se sugiere utilizar la tabla XII o bien las especificaciones propias del producto dadas por el fabricante.

9.5.3.2. Calidad y conformación de normas

Las herramientas forenses deben estar certificadas o avaladas por una institución que garantice su desempeño, debido especialmente, por los requerimientos de los tribunales de justicia. De preferencia, deben adquirirse productos aprobados por *NIST* e *ISO*, dos de las instituciones más prestigiosas en el ámbito de definición de estándares forenses o bien por una autoridad idónea. El hecho de tener productos certificados, garantiza su calidad (adecuados, confiables, exactos, durables, etc.).

9.6. Revisión de procesos y diagramas

A pesar que en el presente trabajo, se incluyó en el capítulo dos de este documento, la descripción general de siete procedimientos básicos de Informática Forense, se hace necesario - debido a los cambios en tecnología, cambios en las leyes, buenas prácticas y normas, etc. – la implementación de un grupo que vele por la actualización de los diagramas de los procesos forenses realizados, tal como lo haría un departamento de investigación, organización y métodos.

9.6.1. Definición de tareas

De lo anterior, es fundamental la definición y delimitación de cada actividad realizada en los procesos, herramientas y materiales utilizados, tiempos y holguras aproximadas, revisión de formularios, etc., con la finalidad de realizar los trabajos en forma eficaz y eficiente.

El administrador del laboratorio tendrá, por lo tanto, que desarrollar un mecanismo de verificación de los procesos, los cuales deberán ser analizados por lo menos cada seis meses. Por supuesto, este mecanismo debe incluir a los peritos, las investigaciones de las tendencias tecnológicas, la información del sistema informático de seguimiento, etc.

9.6.2. Verificación de estándares y normas

Actualmente, los tribunales requieren que los trabajos o peritajes estén certificados para garantizar la fidelidad de los resultados obtenidos en los laboratorios forenses, por lo tanto, así como se realizó con las herramientas

informáticas, se precisa que el laboratorio y el *staff* obtengan las acreditaciones o certificaciones pertinentes.

9.6.3. Examen de herramientas e instrumentos

Parte del proceso de certificación de herramientas forenses son las pruebas realizadas con las mismas. Como se ha mencionado previamente, existe una necesidad crítica en la comunidad de administración de justicia de garantizar la confiabilidad de las herramientas forenses. La finalidad de estos *test* o pruebas es establecer una metodología que permita desarrollar especificaciones, procedimientos, criterios, etc. que provean la información necesaria para que las empresas desarrolladoras de estas herramientas puedan mejorarlas, sean consistentes, produzcan resultados exactos y brinden información que sea legalmente aceptada.

Por tanto, durante el desempeño de las actividades, el *staff* debe realizar las pruebas respectivas para considerar, la forma de trabajo de las mismas (y si esta se puede mejorar), el tiempo de respuesta (útil, para los diagramas de procesos), el estilo de los formatos de la información obtenida, etc. Estas observaciones, pueden ser enviadas posteriormente a los proveedores o las empresas para que se realicen los ajustes, la verificación de las especificaciones o para la retroalimentación de los productos.

9.7. Reclutamiento

9.7.1. Revisión, cambios y mejoras del perfil del perito

En el capítulo siete del presente trabajo, se mencionaron algunas características, en forma preliminar, del perfil del perito; sin embargo, éstas

también deben ser sometidas a escrutinio por los encargados de contratación de personal. Es decir, deben incluirse los requerimientos profesionales básicos así como algún grado de especialización. Sin descuidar las pruebas psicológicas, los requerimientos legales (v.g. antecedentes penales, policíacos, etc.), las pruebas de detección (si es que la gerencia determina que sea pertinente), etc. Estos cambios y mejorar en el perfil esperado del perito permitirán el establecimiento de filtros así como la especificidad del puesto en la hora de la publicación en los medios para la contratación.

9.7.2. Revisión de perfiles puestos administrativos

Al igual que los requerimientos de los peritos, también se deben realizar los perfiles para los puestos administrativos dependiendo del área específica, por ejemplo, se deben definir las funciones de las secretarías de gerencia, los profesionales del área técnica jurídica, el personal de seguridad y bodega, etc.

