UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA DE INGENIERIA DE SISTEMAS INFORMATICOS

INVESTIGACIÓN DE LAS HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE EN EL SALVADOR

PRESENTADO POR:

RICARDO ERNESTO AYALA VÁSQUEZ

EMERSON ALFREDO CORTEZ ARGUETA

JUAN CARLOS GUIDOS JUÁREZ

CRISTIANE DANIEL RUIZ SÁNCHEZ

PARA OPTAR AL TITULO DE:

INGENIERO DE SISTEMAS INFORMATICOS

CIUDAD UNIVERSITARIA, ENERO 2010

UNIVERSIDAD DE EL SALVADOR

RECTOR :

MSc. RUFINO ANTONIO QUEZADA SÁNCHEZ

SECRETARIO GENERAL :

LIC. DOUGLAS VLADIMIR ALFARO CHÁVEZ

FACULTAD DE INGENIERIA Y ARQUITECTURA

DECANO :

ING. MARIO ROBERTO NIETO LOVO

SECRETARIO :

ING. OSCAR EDUARDO MARROQUÍN HERNÁNDEZ

ESCUELA DE INGENIERIA DE SISTEMAS INFORMATICOS

DIRECTOR :

ING. CARLOS ERNESTO GARCÍA GARCÍA

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA DE INGENIERIA DE SISTEMAS INFORMATICOS

Trabajo de Graduación previo a la opción al Grado de:

INGENIERO DE SISTEMAS INFORMATICOS

Título :

INVESTIGACIÓN DE LAS HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE EN EL SALVADOR

Presentado por :

RICARDO ERNESTO AYALA VÁSQUEZ

EMERSON ALFREDO CORTEZ ARGUETA

JUAN CARLOS GUIDOS JUÁREZ

CRISTIANE DANIEL RUIZ SÁNCHEZ

Trabajo de Graduación Aprobado por:

Docente Director :

Ing. Julio Alberto Portillo

San Salvador, Enero 2010

Trabajo de Graduación Aprobado por:

Docente Director :

Ing. Julio Alberto Portillo

AGRADECIMIENTOS

AGRADECIMIENTOS

Agradezco a Dios Todopoderoso y a la Virgen María que no me permitieron desistir en el transcurso de la carrera aun cuando tuve muchas dificultades.

Agradezco a Mis padres y mis hermanos que me han apoyado durante toda mi vida y este logro se los debo también a ellos.

A mis amigos que me acompañaron, aunque no directamente formaron una parte muy importante en este proceso.

Al Ing. Julio Portillo por habernos asesorado en este Trabajo de Graduación brindándonos su tiempo y experiencia para el desarrollo del mismo.

A mis compañeros de Grupo de Trabajo de Graduación, con los cuales sufrimos desveladas, comidas de Vikingos y una que otra discusión entre colegas.

En nombre de Dios, Lo logramos.

Ricardo Ernesto Ayala Vásquez

AGRADECIMIENTOS

A Dios Todopoderoso.

A mi familia.

A mis amigos.

A mi grupo de tesis.

Emerson Cortez.

Son tantas las personas que de manera directa o indirecta me han ayudado a alcanzar este triunfo y poder lograr la culminación de mi vida académica. Es por esta razón que deseo utilizar este espacio para poder expresar mis más sinceros agradecimientos.

En primer lugar, a Dios todopoderoso por haberme dado vida y salud suficiente para poder alcanzar esta meta y poder disfrutar de esta alegría.

A mis padres, Juan y María por brindarme la suficiente estabilidad moral, sentimental y económica para poder llegar a este momento, que definitivamente hubiera sido imposible sin su ayuda. Gracias por su paciencia.

A mi hermano Ernesto, a mis sobrinos Ernesto Jr., Diana y Marcela por ofrecerme su apoyo incondicional durante esta ardua etapa.

A mi abuelita Luisa, aunque ya no estuvo presente en este mundo para poder compartir con ella esta gran felicidad sé que desde el cielo me brindo todo su cariño y confianza.

A mis compañeros de trabajo de graduación, los heroicos miembros del Grupo 16 por su determinación y sacrificio en la búsqueda una misma meta… Esta es para Ustedes!!!

Para finalizar a nuestro asesor, por su guía y dirección, elementos claves para el éxito de este proyecto académico.

Juan Carlos Guidos Juárez.

Primeramente quiero dar gracias a Dios Todopoderoso por haberme dado la oportunidad de realizar este esfuerzo y haber podido culminar esta etapa en mi formación profesional.

Quiero agradecer infinitamente el apoyo incondicional por parte mi familia: mi querida madre María Elia de Ruiz, mi padre Daniel Arístides Ruiz, mi hermana Daniela Quinteros, mi cuñado Carlos Quinteros, mi sobrinito Joshua Enrique y familia Quinteros. También quiero hacer mención de una persona muy especial, mi abuela María Dolores Sánchez que agradezco a Dios este con nosotros para compartir este logro, a mi abuela María Estebana Ruiz que Dios tenga en su Gloria y a todas las personas que son y considero parte de mi familia por haberme brindado su apoyo durante mi formación profesional.

A mis compañeros de este trabajo de graduación: Juan Carlos, Ricardo y Emerson, quiero agradecerles por el esfuerzo que realizamos como grupo y haber logrado superar las adversidades que se presentaron a lo largo de este proyecto. A la vez, quiero expresar mi agradecimiento al ingeniero Julio Alberto Portillo, por haber asesorado nuestro trabajo de graduación y además habernos apoyado en la culminación exitosa de este esfuerzo. Sumado a ello, el agradecimiento al ingeniero Rubén Asencio quién también nos apoyó para haber logrado esta meta.

Gracias a Dios Todopoderoso, familia, amigos y todas las personas que de alguna manera ayudaron a que pudiera culminar esta etapa de mi formación profesional.

Cristiane Daniel Ruiz

INDICE

INTRODUCCIÓN ..... **xx**

OBJETIVOS DEL PROYECTO ..... **xxiii**

A. GENERAL xxiii

B. ESPECÍFICOS xxiii

IMPORTANCIA **2**

JUSTIFICACIÓN **4**

A. JUSTIFICACIÓN 4

B. VIABILIDAD DE LA INVESTIGACIÓN 5

ALCANCES Y LIMITACIONES **7**

A. ALCANCES 7

B. LIMITACIONES 7

CAPÍTULO I: INVESTIGACIÓN PRELIMINAR **9**

A. ANTECEDENTES 9

I. EVOLUCIÓN DE LAS HERRAMIENTAS DE SOFTWARE 9

II. EVOLUCIÓN DE LAS TÉCNICAS 11

III. INVESTIGACIONES PREVIAS 11

IV. INFORMÁTICA FORENSE EN EL SALVADOR 11

B. SITUACIÓN ACTUAL 12

I. DESCRIPCIÓN 12

II. ESTRUCTURA 14

C. FORMULACIÓN DEL PROBLEMA 16

I. SITUACIÓN PROBLEMÁTICA 16

II. DIAGRAMA CAUSA – EFECTO 17

III. FORMULACIÓN DEL PROBLEMA 20

IV. ANÁLISIS DEL PROBLEMA 20

V. ENUNCIADO DEL PROBLEMA 21

VI. PREGUNTAS DE LA INVESTIGACIÓN 21

D. FORMULACIÓN DE HIPÓTESIS 23

I. HIPÓTESIS DE LA INVESTIGACIÓN 23
II. HIPÓTESIS NULA 23
III. HIPÓTESIS ALTERNATIVAS 23
E. MARCO TEÓRICO 24
I. MARCO TEÓRICO 24
II. MARCO REFERENCIAL 42
CAPÍTULO II: DISEÑO DE LA INVESTIGACIÓN 47
A. CLASE DE INVESTIGACIÓN A REALIZAR 47
B. TIPO DE DISEÑO DE LA INVESTIGACIÓN 48
C. FASES DE LA INVESTIGACIÓN 50
I. SELECCIÓN DE POBLACIÓN Y MUESTRA 51
II. RECOLECCIÓN DE DATOS 52
III. TABULACIÓN DE DATOS 53
IV. ANÁLISIS DE RESULTADOS 54
V. RESPUESTAS A PREGUNTAS DE INVESTIGACIÓN 54
VI. COMPROBACIÓN DE HIPÓTESIS 55
VII. CREACIÓN DE INDICADORES 55
VIII. IDENTIFICACIÓN DE LAS HERRAMIENTAS DE INFORMÁTICA FORENSE 56
IX. SELECCIÓN DE LAS HERRAMIENTAS DE INFORMATICA FORENSE A ESTUDIAR 56
X. INVESTIGACIÓN DE LAS HERRAMIENTAS DE SOFTWARE SELECCIONADAS 57
XI. DISEÑO DE CASOS Y PRUEBAS 57
XII. RESOLUCIÓN DE LOS CASOS Y PRUEBAS 58
XIII. ANALISIS DE RESULTADOS DE CASOS Y PRUEBAS REALIZADAS 58
XIV. JERARQUIZACIÓN DE LAS HERRAMIENTAS DE SOFTWARE ESTUDIADAS 58
XV. ELABORACIÓN DE CONCLUSIONES Y RECOMENDACIONES 59
D. CRONOGRAMA DE ACTIVIDADES 60
I. CRONOGRAMA ANTEPROYECTO: DEFINICIÓN Y DISEÑO DE LA INVESTIGACIÓN 60
II. CRONOGRAMA ETAPA I: RECOLECCIÓN, TABULACIÓN Y ANÁLISIS DE DATOS 61
III. CRONOGRAMA ETAPA II: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL Y ESTUDIO DE LAS HERRAMIENTAS 62
IV. CRONOGRAMA CONSOLIDADO 63

E. PLANIFICACIÓN DE LOS RECURSOS 64
I. RECURSO HUMANO 64
II. RECURSO TECNOLÓGICO 65
III. RECURSOS CONSUMIBLES 66
IV. RECURSOS DE OPERACIONES 68
V. TOTAL DE LA INVERSIÓN 71
CAPÍTULO III: RECOLECCIÓN, TABULACIÓN Y ANÁLISIS DE DATOS 73
A. SELECCIÓN DE POBLACIÓN Y MUESTRA 73
I. SECTOR LEGAL 73
II. SECTOR EDUCATIVO 79
III. SECTOR PROFESIONAL 84
B. DISEÑO DE LAS HERRAMIENTAS DE RECOLECCIÓN DE DATOS 85
I. DISEÑO DEL INSTRUMENTO RECOLECTOR DE DATOS PARA EL SECTOR LEGAL 85
II. DISEÑO DEL INSTRUMENTO RECOLECTOR DE DATOS PARA EL SECTOR EDUCATIVO 88
III. DISEÑO DEL INSTRUMENTO RECOLECTOR DE DATOS PARA EL SECTOR PROFESIONAL 90
C. TABULACIÓN Y ANÁLISIS DE LOS RESULTADOS OBTENIDOS 93
I. SECTOR LEGAL 93
D. MATRIZ DE PUNTOS DE ANÁLISIS 114
E. RESPUESTAS A LAS PREGUNTAS DE LA INVESTIGACIÓN 115
I. COMUNIDAD EDUCATIVA 115
II. SECTOR LEGAL 116
III. SECTOR PROFESIONAL 116
IV. TODOS LOS SECTORES 118
F. COMPROBACIÓN DE HIPÓTESIS 120
CAPÍTULO IV: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL 127
A. INTRODUCCIÓN 127
B. CREACIÓN DE INDICADORES PARA LA INVESTIGACIÓN 128
I. CONCEPTO DE INDICADOR 128
II. CARACTERÍSTICAS DE LOS INDICADORES 128
III. TIPOS DE INDICADORES 129
IV. SELECCIÓN DEL TIPO DE INDICADOR A UTILIZAR 129

V. CRITERIOS PARA LA SELECCIÓN DE INDICADORES SOCIALES 130
VI. METODOLOGÍA UTILIZADA EN LA CREACIÓN DE LOS INDICADORES..... 131
VII. APLICACIÓN DE LA METODOLOGÍA PARA LA CREACIÓN DE INDICADORES 133
C. APLICACIÓN DE LOS INDICADORES..... 146
I. INDICADORES RELACIONADOS A LA EVIDENCIA DIGITAL 147
II. INDICADORES RELACIONADOS A LAS HERRAMIENTAS DE SOFTWARE 149
III. INDICADORES RELACIONADOS AL RECURSO HUMANO..... 159
IV. INDICADORES RELACIONADOS A LOS DELITOS INFORMÁTICOS..... 161
D. ELABORACIÓN DEL DIAGNÓSTICO..... 163
I. DIAGNÓSTICO CONCERNIENTE AL SECTOR LEGAL..... 163
II. DIAGNÓSTICO CONCERNIENTE AL SECTOR EDUCATIVO..... 165
III. DIAGNÓSTICO CONCERNIENTE AL SECTOR PROFESIONAL 167
IV. DIAGNÓSTICO GENERALIZADO 170
CAPÍTULO V: ESTUDIO DE LAS HERRAMIENTAS DE SOFTWARE PARA LA INFORMÁTICA FORENSE 175
A. SELECCIÓN DE LAS HERRAMIENTAS DE SOFTWARE A SER ESTUDIADAS..... 175
B. INVESTIGACIÓN DE LAS HERRAMIENTAS SELECCIONADAS..... 178
I. HERRAMIENTAS PARA EL CÁLCULO DE HASH 179
C. PROPUESTAS DE HERRAMIENTAS..... 183
I. CRITERIOS A TOMAR EN CUENTA..... 183
II. CARACTERÍSTICAS A EVALUAR 185
III. CRITERIOS PARA LA SELECCIÓN DE SUITES 186
IV. COMPARACIONES DE LAS HERRAMIENTAS EN BASE A LOS CRITERIOS..... 188
V. PUNTUACIONES DE HERRAMIENTAS SEGÚN PONDERACIONES DE CRITERIOS..... 191
VI. JERARQUIZACIÓN DE LAS HERRAMIENTAS..... 194
CAPÍTULO VI: PROPUESTA DE LABORATORIO PARA INFORMÁTICA FORENSE..... 197
A. DESCRIPCIÓN DE REQUERIMIENTOS 197
B. PROPUESTA PARA LA IMPLEMENTACIÓN 198
CAPÍTULO VII: RESOLUCIÓN DE CASO SIMULADO DE DELITO INFORMÁTICO..... 203
A. FLUJOGRAMA DEL PROCEDIMIENTO DE ANALISIS 203
B. DESCRIPCIÓN DE LA SITUACIÓN 204

CONCLUSIONES **206**
A. EN BASE A LOS OBJETIVOS DE LA INVESTIGACIÓN 206
B. EN BASE A LA INVESTIGACIÓN DE CAMPO 207
C. EN BASE AL DIAGNÓSTICO 209
RECOMENDACIONES **212**
A. A LAS INSTITUCIONES RELACIONADAS CON LA PERSECUCIÓN DE LOS DELITOS INFORMÁTICOS 212
B. A LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR 213
REFERENCIA BIBLIOGRÁFICA **215**
A. LIBROS 215
B. PÁGINAS WEB 215
C. OTROS DOCUMENTOS 218
GLOSARIO DE TÉRMINOS **220**
ANEXOS **230**
ANEXO #1: MODELO DE ENTREVISTA PRELIMINAR 230
ANEXO #2: PLANES DE ESTUDIO DE UNIVERSIDADES CONSULTADAS 231
ANEXO #3: DEFINICIONES DE DELITO INFORMÁTICO 232
ANEXO #4: TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR LA ORGANIZACIÓN DE LAS NACIONES UNIDAS (O.N.U.) 233
ANEXO #5: TABLA ÁREAS BAJO LA CURVA NORMAL TIPIFICADA DE 0 A Z PARA DETERMINAR EL NIVEL DE CONFIANZA Y EL COEFICIENTE DE CONFIABILIDAD 235
ANEXO #6: MODELO DE ENCUESTAS PARA EL SECTOR LEGAL 236
ANEXO #7: MODELO DE CODIFICACIÓN DE LAS ENCUESTAS PARA EL SECTOR LEGAL 238
ANEXO #8: MODELO DE ENCUESTAS PARA EL SECTOR EDUCATIVO 240
ANEXO #9: MODELO DE CODIFICACIÓN DE LAS ENCUESTAS PARA EL SECTOR EDUCATIVO ... 243
ANEXO #10: MODELO DE ENCUESTAS PARA EL SECTOR PROFESIONAL 245
ANEXO #11: MODELO DE CODIFICACIÓN DE LAS ENCUESTAS PARA EL SECTOR PROFESIONAL 249
ANEXO #12: TABLA DE DISTRIBUCIÓN CHI CUADRADO 251
ANEXO #13: HERRAMIENTAS SELECCIONADAS PRELIMINARMENTE 252
ANEXO #14: MATRIZ CRITERIOS-HERRAMIENTAS 259

INDICE DE TABLAS

Tabla No 1: Evolución de la informática forense 9
Tabla No 2: Delitos informáticos acontecidos en El Salvador 13
Tabla No 3: Elementos considerados en la formulación de la hipótesis general 23
Tabla No 4: Tipos de Sistemas de ficheros 34
Tabla No 5: Tipos de diseños muéstrales 51
Tabla No 6: Cálculo del costo diario total incurrido en recurso humano 64
Tabla No 7: Costo de recurso de equipo informático 65
Tabla No 8: Costo de otros recursos tecnológicos 66
Tabla No 9: Costo de papelería 66
Tabla No 10: Costo de anillado y empastado 67
Tabla No 11: Total de KWh utilizados en el mes 68
Tabla No 12: Costo mensual de telefonía celular 69
Tabla No 13: Total en recursos de operación 70
Tabla No 14: Costo total de recursos 71
Tabla No 15: Distribución de abogados defensores 77
Tabla No 16: Resumen del tamaño de las muestras calculadas para cada sector 79
Tabla No 17: Universidades privadas de El Salvador con carreras relacionadas a la informática 81
Tabla No 18: Docentes que imparten materias informáticas en las universidades 82
Tabla No 19: Detalle del total de docentes de universidades privadas a encuestar 83
Tabla No 20: Detalles de los peritos a ser consultados 84
Tabla No 21: Resultados pregunta 1, Sector Legal, Jueces 93
Tabla No 22: Resultados pregunta 2, Sector Legal, Jueces 94
Tabla No 23: Resultados pregunta 3, Sector Legal, Jueces 95
Tabla No 24: Resultados pregunta 4, Sector Legal, Jueces 96
Tabla No 25: Resultados pregunta 5, Sector Legal, Jueces 97
Tabla No 26: Resultados pregunta 6, Sector Legal, Jueces 98
Tabla No 27: Resultados pregunta 7, Sector Legal, Jueces 100
Tabla No 28: Resultados pregunta 8, Sector Legal, Jueces 101
Tabla No 29: Resultados pregunta 9, Sector Legal, Jueces 102
Tabla No 30: Resultados pregunta 10, Sector Legal, Jueces 104
Tabla No 31: Resultados pregunta 11, Sector Legal, Jueces 106

Tabla No 32: Resultados pregunta 12, Sector Legal, Jueces 107
Tabla No 33: Matriz de puntos Coincidentes..... 114
Tabla No 34: Operalización de las variables a utilizar..... 121
Tabla No 35: Cantidad de personas encuestadas por población..... 123
Tabla No 36: Valores Observados..... 124
Tabla No 37: Valores Observados..... 124
Tabla No 38: Conceptos a utilizar para la creación de los indicadores..... 134
Tabla No 39: Formato de presentación de los indicadores creados 134
Tabla No 40: Descripción del indicador IED..... 136
Tabla No 41: Descripción del indicador VED..... 137
Tabla No 42: Descripción del indicador CSL..... 138
Tabla No 43: Descripción del indicador CSP 139
Tabla No 44: Descripción del indicador UDU..... 140
Tabla No 45: Descripción del indicador USIF 141
Tabla No 46: Descripción del indicador PDC..... 142
Tabla No 47: Descripción del indicador PIC 143
Tabla No 48: Descripción del indicador CDI..... 144
Tabla No 49: Descripción del indicador ODI 145
Tabla No 50: Formato para la presentación de la evaluación de los indicadores 146
Tabla No 51: Evaluación del indicador IED 147
Tabla No 52: Evaluación del indicador VED 148
Tabla No 53: Evaluación del indicador CSL..... 149
Tabla No 54: Evaluación del indicador CSP..... 150
Tabla No 55: Evaluación del indicador UDU 151
Tabla No 56: Evaluación del indicador USIF (1) 152
Tabla No 57: Evaluación del indicador USIF (2) 153
Tabla No 58: Evaluación del indicador USIF (3) 154
Tabla No 59: Evaluación del indicador USIF (4) 155
Tabla No 60: Evaluación del indicador USIF (5) 156
Tabla No 61: Evaluación del indicador USIF (6) 157
Tabla No 62: Evaluación del indicador USIF (7) 158
Tabla No 63: Evaluación indicador PDC..... 159
Tabla No 64: Evaluación del indicador PIC..... 160

Tabla No 65: Evaluación del indicador CDI 161
Tabla No 66: Evaluación del indicador ODI 162
Tabla No 67: Indicadores relacionados a la evidencia digital 170
Tabla No 68: Indicadores relacionados a las herramientas de software 171
Tabla No 69: Indicadores relacionados al Recurso Humano 171
Tabla No 70: Indicadores relacionados a los delitos informáticos 171
Tabla No 71: Criterios de selección de herramientas para informática forense 176
Tabla No 72: Comparación de herramientas para calculo de hash 188
Tabla No 73: Comparación de herramientas para copia de medios 188
Tabla No 74: Comparación de herramientas para recuperación de contraseñas 189
Tabla No 75: Comparación de Kits para informática Forense 189
Tabla No 76: Comparación de herramientas para recuperación de números de licencia 190
Tabla No 77: Comparación de herramientas para recuperación de datos eliminados 190
Tabla No 78: Puntuaciones de herramientas para calculo de Hash 191
Tabla No 79: Puntuaciones de herramientas para copia de Medios 191
Tabla No 80: Puntuaciones de herramientas para recuperación de contraseñas 192
Tabla No 81: Puntuaciones de herramientas para recuperación de números de licencia 192
Tabla No 82: Puntuaciones de herramientas para recuperación de datos eliminados 193
Tabla No 83: Puntuaciones de Kits de herramientas para informática forense 193

INDICE DE FIGURAS

Figura No. 1: Enfoque de Sistemas correspondiente a la situación actual. 14
Figura No. 2: Diagrama Causa – Efecto utilizado para la identificación de la problemática..... 19
Figura No. 3: Proceso solucionador de problemas utilizado para la formulación del problema..... 20
Figura No. 4: Etapas del proceso de investigación..... 36
Figura No. 5: Diseño de la investigación. 49
Figura No. 6: Diagrama de flujo del diseño de la investigación 50
Figura No. 7: Resultados pregunta 1, Sector Legal, Jueces 93
Figura No. 8: Resultados pregunta 2, Sector Legal, Jueces 94
Figura No. 9: Resultados pregunta 3, Sector Legal, Jueces 95
Figura No. 10: Resultados pregunta 4, Sector Legal, Jueces 96
Figura No. 11: Resultados pregunta 5, Sector Legal, Jueces 97
Figura No. 12: Resultados pregunta 6, Sector Legal, Jueces 98
Figura No. 13: Resultados pregunta 7, Sector Legal, Jueces 100
Figura No. 14: Resultados pregunta 8, Sector Legal, Jueces 101
Figura No. 15: Resultados pregunta 9, Sector Legal, Jueces 102
Figura No. 16: Resultados pregunta 10, Sector Legal, Jueces 104
Figura No. 17: Resultados pregunta 11, Sector Legal, Jueces 106
Figura No. 18: Resultados pregunta 12, Sector Legal, Jueces 107
Figura No. 19: Metodología para la elaboración de indicadores. 131
Figura No. 20: Formato de la ficha resumen propuesta para cada herramienta 178
Figura No. 21: Figura correspondiente al flujograma del procedimiento de análisis 203

INTRODUCCIÓN

INTRODUCCIÓN

La informática forense actúa como contraparte ante el surgimiento de los delitos informáticos, como una forma mediante la cual obtener la evidencia digital que sea válida dentro de un proceso legal. Para obtener esta evidencia digital la informática forense se auxilia de herramientas de software para realizar todas las operaciones necesarias al momento de extraer la información, con el fin de mantener la integridad de los datos y del procesamiento de los mismos.

Debido a la relevancia de esta área de la informática y a los procedimientos que se realizan para obtener evidencia digital válida, surge la necesidad de realizar una investigación sobre las herramientas de software que son utilizadas para lograr este objetivo.

Dentro del desarrollo de la investigación se desarrollaron diferentes etapas de la misma como se expone a continuación:

Investigación preliminar. Se realizo una investigación preliminar, tomando en cuenta peritos para conocer un poco de cómo se encuentra esta área de la informática en el país. Además nos apoyamos en la misma para poder establecer una situación problemática con la cual plantear posteriormente las hipótesis y procedimientos que seguimos para el desarrollo de la investigación de campo.

Diseño de la investigación. La investigación fue de carácter correlacional, ya que se buscaba conocer la relación entre el uso de las herramientas de software para la informática forense y la validez dada a la evidencia digital obtenida.

En cuanto al diseño de la investigación se realizó uno de tipo No Experimental, debido a que el objetivo es analizar las relaciones entre las variables de estudio en su ambiente natural sin llevar a cabo ninguna alteración intencional.

También se clasificó como transaccional ya que las observaciones que se realizaron sobre las distintas poblaciones seleccionadas, se efectuaron en un solo momento del tiempo. Como parte de la misma se definieron poblaciones, muestras y se diseñaron los instrumentos de recolección de datos en este caso fueron las encuestas.

Recolección tabulación y análisis de datos. Dentro de esta etapa se desarrollo la recolección de datos pasando las encuestas a las diferentes personas parte de las muestras seleccionadas, entre estas docentes universitarios por el sector educativo; abogados jueces y fiscales por el sector legal; y peritos por el sector Profesional relacionado a la Informática Forense y a la Aplicación de sus herramientas.

Posteriormente se procedió a realizar la tabulación de los datos recolectados en hojas electrónicas de Excel y a realizar graficas de las mismas para facilitar el análisis de los datos recolectados los cuales serian utilizados para plasmar la situación actual de las variables en estudio.

Diagnóstico de la situación actual del uso de las herramientas de software para la informática forense en el salvador para el año 2009. Nos apoyamos en la creación de indicadores para poder cuantificar los aspectos tomados en cuenta para el diagnóstico, en base a la información recolectada mediante las encuestas realizadas a peritos, docentes y operadores de justicia (abogados, fiscales y jueces), posterior a la aplicación de los indicadores se plasma el diagnóstico por indicador y la valoración con respecto al resultado de cada uno.

Estudio sobre herramientas de software para informática forense donde se realizó un análisis técnico y aplicativo de 26 herramientas seleccionadas de un conjunto de 61 herramientas. Para cada herramienta seleccionada se elaboró una ficha técnica tomando en cuenta las características de la misma, un manual de instalación y un manual de uso básico.

Las herramientas seleccionadas fueron evaluadas mediante factores ponderados y se realizó la jerarquización de las herramientas estudiadas como una propuesta para la elección idónea de herramientas según su utilidad.

Propuesta para un laboratorio para informática forense. Como complemento a la investigación sobre las herramientas de informática forense utilizadas en El Salvador, se incluye los requerimientos en herramientas de hardware y software que debe poseer un laboratorio de informática forense para la realización de peritajes informáticos.

Resolución de caso simulado de delito informático. Se planteo un caso simulado sobre el delito de Pornografía infantil y se expone el procedimiento para la solución del mismo paso a paso con la generación de un reporte generado por el software seleccionado para la solución del caso y la creación de un reporte técnico como se presentaría a la fiscalía.

Como complemento al presente documento se entrega un CD conteniendo los documentos en formato digital, las tabulaciones y análisis de datos recolectados, los manuales de instalación y uso del software investigado, las fichas resumen de las herramientas de software y el detalle de la resolución del caso simulado.

Es de aclarar, que en el CD viene el software utilizado en la resolución del caso, todo esto sin ánimos de lucro sino que con fines académicos.

OBJETIVOS DEL PROYECTO

OBJETIVOS DEL PROYECTO

A. GENERAL

- ✓ Realizar una investigación acerca de las herramientas de software utilizadas en la informática forense en El Salvador para conocer el estado actual de su aplicación y su importancia en los procesos judiciales.

B. ESPECÍFICOS

- ✓ Conocer cuáles son las herramientas de informática forense utilizadas en El Salvador y su clasificación.
- ✓ Determinar el nivel de uso de las herramientas de informática forense en El Salvador.
- ✓ Conocer el grado de incidencia que tienen las herramientas de informática forense en la resolución de casos de delitos informáticos debido al valor de la evidencia digital que aportan.
- ✓ Determinar si los factores económicos, humanos, tecnológicos, educativos o legales son importantes a la hora de la utilización de las herramientas de informática forense y cuál es su nivel de importancia.
- ✓ Conocer las ventajas y desventajas que trae consigo la utilización de las herramientas de informática forense.
- ✓ Conocer cuál es la orientación que tiene el uso de las herramientas de informática forense en El Salvador.
- ✓ Conocer si el personal está capacitado adecuadamente para la utilización de las herramientas de informática forense.
- ✓ Conocer si existe un marco legal que apoye el uso de las herramientas de informática forense.
- ✓ Definir las poblaciones que formaran parte de la Investigación.
- ✓ Determinar la muestra de cada una de las poblaciones en estudio.
- ✓ Diseñar los instrumentos de recolección de datos a ser utilizados en cada una de las muestras.
- ✓ Validar los instrumentos de recolección de datos.
- ✓ Aplicar los instrumentos de recolección de datos a cada una de la muestras de los sectores seleccionados.
- ✓ Realizar la tabulación de los datos aplicando métodos estadísticos.
- ✓ Analizar e interpretar los datos recolectados para buscar una explicación del fenómeno estudiado.
- ✓ Comprobar las hipótesis planteadas mediante los resultados del análisis de datos.
- ✓ Crear indicadores para cuantificar aspectos relacionados a las herramientas de software para informática forense.
- ✓ Aplicar indicadores creados para obtener datos numéricos acerca de los aspectos a tomar en cuenta para el diagnóstico.

- ✓ Realizar el diagnóstico de las variables tomadas en cuenta a partir de los resultados obtenidos en la aplicación de los indicadores.
- ✓ Estudiar herramientas de software para informática forense para hacer un análisis comparativo de las mismas.
- ✓ Crear fichas técnicas de las herramientas en estudio tomando en cuenta requerimientos de hardware y software, funcionalidades, costos y objetivos de las mismas.
- ✓ Crear manuales básicos de instalación y de usuario de las herramientas estudiadas que sirvan como una guía rápida para el uso de los mismos.
- ✓ Establecer los criterios a tomar en cuenta para la evaluación del software estudiado y su posterior análisis para realizar una jerarquización.
- ✓ Comparar herramientas de un mismo tipo para proponer una jerarquización, basados en criterios ponderados en relación a sus características.
- ✓ Realizar una propuesta de requerimientos de hardware y software necesarios para la implementación de un laboratorio para informática forense.

IMPORTANCIA

IMPORTANCIA

La informática forense en El Salvador es una ciencia relativamente nueva, en otros países, ha demostrado que trae grandes beneficios en la aclaración de delitos informáticos. Sin embargo, esta ciencia no puede ser aplicada sin el uso de herramientas informáticas especializadas en el área. Dentro de la problemática planteada, se ha identificado que uno de los principales problemas en la informática forense radica en que el recurso humano no cuenta con las herramientas y conocimientos para su aplicación.

La importancia de la realización de estudio radica en brindar una fuente de referencia que pretende cubrir cierta carencia de conocimiento que es necesario para poder aplicar la informática forense y la utilización de sus herramientas de software. El estudio a realizar brindará nuevos aportes de conocimientos en la utilización de las herramientas de informática forense.

Dentro de los beneficios que se pretender alcanzar son:

- ✓ Demostrar a las instituciones y personas involucradas que el uso de las herramientas de software en la informática forense ayudan a garantizar la confiabilidad en la obtención de evidencia digital
- ✓ Brindar, a las instituciones y personas involucradas, un catálogo de herramientas especializadas en informática forense incluyendo manuales de instalación, técnicos y formas de aplicación.
- ✓ Brindar indicadores para medir el nivel de avance en la utilización de herramientas de software para la informática forense.

A través de la investigación se podrían ver beneficiados:

- ✓ Los 46 Juzgados de Instrucción. en los que recae la persecución de delitos informáticos, dado que el marco legal salvadoreño no ha tipificado los delitos informáticas.
- ✓ Las instituciones que practican procedimientos de Informática Forense, PNC, INTERPOL ya que se darán a conocer herramientas para el análisis forense informático.
- ✓ Los peritos informáticos, minimizando el tiempo de detección de evidencia digital y a su vez el tiempo de resolución de los casos.
- ✓ Instituciones estatales que han sido víctimas de sabotaje en sus sistemas de información como por ejemplo el Ministerio de Trabajo y recientemente el Tribunal Supremo Electoral; la disminución de este tipo de delitos generara ahorros a dichas instituciones ya que estos incurren en gastos para restablecer los sistemas de Información, los costos de estos sistemas pueden llegar hasta $670,000.

JUSTIFICACIÓN

JUSTIFICACIÓN

A. JUSTIFICACIÓN

El rápido avance registrado en el área de las tecnologías de información y comunicaciones ha permitido un desarrollo en las diferentes actividades realizadas por los distintos sectores que conforman la sociedad, pero al mismo tiempo ha abierto las puertas al uso fraudulento de las computadoras con el fin de la realización de actividades ilícitas, de esta forma la informática se ha convertido en el objeto o medio para cometer delitos

Actualmente en El Salvador la Fiscalía General de la República hace uso de la evidencia científica solamente en un 8% de los procesos penales, esto indica que la gran parte de la evidencia presentada es de tipo testimonial. Dicha evidencia científica no solo implica hacer pruebas de ADN, balística o similares, sino que también incluye evidencia obtenida mediante la informática forense, a la cual se le denomina, evidencia digital.

Este tipo de evidencia resulta crucial en la persecución de los delitos informáticos. Realizando una cuantificación de los afectados y las pérdidas originadas por estos delitos se presentan a continuación algunos ejemplos:

- ✓ A partir de estafas a través de compras por Internet en falsas subastas se registraban a finales del 2007 un promedio de 5 denuncias mensuales.
- ✓ Aproximadamente 250 denuncias anuales por cobros en tarjetas de débito y crédito debido a compras no autorizadas.
- ✓ Por piratería de software se registran pérdidas de más de 28 millones de dólares anuales según un estudio de la BSA[1].
- ✓ Por pornografía infantil se registran más de 1400 denuncias en la FGR por producción y comercialización.
- ✓ Referentes a violaciones de privacidad de datos personales, la empresa INFORNET comercializa información personal de más de 4 millones de salvadoreños.
- ✓ En El Salvador, existe más de un 75% de computadoras que no cuentan con licencias que amparen el software que utilizan.
- ✓ El Cuarto Estudio Anual de Piratería de Software para computadores personales difundido por la BSA en el año de 2007, ubica a El Salvador dentro de la lista de los veinte países con tasas más altas de piratería de software en el mundo.

La evidencia digital necesita ser recolectada por herramientas especializadas, de su calidad depende la contundencia de esta en un proceso legal. Por tanto es necesario que las herramientas sean las correctas y que su aplicación sea la adecuada. Con este estudio, pretendemos conocer el nivel de uso que se les da a las herramientas de informática forense en El Salvador para poder hacer propuestas que permitan que la evidencia digital recolectada sea altamente confiable y que esto permita resolver casos de delitos informáticos más ágil y eficientemente, claro que no sólo de las herramientas depende la calidad de la evidencia, sino también del recurso humano que hace uso de ellas, por lo tanto, se necesita personal calificado para llevar a cabo la aplicación.

[1] Business Software Alliance

B. VIABILIDAD DE LA INVESTIGACIÓN

Para evaluar la factibilidad de llevar a cabo el estudio tomaremos en cuenta el tiempo, recursos financieros, humanos y materiales, acceso a la información, acceso a las herramientas.

1. **¿Se cuenta con el tiempo suficiente para llevar a cabo esta investigación?**

Para realizar la investigación se cuenta con un tiempo de 8 meses. Se han programado las actividades de la investigación en el tiempo brindado, demostrando que las actividades necesarias para la investigación son posibles de realizarlas. **(Ver el Capítulo II, Cronograma de Actividades)**

2. **¿Se cuenta con los recursos financieros, humanos y materiales necesarios para llevar a cabo esta investigación de campo?**

Para contestar a esta pregunta, como se puede ver, los recursos disponibles, si bien es cierto no son todos los que quisiéramos, si son los mínimos necesarios para llevar a cabo esta investigación. Para mayor detalle, remítase a la sección de planificación de recursos.

3. **¿Se tiene acceso a las personas e información necesaria?**

En El Salvador, la informática forense es una ciencia relativamente nueva, sin embargo, según la información consultada previamente a esta investigación, se muestra que existe personal, aunque mínimo, que lleva a cabo estas actividades. El acceso a estas personas es posible, en este sentido se han establecido contactos con la División Policía Técnica Científica. En cuanto a la información, existe una buena documentación respecto a la informática forense, sin embargo, de esta poca es de El Salvador. A pesar de esto, existen procedimientos de informática forense bien definidos que servirán como guía para desarrollar esta investigación. En resumen, se puede tener acceso a las personas y recursos y materiales de información necesarios para llevar a cabo esta investigación.

4. **¿Se tiene acceso a las herramientas de informática forense?**

El acceso a las herramientas de informática forense se hará principalmente utilizando internet, tomando en cuenta herramientas de software privativo y libre. A medida se desarrolle la investigación, se irán obteniendo las herramientas necesarias para realizar una serie de propuestas de herramientas de software para la informática forense.

ALCANCES Y LIMITACIONES

ALCANCES Y LIMITACIONES

A. ALCANCES

Con la realización de esta investigación se conocerá la situación actual del uso de las herramientas de software para la informática forense, la utilización de las mismas por parte de los distintos sectores involucrados, específicamente el sector profesional y el educativo. Además se establecerá el valor que el sector legal le da a la evidencia digital obtenida mediante la aplicación de las herramientas de software.

No se contempla en la realización de esta investigación el desarrollo de herramientas de software para la informática forense.

Este proyecto estará centrado en las herramientas de software y no serán incluidas las herramientas especializadas en hardware.

B. LIMITACIONES

Para realizar el estudio propuesto, se han identificado las siguientes limitaciones:

- ✓ El poco desarrollo de la informática forense y el uso de sus herramientas dentro del derecho informático en el país.
- ✓ Escasa existencia de profesionales informáticos especializados en informática forense en El Salvador.
- ✓ Poca difusión de herramientas de software que se utilizan en la práctica de la informática forense.

CAPÍTULO I

INVESTIGACIÓN PRELIMINAR

CAPÍTULO I: INVESTIGACIÓN PRELIMINAR

A. ANTECEDENTES

I. EVOLUCIÓN DE LAS HERRAMIENTAS DE SOFTWARE

Con el objetivo de conocer la evolución de las técnicas y las herramientas de software utilizadas en la informática forense es necesario conocer primero el desarrollo de la misma y la de los delitos informáticos acontecidos.

En la tabla que se presenta a continuación se resume la evolución de la informática forense en relación con el tipo de tecnología existente, los delitos informáticos más comunes y la conformación de los equipos forenses.

FECHA	TECNOLOGÍA	DELITO	EQUIPO FORENSE
1950	Transistores	Ninguno	
1960	Aplicaciones Comerciales	Fraude Local	
1970	Bases de datos ARPANET Silicio	Incidente por Fraude de Hackers	
1980	Computador Personal TELNET LAN WAN	Violación de Seguridad Hardware Robado Violación de derechos de autor Virus	Unidad de Crimen local y nacional.
1990	Internet	Fraude en línea Pornografía en Web Guerra de Información Hurto de identidad Abuso de email	Grupo de tarea Nacional. Grupo de tarea Global.
2000	Internet	Fraude corporativo Terrorismo global	Entrenamiento y certificación en Computación forense.

Tabla No 1: Evolución de la informática forense

Al realizar un análisis de la tabla mostrada logramos observar que surge equipo forense hasta los años 80 donde los delitos que se presentan son violaciones a la seguridad, virus, hardware robado y violaciones de derechos de autor, al existir este tipo de hechos surge la necesidad de conocimientos que permitan verificar que estos han sido cometidos.

Inicialmente el análisis forense se realizaba de manera manual verificando la existencia de modificaciones en los archivos realizados por seres humanos o códigos maliciosos introducidos en el sistema, por ejemplo, para recuperar archivos eliminados en MS-DOS se contaba con un comando llamado *undelete* que servía de apoyo para recuperar datos que habían sido eliminados accidental o intencionalmente.

En 1984 el FBI inició un programa llamado *programa de medios magnéticos* que dio origen al CART, un equipo de análisis computacional. En 1988 Michael Anderson un agente del IRS armó un grupo de especialistas y se reunieron con 3 compañías involucradas en la recuperación de datos, compañías que después se convertirían en Symantec.

En una de estas reuniones se crearon las clases de especialistas de recuperación de evidencia computacional, en 1988 y 1989 en el centro de entrenamiento federal FLETC, y también se creó la IACIS[2].

El fraude y el robo con la ayuda de las computadoras eran los primeros crímenes que trataba de solucionarse en el área informática, Canadá era el primer país en decretar una ley federal para tratar el delito informático. El acto federal del fraude y del abuso de computadora de los EE.UU., fue pasado en 1984 y enmendado en 1986, 1988, 1989, y 1990.

En los años 90, la comercialización del Internet y el desarrollo del World Wide Web (WWW) popularizaron el Internet", haciéndolo accesible a millones de personas. Mientras que la gama de los crímenes que eran confiados con la ayuda de computadoras aumentó, en Estados Unidos se crearon grupos de investigación sobre crímenes informáticos. Sin embargo, las demandas en estos grupos agotaron rápidamente sus recursos y los centros regionales para procesar evidencia digital fueron desarrollados.

En esta década surgen las primeras herramientas de software para informática forense. Podemos mencionar *SafeBack* la cual es una herramienta para realizar copias de respaldo de datos de gran fidelidad.

Entre 1993 y 1995 junto con el Departamento de Hacienda de Canadá se formó el programa CIS para incluir a todas las agencias de la tesorería estadounidense en el entrenamiento que se inició en 1988. Al mismo tiempo se formó la IOCE, Organización Internacional en Evidencia Computacional, cuyo propósito es proveer un foro internacional para el intercambio de la información relacionada con la investigación computacional y la informática forense.

Para entonces la informática forense ya se había consolidado como un campo vital en el área de la investigación, y que a medida que la tecnología avanzaba de forma acelerada así tenían que hacerlo las organizaciones encargadas de la informática forense.

En el año 1999 el FBI examinaba más de 17 terabytes de información en 2000 casos.

Para el 2003 el CART trabajaba en 6,500 casos y estaba examinando 782 Terabytes de datos.

[2] Asociación Internacional de Especialistas en la Investigación Computacional.

Actualmente las compañías de software producen aplicaciones forenses más robustas y los agentes de la ley y militares entrenan a más personal para responder a los crímenes que involucran tecnología.

II. EVOLUCIÓN DE LAS TÉCNICAS

"La informática forense nació de la necesidad básica de recuperar información de discos que se han dañado física o lógicamente", explicó Adrián Rodríguez[3].

Pero en la actualidad, sostuvo Rodríguez, se han agregado nuevas cualidades de monitoreo que permiten recobrar más información y utilizando los protocolos adecuados, presentar y preservar la evidencia hallada como una prueba válida en un caso legal.

En los inicios de la informática forense, según Igor León, especialista en seguridad de Etek Internacional, era común que los investigadores usaran el equipo comprometido para llevar a cabo la investigación. El riesgo de esta técnica era que el sistema operativo de la máquina podía alterar la evidencia.

León dijo que solo hasta la década de los noventa se desarrollaron herramientas de software como SafeBack que permitieron recolectar los datos en discos, sin alterar la información original.

III. INVESTIGACIONES PREVIAS

Previa a nuestra investigación existe un trabajo de análisis y diagnóstico de la informática forense en El Salvador el cual fue desarrollado hace un año por estudiantes de la Escuela de Ingeniería de Sistemas Informáticos de la Universidad de El Salvador.

La investigación mencionada anteriormente se enfoca en el análisis y diagnostico de la informática forense en El Salvador y su enfoque al estado general de la misma en el país y no a sus herramientas que son en gran medida las que garantizan la fiabilidad de la evidencia digital la cual se utiliza en procesos legales.