CONCLUSIONES

1. Debido a la tendencia actual del uso de tecnología en la vida diaria de las personas y su potencial empleo en hechos delictivos, relacionados directa o indirectamente, se considera que la creación formal de una unidad de Informática Forense es una necesidad en el ámbito de la investigación criminal.
2. El trabajo forense exige el uso de herramientas apropiadas y de alta calidad, éstas al igual que la experticia de los técnicos deben poseer el aval o las certificaciones demandadas por los estándares requeridos por los aparatos judiciales.
3. Las labores de índole forense, por su nivel de detalle, fineza y duración, requieren que el ambiente de trabajo sea el adecuado para el trabajador, a nivel ergonómico, antropométrico, metodológico, de iluminación, temperatura, etc. Por lo tanto, el sitio y la estación de trabajo deben ser lugares especializados con características muy diferentes a las encontradas en las áreas administrativas.
4. Dentro del documento se mencionan detalles de construcción que deben ser tomados en cuenta, no solamente como aspectos visuales, como el uso de ventanas amplias o el uso de materiales transparentes (e.g. vidrio, *plexiglass*, policarbonato), sino como especificaciones de eficiencia en el uso de energía, protección del ambiente y seguridad. Siempre debiera considerarse los requerimientos de edificios “verdes” o planeta-amigable.

5. Los planes de mantenimiento, además de contemplar toda la infraestructura del edificio también debe prever la programación de los dispositivos forenses y los sistemas de protección eléctrica que protejan la inversión realizada y cubran los requerimientos de los proveedores para la ejecución de garantías o instalaciones.
6. Debido a la delimitación del presente documento al análisis *post mortem*, la utilización de herramientas forenses en ambientes *Win32*, el trabajo pericial en discos duros, medios de almacenamiento extraíbles, celulares, etc., se requiere que se realicen los estudios, el diseño de operaciones y la adquisición de otros equipos forenses no contemplados en el presente trabajo, para garantizar una gama más completa de servicios.
7. Guatemala siempre ha contado con la ayuda o colaboración de países e instituciones internacionales que aportan en variados rubros al sector justicia. Las indicaciones mostradas pueden resultar útiles para financiar el proyecto en cualquiera de sus fases, la adquisición por donación de los equipos forenses, la gestión de capacitación, acreditaciones, certificaciones, asesorías, etc.
8. Finalmente, cualquier proyecto posee sus ciclos de control y seguimiento, los cuales deben planearse en comisiones a fin de delimitar y delegar la dirección del mismo, a fin de evitar la sobrecarga de la gerencia de proyecto. La política de dividir y conquistar rinde sus beneficios y permite el enfoque, las correcciones, las enmiendas, los reajustes, etc., que posee cualquier proyecto, especialmente, en su etapa inicial.

RECOMENDACIONES

1. Debe considerarse la adquisición y la elaboración de los procesos para análisis forense en vida o tiempo real.
2. Deben analizarse y estudiarse las tendencias en el mercado respecto a productos nuevos de potencial uso masivo (por ejemplo *tablets*, *pads*, *smartphones*, *etc.*), a fin de tomar las decisiones pertinentes para la realización de peritajes forenses en estos nuevos dispositivos.
3. El espectro de cobertura respecto a otros sistemas operativos también puede considerarse importante, especialmente por el crecimiento en nuestro medio de plataformas *MacOs*, *Unix*, *Linux*, *etc.* Y la proliferación de *Software* gratuito, especialmente para estas últimas.
4. La gerencia del laboratorio deberá considerar los temas del uso de tecnología como referencia. Por ejemplo, una de las solicitudes más comunes en el Ministerio Público es la interpretación de fotografías, bien sean para la individualización de un sospechoso, las placas de automóvil, ampliación de detalles, *etc.* Por tanto, se debe planificar la adquisición de *software* especializado de análisis fotográfico, por ejemplo, por métodos de interpolación y la capacitación respectiva del personal que trabajará en dichas áreas.
5. El auge de los servicios de comunicación entre personas (*chat*, redes sociales, correo electrónico, *etc.*) seguramente hará que el número de casos de chantaje, extorsión, difamación, fraude, *etc.* se eleve a un nivel

dramático. Consecuentemente, se deben generar los procedimientos de investigación delictiva que este tipo de comunicaciones puedan acarrear. Igual atención merecen el estudio de redes de telefonía, la interpretación y rastreo de sistemas de posicionamiento global (*GPS*), el análisis biométrico, análisis fotográfico de imágenes y sistemas de video vigilancia, etc., para la resolución de casos.