Además se realizó una consulta a un estudio acerca de la informática forense presentada por alumnos de la Universidad Centroamericana "José Simeón Cañas" a la Lic. Alicia Alvarenga Conde. En dicha investigación solamente se trata la informática forense desde un punto de vista teórico presentado historia, evolución, clasificación, aplicaciones y retos. Desde el punto de vista de las herramientas solamente se enfocaron en lo que es la recuperación de datos e información de un disco duro dejando a un lado las distintas ramas o aplicaciones de las mismas.

IV. INFORMÁTICA FORENSE EN EL SALVADOR

En el país la pericia en el área informática nace aproximadamente en el año 2000 cuando surgen delitos en los que se vieron involucradas computadoras.

Al surgir esta necesidad se toma la ley[4] donde se especifica que los peritos se asignan según su pericia y que de no existir una academia o institución capacitadora se elegirán por idoneidad, se

[3] Consultor de seguridad de la empresa Digiware Colombia.
[4] Artículo 196, Código procesal penal.

buscarán personas que tengan conocimientos en el área en que sea necesario y que cuenten con documentos que respalden el conocimiento técnico.

A partir de ese momento ha existido una evolución en la informática forense y en las herramientas que se utilizan para desarrollar las actividades que esta incluye.

La distribución de software para informática forense en los países es muy importante ya que la obtención de estas herramientas que apoyan la investigación forense depende de su disponibilidad en el mercado. En varios países de América Latina ya existe una distribución de Software para informática forense lo cual fortalece las investigaciones entre ellas podemos mencionar:

- ✓ Bolivia desde el año 2008 cuenta con la Distribución del Software para Informática Forense de Guidance Software entre los que se encuentra el ENCASE una de las Suites para investigación forense de más renombre en la actualidad.
- ✓ ETEK es parte de ETEK International Holding Corp. Con oficinas directas en Argentina, Brasil, Chile, Colombia y oficina Principal en Estados Unidos, ETEK es proveedor líder latinoamericano en soluciones integrales de seguridad de la información.

B. SITUACIÓN ACTUAL

Para obtener la situación actual nos basamos en entrevistas realizadas a personas que están familiarizadas o practican el uso de herramientas de informática forense en el país[5].

I. DESCRIPCIÓN

A partir de la investigación inicial sobre el estado de la aplicación de herramientas de software para informática forense en El Salvador se obtuvo lo siguiente:

Recurso Humano poco capacitado: Referente a esto, el Jefe de Informática de la División Policía Técnica Científica expresó la no existencia de una academia capacitadora en el área de informática forense en el país que brinde los conocimientos teóricos y prácticos necesarios para la aplicación adecuada de las herramientas de software que apoyan el análisis forense informático, dentro de este mismo punto vale la pena mencionar que en el país no existe alguna entidad certificadora en el área de informática forense y los profesionales informáticos que desarrollan peritaje informático solo cuentan con los títulos que certifican sus conocimientos en el área de tecnologías de información y no específicamente en informática forense, como expresa Francisco Rivas (perito informático independiente) los peritos se ven obligados a auto capacitarse y en algunos casos a obtener ellos mismos las herramientas que apoyen el desempeño de sus actividades profesionales.

Instituciones educativas que no imparten conocimientos relacionados con la informática forense y sus herramientas: luego de analizar los planes de estudio de las 16 diferentes universidades[6] que imparten carreras en el área Informática logramos observar que no existen materias que contemplen contenidos referentes a la informática forense y sus herramientas de software lo cual muestra un vacío dentro de las carreras impartidas en las universidades del país con respecto a esta área de las tecnologías de información.

[5] Ver Anexo # 1: Formato de entrevista preliminar
[6] Ver Anexo # 2: Planes de estudio de universidades consultadas

Marco legal que no incluye el tratamiento de los delitos informáticos: en nuestro país no existe una ley específica que tipifique los delitos informáticos, por lo cual las autoridades y personas ligadas a la persecución de estos se auxilian de la ley clasificando por afinidad los delitos como por ejemplo si es un fraude electrónico se persigue aplicando la ley referente a la comisión de un fraude sin importar si ha sido a través de medios electrónicos; con respecto a los peritos según el código procesal penal de El Salvador en el Art. 196. Los peritos deberán tener título en la materia a que pertenezca el punto sobre el que han de pronunciarse, siempre que la profesión, arte o técnica estén reglamentadas. En caso contrario, podrá designarse a personas de idoneidad manifiesta. También podrá designarse a un perito con título obtenido en el extranjero cuando posea una experiencia o idoneidad especial. Con respecto a lo anterior se justifica que el peritaje Informático sea desempeñado por profesionales en informática ya que no existe una entidad capacitadora en informática forense.

Bajo presupuesto para adquirir herramientas y tecnologías necesarias para el desarrollo de la informática forense: Según lo expresado por las autoridades de la División Policía Técnica Científica, existe un presupuesto limitado que dificulta la adquisición de herramientas de software y la capacitación en la utilización de las mismas.

A continuación se presentan algunos de los delitos que se cometen en El Salvador donde se puede ver que es una realidad que se vive en el país; no se encuentran estadísticas exactas de delitos informáticos ya que no existe una tipificación de los mismos como tales.

DELITOS INFORMÁTICOS	DETALLES
Cobros por gastos no autorizados entre ellos por clonación de tarjetas de crédito o debito.	250 anuales según datos de la Defensoría del Consumidor.
Perdidas por piratería de software	Más de 18 millones de dólares según el Informe sobre piratería de la Business Software Alliance.
Violación de privacidad de datos	La empresa INFORNET comercializa datos personales de más de 4 millones de salvadoreños. **http://indatasv.blogspot.com/search?q=infornet**
Pedófilos en Internet	Existen 14 casos y 4 en investigación según la Interpol en el País **http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=8613&idArt=3479512**
Piratería de software	Los allanamientos en establecimientos que utilizan o distribuyen software pirata se aumentaron en un 150% en 2008 **http://www.revistaitnow.com/-know-how/595-realizan-allanamientos-por-pirateria-de-software-en-el-salvador**
Pornografía infantil	Desde el año 2006 un total de 20 delitos relacionados con pornografía infantil han sido judicializados en el país. **http://www.laprensagrafica.com/el-salvador/social/39006-pornografia-infantil-utiliza-de-medio-la-web.html**

Tabla No 2: Delitos informáticos acontecidos en El Salvador

Los peritos informáticos que hacen uso de herramientas para informática forense desarrollan sus actividades, ya sea formando parte de las instituciones encargadas de la persecución de crímenes como son la Policía Nacional Civil a través de la División Policía Técnica Científica y la División Interpol las cuales son encargadas de investigar los crímenes tecnológicos o delitos informáticos; también existen peritos independientes de estas instituciones los cuales son requeridos por los Jueces como apoyo a los fiscales que llevan casos referentes a estos tipos de delitos, según Rivas.

A partir de todo lo anterior es notorio el desconocimiento generalizado de herramientas para informática forense en el país comenzando desde la inexistencia de un marco legal que apoye la persecución de delitos informáticos, la falta de una academia o instituto capacitador y certificador de conocimientos, la falta de cultura en derecho informático en el país y el desconocimiento por parte de los fiscales sobre pericias Informáticas son los principales factores que provocan la realidad que se plasma en esta sección.

II. ESTRUCTURA

A continuación se muestra el enfoque de sistemas de la situación actual el cual muestra de una manera práctica los elementos que forman el sistema que engloba la aplicación de herramientas de software para informática forense en El Salvador.

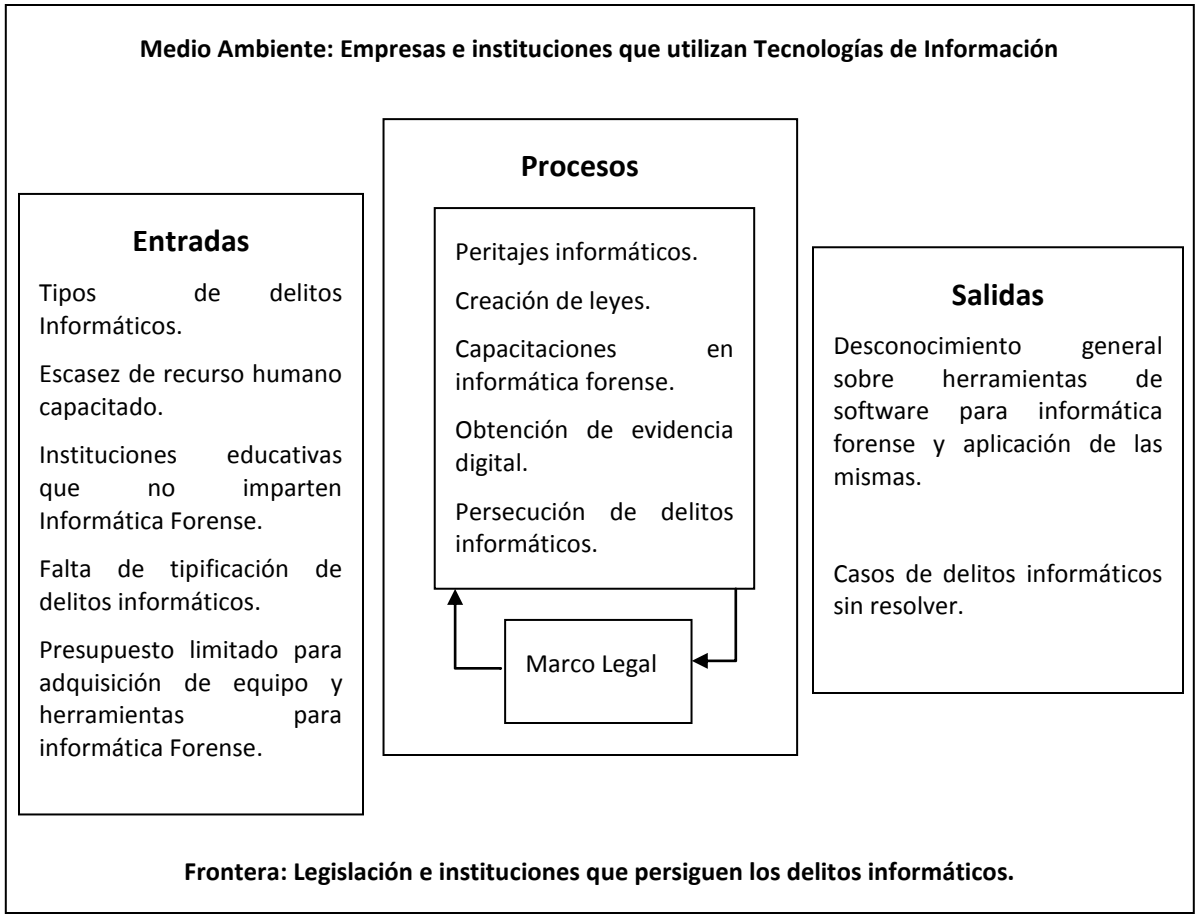

Figura No. 1: Enfoque de Sistemas correspondiente a la situación actual.

Descripción del Enfoque de Sistemas de la Situación Actual

Salidas

Desconocimiento general sobre herramientas de software para informática forense y aplicación de las mismas: el conocimiento técnico en el área de informática forense es limitado.

Casos de delitos informáticos sin resolver: La cantidad de casos sin resolver son producidos por la falta de conocimientos de herramientas de apoyo para recolectar evidencia digital.

Entradas

Tipos de delitos informáticos: dentro de los delitos que se presentan en el país tenemos fraudes electrónicos, estafas, piratería de software, reproducciones ilegales de audio o video con derechos de autor, pornografía Infantil y extorsiones entre otros.

Escasez de recurso humano capacitado debido a la poca difusión del tipo de herramientas que se aplican en esta área del derecho informático, no hay suficiente personal capacitado como para satisfacer la demanda que tiene y tendrá en el tiempo subsiguiente.

Instituciones educativas sin personal especializado: el desconocimiento de esta nueva especialización en el área de tecnologías de información provoca que las instituciones que imparten educación a nivel superior no cuenten con personal especializado.

Falta de tipificación de delitos informáticos: la legislación salvadoreña no posee un apartado que tipifique los delitos en los cuales se han utilizado medios electrónicos como delitos informáticos lo cual entorpece la persecución de los mismos.

Falta de academia o entidad capacitadora en informática forense: el no poseer una academia que capacite o certifique forenses informáticos obliga a los encargados de aplicar la ley a buscar en personal con conocimientos en tecnologías de información que posea un grado que certifique sus conocimientos.

Presupuesto limitado para adquisición de equipo y herramientas para informática forense tanto en las instituciones que realizan análisis sobre delitos informáticos como en las instituciones educativas. El recurso económico es de gran importancia y al ser limitado o insuficiente provoca la no adquisición de las tecnologías más adecuadas para realizar análisis forenses.

Procesos

Peritajes informáticos: Este proceso se refiere al análisis que realizan los peritos sobre equipo informático que ha sido utilizado como medio o fin de un delito.

Creación de leyes: Las leyes que apoyan la persecución de delitos promueven el desarrollo de las diferentes aéreas de investigación entre ellas la informática forense.

Capacitaciones en informática forense: dentro de este proceso se incluyen las capacitaciones que se realizan por parte de las instituciones a los peritos encargados de realizar el análisis forense informático.

Obtención de evidencia digital: es el proceso mediante el cual, a través de herramientas de software especializadas, se obtiene evidencia digital para demostrar que un delito informático ha sido cometido.

Persecución de delitos informáticos: Dentro de este participan entidades como la Fiscalía General de la República, apoyada por la Policía Nacional Civil.

Frontera

Legislación e instituciones que persiguen los delitos informáticos.

Medio Ambiente

Empresas e instituciones que utilizan Tecnologías de Información.

Elemento de Control

Marco Legal a través del cual se persiguen y juzgan los delitos informáticos.

C. FORMULACIÓN DEL PROBLEMA

I. SITUACIÓN PROBLEMÁTICA

Mediante el análisis de la situación actual obtenida de la investigación preliminar, hemos identificado la siguiente situación problemática:

Las instituciones que persiguen los delitos informáticos tienen que prepararse y actualizarse. Para esto es necesario que se mantengan al día con respecto a las herramientas (ya sea libres o con licencias) que les permitan obtener la evidencia digital necesaria. El desempeño de estas instituciones (P.N.C, Interpol, F.G.R.) depende en gran medida de la capacidad técnica de su recurso humano, el aprovechamiento de las herramientas de informática forense existentes y en el presupuesto con el que cuentan.

Otro punto importante es el hecho que en nuestro país no existen academias destinadas ya sea a la formación o capacitación de profesionales en la materia. Es más ni siquiera las instituciones de educación superior proporcionan este tipo de conocimientos a sus estudiantes durante su proceso formativo, lo que origina que los profesionales recién formados no tengan conocimientos en esta área de la informática. Además, la legislación salvadoreña todavía no ha establecido leyes destinadas a la tipificación y persecución de los delitos informáticos como tales, caso contrario a países como Venezuela o Argentina, naciones latinoamericanas que han elaborado y aprobado proyectos de ley que persiguen este tipo de delitos.

Todos estos puntos expuestos corroboran la necesidad de fomentar el conocimiento y uso de las herramientas de software utilizadas en la informática forense y de esta forma ayudar al combate de los crímenes o delitos que utilizan a los recursos tecnológicos como herramientas u objetivos.

II. DIAGRAMA CAUSA – EFECTO

Para analizar el problema a estudiar nos auxiliaremos del **diagrama causa – efecto** que también es conocido como diagrama de Ishikawa.

El diagrama de Ishikawa, o **Diagrama Causa-Efecto**, es una herramienta que ayuda a identificar, clasificar y poner de manifiesto posibles causas que originan un problema. Este problema puede ser de cualquier índole ya sea económico, científico, social, etc. Ilustra gráficamente las relaciones existentes entre un resultado dado (efectos) y los factores (causas) que influyen en ese resultado.

El diagrama de Ishikawa es una de las diversas herramientas que facilita el análisis de problemas y sus soluciones. Este tipo de herramienta permite un análisis participativo mediante grupos de mejora o grupos de análisis, que mediante técnicas como por ejemplo la lluvia de ideas, sesiones de creatividad, y otras, facilita un resultado óptimo en el entendimiento de las causas que originan un problema, con lo que puede ser posible la solución del mismo.

Las razones por la que hemos decidido utilizar esta técnica para en análisis de problemas son:

- Permite que el grupo se concentre en el contenido del problema, no en la historia del problema ni en los distintos intereses personales de los integrantes del equipo.
- Ayuda a determinar las causas principales de un problema, o las causas de las características de calidad, utilizando para ello un enfoque estructurado.
- Estimula la participación de los miembros del grupo de trabajo, permitiendo así aprovechar mejor el conocimiento que cada uno de ellos tiene sobre el proceso.
- Incrementa el grado de conocimiento sobre un proceso.

Para entender cómo interpretar el diagrama de Ishikawa, se debe conocer su estructura. Este diagrama está formado por un eje horizontal que representa el problema a analizar, a este eje horizontal le van llegando líneas oblicuas que representan las posibles causas de este problema. Estas causas pueden estar clasificadas en categorías primarias, secundarias, terciarias, etc., de acuerdo al nivel de importancia de éstas en el problema.

Los pasos realizados para la construcción del diagrama de Ishikawa fueron los siguientes:

1. Definimos el problema o efecto que queremos analizar, en nuestro caso es **¿En qué medida, la falta de aplicación de las herramientas de software para la informática forense influye en la evidencia digital presentada en los procesos judiciales?**

2. Identificamos las causas primarias involucradas en el problema. Las causas principales identificadas fueron: Recurso humano, recurso tecnológico, recurso económico, instituciones de educación superior, legislación salvadoreña y evidencia digital.

   Los elementos de la problemática que han sido identificados son:

   a. **Recurso humano:** Encargado de la aplicación de las herramientas informáticas para la obtención de la evidencia digital.

b. **Recurso tecnológico:** Equipo necesario para poder aplicar las herramientas de informática forense. Este equipo comprende hardware y software.
c. **Recurso económico:** Necesario para obtener los recursos tecnológico y humano para la aplicación de las herramientas de informática forense.
d. **Instituciones de educación superior:** Universidades encargadas de preparar los profesionales en informática.
e. **Marco legal salvadoreño:** Bajo el cual se rigen los procedimientos legales.
f. **Evidencia digital:** Se presenta como prueba en los procesos legales, debe contar con la confiabilidad necesaria para tomarse como cierta en este tipo de procesos.

3. Identificamos las causas secundarias del problema dentro de cada una de las causas principales. Las causas secundarias identificadas fueron:
    a. Para el factor recurso humano:
        i. Capacitación sobre la Informática forense y sus herramientas pobres o nulas.
        ii. Resistencia al cambio.
        iii. Desconocimiento de las herramientas de informática forense.
        iv. Personal no calificado.
    b. Recurso tecnológico:
        i. Alto costo de adquisición.
        ii. Recurso tecnológico actual obsoleto.
        iii. Falta de laboratorios especializados.
    c. Recurso económico:
        i. Presupuesto insuficiente para obtener herramientas o capacitaciones.
    d. Instituciones de educación superior:
        i. Carencia de institutos especializados en la informática forense.
        ii. Falta de personal con conocimiento para enseñar informática forense.
        iii. Carencia del equipo necesario para enseñar.
    e. Legislación salvadoreña:
        i. No existe una tipificación de los delitos informáticos en el marco legal salvadoreño.
    f. Evidencia digital:
        i. Herramientas no adecuadas para su recolección.
        ii. Falta de soporte legal.

Las causas primarias y secundarias planteadas en el diagrama de Ishikawa fueron determinadas por el grupo de trabajo mediante la técnica de lluvia de ideas.

A continuación se presenta el diagrama Causa – Efecto utilizado para identificar la problemática antes expuesta:

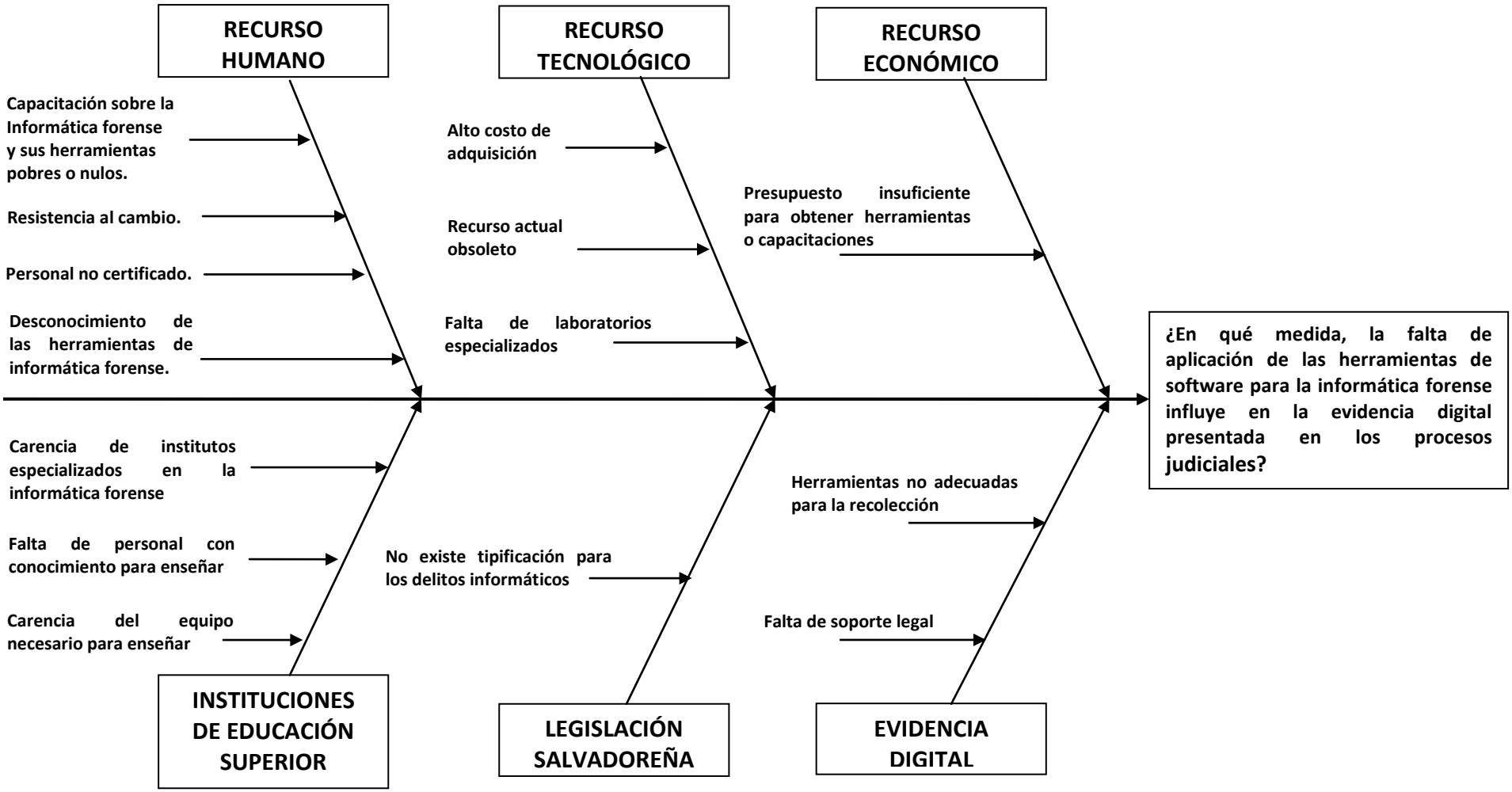

Figura No. 2: Diagrama Causa – Efecto utilizado para la identificación de la problemática.