BIBLIOGRAFÍA

1. ACCESS DATA. *Products*. [en línea]
<<http://accessdata.com/products/computer-forensics>>.
[Noviembre 2010]
2. ACCESSDATA CORPORATION. *Forensic toolkit manual, find, organize and analyze computer evidence*. Lindon, UT: AccessData Corp., 2007. 337 p.
3. ALABAMA DISTRICT ATTORNEY'S ASSOCIATION. *Best practices for seizing electronic evidence*. Alabama, AL: Alabama District Attorney's Association - Office of Prosecution Services, [2006]. 24 p.
4. ASHRAE. *Standards and Guidelines*. [en línea]
<http://www.techstreet.com/lists/ashrae_standards>
[Noviembre 2010]
5. AYERS, Rick; JANSE Wayne. *PDA forensic tools: an overview and analysis*. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2004. 67 p.
6. BALL, Craig. *6 on Forensics: Six articles on Computer Forensics for Lawyers*. [USA], 2005. 106 p.

7. BK FORENSICS. *Cell phone forensic solutions*. [en línea]
<<http://www.bkforensics.com/solutions.html>> [Noviembre 2010]
8. BRENNER, John C. *Forensic science: an illustrated dictionary*. Boca Raton, FL: CRC Press, 2004. 281 p.
9. BROWN, Christopher L.T. *Computer evidence: collection & preservation*. Hingham, MA: Charles River Media, 2006. 394 p.
10. CELLEBRITE. *Cellebrite Universal Forensics Extraction Device (UFED)*. [en línea] <<http://www.cellebrite.com/forensic-products/forensic-products.html>> [Noviembre 2010]
11. CENTER FOR MAGNETIC RECORDING RESEARCH. *Tutorial on disk drive data sanitization*. [en línea]
<<http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml>>
[Enero 2011]
12. COMPUTER FORENSICS AND INCIDENT RESPONSE WITH ROB LEE. *SIFT Workstation Capabilities*. [en línea]
<<http://blogs.sans.org/computer-forensics>> [Noviembre 2010]
13. COMPUTER FORENSICS WORLD. *Forum*. [en línea]
<<http://www.computerforensicsworld.com>> [Febrero 2011]
14. CONSTRUMATICA. *Vermiculita*. [en línea]
<<http://www.construmatica.com/construpedia/Vermiculita>>
[Agosto 2010]

15. DARIK'S BOOT AND NUKE. DBAN. [en línea]
<<http://www.dban.org>> [Enero 2011]
16. DATALIFTER. *Products*. [en línea]
<<http://www.datalifter.com/products.htm>> [Diciembre 2010]
17. DEREK NEWTON, INFORMATION SECURITY INSIGHTS. *Write Blockers – Hardware vs Software*. [en línea]
<<http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml>>
[Enero 2011]
18. DIGITAL INTELLIGENCE. *Forensic software*. [en línea] <> [Julio 2010]
19. DISKLABS. *Computer forensics crime*. [en línea] <<http://computer-forensics.co.uk/computer-forensics-crime.php>> [Septiembre 2010]
20. DISKOLOGY. *Products*. [en línea] <<http://diskology.com>> [Diciembre 2010]
21. DTSEARCH. *Products*. [en línea]
<<http://www.dtsearch.com/index.html>> [Diciembre 2010]
22. DUL, Jan; WEERDMEEESTER, Bernhard. *Ergonomics for beginners, a quick reference guide*. 3rd. Ed. Boca Raton, FL: CRC Press, 2008. 147 p.

23. ECONOMIA DE LA ENERGIA. Reciclaje. [en línea]
<<http://www.economiadelaenergia.com/reciclaje/>> [Noviembre 2010]
24. EDISON, APRENDIZAJE BASADO EN INTERNET. Luminotecnia.
[en línea] <<http://edison.upc.edu/curs/llum/>> [Febrero 2011]
25. EL PRISMA. Luminotecnia e iluminación. [en línea]
<http://www.elprisma.com/apuntes/ingenieria_electrica_y_electrónica/luminotecniaailuminacion/> [Enero 2011]
26. ENGLAND ASSOCIATION OF CHIEF POLICE OFFICERS. *Good practice guide for computer based evidence*. England: Association of Chief Police Officers, Computer Crime Group, 1999. 58 p.
27. EOGHAN, Casey. *Digital evidence and computer crime - Forensic science, computers and the Internet*. 2nd. Ed. San Diego, CA: Academic Press, 2004. 688 p.
28. FORENSIC FOCUS. *Forum*. [en línea]
<<http://www.forensicfocus.com/computer-forensics-forums>>
[Agosto 2010]
29. FORENSIC SOFT. *Windows forensic boot disk*. [en línea]
<<http://www.forensicsoft.com/safe.php>> [Septiembre 2010]

30. FORENSIC COMPUTERS, INC. *Forensic investigative hardware*. [en línea] <<http://www.forensic-computers.com/hardware.php>> [Noviembre 2010]
33. GREENDISK. *Services*. [en línea] <<http://www.greendisk.com/gdsite/services.aspx>> [Marzo 2011]
34. GRIFFIN, Brian. *Laboratory design guide*. 3rd. Ed. Burlington, MA: Elsevier, 2005. 402 p.
35. GUIDANCE SOFTWARE. *Encase forensic*. [en línea] <<http://www.guidancesoftware.com/forensic.htm>> [Julio 2010]
36. HERMANMILLER. *Aeron chair*. [en línea] <<http://www.hermanmiller.com/Products/Aeron-Chairs>> [Agosto 2010]
37. ILUMINET. Alumbrado público. [en línea] <<http://www.iluminet.com.mx/category/alumbrado-publico-2/>> [Marzo 2010]
38. INFORMATION TECHNOLOGY LABORATORY (NIST). *Computer forensics tool testing program, Hardware write block*. [en línea] <http://www.cfft.nist.gov/hardware_write_block.htm> [Diciembre 2010]

39. _____ . *Computer forensics tool testing program, Software write block*. [en línea]
<http://www.cfft.nist.gov/software_write_block.htm> [Diciembre 2010]
40. INSTITUTO MEXICANO DEL SEGURO SOCIAL. Normas del IMSS para discapacitados. [en línea]
<<http://es.scribd.com/doc/21990677/Normas-Del-IMSS-Para-Discapacitados>> [Febrero 2011]
41. INTEGRITY. *Hardware and software inventory*. [en línea]
<<http://www.softwaremetering.com/>> [Agosto 2010]
42. JANSEN, Wayne; AYERS Rick. *Guidelines on PDA forensics*. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2004. 67 p.
43. JONES, Andy; VALLI Craig. *Building a digital forensic laboratory*. Burlington, MA: Syngress Publishing, 2009. 285 p.
44. KILLDISK. *Killdisk*. [en línea] <<http://www.killdisk.com/>> [Diciembre 2010]
45. KUCHTA, Kelly J. "*Building a Computer Forensics Laboratory*". Information System Security. USA, 2001. 98 p.

46. LEONARDO ARGUETA, Fredy Armando. "La realidad de la cadena de custodia dentro de la fase de investigación en el proceso penal y sus implicaciones para su utilización en el debate". Trabajo de graduación Facultad de Ciencias Jurídicas y Sociales. Universidad de San Carlos de Guatemala, 2001. 71 p.
47. LOGICUBE, COMPUTER FORENSICS DIVISION. *Products*. [en línea] <<http://logicubeforensics.com/products>> [Diciembre 2010]
48. MAIL X MAIL. Control y extinción del fuego. [en línea] <<http://www.mailxmail.com/curso-control-extincion-fuego>> [Junio 2010]
49. MANUTAN. Productos. [en línea] <<http://www.manutan.es/>> [Septiembre 2010]
50. MEDLINE PLUS. Hernia discal. [en línea] <<http://www.nlm.nih.gov/medlineplus/spanish/ency/article/000442.htm>> [Marzo 2011]
51. MEYERS, Matthew; ROGERS, Marc. *Computer Forensics: The need for standarization and certification*. West Lafayette, IN: Purdue University, 2004. 11p.
52. MIDDLETON, Bruce. *Cyber crime investigator's field guide*. Boca Ratón, FL: Auerbach Publications, CRC Press, 2002. 330 p.
53. MINISTERIO PÚBLICO. Guía práctica del investigador criminalista. Guatemala: Ministerio Público, 1999. 145 p.

54. _____. Manual de técnicas para el debate. Guatemala: Ministerio Público, 2000. 166 p.
55. MOBILEEDIT! FORENSIC SOFTWARE. *Products*. [en línea] <<http://cellforensics.com>> [Diciembre 2010]
56. MONDELO, Pedro R. et. al. Ergonomía 3: Diseños de puestos de trabajo, 2da. Edición. Cataluña, España: Edicions UPC, 1999. 267 p.
57. MONDELO, Pedro R. y Enrique Gregory Torada. La ergonomía en la Ingeniería de Sistemas, 1ra. Ed. Madrid: Isdefe, 1996. 202 p.
58. NATIONAL FIRE PROTECTION ASSOCIATION. *Codes and standards*. [en línea] <<http://www.nfpa.org/categoryList.asp?categoryID=124&URL=Codes%20&%20Standards>> [Julio 2010]
59. NATIONAL INSTITUTE OF JUSTICE. *A guide for planning and implementing a computer forensics unit*. National Center for Forensic Science. Washington, DC 2008. 43 p.
60. _____. *Electronic crime scene investigation: a guide for first responders*. Washington, DC. 2001. 83 p.
31. _____. *Forensic examination of digital evidence: a guide for law enforcement*. Washington, DC. 2004. 89 p.
32. _____. *Forensic Laboratories: Handbook for facility, planning, design, construction and moving*. Washington, DC. 1998. 70 p.