III. FORMULACIÓN DEL PROBLEMA

Con la finalidad de poder entender de una manera más clara los elementos que conforman la situación problemática, se hace uso del proceso solucionador de problemas:

Figura No. 3: Proceso solucionador de problemas utilizado para la formulación del problema.

IV. ANÁLISIS DEL PROBLEMA

Entrada: Desconocimiento en la aplicación de las herramientas de informática forense.

Variables de entrada:

- ✓ Recurso humano poco o nulamente capacitado o no certificado.
- ✓ Instituciones educativas sin personal con conocimiento para la enseñanza.
- ✓ Marco legal que no incluye el tratamiento de los delitos informáticos.
- ✓ Poco presupuesto para adquirir herramientas y tecnologías necesarias para el desarrollo de la informática forense y sus herramientas.
- ✓ Recurso humano sin conocimiento de la correcta aplicación de las herramientas de informáticas forenses.

Salida: Estudio e investigación de las herramientas utilizadas en la informática forense en El Salvador y propuestas de herramientas para la informática forense.

Variables de Salida:

- ✓ Diagnostico de la situación actual de las herramientas de informática forense utilizadas en El Salvador.
- ✓ Demostración de la forma de aplicación de las herramientas de informática forense utilizadas actualmente.
- ✓ Herramientas propuestas que pueden ser aplicadas a la informática forense en El Salvador.
- ✓ Documentos de referencia de las herramientas propuestas que sirvan para tomar decisiones respecto a que herramienta utilizar.

- ✓ Corroborar la confiabilidad de la evidencia digital obtenida mediante la aplicación correcta de las herramientas informáticas.

Variables de solución:

- ✓ Metodología de investigación aplicada las herramientas de informática forense en El Salvador.
- ✓ Conocimientos de las herramientas de informática forense y su funcionamiento.
- ✓ Tipos de delitos informáticos que se cometen en El Salvador.

V. ENUNCIADO DEL PROBLEMA

Después de realizar el análisis del problema, se presenta el siguiente enunciado:

¿En qué medida, la falta de aplicación de las herramientas de software para la informática forense influye en la evidencia digital presentada en los procesos judiciales?

VI. PREGUNTAS DE LA INVESTIGACIÓN

Dentro de las preguntas de investigación que pretendemos responder están las siguientes:

1. **Para la comunidad educativa:**
   - ¿Cuentan las instituciones de educación superior con personal para enseñar herramientas de informática forense?
   - ¿Qué factores son los que impiden o facilitan la enseñanza de la informática forense y sus herramientas como disciplina?
   - ¿Qué factores influyen para que las instituciones de educación superior no brinden conocimientos relacionados con la informática forense y las herramientas de software que se utilizan?

2. **Sector legal:**
   - ¿Existe un marco legal que soporte la utilización de herramientas de informática forense?

3. **Sector profesional:**
   - ¿Cuáles son las herramientas de informática forense que se utilizan en El Salvador?
   - ¿Cuál es el nivel de uso de las herramientas de informática forense en El Salvador?
   - ¿Cómo se clasifican las herramientas de informática forense son utilizadas en El Salvador?
   - ¿Qué nivel de incidencia tiene las herramientas de informática forense en la resolución de delitos informáticos?
   - ¿Cómo ayudan las herramientas de informática forense a obtener evidencia digital confiable?

- ¿Tiene el recurso humano el suficiente conocimiento en la aplicación de las herramientas de informática forense?

4. **Para todos los sectores:**
    - ¿Qué factores afectan el nivel de uso de las herramientas de informática forense, tanto positiva como negativamente?
    - ¿Se cuenta con el recurso humano, tecnológico, financiero, educativo para hacer del uso de las herramientas de informática forense una disciplina difundida?
    - ¿Qué ventajas o desventajas trae la utilización de herramientas de software en la informática forense a las personas o instituciones que las utilizan?

D. FORMULACIÓN DE HIPÓTESIS

A continuación se presenta la formulación de las hipótesis bajo las cuales realizaremos la investigación. Se plantean tres tipos de hipótesis: la hipótesis de investigación que refleja la posible causa del problema, la hipótesis nula que nos permitirá refutar la hipótesis de investigación y las hipótesis alternativa, que pueden ser explicaciones alternativas al problema en estudio.

I. HIPÓTESIS DE LA INVESTIGACIÓN

"El poco conocimiento de las herramientas de informática forense y su aplicación en casos prácticos impide obtener evidencia digital valida que ayude a la resolución de delitos informáticos de forma contundente en un 60%".

UNIDAD DE ANÁLISIS	VARIABLES	ELEMENTOS
Conocimiento acerca de la aplicación de herramientas de informática forense.	Independiente: Aplicación de las herramientas de informáticas forense a casos prácticos. Dependiente: Evidencia digital válida.	Afecta, 60 %.

Tabla No 3: Elementos considerados en la formulación de la hipótesis general

II. HIPÓTESIS NULA

Como se mencionó en el marco teórico de la metodología de investigación, la hipótesis nula constituye, en un sentido, el reverso de la hipótesis de investigación, por tanto, la hipótesis nula es:

"El poco conocimientos sobre la aplicación de las herramientas de informática forense a casos prácticos no constituye un impedimento para obtener evidencia digital válida".

III. HIPÓTESIS ALTERNATIVAS

Otras explicaciones al fenómeno de las herramientas de informática forense en El Salvador, estaría dado por las siguientes hipótesis alternativas:

1. "El factor económico constituye un impedimento para la obtención de evidencia digital válida en un 50% de los casos".
2. "La nula enseñanza de las instituciones de educación superior impide que la aplicación de las herramientas informáticas se convierta en una disciplina ampliamente difundida".
3. "La validez de la evidencia digital está influida negativamente por la metodología utilizada para su recolección en el 75% de los casos".
4. "La utilización de las herramientas de informática forense está ligada, principalmente, a la definición de metodologías para su aplicación, en un 45%".

E. MARCO TEÓRICO

Con el objetivo de obtener una mejor comprensión acerca del tema a tratar en la investigación, es necesario conocer los aspectos teóricos que fundamenten y ayuden a aclarar los elementos que serán expuestos en el presente documento. Es con esta finalidad que se presenta en este apartado la respectiva información teórica dividida en 2 secciones, las cuales son:

a) Marco teórico.
b) Marco referencial.

I. MARCO TEÓRICO

Para poder entender lo que son las herramientas de software para la informática forense es necesario conocer primero el campo donde son aplicadas, cual es el objetivo de su utilización, sobre qué medios o dispositivos trabajan así como los principios físicos en los que basan su funcionamiento.

DELITO INFORMÁTICO.

- ✓ **Definición:**

Después de estudiar una serie de definiciones de delitos informáticos presentadas por diferentes fuentes[7] se ha decidido tomar como referencia la realizada por Julio Téllez Valdés[8]: "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".

Esta definición abarca el uso de las computadoras como un objeto o instrumento para la realización de actividades que son contempladas como ilícitas por un marco legal. Además se incluyen las actividades que están destinadas a causar acciones sobre equipos de cómputo que pueden ser catalogadas como delitos.

- ✓ **Características:**

Según Julio Téllez Valdés, los delitos informáticos presentan las siguientes características principales:

a) Son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d) Provocan serias pérdidas económicas, ya que casi siempre producen grandes beneficios a aquellos que las realizan.

[7] Ver anexo #3: Definiciones de delito informático.
[8] Investigador titular "B" de tiempo completo en el Instituto de Investigaciones Jurídicas de la UNAM.

e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f) Son muy sofisticados y relativamente frecuentes en el ámbito militar.
g) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
h) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

✓ **Clasificación según la actividad informática[9]:**

En el siguiente resumen se presentan los delitos informáticos reconocidos por las Naciones Unidas:

Fraudes cometidos mediante manipulación de computadoras.

a) Manipulación de los datos de entrada.
b) La manipulación de programas.
c) Manipulación de los datos de salida.
d) Fraude efectuado por manipulación informática.

Falsificaciones informáticas.

a) Como objeto.
b) Como instrumentos.

Daños o modificaciones de programas o datos computarizados.

a) Sabotaje informático.
    i) Virus.
    ii) Gusanos.
    iii) Bomba lógica o cronológica.
b) Acceso no autorizado a servicios y sistemas informáticos.
    i) Piratas informáticos o hackers.
c) Reproducción no autorizada de programas informáticos de protección legal.

✓ **Clasificación según el instrumento o medio, fin u objetivo[10]:**

Como instrumento o medio

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
b) Variación de los activos y pasivos en la situación contable de las empresas.
c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
d) Lectura, sustracción o copiado de información confidencial.
e) Modificación de datos tanto en la entrada como en la salida.
f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

[9] Ver Anexo #4: Tipos de delitos informáticos reconocidos por la Organización de las Naciones Unidas.
[10] Clasificación propuesta por Julio Téllez Valdés.

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
h) Uso no autorizado de programas de cómputo.
i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.
l) Acceso a áreas informatizadas en forma no autorizada.
m) Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo.

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.
b) Destrucción de programas por cualquier método.
c) Atentado físico contra la máquina o sus accesorios.
d) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
e) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

INFORMÁTICA FORENSE.

- ✓ **Definición:**

Para la ISACA[11] "es el proceso de extracción de datos e información de un medio de almacenamiento computacional utilizando la tecnología disponible estableciendo su exactitud y confiabilidad con el objetivo de ser usado como evidencia en una corte de justicia".

- ✓ **Objetivos:**

La informática forense tiene 3 objetivos:

a) La compensación de los daños causados por los criminales o intrusos.
b) La persecución y procesamiento judicial de los criminales.
c) La creación y aplicación de medidas para prevenir casos similares.

- ✓ **Usos:**

Muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense:

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

[11] Information Systems Audit and Control Association

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

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

4. Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.

5. Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

- ✓ **Principios Forenses:**

Sin importar si el análisis forense es realizado a un cadáver o a un ordenador, es necesario tener en cuenta una serie de principios básicos[12], los cuales son:

1. Evitar la contaminación: La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense en informática.

2. Actuar metódicamente: El investigador debe ser el custodio de su propio proceso, por tanto cada uno de los pasos realizados, las herramientas utilizadas, los resultados obtenidos del análisis de los datos, deben estar claramente documentados.

3. Controlar la cadena de evidencia: es decir, conocer quien, cuando y donde ha manipulado la evidencia, este punto es complemento del anterior.

EVIDENCIA DIGITAL

- ✓ **Definición:**

Eoghan Casey[13] define la evidencia digital como: "Es un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizadas con herramientas y técnicas especiales".

La evidencia digital, siempre estará almacenada en un soporte real, como lo son los medios de almacenamiento magnéticos o magneto ópticos u otros que se encuentran en fase de desarrollo, siendo todos estos de tipo físicos por lo que este tipo de evidencia es igualmente física.

- ✓ **Características:**

a) Es un tipo de evidencia física que presenta ciertas ventajas, debido a que puede ser duplicada de una forma exacta, por lo que es posible peritar sobre copias, tal cual como si se tratará de

[12] Propuestos por Addison Wesley, Dan Farmer y Wietse Venema en su libro "Forensic Discovery".
[13] Página 4 de su libro "Digital evidence and Computer Crime", 2000.

la evidencia original, lo cual permite realizar diversos tipos de análisis y pruebas sin correr el riesgo de alterar o dañar la evidencia original.

b) Es relativamente fácil determinar si una evidencia digital ha sido modificada o alterada a través de la comparación con su original o bien con el análisis de sus metadatos.

c) La evidencia digital no puede ser destruida fácilmente. El disco duro de un sistema informático, guarda los datos en sectores creados en el momento del formateo del mismo.

HASH

✓ **Definición:**

Es una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un numero hash es el resultado de dicha función o algoritmo.

✓ **Aplicación:**

Una función de hash es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor (un subconjunto de los números naturales por ejemplo). Varían en los conjuntos de partida y de llegada y en cómo afectan a la salida similitudes o patrones de la entrada. Una propiedad fundamental del hashing es que si dos resultados de una misma función son diferentes, entonces las dos entradas que generaron dichos resultados también lo son.

INTEGRIDAD DE ARCHIVOS

✓ **Definición:**

El término integridad de archivos se refiere a la corrección y completitud de los archivos a partir de una copia de los originales , la integridad de los archivos almacenados puede perderse de muchas maneras diferentes. Pueden añadirse nuevos archivos o eliminarse archivos, lo cual daña la integridad de los archivos o medio que han sido copiados o duplicados.

✓ **Aplicación:**

La Integridad de archivos, ayuda a verificar que una copia de archivos o de un medio es exactamente igual a la original, esta es aplicable en los Análisis de Informática Forense, para esta se realiza Cálculos de Hash y se comparan los de los medios o archivos originales con los de las copias sobre las cuales se trabaja, lo cual apoya la autenticidad de la invidencia que pueda ser recolectada

SISTEMAS VIVOS

- ✓ **Definición:**

En Informática forense el termino sistema vivo es utilizado para hacer referencia a un sistema encendido una de las ventajas de trabajar sobre un sistema vivo (haciendo referencia a que no ha sido apagado desde cometido el delito) es que puede obtenerse información en memoria RAM los cuales son volátiles y posterior a ser apagado son eliminados y no pueden ser recuperados.

SISTEMAS MUERTOS

- ✓ **Definición:**

En Informática forense el termino sistema muerto es utilizado para hacer referencia a un sistema apagado las ventajas de trabajar sobre un sistema muerto son entre otras que puede extraerse los medios de almacenamiento del mismo y bloquearlos para evitar cualquier modificación en los mismos, a su vez realizar copias de los medios en medios externos para su análisis en búsqueda de evidencia digital.

COPIAS BIT A BIT

- ✓ **Definición:**

Una copia bit a bit es una copia exacta física y lógica de un medio o archivo; en informática forense son utilizadas para realizar los análisis forenses sobre ellas y de esta manera evitar contaminar o dañar el medio original comprometido en un delito informático.

RECUPERACION DE ARCHIVOS ELIMINADOS

- ✓ **Definición:**

La recuperación de archivos eliminados consiste en regresar al espacio lógico de un medio un archivo que lógicamente ha sido eliminado aunque físicamente se mantiene en el medio; el objetivo de la recuperación de archivos en la informática forense es obtener archivos que hayan sido eliminados intencionalmente para ocultar información que pueda considerarse evidencia digital en casos de delitos informáticos.

MEDIOS DE ALMACENAMIENTO

- ✓ **Definición:**

Una **unidad de almacenamiento** o un **dispositivo de almacenamiento** es aquel aparato, que realiza las operaciones de lectura y/o escritura de los medios o soportes donde se almacenan o guardan, lógica y físicamente los archivos de un sistema informático.

- ✓ **Tipos:**

Discos Duros

Es un dispositivo de almacenamiento no volátil, que conserva la información aun con la pérdida de energía, que emplea un sistema de grabación magnética digital. Dicha unidad puede ser interna (fija) o externa (portátil) dependiendo del lugar que ocupe en el gabinete o carcasa de la computadora y se encuentra formado por varios discos apilados sobre los que se mueve una pequeña cabeza magnética que graba y lee la información.

Dentro de un disco duro hay uno o varios platos, que son discos (de aluminio o cristal) concéntricos y que giran todos a la vez. El cabezal (dispositivo de lectura y escritura) es un conjunto de brazos alineados verticalmente que se mueven hacia dentro o fuera según convenga, todos a la vez. En la punta de dichos brazos están las cabezas de lectura/escritura, una para cada cara, que gracias al movimiento del cabezal pueden leer tanto zonas interiores como exteriores del disco.

Discos Flexibles

Un disco flexible o disquete es un medio o soporte de almacenamiento de datos formado por una pieza circular de material magnético, fina y flexible encerrada en una cubierta de plástico cuadrada o rectangular. Los disquetes se leen y se escriben mediante un dispositivo llamado disquetera y es un disco más pequeño que el CD (tanto en tamaño externo como en capacidad), que está encerrado en una funda de pasta que lo protege. En las unidades de disquete sólo han existido dos formatos físicos considerados como estándar, el de 5¼" y el de 3½".

CD-ROM

Las unidades de CD-ROM son sólo de lectura. Es decir, pueden leer la información en un disco, pero no pueden escribir datos en él.

Una regrabadora (CD-RW) puede grabar y regrabar discos compactos. Las características básicas de estas unidades son la velocidad de lectura, de grabación y de regrabación. En discos regrabables es normalmente menor que en los discos grabables una sola vez. Es habitual observar tres datos de velocidad, según la expresión ax bx cx *(a:velocidad de lectura; b: velocidad de grabación; c: velocidad de regrabación)*.

En el disco CD-RW la capa que contiene la información está formada por una aleación cristalina de plata, indio, antimonio y telurio que presenta una interesante cualidad: si se calienta hasta cierta temperatura, cuando se enfría deviene cristalino, pero si al calentarse se alcanza una temperatura aún más elevada, cuando se enfría queda con estructura amorfa. La superficie cristalina permite que la luz se refleje bien en la zona reflectante mientras que las zonas con estructura amorfa absorben la luz.

DVD-ROM

Un DVD de capa simple puede guardar aproximadamente 4,377 gigabytes. El DVD usa un método de codificación más eficiente en la capa física, por lo que el formato DVD es un 47% más eficiente que el CD-ROM, que usa una tercera capa de corrección de errores.

Memoria Flash

Una memoria Flash es un pequeño dispositivo de almacenamiento que utiliza memoria flash para guardar la información que puede requerir o para guardar fotografías o videos tomados con medios externos. Los sistemas operativos actuales pueden leer y escribir en las memorias sin más que enchufarlas a un conector USB o lector de memorias del equipo encendido, recibiendo la energía de alimentación a través del propio conector entre las memorias flash tenemos USB(Bus de Serie Universal) SD(Secure Digital) MS(Memory Stick) entre otros.

- ✓ **Principios físicos:**

En general, los medios de almacenamiento magnético se basan directamente en cuatro fenómenos físicos:

1. Una corriente eléctrica produce un campo magnético.
2. Algunos materiales se magnetizan con facilidad cuando son expuestos a un campo magnético débil. Cuando el campo se apaga, el material de desmagnetiza rápidamente. Se conocen como *Materiales Magnéticos Suaves*.
3. En algunos materiales magnéticos suaves, la resistencia eléctrica cambia cuando el material es magnetizado. La resistencia regresa a su valor original cuando el campo magnetizante es apagado. Esto se llama *Magneto-Resistencia*, o efecto MR. La Magneto-Resistencia Gigante, o efecto GMR, es mucho mayor que el efecto MR y se encuentra en sistemas específicos de materiales de películas delgadas.
4. Otros materiales se magnetizan con dificultad (es decir, requieren de un campo magnético fuerte), pero una vez se magnetizan, mantienen su magnetización cuando el campo se apaga. Se llaman *Materiales Magnéticos Duros*, o *Magnetos Permanentes*.

Los fenómenos antes descritos son usados de la siguiente manera:

1. Cabezas de Escritura: Cabezas usadas para escribir bits de información en un disco magnético giratorio, dependen de un campo magnético, de los medios magnéticos suaves y la Magneto-Resistencia, para producir y controlar campos magnéticos fuertes.
2. Cabezas de lectura: Éstas dependen de un campo magnético, de los medios magnéticos suaves y la Magneto-Resistencia y son sensibles a los campos magnéticos residuales de los medios de almacenamiento magnetizados.
3. Medios de Almacenamiento: (Como discos de computador) Los medios de almacenamiento magnético son magnetizados de manera permanente en una dirección (Norte o Sur) determinada por el campo de escritura. Estos medios explotan los Magnetos permanentes.
4. Los cabezales **escriben** datos en los platos al alinear partículas magnéticas sobre las superficies de éstos. Los cabezales **leen** datos al detectar las polaridades de las partículas que ya se han alineado.

SISTEMAS DE ARCHIVOS

✓ Conceptos básicos:

Se denomina sistema de archivos al conjunto de archivos en una unidad de disco. El sistema de archivos está compuesto por los datos de los archivos, así como toda la información auxiliar que requiere.

La **metainformación** es toda la información auxiliar que es necesario mantener en un volumen y se encuentra compuesta por los siguientes elementos:

- Estructura física de los archivos.
- Directorios (archivos que contienen las tablas nombre-puntero).
- Estructura física del sistema de archivos.
- Estructura de información de bloques y nodos-i libres (mapas de bits)

Cada sistema operativo organiza las particiones de disco de una determinada forma, repartiendo el espacio disponible entre el programa de carga (boot) del sistema operativo, la metainformación y los datos. Normalmente, las tablas de subdirectorios se almacenan como archivos, por lo que compiten por los bloques de datos con los archivos de datos.

✓ Estructura:

Cuando se crea un sistema de archivos en una partición de un disco, se crea una entidad lógica auto contenida con espacio para la información de carga del sistema operativo, descripción de su estructura, descriptores de archivos, información del estado de ocupación de los bloques del sistema de archivos y bloques de datos.

Bloque de carga: contiene el código que ejecuta el programa de arranque del programa almacenado en la ROM de la computadora.

Metainformación: describe el sistema de archivos y la distribución de sus componentes. Suele estar agrupada al principio del disco y es necesaria para acceder al sistema de archivos.

Sus componentes son:

- Superbloque: contiene información que describe toda la estructura del sistema de archivos.
- Información de gestión de espacio, que permite al servidor de archivos implementar distintas políticas de asignación de espacio y para reutilizar los recursos liberados para nuevos archivos y directorios.
- Descriptores físicos de archivos.
- Bloques de datos, tratados de forma individual o bien en grupos, son asignados a los archivos por el servidor de archivos, que establece una correspondencia entre el bloque y el archivo a través del descriptor del archivo.

- ✓ **Operaciones con los archivos:**

Las operaciones que se pueden hacer con los ficheros pueden utilizar todos los registros del fichero o solo una parte de ellos. Entre estas operaciones estan:

a) Creación.
b) Apertura y cierre.
c) Borrado
d) Ordenado o clasificación.
e) Duplicado o copiado.
f) Fusión o intercalación.
g) Partición.
h) Actualización o mantenimiento.
i) Recuperación.

- ✓ **Tipos de organización:**

Organización Secuencial

Un fichero con organización secuencial es aquel en el que los registros se van grabando uno a continuación de otro, sobre el soporte informático, sin dejar huecos en medio.

En este tipo de ficheros existe, por tanto, una correspondencia total entre el orden lógico y el orden físico, si entendemos por ***orden lógico*** el orden en que son dados de alta y recuperados los registros, y por ***orden físico*** el orden en que están grabados los registros en el soporte.

Con el fin de mejorar las prestaciones de la organización secuencial surgen una serie de organizaciones que son una variante de esta y que pueden ser utilizados con soportes direccionables. Las más empleadas son:

a) La organización *secuencial indexada,* en la que los registros con los datos se graban en un fichero secuencialmente, pero se pueden recuperar con acceso directo gracias a la utilización de un fichero adicional, llamado de **índices,** que contiene información de la posición que ocupa cada registro en el fichero de datos.

b) La organización *secuencial encadenada,* que nos permite tener los registros ordenados según un orden lógico diferente del orden físico en el que están grabados gracias a la utilización de unos campos adicionales llamados **punteros.**

Organización Directa

La organización directa está basada en la independencia entre el orden en que se dan de alta los registros y la posición en la que se graban en el soporte. La posición en la que se graban los registros está en función de la información que tenga el campo clave del registro.

En esta organización el espacio total disponible para el fichero se divide en *celdas* destinadas cada una de ellas a contener un registro y sólo uno. Las celdas están numeradas correlativamente y se puede acceder al contenido de un registro, de forma directa, si conocemos la dirección relativa de la celda en la que está grabado. Esta organización sólo es posible en soportes direccionables, pues el acceso a los registros se hace sin necesidad de leer los anteriores.

- ✓ **Tipos de sistemas de archivos:**

A continuación se presenta una tabla resumen acerca de los tipos de sistemas de archivos más utilizados:

NOMBRE	DESCRIPCIÓN
FAT	Sistema de archivos desarrollado para MS-DOS, así como el sistema de archivos principal de las ediciones no empresariales de Microsoft Windows hasta Windows Me.
NTFS	Sistema de archivos diseñado específicamente para Windows NT incluyendo las versiones Windows 2000, Windows 2003, Windows XP y Windows Vista.
EXT2	Sistema de archivos para el kernel de Linux, fue el sistema de ficheros por defecto de las distribuciones de Linux Red Hat Linux, Fedora Core y Debian
EXT3	Sistema de archivos con registro por diario (journaling). Es el sistema de archivo más usado en distribuciones Linux.
JFS	Sistema de archivos de 64-bit con respaldo de transacciones. Fue diseñado con la idea de conseguir "servidores de alto rendimiento y servidores de archivos de altas prestaciones, asociados a e-business".
XFS	Se incorporó a Linux a partir de la versión 2.4.25, los programas de instalación de las distribuciones de SuSE, Gentoo, Mandriva, Slackware, Fedora lo ofrecen como una opción.
ZFS	Sistema de archivos desarrollado por Sun Microsystems para su sistema operativo Solaris.
REISER	Es el sistema de archivos por defecto en varias distribuciones, como SuSE (excepto en openSuSE 10.2 que su formato por defecto es ext3), Xandros, Yoper, Linspire, Kurumin Linux, FTOSX, Libranet y Knoppix.
REISER4	Se trata de la versión más reciente del sistema de archivos ReiserFS, reescrito desde cero
HFS	Sistema de Archivos Jerárquicos o Hierarquical File System (HFS), es un sistema de archivos desarrollado por Apple Inc. para su uso en computadores que corren Mac OS
HFS+	Es un sistema de archivos desarrollado por Apple Inc. para reemplazar al HFS. También es el formato usado por el iPod al ser formateado desde un Mac.
ISO 9660	Es una norma publicada inicialmente en 1986 por la ISO, que especifica el formato para el almacenaje de archivos en los soportes de tipo disco compacto. Su propósito es que tales medios sean legibles por diferentes sistemas operativos de diferentes proveedores y en diferentes plataformas, por ejemplo, MS-DOS, Microsoft Windows, Mac OS y UNIX.
JOLIET	Joliet es, de hecho, una ampliación de ISO9660, y en muchos aspectos exactamente igual al mismo, permite nombres largos de archivos y una estructura de carpetas substancialmente muy profunda.
UDF	Este formato permite leer, escribir o modificar los archivos contenidos en discos CD/DVD re escribibles (RW) del mismo modo que se hace en el disco duro, memorias USB o diskettes.

Tabla No 4: Tipos de Sistemas de ficheros

METODOLOGÍA DE LA INVESTIGACIÓN

Para llevar a cabo una investigación, es necesario contar con una metodología a seguir. A continuación se presenta la información referente a la metodología de investigación a ser utilizada.

✓ Definición de metodología de investigación:

La investigación científica se puede definir como un tipo de investigación sistemática, controlada, empírica y crítica, de proposiciones hipotéticas sobre las presumidas relaciones entre fenómenos naturales.

La investigación cuenta con las siguientes características:

- Es **sistemática** y **controlada,** dado que es una disciplina constante para hacer investigaciones científicas y que no se dejan los hechos a la casualidad.
- **Empírica**, significa que se basa en fenómenos observables de la realidad.
- **Crítica** quiere decir que se juzga constantemente de manera objetiva y se eliminan las preferencias personales y los juicios de valor.

✓ Propósito de la investigación:

La investigación cumple dos propósitos fundamentales:

1. Producir conocimiento y teorías (investigación básica).
2. Resolver problemas prácticos (investigación aplicada).

✓ Etapas del proceso de investigación:

El proceso de investigación a utilizar sigue los pasos presentados a continuación en la **Figura No. 4**:

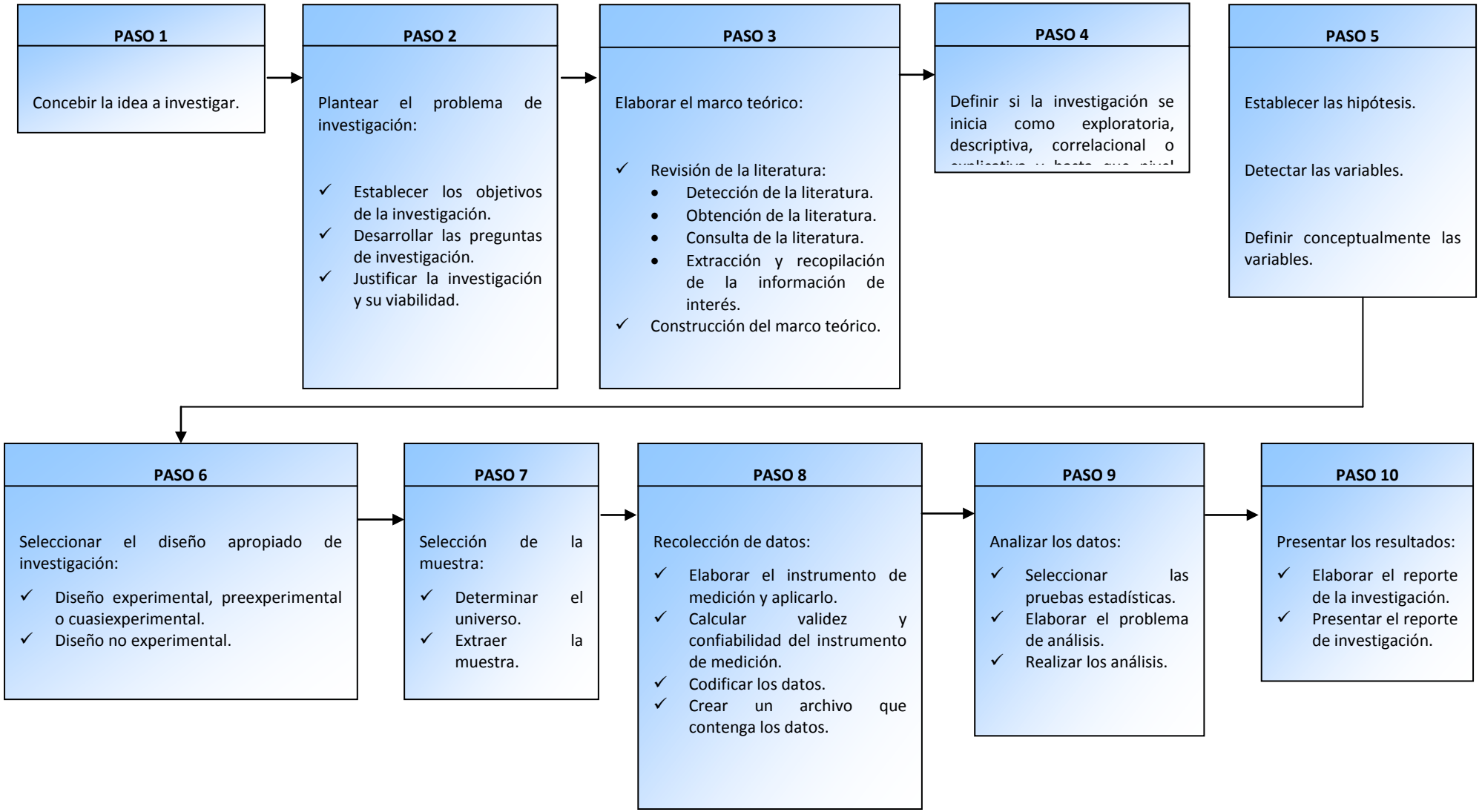

Figura No. 4: Etapas del proceso de investigación[14]

[14] Sampieri,R.H., Fernandez-Collado, C. Baptista Lucio, P. 2006. Metodología de la Investigación. 4ta. Edición McGraw-Hill Interamericana, Pags. XXII, XXIII

- ✓ **Planteamiento del problema:**

Plantear el problema de investigación no es más que afinar y estructurar más formalmente la idea de investigación. Esto se realiza con el objetivo de saber que información se debe recolectar, por qué métodos y como se analizarán los datos que obtenga.

Para plantear adecuadamente un problema se deben tomar en cuenta los siguientes criterios:

1. El problema debe expresarse como una relación entre dos o más variables.
2. El problema debe estar formulado claramente y sin ambigüedad en forma de pregunta.
3. El planteamiento del problema implica la probabilidad de prueba empírica. Es decir, que las variables que se relación deben estar sujetas a observación en la realidad.

Los elementos para plantear un problema son tres y están relacionados entre sí. Estos elementos son:

1. **Objetivos de la investigación:** Se pretende definir qué fines persigue la investigación. Estos fines pueden ser desde resolver un problema hasta comprobar una teoría. Los objetivos deben expresarse con claridad y ser susceptibles de alcance, además se deben tener presente durante todo el desarrollo de la investigación y deben ser congruentes entre sí.
2. **Preguntas de la investigación:** Pretende plantear a través de preguntas el problema que se estudiará. Las preguntas de investigación deben ser expresadas de tal forma que sean concretas y delimiten el problema en estudio.
3. **Justificación del estudio:** Sirve para justificar cuales son las razones que motivan el estudio. El propósito de una investigación debe ser lo suficientemente fuerte para que se justifique la realización.

- ✓ **Fuentes de información:**

Para la elaboración del marco teórico se deben conocer las fuentes de información a tomar en cuenta. Se describen tres tipos de fuentes de información:

1. **Fuentes primarias.** Constituyen el objetivo de la investigación; del cual se obtiene información de primera mano, en esta se contemplan las personas entrevistadas y encuestadas, además investigaciones previas referentes al tema, como tesis monografías o artículos científicos.
2. **Fuentes secundarias.** Entre estos están los resúmenes de algunas publicaciones y listados de referencias publicadas en un área de conocimiento particular en el caso del presente proyecto referentes a la Informática forense y sus herramientas de software.
3. **Fuentes terciarias.** Se trata de documentos que compendian nombres y títulos de revistas y otras publicaciones periódicas. Son útiles para detectar fuentes no documentales como organizaciones que realizan o apoyan estudios o miembros de asociaciones científicas.

✓ **Tipos de investigación:**

Es necesario definir qué tipo de investigación debemos realizar dado que de esta depende la estrategia de la investigación. El diseño, los datos que se recolectan, la manera de obtenerlos, el muestreo y otros componentes del proceso de investigación son diferentes en cada uno de los tipos de investigación. A continuación se detallan los tipos de investigaciones que se pueden realizar así como sus alcances.

Se pueden definir que existen cuatro tipos de investigaciones:

1. Exploratorios.
2. Descriptivos.
3. Correlacionales.
4. Explicativos.

La elección del tipo de estudio a realizar depende principalmente de dos factores: El estado del conocimiento en el tema de investigación que nos revele la investigación de la literatura y el enfoque que el investigador le pretenda dar a su estudio.

✓ **Formulación de Hipótesis:**

Hipótesis.

Son guías que nos permiten llegar hacia el problema de investigación o fenómeno que estamos estudiando. En una investigación se puede tener una, dos, tres, n hipótesis e incluso puede haber ninguna hipótesis. Las hipótesis pueden definirse como explicaciones tentativas del fenómeno investigado formuladas a manera de proposiciones y que se apoyan en conocimientos organizados y sistematizados. Se debe tomar en cuenta que la hipótesis no necesariamente son verdaderas, de lo único que se puede estar seguro es que una hipótesis representa una explicación tentativa, no lo hechos en sí.

Características de una hipótesis.

Para que una hipótesis sea digna de tomarse en cuenta, debe reunir los siguientes requisitos:

- La hipótesis debe referirse a una situación real, dado que las hipótesis solo pueden ser sometidas a prueba en un universo y contexto bien definido.
- Los términos (variables) de la hipótesis tienen que ser compresibles, precisos y lo más concretos posibles.
- La relación entre variables propuestas por una hipótesis debe ser clara y lógica. Se debe describir claramente como están relacionadas las variables y que esta relación no sea ilógica.
- Los términos de la hipótesis y la relación planteada entre ellos deben poder ser observados y medibles, o sea ser referentes en la realidad.
- La hipótesis deben estar relacionadas con técnicas disponibles para probarlas. Al establecer hipótesis debemos analizar si existen técnicas o herramientas de la investigación (instrumentos para recolectar datos, diseños, análisis estadísticos o cualitativos, etc.) para poder verificarla, si es posible desarrollarlas y si se encuentran a nuestro alcance.

Tipos de hipótesis.

Las hipótesis se pueden clasificar en cuatro tipos, los cuales son:

1. **Hipótesis de investigación:** son proposiciones tentativas acerca de las posibles relaciones entro dos o más variables que cumplen con los requisitos anteriormente mencionados. Se simbolizan con $\mathbf{H_i}$ donde i es un número entero positivo.
2. **Hipótesis nulas**: son, en un sentido, el reverso de las hipótesis de investigación. También constituyen proposiciones acerca de la relación entre variables solamente que sirven para refutar o negar lo que afirma la hipótesis de investigación. Se simbolizan con $\mathbf{H_o}$.
3. **Hipótesis alternativas:** son posibilidades alternativas ante la hipótesis de investigación y nula. Ofrecen otra descripción o explicación distintas a las que proporcionan estos tipos de hipótesis. Se simbolizan con $\mathbf{H_a}$ y solo pueden formularse cuando efectivamente hay otras posibilidades adicionales a las hipótesis de investigación y nula.
4. **Hipótesis estadísticas.** Las hipótesis estadísticas son la transformación de las hipótesis de investigación, nulas y alternativas en símbolos estadísticas. Se pueden formular solamente cuando los datos del estudio que se van a recolectar y analizar para aprobar o desaprobar las hipótesis son cuantitativos.

Pruebas de hipótesis.

Como se ha mencionado anteriormente, la hipótesis científicas se someten a prueba para determinar si son apoyadas o refutadas de acuerdo a lo que el investigador observa. No se puede probar que una hipótesis sea verdadera o falsa, sino argumentar que de acuerdo con ciertos datos obtenidos en una investigación particular, fue a poyada o no. Desde el punto de vista técnico no se acepta una hipótesis o través de un estudio, sino que se aporta evidencia a su favor o en contra. Las hipótesis se someten a prueba en la realidad mediante la aplicación de un diseño de investigación, recolectando datos a través de uno o varios instrumentos de medición y analizando e interpretando dichos datos.

Utilidad de las hipótesis.

La utilidad de las hipótesis se resume en los cuatro puntos siguientes:

1. **Son las guías de una investigación.** El formularlas nos ayuda a saber que estamos tratando de probar o buscar. Proporcionan orden y lógica al estudio.
2. **Tienen una función descriptiva y explicativa.** Cada vez que una hipótesis recibe evidencia empírica en su favor o en contra, nos dice algo acerca del fenómeno al cual está asociado o hace referencia.
3. **Prueba teorías** si se aporta evidencia a favor de una.
4. **Sugiere teorías.** Algunas hipótesis no están asociadas con teoría alguna; pero puede ocurrir que como resultado de la prueba de una hipótesis, se pueda construir una teoría o las bases para ésta.

- ✓ **Diseño de la investigación:**

Una vez se han definido el tipo de investigación que se desea realizar y se han establecido las hipótesis de investigación o los lineamientos para la investigación, se debe concebir la manera práctica y concreta de responder a las preguntas de investigación. Esto implica seleccionar o desarrollar un diseño de investigación y aplicarlo al contexto particular de estudio. En el diseño de la investigación se propone la idea o el plan para responder a las preguntas de investigación. Es de recalcar que si el diseño de la investigación está bien concebido, los resultados tienen más probabilidades de ser validos.

La selección del tipo de diseño dependerá de los objetivos que se hayan trazado, las preguntas planteadas, el tipo de estudio a realizar y las hipótesis formuladas.

- ✓ **Muestreo:**

Con la determinación de la muestra de estudio se pretende conocer quiénes son los sujetos de medición, lo cual depende directamente del planteamiento de la investigación. Para seleccionar una muestra, lo primero que se debe hacer es definir una unidad de análisis. El quienes van a ser medidos depende de precisar claramente el problema a investigar y los objetivos de la investigación. Para poder tomar una muestra es necesario delimitar la población.

Una vez se han definido cual será nuestra unidad de análisis, se procede a delimitar la población que va a ser estudiada y sobre la cual se pretende generalizar los resultados. Una población se define como el conjunto de todos los casos que concuerdan con una serie de especificaciones. La muestra suele ser tomada como un subgrupo de la población. Para seleccionar la muestra es necesario delimitar las características de la población para definir cuáles serán los parámetros muéstrales.

- ✓ **Selección de muestra:**

Una vez se ha definido cual será la unidad de análisis, debemos definir que muestra utilizaremos. Se puede definir que las muestras se pueden clasificar en dos ramas:

1. **Muestras no probabilísticas:** la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características del investigador o del que hace la muestra.
2. **Muestras probabilísticas**, donde todos los elementos de la población tienen la misma posibilidad de ser escogidos. Dentro de este tipo de muestreo se encuentran: Muestreo aleatorio simple, Muestreo aleatorio sistemático, Muestreo estratificado, Muestreo por conglomerados

La elección del tipo de muestra depende de los objetivos del estudio, del esquema de investigación y de la contribución que se piensa hacer con dicho estudio.

Determinar el tamaño de la muestra es muy importante, dado que tenemos que definir cuantos elementos de estudio o unidades de análisis tenemos que tomar para asegurar que el error estándar sea aceptable. Para determinar el tamaño de la muestra (n) nos auxiliaremos de la siguiente fórmula:

$$n = \frac{Z^2 * P * Q * N}{(N-1) * e^2 + Z^2 * P * Q}.$$

Donde:

n: Número de personas a encuestar.

Z: Coeficiente de confianza de la investigación.

P: Probabilidad de éxito de ocurrencia de un evento.

Q: Probabilidad de rechazo (Q = 1-P)

N: Población

e: Error muestra máximo permitido.

Luego de haber determinado la muestra a estudiar tenemos que elegir cuales de esos elementos totales (universo) se elegirán para ser analizados. Las unidades de análisis o elementos muéstrales se eligen siempre aleatoriamente para asegurarnos que cada elemento tenga la misma probabilidad de ser elegidos.

✓ **Recolección de datos:**

Recolectar los datos implica tres actividades estrechamente relacionadas entre sí:

- **Seleccionar un instrumento de medición** o desarrollar uno. Este instrumento debe ser válido y confiable, de lo contrario no podemos basarnos en sus resultados.
- **Aplicar este instrumento de medición.**
- **Analizar las mediciones obtenidas.**

Un instrumento de medición debe cumplir con dos requisitos: ser confiable y ser válido. La confiabilidad se refiere al grado en que su aplicación repetida al mismo sujeto u objeto produce iguales resultados. La validez de un instrumento de medición se refiere al grado en que un instrumento realmente mide la variable que pretende medir.

✓ **Construcción de los instrumentos de medición:**

Para construir un instrumento de medición se pueden seguir los siguientes pasos.

1. Listar las variables que se pretenden medir u observar.
2. Revisar su definición conceptual y comprender su significado.
3. Revisar como han sido definidas operacionalmente las variables, es decir como se ha medido cada variable.

4. Elegir o desarrollar el instrumento o instrumentos de medición o recopilación de datos asegurándose de que sean válidos y confiables.
5. Indicar la manera como se habrán de codificar los datos en cada ítem y variable. Codificar los datos significa asignarles un valor numérico que los represente. Es decir, a las categorías de cada ítem y variable se les asignan valores numéricos que tienen un significado.
6. Aplicar una prueba "piloto" del instrumento de medición. Es decir, se aplica a personas con características semejantes a las de la muestra o población objeto de la investigación. En esta prueba se analiza si las instrucciones se comprenden y si los ítems funciona adecuadamente.
7. Realizar las modificaciones, ajustes o mejoras si las hay, de los resultados obtenidos de la aplicación piloto.