61. NATIONAL INSTITUTE OF JUSTICE. *Internet and electronic crimes*. [en línea] <<http://www.nij.gov/topics/crime/internet-electronic/welcome.htm>> [Septiembre 2010]
62. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Cell phone forensic tools: an overview and analysis update*. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2007. 165 p.
63. _____. *Guidelines on cell phone forensics*. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2007. 104 p.
64. NTI. *Software suites*. [en línea] <<http://www.forensics-intl.com/tools.html>> [Noviembre 2010]
65. OEA-OAS DEPARTAMENTO DE COOPERACION JURIDICA. Delito cibernético. [en línea] <<http://www.oas.org/juridico/spanish/cybersp.htm>> [Febrero 2011]
66. ORACLE. *Crypto-Politics: Decoding the New Encryption Standard*. [en línea] <<http://labs.oracle.com/features/encryption/>> [Noviembre 2010]
67. PARABEN CORPORATION. *Device seizure*. [en línea] <<http://www.paraben.com/device-seizure.html>> [Enero 2011]

68. REYES CALDERON, José Adolfo. Técnicas criminalísticas para el fiscal. Guatemala: Fiscalía General de la República, 1988. 693 p.
69. REYES, Anthony et. al. *Cyber crime investigations: bridging the gaps between security professionals, law enforcement and prosecutors*. Rockland, MA: Syngress Publishing, Inc., 2007. 412 p.
70. ROMPICH IQUIC, Ancelmo. La cadena de custodia en el proceso penal guatemalteco. Trabajo de graduación Facultad de Ciencias jurídicas y sociales. Universidad de San Carlos de Guatemala, 1999. 162 p.
71. SAMMES, Tony; JENKINSON Brian. *Forensic computing: a practitioner's guide*. 2nd. Ed. London: Springer-Verlag, 2007. 465 p.
72. SCHMITKNECHT, Douglas A. "*Building FBI computer forensics capacity: one lab at a time*". Digital Investigation. [USA], 2004. 243 p.
73. SMITH, Fred Chris; GURLEY BACE Rebecca. *A guide to forensic testimony. The art and practice of presenting testimony as an expert technical witness*. Boston, MA: Addison-Wesley, 2002. 560 p.
74. SOLAR LUX. Alumbrado público solar. [en línea] <<http://www.iluminacionsolar.com.mx/EnergiasRenovables/CeldasSolares/Postessolaresdeiluminacionpublica.aspx>> [Agosto 2010]

75. SOLOMON, Michael G. et. al. *Computer forensics jumpstart*. Alameda, CA: Sybex, 2005. 283 p.
76. STEPHENSON, Peter. *Investigating computer-related crime, a handbook for corporate investigators*. Boca Raton, FL: CRC Press, 2000. 294 p.
77. TABLEAU. *Products*. [en línea]
<<http://www.tableau.com/index.php?pageid=products>>
[Noviembre 2010]
78. VIA FORENSICS. *Products*. [en línea]
<<http://viaforensics.com/products>> [Noviembre 2010]
79. WESTERN DIGITAL. *External portable hard drives*. [en línea]
<<http://www.wdc.com/en/products/external/portable/>> [Enero 2011]
80. WETSTONE. *Products*. [en línea]
<<http://www.wetstonetech.com/product/us-latt/>> [Septiembre 2010]
81. WIEBETECH. *Forensic field kits*. [en línea]
<<http://www.wiebetech.com/products/forensicffk.php>> [Agosto 2010]
82. WILES, Jack et. al. *Technosecurity's guide to e-discovery and digital forensics*. Burlington, MA: Syngress Publishing, 2007. 405 p.

83. WOLFE, Hank. "*Setting up an electronic evidence forensics laboratory, Computers and Security*". University of Otago, Dunedin, New Zealand. 687 p.

84. X-WAYS SOFTWARE TECHNOLOGY AG. *Winhex*. [en línea] <<http://www.x-ways.net/winhex/index-e.html>> [Agosto 2010]