- ✓ **Análisis de datos:**

Una vez se hayan codificado y transferidos a una matriz, asi como guardados en un archivo, se procede al análisis de datos. Para estas tareas, se puede auxiliar de una computadora y más cuando el volumen de datos a analizar es considerable.

El análisis a practicar depende de tres factores:

a. El nivel de medición de las variables.
b. La manera como se hayan formulado las hipótesis.
c. El interés del investigador.

Usualmente se busca describir los datos para posteriormente realizar el análisis estadístico para relacionar las variables. Este tipo de análisis se denomina estadística descriptiva para cada una de sus variables y luego describe la relación entre estas.

En este análisis la primera tarea es describir los datos, valores o puntuaciones obtenidas para cada variable. Para describir los datos se hace uso de las distribución de frecuencias o puntuaciones, medidas de tendencia central y medidas de variabilidad.

II. MARCO REFERENCIAL

En este apartado se presenta la teoría que ha sido obtenida mediante la consulta a investigaciones similares, seleccionando las partes relevantes y que sirven como apoyo en la realización del presente trabajo de investigación.

En el documento "INFORMÁTICA FORENSE: GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS[15]" se presenta la siguiente clasificación de las herramientas de informática forense:

[15] Autores: Óscar López, Haver Amaya, Ricardo León, Beatriz Acosta. Universidad de Los Andes, Bogotá, Colombia.

HERRAMIENTAS DE INFORMÁTICA FORENSE

Existen varios tipos básicos de herramientas, no todas sirven para todo, algunos están diseñadas para tareas muy especificas y más aún, diseñados para trabajar sobre ambientes muy específicos, como un determinado sistema operativo.

Siendo la recolección de evidencia una de las tareas más críticas, donde asegurar la integridad de esta es fundamental, es necesario establecer ese nivel de integridad esperado, pues algunas herramientas no permiten asegurar que la evidencia recogida corresponda exactamente a la original. Igual de importante es que durante la recolección de la evidencia se mantenga inalterada la escena del "crimen" Son todas estas consideraciones que se deben tener en cuenta a la hora de seleccionar una herramienta para este tipo de actividad.

En este parte se presenta una clasificación que agrupa en cuatro los tipos de herramientas de computación forense:

- ✓ **Herramientas para la recolección de evidencia:**

Las herramientas para la recolección de evidencia representan el tipo de herramienta más importante en la computación forense, porque su centro de acción está en el que es su punto central. Su uso es necesario por varias razones:

- Gran volumen de datos que almacenan los computadores actuales.
- Variedad de formatos de archivos, los cuales pueden variar enormemente, aún dentro del contexto de un mismo sistema operativo.
- Necesidad de recopilar la información de una manera exacta, que permita verificar que la copia es fiel y además mantener inalterada la escena del delito.
- Limitaciones de tiempo para analizar toda la información.
- Volatilidad de la información almacenada en los computadores, alta vulnerabilidad al borrado, con una sola información se pueden eliminar hasta varios gigabytes.
- Empleo de mecanismos de encriptación, o de contraseñas.
- Diferentes medios de almacenamiento, como discos duros, CDs y cintas.

Por esto mismo, las herramientas de recolección de evidencia deben reunir características que permitan manejar estos aspectos, pero además incluir facilidades para el análisis.

A continuación se presentan las principales facilidades de recolección y análisis que se esperaría de una buena herramienta, para lo cual se siguió como guía las que ofrecen EnCase de Guidance Software y la familia de productos Image Master de Law Enforcement & Comp. Forensic:

- Dispositivos que permitan copiado a una alta velocidad y de diferentes medios, claro, limitado eso si por el medio original de los datos, esto brindando diferentes tipos de dispositivos como cables paralelos, seriales, USB, etc.
- Asegurar un copiado sin pérdida de datos y que corresponde a una copia fiel.
- Copia comprimida de discos origen para facilitar el manejo y conservación de grandes volúmenes de información.
- Búsqueda y análisis de múltiples partes de archivos adquiridos. Debe permitir la búsqueda y análisis de múltiples partes de la evidencia en forma paralela en diferentes medios como discos duros, discos extraíbles, discos "zip" CDs y otros.

- Capacidad de almacenamiento en varios medios: También es necesario poder almacenar la información recabada en diferentes medios, como discos duros IDE o SCSI, drives ZIP, y Jazz. Uno de los medios ideales son los CD-ROM pues contribuyen a mantener intacta la integridad forense de los archivos.
- Variables de ordenamiento y búsqueda: debe permitir el ordenamiento y búsqueda de los archivos de la evidencia de acuerdo con diferentes campos, incluyendo campos como las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos, extensiones y propiedades.
- Capacidad para visualización de archivos en diferentes formatos, además de galerías de archivos gráficos.
- Capacidad para representar en forma gráfica estructuras de datos, archivos, volúmenes, directorios, árboles, organización y en general tópicos de interés que faciliten el trabajo de análisis.
- Búsqueda automática y análisis de archivos de tipo Zip, Cab, Rar, Arj y en general formatos comprimidos, así como archivos adjuntos de correos electrónicos.
- Identificación y análisis de firmas de archivos, es decir aquellos bytes que generalmente se encuentran al comienzo de un archivo y están directamente relacionadas con el tipo de este y por consiguiente con su extensión. Con la capacidad de análisis de firmas es posible detectar si un archivo fue renombrado, pues el solo cambio de su extensión para hacerlo aparecer de otro tipo, no genera cambios en su firma.
- Análisis electrónico del rastro de intervención. Facilidades para recuperar de manera eficiente y no invasiva información critica como sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento.
- Soporte de múltiples sistemas de archivo. Una herramienta de recopilación de evidencia debe estar en capacidad de recuperar información de diversos sistemas de archivos; DOS, Windows (todas las versiones), Macintosh (MFS, HFS, HFS+), Linux, UNIX (Sun, Open BSD), CD-ROM, y los sistemas de archivos DVDR. Esta es la limitación de algunas herramientas, pues está diseñadas para un número limitado de sistemas de archivos o es necesario adquirir módulos aparte, lo que incrementa su costo.
- Captura y manejo automático de cualquier sistema operativo: reconocimiento automático del sistema operativo origen, haciendo cero invasiva la extracción de la información y asegurando la más alta fidelidad.
- Vista de archivos y otros datos en el espacio unallocated: Una buena herramienta deberá proveer facilidades para tener una vista del disco duro de origen, de los archivos borrados y todos los datos en el espacio unallocated, el espacio ocupado por el archivo dentro del cluster, archivos Swap y Print Spooler, todo esto de manera gráfica.
- Recuperación de passwords: en muchas ocasiones la información recuperada puede estar protegida con passwords por lo que será necesario descifrarlos. Generalmente esta facilidad no viene incluida en estas herramientas, se deben comprar a parte.
- Herramientas de gestión; por último una herramienta debería incluir facilidades de gestión para el manejo mismo de los expedientes y reportes de las investigaciones.

Existen otros productos tradicionales cuyo objetivo primordial no es la computación forense, pero por incluir herramientas para la recuperación de archivos, en ocasiones pueden ser útiles, aunque la integridad de la evidencia recabada a través de estas herramientas podría estar más expuesta y su valor probatorio podría ser menor que el de evidencias obtenidas a través de herramientas

altamente especializadas que garantizan la veracidad de la evidencia. Ejemplo típico de herramientas no propiamente forenses es Norton Systemworks y Norton Utilities.

- ✓ **Herramientas para el monitoreo y/o control de computadores:**

Si se requiere conocer el uso de los computadores es necesario contar con herramientas que los monitoreen para recolectar información. Existen herramientas que permiten recolectar desde las pulsaciones de teclado hasta imágenes de las pantallas que son visualizadas por los usuarios y otras donde las máquinas son controladas remotamente.

Algunas veces se necesita información sobre el uso de los computadores, por lo tanto existen herramientas que monitorean el uso de los computadores para poder recolectar información Existen algunos programas simples como *key loggers* o recolectores de pulsaciones del teclado que guardan información sobre las teclas que son presionadas.

Estas herramientas pueden ser útiles cuando se quiere comprobar actividad sospechosa ya que guardan los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de 'retroceder', esto es guardado en un archivo o enviado por e-mail. Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

Existen otras que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente. Es importante tener en cuenta que herramientas de este tipo han llegado a ser usadas con fines fraudulentos (captura de claves de los clientes en cafés Internet u otros sitios públicos).

- ✓ **Herramientas de marcado de documentos:**

El objetivo de este tipo de herramientas es el de insertar una marca a la información sensible para poder detectar el robo o tráfico con la misma, si bien no equivale al sistema LoJack de rastreo y localización de vehículos hurtados, si podría compararse con las marcas que se hace a los vehículos. A través de estas herramientas es posible marcar no solo documentos, sino software también.

- ✓ **Herramientas de Hardware:**

El proceso de recolección de evidencia debe ser lo menos invasivo posible con el objetivo de no modificar la información. Esto ha dado origen al desarrollo de herramientas que incluyen dispositivos como conectores, unidades de grabación, etc.

Asimismo, debido a la vulnerabilidad de la copia y modificación de los documentos almacenados en archivos magnéticos, los investigadores deben revisar con frecuencia que sus copias son exactas a las del disco del sospechoso y para esto utilizan varias tecnologías como *checksums* o Hash MD5.

CAPÍTULO II

DISEÑO DE LA INVESTIGACIÓN

CAPÍTULO II: DISEÑO DE LA INVESTIGACIÓN

En este capítulo se definen cada una de las etapas que conforman el diseño de la investigación a realizar acerca de las herramientas de software utilizadas en la informática forense en El Salvador. Además se expondrán los criterios que son tomados en cuenta al momento de realizar la selección del tipo de estudio a desarrollar.

A. CLASE DE INVESTIGACIÓN A REALIZAR

Según el carácter de una investigación científica, esta puede ser catalogada en cuatro clases[16]:

- ✓ Investigaciones exploratorias[17]: se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes.

- ✓ Investigaciones descriptivas[18]: los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis. Se selecciona una serie de cuestiones y se mide cada una de ellas independientemente, para así describir lo que se investiga.

- ✓ Investigaciones correlacionales[19]: tienen como propósito medir el grado de relación entre dos o más conceptos o variables.

- ✓ Investigaciones explicativas[20]: van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre los conceptos; están dirigidos a responder a las causas de los eventos físicos o sociales.

Luego de analizar las diferentes clases presentadas se ha decidido realizar una investigación esencialmente de **carácter correlacional**, en este caso en particular se busca conocer en qué forma está relacionada la aplicación y uso de las herramientas de software para la informática forense con la validez dada a la evidencia digital obtenida.

Luego en base a observaciones sobre fenómenos y características de poblaciones seleccionadas se buscará realizar una **descripción** que nos permita establecer la situación actual, por ejemplo el nivel de enseñanza de las herramientas de software para la informática forense, cuales son las más utilizadas por los peritos, cuales son los delitos más comunes que se persiguen, etc. En base a toda la información que se pueda reunir es que se establecerá la correlación existente entre las variables mencionadas anteriormente. Luego en base a su respectivo análisis se tratará de **explicar**

[16] Sampieri, R.H., Fernández-Collado, C. Baptista Lucio, P. 2006. Metodología de la Investigación. 4ta. Ed. McGraw-Hill Interamericana, pág. 57
[17] Sampieri, R.H. Op. cit., pág. 59
[18] Sampieri, R.H. Op. cit., pág. 60
[19] Sampieri, R.H. Op. cit., pág. 63
[20] Sampieri, R.H. Op. cit., pág. 66

la relación identificada; si por ejemplo, el uso de las herramientas no influye en la validez de la evidencia digital ante los aplicadores de la justicia en El Salvador, conocer cuáles son las causas que originan esta situación.

B. TIPO DE DISEÑO DE LA INVESTIGACIÓN

Con el objetivo de responder a las preguntas de investigación establecidas y poder realizar la comprobación de las hipótesis formuladas es necesario establecer un diseño específico de investigación, este puede ser:

- ✓ Diseño experimental: le esencia de este tipo de diseño es la concepción de experimentos, lo cual requiere una manipulación intencional de la variable independiente para analizar los posibles resultados sobre la variable dependiente.

- ✓ Diseño no experimental: es observar fenómenos tal como se dan en su contexto natural, para después analizarlos, en este tipo de investigación no es posible manipular las variables en estudio.

En el caso del presente estudio su diseño es **no experimental,** ya que sus características son las que más se apegan al objetivo de la investigación, el cual es el de analizar la relación existente entre el uso de las herramientas para la informática forense (variable independiente) y la validez de la evidencia digital que permita la resolución de los delitos (variable dependiente), esto se hará realizando observaciones sobre las variables en su ambiente natural sin llevar a cabo ninguna alteración intencional. No existirá una manipulación de la variable independiente ya que no se tiene un control directo sobre ella ni sobre sus efectos.

A su vez, el diseño no experimental se puede clasificar en:

- ✓ Diseño no experimental transeccional o transversal: recolectan datos es un solo momento. Su propósito es describir variables y analizar su incidencia e interrelación en un momento dado.

Diseño no experimental longitudinal: realizan observaciones en dos o más momentos o puntos en el tiempo con el fin de realizar inferencias con respecto al cambio.

Las observaciones a realizar sobre las distintas poblaciones seleccionadas se efectuarán en un solo momento del tiempo por lo que es un **tipo transeccional**.

El diseño transeccional se subdivide en: exploratorios, descriptivos y en correlacionales/causales.

- ✓ Exploratorios: su finalidad es la de comenzar a conocer la situación de una población o conjunto de variables.
- ✓ Descriptivos: tienen como objetivo indagar las incidencias y los valores en que se manifiesta una o más variables.
- ✓ Correlacionales/Causales: su objetivo es describir relaciones entre dos o más variables en un momento determinado. Dichas descripciones no son de las variables individuales sino que son sobre sus relaciones.

El diseño de la investigación en un momento inicial es exploratorio, ya que se realiza un estudio previo que tiene como objetivo conocer la situación actual de las herramientas de software para la informática forense y de esta forma identificar la situación problemática y las poblaciones a tomar en cuenta por su interacción con el objeto de estudio.

Luego se realizará una descripción de las variables y las poblaciones seleccionadas, en este caso en particular se recopilara información acerca de los peritos informáticos y sobre las instituciones de educación superior, ambas relacionadas con la aplicación de las herramientas de software para la informática forense. Con respecto a la evidencia digital, se obtendrá información sobre esta variable en el sector legal, que es el que la utiliza con el fin de resolver los delitos informáticos.

Además, será un diseño correlacional ya que se estudiaran dos variables y se determinará la relación existente entre ellas, conocer en qué manera una correcta aplicación de las herramientas influye en la validez de la evidencia digital que es utilizada por el sector legal para la resolución de delitos informáticos.

El diseño de la investigación puede ser presentado en forma resumida en la siguiente figura:

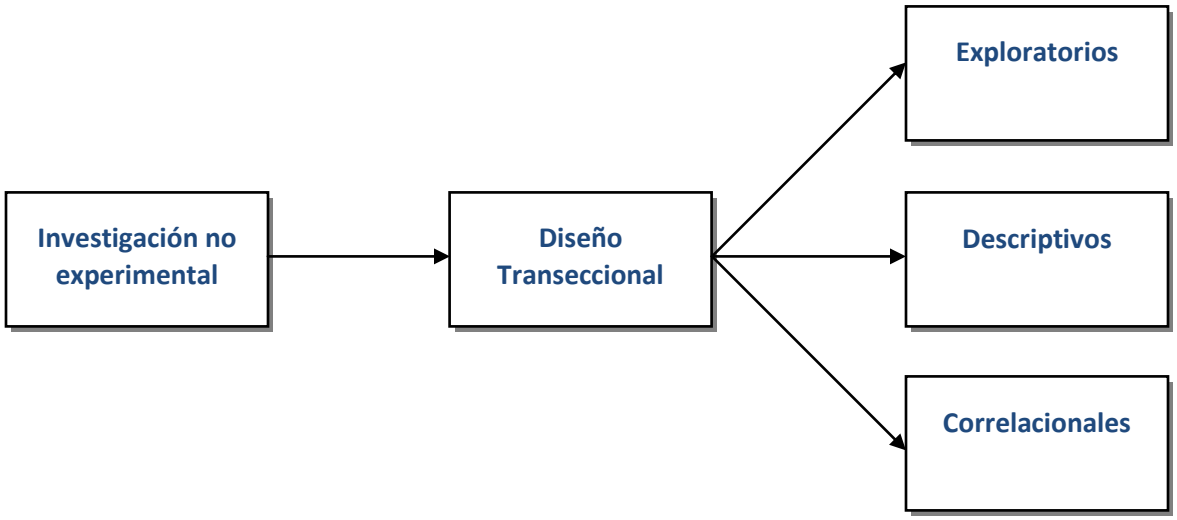

Figura No. 5: Diseño de la investigación.

C. FASES DE LA INVESTIGACIÓN

Con el objetivo de mostrar de manera gráfica la secuencia con la que se llevarán a cabo cada uno de los pasos de la investigación, se presenta la siguiente figura:

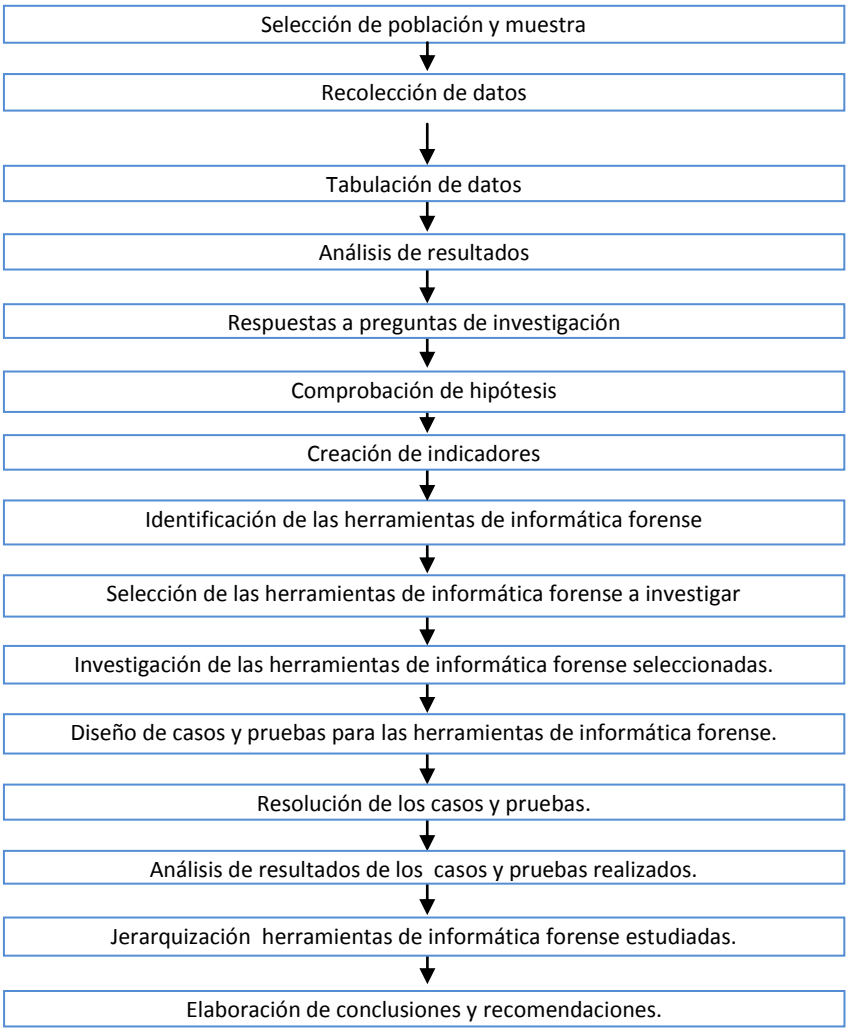

Figura No. 6: Diagrama de flujo del diseño de la investigación

I. SELECCIÓN DE POBLACIÓN Y MUESTRA

Identificación de población de interés

El primer paso para realizar la investigación, consiste en definir las unidades de análisis o sectores sobre los cuales se realizará la recolección de datos delimitando de esta forma la población a ser estudiada.

Se han identificado 3 tipos de poblaciones a tomar en cuenta por su interacción con el objeto de estudio. Dichos sectores son el educativo, legal y el profesional.

Selección de población por sector

Después de identificar los sectores de interés, se seleccionaran dentro de ellos poblaciones más específicas realizando de esta forma una estratificación que tendrá como objetivo la identificación de sus respectivas características.

Dicha identificación da como resultado la siguiente clasificación:

- ✓ ***Sector Educativo:*** la población en estudio dentro de este sector estará formada por catedráticos que imparten materias en las carreras relacionadas con la informática en 12 universidades en el área metropolitana de San Salvador.
- ✓ ***Sector Legal:*** estará conformado por jueces, dependencias operativas jurídicas de la Fiscalía General de la República y abogados defensores de Procuraduría General de la República.
- ✓ ***Sector Profesional:*** formado por los profesionales encargados de la aplicación de las herramientas de software para la informática forense en El Salvador.

Selección del tipo de muestra

Se establece el tipo de muestreo a realizar en las poblaciones previamente seleccionadas. En la tabla presentada a continuación se expone de forma resumida los principales tipos de muestreo y su descripción:

TIPO DE MUESTREO	DESCRIPCIÓN
Diseños probabilísticos	Todos los elementos de la población tienen igual probabilidad de ser tomados en cuenta.
Diseños no probabilísticos o determinísticos.	Están basados en el juicio personal del investigador.

Tabla No 5: Tipos de diseños muéstrales

El principal objetivo del diseño del muestreo es el de poder realizar una selección de una muestra que sea representativa de la población que se desea investigar y de esta forma garantizar la obtención de una cantidad de información suficiente que permita llevar a cabo un análisis de calidad.

Con el fin de cumplir el objetivo anterior, se utilizará una combinación de los dos tipos de muestreos, el criterio de selección del tipo para cada población en especifico será expuesta en el momento de la definición de la muestra.

Selección de muestra de interés por cada uno de los sectores a estudiar

Luego de haber definido el tipo de muestreo a utilizar, se procederá a obtener la muestra representativa de las poblaciones que están ubicadas dentro de cada uno de los tres sectores identificados, los cuales son: educativo, legal y profesional.

II. RECOLECCIÓN DE DATOS

Se refiere al uso de una serie de técnicas y herramientas que pueden ser utilizadas por los investigadores con el fin de buscar y recolectar datos que serán de gran utilidad para cumplir con los objetivos de la investigación.

Diseño de instrumentos de recolección de datos

En este paso se elaborarán los instrumentos mediante los cuales se obtendrán los datos de las muestras de cada población a ser estudiada, además se determinan las variables que serán medidas con dicho mecanismo.

Para el desarrollo del presente trabajo se ha seleccionado la encuesta como la herramienta de recolección de datos a ser aplicada. Este tipo de instrumento permite al investigador recopilar datos que están relacionados con los objetivos de la investigación y de esta forma obtener información necesaria para poder probar o rechazar las hipótesis.

Además se han tomado en cuenta las siguientes ventajas:

- ✓ Recolección en un breve tiempo de información acerca de grupos numerosos.
- ✓ La persona que lo responde proporciona datos sobre sí mismo o sobre situaciones dadas.
- ✓ Puede ser llenado con facilidad y requiere poco tiempo.
- ✓ La tabulación y su análisis se facilitan, en especial ya que las mayorías de las repuestas serán cerradas.

Validación de instrumentos de recolección

Después de la creación de los instrumentos, se verificará que estos se encuentren bien diseñados a través de:

- ✓ Cálculo de la validez. La validez de una encuesta se refiere a lo que mide y a cómo lo mide. Los cuestionarios se diseñan para unos propósitos concretos y, por lo tanto, no existe el cuestionario perfecto para cuantificar cualquier aspecto. Así, no podemos hablar de la validez de un cuestionario en términos generales, diciendo que su validez es alta o baja en abstracto, sino que ésta se determinará respecto al objetivo específico para el que fue diseñado

- ✓ La confiabilidad de los instrumentos de datos se refieren al grado en que la aplicación repetida al mismo sujeto produce los mismos resultados.

Distribución de los instrumentos de recolección a cada una de las poblaciones identificadas

En este procedimiento se designará que tipo de instrumento de recolección de datos se implementará, dependiendo si es el sector educativo, legal o profesional; a que se esté enfocando.

Luego de distribuir los instrumentos de recolección de datos a su correspondiente sector de interés, se llevará a cabo su implementación por parte de los investigadores.

III. TABULACIÓN DE DATOS

La tabulación de datos se considera como el primer paso del análisis, en esta tapa los datos obtenidos en la recolección son ordenados y agrupados, de esta forma se convirtiéndolos en información, la cual es fundamental para poder lleva a cabo el análisis sobre una situación o fenómeno.

En muchos casos la agrupación y ordenamiento de los datos no es suficiente para poder llevar a cabo la lectura y análisis de los mismos, es por esto que se han desarrollado una serie de métodos para realizar y presentar la tabulación, entre estos tenemos: representaciones tabulares, representaciones gráficas y representaciones mixtas.

La presente investigación hará uso de las **representaciones mixtas**, en un primer momento los datos serán ordenados según características o criterios en forma de filas y columnas mediante la utilización de tablas presentando la información susceptible de cuantificación numérica en forma concreta, breve, ordenada y de fácil comprensión. Luego en base a las tablas se realizará una representación gráfica de los mismos que tienen como objetivo presentar en una forma más atractiva y expresiva los datos tabulados, además resulta útil al momento de llevar a cabo comparaciones.

Validación de los datos

Se realizará una filtración de los datos recolectados para descartar información incorrecta, que no corresponda al sector de donde se obtuvo o que no tenga relación con los objetivos de la investigación.

Organizar las mediciones obtenidas

Se ordenarán los datos recolectados, identificando y organizando variables tanto cualitativas como cuantitativas.

Conteo y procesamiento de los datos

Luego de ordenar y validar los datos recolectados, se procederá a estructurar la información.

Representación gráfica de los datos

Una vez estructurada la información se representará por medio de gráficos estadísticos.

Se utilizará una codificación definida previamente para el proceso de tabulación y presentada en el diseño de los instrumentos de recolección de datos. Se realizará la tabulación en hojas electrónicas de Microsoft Excel 2007 y se generarán los respectivos gráficos que representen los resultados de dichas tabulaciones.

IV. ANÁLISIS DE RESULTADOS

Con la información procesada, se realizará su análisis de la siguiente forma:

- ✓ Análisis para cada población que conforman cada sector.
- ✓ Análisis por cada sector investigado.

V. RESPUESTAS A PREGUNTAS DE INVESTIGACIÓN

Después del análisis de los resultados, se responderán las preguntas de investigación realizadas para los sectores educativo, legal y profesional, como también a dichos sectores en conjunto.

Las preguntas a las que se les buscará solución en base a los análisis realizados son:

Para la comunidad Educativa:

- ✓ ¿Cuentan las instituciones de educación superior con personal para enseñar herramientas de informática forense?
- ✓ ¿Qué factores son los que impiden o facilitan la enseñanza de la informática forense y sus herramientas como disciplina?
- ✓ ¿Qué factores influyen para que las instituciones de educación superior no brinden conocimientos relacionados con la informática forense y las herramientas de software que se utilizan?

Para el sector Legal:

- ✓ ¿Existe un marco legal que soporte la utilización de herramientas de informática forense?

Para el sector Profesional:

- ✓ ¿Cuáles son las herramientas de informática forense que se utilizan en El Salvador?
- ✓ ¿Cuál es el nivel de uso de las herramientas de informática forense en El Salvador?
- ✓ ¿Cómo se clasifican las herramientas de informática forense son utilizadas en El Salvador?
- ✓ ¿Qué nivel de incidencia tiene las herramientas de informática forense en la resolución de delitos informáticos?
- ✓ ¿Cómo ayudan las herramientas de informática forense a obtener evidencia digital confiable?
- ✓ ¿Tiene el recurso humano el suficiente conocimiento en la aplicación de las herramientas de informática forense?

Para todos los sectores:

- ✓ ¿Qué factores afectan el nivel de uso de las herramientas de informática forense, tanto positiva como negativamente?
- ✓ ¿Se cuenta con el recurso humano, tecnológico, financiero, educativo para hacer del uso de las herramientas de informática forense una disciplina difundida?
- ✓ ¿Qué ventajas o desventajas trae la utilización de herramientas de software en la informática forense a las personas o instituciones que las utilizan?

VI. COMPROBACIÓN DE HIPÓTESIS

La comprobación sirve para poner a prueba las afirmaciones realizadas en las hipótesis planteadas, esta prueba se realizará utilizando la información obtenida a través de una investigación, mediante dicho resultado podemos llegar a refutar o aceptar la hipótesis del estudio.

Entre los métodos para la prueba de hipótesis podemos mencionar:

- ✓ Prueba de hipótesis de proporciones para una sola muestra.
- ✓ Prueba de Hipótesis para Diferencias entre Dos Proporciones (muestras independientes).
- ✓ Prueba Chi-Cuadrado.

Prueba estadística chi cuadrado

Para la prueba de hipótesis se utilizará la prueba estadística chi cuadrado. Este tipo de prueba es utilizada cuando la información con la que se trabaja es de carácter no-métrico nominal.

Es una prueba estadística no paramétrica para diferencias entre dos o más muestras donde frecuencias esperadas son comparadas en relación con frecuencias obtenidas.

Elaboración de conclusiones

A partir del análisis de la información y la formulación de las hipótesis, se realizarán las pertinentes conclusiones de lo realizado.

Específicamente, se elaboran conclusiones con respecto a la investigación hecha y conclusiones de la etapa a ser entregada.

VII. CREACIÓN DE INDICADORES

a) ***Declaración de variables del estudio:*** Se definirán cuales son las variables que intervienen en la investigación.
b) ***Selección de indicadores:*** Se seleccionará que tipo de indicadores se elaborarán.
c) ***Criterios de evaluación de indicadores seleccionados:*** Se definirán los criterios para la evaluación de los indicadores seleccionados.
d) ***Definición de indicadores seleccionados:*** Se detallarán las especificaciones de los indicadores a desarrollar.
e) ***Construcción de indicadores:*** Luego de definir los indicadores a desarrollar se procederá a construirlos.
f) ***Presentación de indicadores:*** Se presentarán los indicadores elaborados.

VIII. IDENTIFICACIÓN DE LAS HERRAMIENTAS DE INFORMÁTICA FORENSE

Se identificarán los tipos de herramientas de informática forense que existen con el objetivo de determinar cuáles herramientas serán objetos de estudio. Para este proceso se realizaran los siguientes pasos:

a) ***Selección de los tipos de herramientas:*** se seleccionaran basados en las funciones que realizan dentro del proceso del análisis forense. Se tomaran en cuenta los resultados obtenidos en el transcurso de la investigación para incluir de esta forma los utilizados por los peritos informáticos en El Salvador.

b) ***Identificación de las herramientas:*** una vez establecidas las categorías, se realizará una investigación previa con el fin de conocer las herramientas de software existentes en dicha categoría. Para poder identificar la mayor cantidad de herramientas para informática forense que existen, se tomará en cuenta tanto las que actualmente están en el mercado y son de código propietario, como también las herramientas de software libre que se encuentran disponibles.

Este proceso tiene como objetivo empezar el análisis en base a las herramientas que en la actualidad son más utilizadas en El Salvador, ya sea en el sector educativo para su enseñanza o en el sector profesional, específicamente en la obtención de la evidencia digital.

IX. SELECCIÓN DE LAS HERRAMIENTAS DE INFORMATICA FORENSE A ESTUDIAR

Después de identificar las diferentes herramientas de software para la informática forense que se encuentran catalogadas en las categorías identificados, se seleccionarán específicamente las que serán estudiadas. Para ello, se llevaran a cabo los siguientes pasos:

a) ***Establecimiento de criterios de selección:*** se definirán una serie de criterios para ser utilizados en la selección final de las herramientas que serán investigadas.

b) ***Verificación del cumplimiento de los criterios:*** se realizará un análisis en el que se verificara si las herramientas identificadas cumplen o no con los criterios establecidos.

c) ***Selección de las herramientas de software a estudiar:*** concluido el análisis, dentro de cada categoría serán escogidas las herramientas que cumplen con la mayor cantidad de los criterios establecidos.

Al concluir esta fase de la investigación, se espera haber seleccionado al menos 4 herramientas de software para la informática forense por cada categoría identificada previamente.

X. INVESTIGACIÓN DE LAS HERRAMIENTAS DE SOFTWARE SELECCIONADAS

Con las herramientas de informática forense seleccionadas, se realizará una investigación de todas las características y capacidades que poseen cada una de ellas. Para ello se recopilara información bibliográfica de distintas fuentes, entre las que podemos mencionar: sitios web, estudios previos, etc.

Los resultados obtenidos en esta etapa de investigación serán utilizados para la elaboración de los siguientes productos:

a) ***Fichas técnicas:*** para cada herramienta estudiada se elaborara una ficha técnica resumen, en la que serán presentadas las principales características de las mismas.

b) **Manuales de instalación:** se creará un manual para cada herramienta en el que se detallaran los pasos necesarios para poder llevar a cabo su respectiva instalación.

c) **Manual de uso:** se diseñara un manual en el que se describen los pasos necesarios para que el usuario pueda hacer uso de las funciones principales de las herramientas que han sido estudiadas.

Esta fase de la investigación requerirá la realización de una serie de pruebas de cada una de las herramientas con el objetivo de conocer de forma directa cada una de sus funcionalidades.

XI. DISEÑO DE CASOS Y PRUEBAS

Se elaborarán escenarios para recrear posibles delitos informáticos, donde puedan ser utilizadas las herramientas de informática forense investigadas. Para la realización de esta fase, se llevaran a cabo los siguientes pasos:

a) ***Identificación de los delitos informáticos:*** en base a los resultados obtenidos por los instrumentos de recolección de datos, se identificaran y seleccionaran los delitos informáticos más comunes y que afectan de una manera más significativa a la sociedad salvadoreña.

b) ***Creación de los escenarios***: una vez seleccionados los delitos informáticos, se establecerán las características de los escenarios a recrear, definiendo por ejemplo el tipo de dispositivo a utilizar, la modificación de archivos con el fin de ocultar su contenido, eliminación de información comprometedora de los medios de almacenamiento, etc.

Estas pruebas tienen como objetivo emular los casos y condiciones a las que se enfrentan los peritos informáticos para poder llevar a cabo los análisis de informática forense.

XII. RESOLUCIÓN DE LOS CASOS Y PRUEBAS

Se hará uso de las herramientas de software para informática forense con la finalidad de demostrar sus capacidades en la resolución de las pruebas diseñadas anteriormente.

Mediante la utilización del tipo de herramientas de software para informática forense adecuadas para la resolución de las pruebas diseñadas, se buscará la manera de aprovechar las características conocidas que posee cada herramienta y encontrar nuevas funcionalidades en la práctica.

XIII. ANALISIS DE RESULTADOS DE CASOS Y PRUEBAS REALIZADAS

Se analizarán los resultados obtenidos de la utilización de las herramientas de software para informática forense en la resolución de las pruebas realizadas anteriormente.

En este punto se organizará la información obtenida con las herramientas de software para informática forense que fueron empleadas y además se realizará el análisis del procedimiento llevado a cabo para la obtención de la evidencia digital.

XIV. JERARQUIZACIÓN DE LAS HERRAMIENTAS DE SOFTWARE ESTUDIADAS

Se realizará dentro de cada categoría una jerarquización de las herramientas de software para la informática forense que han sido estudiadas. Este proceso se llevara a cabo mediante la implementación del método de puntos ponderados, realizando los siguientes pasos:

a) Definición de los criterios que serán utilizados para llevar a cabo el análisis por medio de puntos ponderados.

b) Para cada herramienta se llevara a cabo una ponderación para cada uno de los criterios definidos y seleccionados.

c) Dentro de cada categoría las herramientas serán jerarquizadas dependiendo del puntaje obtenido por medio del análisis de puntos ponderados.

En base a esta jerarquización podremos afirmar, en base a un puntaje total, cuales son las herramientas idóneas a utilizar dentro de cada categoría identificada. Se hará uso del método de puntos ponderados ya que éste nos proporcionara de un valor cuantificable y medible que nos permitirá ordenar, según su desempeño y características, a las herramientas estudiadas.

XV. ELABORACIÓN DE CONCLUSIONES Y RECOMENDACIONES

En base a los objetivos de la investigación, se elaborarán una serie de conclusiones y recomendaciones con respecto a todo lo desarrollado durante el transcurso de la investigación. Estas conclusiones y recomendaciones estarán sustentadas en los análisis realizados a los datos recolectados en cada uno de los sectores que han sido objeto de estudio.

D. CRONOGRAMA DE ACTIVIDADES

En este apartado se presenta el cronograma de actividades y evaluaciones elaborado para el desarrollo de la INVESTIGACIÓN DE LAS HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE EN EL SALVADOR.

I. CRONOGRAMA ANTEPROYECTO: DEFINICIÓN Y DISEÑO DE LA INVESTIGACIÓN

II. CRONOGRAMA ETAPA I: RECOLECCIÓN, TABULACIÓN Y ANÁLISIS DE DATOS

III. CRONOGRAMA ETAPA II: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL Y ESTUDIO DE LAS HERRAMIENTAS

IV. CRONOGRAMA CONSOLIDADO

E. PLANIFICACIÓN DE LOS RECURSOS

En esta sección se encuentran definidos los recursos involucrados en el desarrollo de la investigación y que representan un costo para su realización. Dichos elementos se detallan a continuación:

I. RECURSO HUMANO

Con respecto al recurso humano involucrado en el desarrollo de esta investigación, se cuenta con la participación de cuatro integrantes que conforman el equipo de trabajo. En base a esto, se realizó la estimación del salario que percibiría cada integrante partiendo del supuesto que cada miembro está contratado a medio tiempo, debido a que la jornada de trabajo para el desarrollo de la investigación está compuesta por cuatro horas diarias y cinco días a la semana. Por tanto, la jornada de trabajo considerada, se comprende de lunes a viernes, y el tiempo para el desarrollo de la investigación será de ocho meses, iniciando en el mes de marzo y finalizando en octubre.

Entonces, el salario diario individual se calcula tomando como base $ 780.95, de acuerdo a los resultados presentados en la Encuesta de Hogares de Propósitos Múltiples 2008[21]. A continuación se muestra el cálculo del costo para una hora de trabajo en base al salario antes mencionado:

Salario diario de cada integrante: $780.95 / 30 días = ***$26.03/ día***

1 día = 8 horas de trabajo $226.03 / 8 horas de trabajo = ***$3.25 / hora de trabajo***

Por tanto el costo para una hora de trabajo es $3.25

Pero para este caso, se ha considerado que la jornada laboral de cada integrante está compuesta de cuatro horas diarias, por tanto el costo total del recurso humano se muestra a continuación:

Total de horas trabajadas por día = 4

4 x $23.25 / hora de trabajo = ***$ 13.00 / hora de trabajo***

Costo de salario en un día de trabajo = $ 13.00

RECURSO	SALARIO DIARIO	# DE INTEGRANTES	TOTAL
Integrante de grupo de trabajo	$ 13.00	4	$ 52.00

Tabla No 6: Cálculo del costo diario total incurrido en recurso humano

Total salario mensual	=	Total salario diario	x	20 días laborales de cada mes

[21] Ministerio de Economía, Dirección General de Estadística y Censos. Grandes grupos ocupacionales acorde a "CLASIFICACION INTERNACIONAL UNIFORME DE OCUPACIONES, 1988 (CIUO-88)".

	=	$ 52.00	x	20 días / mes
	=	**$ 1,040.00 mensuales**		

Total de costos	=	Total de salario	X	8 meses
	=	$ 1,040.00	X	8
	=	**$ 8,320.00**		

II. RECURSO TECNOLÓGICO

A continuación se presentan en la siguiente tabla el costo del equipo informático a utilizar para el desarrollo de la investigación:

EQUIPO DE COMPUTO	CARACTERÍSTICAS	PRECIO[22]
1 computadora de Escritorio	• Procesador Intel Celeron D 2.13 Ghz • 512 MB memoria RAM • Quemador de DVD 20X • Disco Duro 250 GB • Lector de Tarjetas de Memoria	$ 360.00
1 Computadora de Escritorio	• Procesador AMD Duron 1.0 Ghz • 256 MB memoria RAM • Disco Duro 40 GB • Quemador de DVD 16X	$ 255.00
1 Computador de Escritorio	• Procesador Pentium III 500 Mhz • Disco Duro 8 GB • 128 MB memoria RAM • CD ROM 24X	$ 130.00
1 Computadora Laptop	• Procesador Athlon X2 64 1.9 Ghz • Disco Duro 250 GB • 3 GB Memoria RAM • Quemador de DVD 8X	$ 1,000.00
	TOTAL	**$ 1,745.00**

Tabla No 7: Costo de recurso de equipo informático

[22] Precio de referencia tomado con respecto a COMPUFERIA SA de CV.

En la siguiente tabla se detallan los costos de otros recursos tecnológicos a ser usados en la presente investigación:

OTROS RECURSOS	CARACTERÍSTICAS	CANTIDAD	PRECIO	TOTAL
Impresor	Canon IP1900	1	$35.00	$ 35.00
Disco Duro IDE	Seagate 30 GB	1	$15.00	$ 15.00
Enclosure	Nspire IDE P/Desktop	1	$40.00	$ 40.00
Memorias Flash	Kingston 2 GB	4	$10.00	$ 40.00
Hub	D-Link	1	$20.00	$ 20.00
Licencias de software	Windows Vista	1	$160.00	$ 160.00
Cámara digital	Minolta 3.2 MP	1	$100.00	$ 100.00
Memorias SD	Kingston 1 GB	2	$9.50	$ 19.00
UPS	Centra 750VA	1	$45.00	$ 45.00
Regulador de voltaje	AVTEK 500VA	1	$10.00	$ 10.00
			TOTAL	**$ 484.00**

Tabla No 8: Costo de otros recursos tecnológicos

III. RECURSOS CONSUMIBLES[24]

Costos de papelería

Los costos de papelería se basan en una estimación realizada sobre la cantidad de papel a utilizar para cada etapa del proyecto de investigación.

DOCUMENTO	CANTIDAD DE PÁGINAS	NUMERO DE EJEMPLARES	TOTAL (PÁGS.)
Anteproyecto	75	3	225
Etapa I	250	3	750
Etapa II	200	3	600
Edición final	525	3	1,200
Entrega de avances	1,250	-	1,250
		TOTAL	**4,025**

Tabla No 9: Costo de papelería

[23] Precio en base a TECNOSERVICE, sucursal Roosevelt.
[24] Precios de referencia tomados de OfficeDepot.

Total de páginas a utilizar: 4,025 págs. / 500 págs. = 8.05, aproximadamente 8 resmas de papel bond

Costo total de papelería = Cantidad de resmas x Precio individual de resma de papel bond

Costo total de papelería = 8 x $ 5.00 = **$ 40.00.**

Costo de anillado y empastado

A continuación se presenta la tabla que contiene el detalle de los costos correspondientes a este apartado:

ETAPA	EMPASTADO	ANILLADO	COSTO UNITARIO	COSTO TOTAL
Anteproyecto		3	$2.40	$7.20
Etapa I		3	$3.00	$9.00
Etapa II		3	$3.00	$9.00
Proyecto Completo	3		$9.50	$28.50
			TOTAL	**$53.70**

Tabla No 10: Costo de anillado y empastado

Costos de impresiones

El costo de impresiones se estimó basándose en los precios de los cartuchos de tinta y el papel. En el caso del impresor utilizado, un Canon IP1900, el cartucho de tinta negro cuesta $ 20.00 y el cartucho a color $ 26.00; por tanto el valor de una impresión individual se estima de la siguiente manera:

Cantidad de páginas impresas por cartucho: 400, en base a un cartucho de tinta negro, debido a que el cartucho de tinta a color se combina con el de tinta negra y su uso es poco frecuente.

Costo de una impresión = Costo de cartucho de tinta / Cantidad de páginas por cartucho

Costo de una impresión = $ 20.00 / 400 pág. = $ 0.05/pág.

Costo total de impresión = Cantidad de hojas a imprimir X Costo de una impresión

= 4,025 X $ 0.05

= **$ 201.25**

Costos de CD / DVD

1 torre de 50 DVD's en blanco $ 18.00

1 torre de 50 CD's en blanco $ 14.00

Costo total = $ 32.00

Marcadores, bolígrafos, cuadernos, etc.

Costo promedio aproximado entre todos los artículos = **$ 10.00**

Total en recursos consumibles

Costo total = Costo total de papelería + Costo total de anillado y empastado +Costo total de impresión + Costo total de CD y DVD + Costo de Marcadores, bolígrafos y cuadernos.

Costo Total= $ 40.00 + $ 53.70 + $ 201.25 + $ 32.00 + $ 10.00 = $ 336.95

IV. RECURSOS DE OPERACIONES

A continuación se presenta el detalle de los costos de operaciones necesarios para la realización de la investigación planteada:

Costo mensual de energía eléctrica

APARATO	CONSUMO EN KW[25]	HORAS DE USO AL MES	TOTAL KWH USADOS
1 Computador Intel	0.525	80	42
1 Computador AMD Duron	0.450	80	36
1 Computador Pentium III	0.350	80	28
1 Monitor CRT 14'' LG	0.075	80	6
1 Monitor CRT Compaq	0.075	80	6
1 Monitor CRT AOC 14''	0.075	80	6
1 Laptop	0.065	80	5.2
1 UPS	0.072	80	5.76
2 Lámparas	0.080	80	6.4
1 Impresor IP1900	0.084	12	1.008
		Total	**142.368**

Tabla No 11: Total de KWh utilizados en el mes

[25] Especificaciones técnicas que se encuentran detalladas en cada aparato

De acuerdo a los publicados[26] de la empresa distribuidora CAESS y la SIGET los costos por el consumo entre 100 y 199 KWh, son los siguientes:

Valores constantes que se aplican a la tarifa:

Cargo de distribución $ 0.040401/KWh x Total de KWh utilizados

Cargo de comercialización $0.813324

Cargo de energía $ 0.153730/KWh x Total de KWh utilizados

Aplicando los valores al total de KWh utilizados:

Cargo de distribución 142.368 KWh x $ 0.040401/KWh = $ 5.751809568

Cargo de comercialización $0.813324

Cargo de energía 142.368 KWh x $ 0.153730/KWh = $ 21.88623264

Costo mensual de energía eléctrica = $ 5.751809568+$0.813324+$ 21.88623264

= $ 28.451366208, aproximadamente $ 28.45

Costo total de energía eléctrica durante 8 meses del proyecto de investigación:

8 meses x $28.45/mes= $ 227.60

Costo de telefonía celular

RECURSO	TIPO DE SERVICIO	COSTO MENSUAL
1 Teléfono celular	Post-pago	$13.59
1 Teléfono celular	Post-pago	$12.12
2 Teléfonos celulares	Pre-pago	$20.00
	Total	$45.71

Tabla No 12: Costo mensual de telefonía celular

Costo total de telefonía celular = Costo mensual de celulares x 8 meses de la investigación

Costo total de telefonía celular = $ 45.71 x 8 = $ 365.68

[26] Pliegos tarifarios vigentes, http://www.siget.gob.sv

Servicio de Internet

El costo de servicio de Internet tiene un costo mensual de $ 28.25 para una conexión de 512kbps, y durante los 8 meses de la investigación asciende a **$ 226.00.**

Alquiler local

El costo de alquiler del lugar de trabajo es de $ 80.00 mensual, y hace un total de **$ 640.00** en los 8 meses que se utilizará para desarrollar el proyecto de investigación.

Pasaje / Gasolina

El grupo de trabajo cuenta con dos vehículos para transportarse, y en la semana de trabajo se gasta un promedio de $ 10.00 por vehículo, haciendo un total de $ 80.00 en el mes entre ambos. En cuanto a gasto por transporte colectivo se tiene un promedio diario de $2.40, lo cual hace un monto de $ 48.00, al multiplicarlo por los 20 días laborales que se trabajan por mes. Por tanto, los costos de transporte considerando precios de pasajes y gasolina equivalen a $ 128.00 mensuales, y hacen un total de **$ 1,024.00** durante los 8 meses en que se desarrollará el proyecto de investigación.

En la tabla que se presenta a continuación se hace un resumen de los gastos de operación y se muestra el consolidado total del mismo:

COSTO	TOTAL
Costo total de energía eléctrica	$ 227.60
Costo total de telefonía celular	$ 365.68
Costo total de servicio de agua	$ 52.40
Costo total de servicio de Internet	$ 226.00
Costo total de alquiler de local	$ 640.00
Costo total de pasaje y gasolina	$ 1,024.00
Total de recursos de operación	**$ 2,535.68**

Tabla No 13: Total en recursos de operación

V. TOTAL DE LA INVERSIÓN

A continuación se presenta el resumen total de los costos de los recursos a ser usados durante la investigación:

COSTO	TOTAL
Costo total de recurso humano	$ 8,320.00
Costo total de recursos tecnológicos	$2,229.00
Costo total de recursos consumibles	$ 336.95
Costo total de recursos de operaciones	$ 2,535.68
Costo total del proyecto de investigación	**$ 13,421.63**
Imprevistos[27] (10%)[28]	**$ 1,342.16**

Tabla No 14: Costo total de recursos

Costo total del proyecto de investigación = $ 14,763.79

[27] Dentro de los imprevistos están considerados gastos extra que se puedan presentar en recursos consumibles.

[28] Factores ponderables que pueden incrementar los estimados, libro: Gerencia Informática, Quinta Edición.

CAPÍTULO III

RECOLECCIÓN, TABULACIÓN Y ANÁLISIS DE DATOS

CAPÍTULO III: RECOLECCIÓN, TABULACIÓN Y ANÁLISIS DE DATOS

A. SELECCIÓN DE POBLACIÓN Y MUESTRA

Con el objetivo de conocer el nivel de uso de las herramientas de software para la informática forense en El Salvador y tomando en cuenta los elementos de la problemática identificados en la formulación del problema, la investigación a realizar será enfocada a los sectores mencionados a continuación:

I. SECTOR LEGAL

Un sector de importancia para poder cumplir los objetivos de la investigación. Los operadores de justicia en El Salvador son los que utilizan de forma directa la evidencia digital, ya sea para probar la existencia de los delitos informáticos o en caso contrario utilizarlas como elementos de descargo en los procesos judiciales. Además, identificar el nivel de conocimiento que tienen acerca de la informática forense y sus herramientas de software.

JUECES

Una de las poblaciones más importantes al hablar de la validez de la evidencia digital la constituyen los jueces que son los que al final toman la decisión de aceptar como válida o no la evidencia digital presentada en los casos de delitos informáticos y que es obtenida mediante la aplicación de las herramientas de informática forense.

- ✓ **Población:**

El sector que se estableció para estudiar el fenómeno de las herramientas de informáticas forenses es el total de jueces titulares de los 46 juzgados de instrucción de El Salvador.

En la fase de instrucción es donde se presentan las pruebas para acusar al imputado por la Fiscalía. En los Juzgados de Instrucción es donde se lleva a cabo el proceso legal donde los actores principales son los fiscales, abogados defensores y el juez. Además es en estos juzgados donde se presentan las evidencias recabadas por la Fiscalía y la Policía Nacional, es decir la evidencia digital.

- ✓ **Muestra Poblacional:**

La muestra poblacional es de tipo probabilístico con un nivel de confianza del 95% y ha sido calculada utilizando la siguiente fórmula:

$$n= \frac{Z^2*P*Q*N}{(N-1)*e^2+Z^2*P*Q}.$$

Donde:

n: Número de personas a encuestar.

Z: Coeficiente de confianza de la investigación.

P: Probabilidad de éxito de ocurrencia de un evento.

Q: Probabilidad de rechazo (Q = 1-P)

N: Población

e: Error muestra máximo permitido.

Se tomara en cuenta un nivel de confianza del 95%, y por tanto, 5% de error, **(Ver Anexo 5)** dando así un valor de **Z = 1.96**.

El valor para z de 1.96 fue obtenido de la siguiente manera:

En el anexo 5 se presenta la tabla de aéreas bajo la curva normal tipificada de 0 a Z. Esta tabla permite determinar el nivel de confianza y el coeficiente de confiabilidad en una muestra. Tenemos que recordar que la tabla de distribución de la curva normal tipificada es simétrica.

La primera columna de la tabla contiene los valores para z en cuanto a unidades y décimas. La primera fila contiene los valores para z en centésimas. El valor de z estaría dado por la suma del valor de la columna y el de la fila donde se encuentre el valor buscado.

Por tanto, para encontrar el valor de z en la tabla se siguieron los siguientes pasos:

- Se utilizó el valor del nivel de confianza de **95 %** o lo que es lo mismo **0.9500**. Este nivel de confianza es el que se utiliza principalmente en las investigaciones sociales.
- La tabla del anexo presenta solo valores para la mitad de la curva aprovechando la propiedad de simetría de la distribución; por tanto, el valor de **0.9500** (nivel de confianza) debe ser dividido en 2 dando el valor de **0.4750**.
- Buscamos este valor en la tabla de distribución normal tipificada.
- El valor de Z estaría dado por el punto donde se interseca la columna y la fila para nuestro valor de 0.4750. Esta intersección ocurre donde Z tienen el valor de **1.9** para la primera columna y 6 (centésimas) para la primera fila. **El valor de z es por tanto 1.9 + 0.06 = 1.96.**

Para la probabilidad de éxito y de rechazo, se tiene igual probabilidad de ser aceptado o rechazado **p = 0.5, q=0.5** por que q = 1-0.5 = 0.5. Es decir existe la posibilidad de que acepten responder a la encuesta o que se abstengan de hacerlo.

Una vez establecidos los valores necesarios en la formula se procede a la determinación del tamaño de la muestra que se utilizara, la cual será de:

$$n= \frac{(1.96^2*0.5*0.5*46)}{\{(46-1)*0.05^2\}+\{1.96^2*0.5*0.5\}}.$$

n= 41.177

Por lo que el total de jueces titulares de juzgados de instrucción encuestados fue de 42 según lo indica el tamaño de la muestra.

FISCALÍA GENERAL DE LA REPÚBLICA

La Fiscalía General es parte del Ministerio Público y es independiente de los demás órganos del estado. La PNC y los organismos de seguridad pública obedecerán las órdenes e instrucciones bajo el concepto de dirección funcional impartidas por la FGR para la investigación de hechos punibles.

La FGR tiene como misión, según el artículo 2 de su ley orgánica "defender los intereses del Estado y de la sociedad; dirigir la investigación de los hechos punibles y los que determinen la participación punible; promover y ejercer en forma exclusiva la acción penal pública, de conformidad con la ley; y desempeñar todas las demás atribuciones que el ordenamiento jurídico les asigne a ella y/o a su titular".

- ✓ **Población:**

La FGR cuenta con dependencias operativas jurídicas que les ayudan a realizar su trabajo. Estas unidades especializadas son las unidades a las que corresponde investigar y tramitar los casos en materia de hechos punibles de crimen organizado, lavado de dinero y activos, de corrupción, de narcotráfico, entre otros de relevante complejidad o trascendencia nacional y /o internacional. Las unidades clasificadas como especializadas responden directamente ante el Fiscal General de la República y estas comprenden las Unidades de Investigación Financiera, delitos de Crimen Organizado, de Extorsión, de Corrupción, de Narcotráfico, de Tráfico de Personas y de Hurto y robo de Automotores y otros. Las dependencias operativas jurídicas identificadas son las siguientes:

- Direcciones de la Defensa de los Interés es de la Sociedad, tendrán a su cargo la dirección y coordinación de la investigación de los hechos punibles en la zona geográfica de su competencia, a fin de promover y ejercer la acción penal pública, la acción penal previa instancia particular.
- Dirección de la Defensa de los Intereses del Estado: Tiene competencia a nivel nacional, tiene a su cargo el ejercicio de la defensa de los intereses del Estado representándolo en toda clase de juicios.

- Oficinas Fiscales: Realizan la gestión operativa fiscal en ámbitos geográficos concretos, además con responsabilidades y funciones administrativas.
- Departamentos o Unidades Operativas o de Investigación Son las unidades a las que corresponde desarrollar la labor fiscal, investigar y tramitar los hechos punibles y otras infracciones a la ley. Las unidades operativas son: Delitos relativos a la Vida e Integridad Física, a Menores un su relación Familiar, al Patrimonio Privado y Propiedad Intelectual, Administración de Justicia, Penal Juvenil, Hurto y Robo de Vehículos, Medio Ambiente, Vigilancia Penitenciaria, Recepción de Denuncias, Criminalística, Penal del Estado, Civil, de Impuestos, Control de Bienes del Estado y de Juicios de Cuentas y Multas.

✓ **Muestra Poblacional:**

A esta población también se le aplicó un muestreo determinístico dirigido o intencional, al visitar la Fiscalía General de la República y debido a la disponibilidad del tiempo de los fiscales para llenar la encuesta se tomó la decisión de tomar una muestra de 20 fiscales ente las diferentes áreas de sus unidades operativas descritas con anterioridad.

PROCURADURÍA GENERAL DE LA REPÚBLICA

La Procuraduría General de la República (PGR) tiene como misión "Proporcionar gratuitamente los Servicios de Mediación, Asistencia Legal y Preventivo Psicosocial a todas las personas que lo soliciten, con el fin de asegurarles el ejercicio de sus Derechos". La PGR es una Institución que forma parte del Ministerio Público, de carácter permanente e independiente, con personalidad jurídica y autonomía administrativa y que para efectos de la prestación de los servicios cuenta con procuradurías auxiliares en todo el país. Corresponde a la Procuraduría General de la República, promover y atender con equidad de género la defensa de la familia, de las personas e intereses de los menores, incapaces y adultos mayores; conceder asistencia legal, atención psicosocial de carácter preventivo y servicios de mediación y conciliación; representar judicial y extrajudicialmente a las personas, especialmente de escasos recursos económicos en defensa de la libertad individual, de los derechos laborales, de familia y derechos reales y personales.

- ✓ **Población:**

La población a tomar en cuenta serán los abogados que trabajan en la PGR, debido a la función que esta tiene. La distribución de los defensores en El Salvador se muestra en la siguiente tabla:

DEPARTAMENTO	NÚMERO DE DEFENSORES
Ahuachapán	14
Santa Ana	29
Sonsonate	17
Chalatenango	11
La Libertad	29
San Salvador	127
Cuscatlán	11
La Paz	13
Cabañas	9
San Vicente	11
Usulután	14
San Miguel	25
Morazán	11
La Unión	10
TOTAL	**331**

Tabla No 15: Distribución de abogados defensores

- ✓ **Muestra Poblacional:**

La muestra poblacional que será utilizada para el desarrollo del estudio de las herramientas de informática forense es el total de abogados defensores, es decir **331**. Con este número de abogados procederemos a establecer la muestra para recabar los datos del estudio.

En este caso en específico el muestreo es aleatorio simple tomando en cuenta niveles de confianza de las Z, ya que cada uno de los 331 defensores que conforman la población a ser estudiada tiene la misma probabilidad de ser considerados como parte de la muestra.

La fórmula para determinar el tamaño de la muestra será la siguiente:

$$n= \frac{Z^2*P*Q*N}{(N-1)*e^2+Z^2*P*Q}.$$

Donde:

- n: Número de personas a encuestar.
- Z: Coeficiente de confianza de la investigación.
- P: Probabilidad de éxito de ocurrencia de un evento.
- Q: Probabilidad de rechazo (Q = 1-P).
- N: Población.
- e: Error muestra máximo permitido.

Se tomara en cuenta un nivel de confianza del 95%, y por tanto, 5% de error, **(Ver Anexo 5)** dando así un valor de **Z = 1.96.** Debido a que el nivel de confianza tomado es el que se acostumbra utilizar en las investigaciones sociales.

Para la probabilidad de éxito y de rechazo, se tiene igual probabilidad de ser aceptado o rechazado **p = 0.5, q=0.5** por que q = 1-0.5 = 0.5. Es decir existe la posibilidad de que acepten responder a la encuesta o que se abstengan de hacerlo.

Una vez establecidos los valores necesarios en la formula se procede a la determinación del tamaño de la muestra que se utilizara, la cual será de:

$$n= \frac{(1.96^2*0.5*0.5*331)}{\{(331-1)*0.05^2\}+\{1.96^2*0.5*0.5\}}.$$

n= 178.05

El valor de la muestra a tomar es de 178 abogados. Esto representa el número mínimo de abogados que debemos encuestar para garantizar la confiabilidad de los datos. Debido a factores como el costo en el que se incurriría a la hora pasar las encuestas, se ha decidido tomar en cuenta los abogados pertenecientes a los departamentos de San Salvador, Libertad y Santa Ana donde se concentran la mayoría de abogados, totalizando **184 abogados** los cuales serán utilizados para obtener la información.

A continuación se presenta una tabla resumen con cada una de las muestras calculadas para cada población perteneciente al sector legal y sujeta a investigación.

No.	SECTOR	N CALCULADO	N APROXIMADO
1	Jueces	41.177	**42**
2	Abogados	178.05	**184**
3	Fiscales	20	**20**
4	Docentes Universidad El Salvador	30	**30**
5	Docentes universidades privadas	94.498	**95**
6	Peritos informáticos	12	**12**
		TOTAL	**383**

Tabla No 16: Resumen del tamaño de las muestras calculadas para cada sector

II. SECTOR EDUCATIVO

Dentro del sector educativo hemos contemplado el total de universidades en El Salvador que imparten carreras relacionadas al área informática, es importante tomarlas en cuenta ya que dentro de ellas se brindan los conocimientos a los profesionales que desarrollan sus actividades en dicha área en el país.

UNIVERSIDADES

- ✓ **Población:**

Se seleccionaron 16 universidades privadas y la Universidad de El Salvador las cuales imparten carreras a nivel de Licenciatura o Ingeniería en el área Informática.

Se ha tomado esta población para realizar la recolección de información correspondiente al nivel de conocimiento y aplicación de las herramientas de software utilizadas en la informática forense y saber si existe la necesidad y la intención por parte de las mismas de capacitar a los futuros profesionales en esta área.

Es importante que el sector educativo tenga desarrollo en todas las aplicaciones de las TICs las cuales incluyen inexorablemente la Informática forense y las herramientas de Software en las que esta se apoya para la obtención de evidencia digital.

- ✓ **Muestra Poblacional:**

Para determinar la muestra de la población, se tomará en cuenta a los docentes que imparten materias relacionadas con la informática en cada una de las 16 universidades privadas y la universidad de El Salvador. La determinación de la muestra se realizara de la siguiente manera:

Universidad Pública

Debido a ser la única institución pública de educación superior en el país, se tomará para la muestra a los **30 docentes** que imparten materias en la carrera de Ingeniería de Sistemas Informáticos de la Universidad de El Salvador. Esta muestra no incluirá al docente director y al docente observador de esta investigación.

Universidades Privadas

Para determinar la muestra de docentes las universidades privadas del país, se tomaron en cuenta los docentes de 16 instituciones, ya que en las mismas se imparten carreras relacionadas a la Informática en el país. Para esta parte de la población es necesario conocer la muestra que permitirá recabar los datos necesarios para el estudio en desarrollo, por lo que utilizamos el diseño de Muestreo Aleatorio Simple, el cual permitió el cálculo de la muestra (n), a través de la siguiente fórmula:

$$n = \frac{Z^2 * P * Q * N}{(N-1) * e^2 + Z^2 * P * Q}.$$

Donde:

n: Número de personas a encuestar.

Z: Coeficiente de confianza de la investigación.

P: Probabilidad de éxito de ocurrencia de un evento.

Q: Probabilidad de rechazo (Q = 1-P)

N: Población

e: Error muestra máximo permitido.

La determinación de esta población se realizo de la siguiente manera:

En la tabla No. 16 se muestra las universidades privadas del País en donde imparten carreras informáticas.

No.	UNIVERSIDAD	SIGLAS	CARRERA
1	Universidad Centroamericana José Simeón Cañas	**UCA**	Licenciatura en Ciencias de la Computación
2	Universidad Francisco Gavidia	**UFG**	Ingeniería en Ciencias de la Computación
3	Universidad Tecnológica	**UTEC**	Ingeniería en Sistemas y Computación
4	Universidad Politécnica de El Salvador	**UPES**	Ingeniería en Ciencias de la Computación
5	Universidad Albert Einstein	**UAE**	Ingeniería en Computación
6	Universidad Evangélica de El Salvador	**UEES**	Ingeniería en Sistemas Computacionales
7	Universidad Luterana Salvadoreña	**ULS**	Licenciatura en Ciencias de la Computación
8	Universidad Don Bosco	**UDB**	Ingeniería en Ciencias de la Computación
9	Universidad Cristiana de las Asambleas de Dios	**UCAD**	Ingeniería en Ciencias de la Computación
10	Universidad Dr. Andrés Bello	**UNAB**	Licenciatura en Computación
11	Universidad Salvadoreña Alberto Masferrer	**USAM**	Licenciatura en Ciencias de la Computación
12	Universidad Modular Abierta	**UMA**	Licenciatura en Informática.
13	Universidad Gerardo Barrios	**UGB**	Licenciatura en Computación Ingeniería en Sistemas
14	Universidad de Oriente	**UNIVO**	Ingeniería en Sistemas Informáticos
15	Universidad Católica de El Salvador	**UNICAES**	Ingeniería en Sistemas Informáticos
16	Universidad de Sonsonate	**USO**	Ingeniería en Sistemas Computacionales

Tabla No 17: Universidades privadas de El Salvador con carreras relacionadas a la informática

La tabla No. 17 muestra la cantidad de docentes que imparten materias informáticas en las 16 universidades privadas.

No.	ACRÓNIMO	# DE DOCENTES
1	UCA	11
2	UFG	9
3	UTEC	12
4	UPES	6
5	UAE	7
6	UEES	9
7	ULS	6
8	UDB	14
9	UCAD	9
10	UNAB	7
11	USAM	7
12	UMA	5
13	UGB	7
14	UNIVO	6
15	UNICAES	7
16	USO	3
TOTAL:		**125**

Tabla No 18: Docentes que imparten materias informáticas en las universidades

Dando como resultado:

N= **125** número de docentes que conforman la población total

Se desea que los resultados del estudio sean confiables en el 95% y un error de 5% (e = 5%), por lo que se tomara en cuenta un nivel de confianza del 95% **(Ver Anexo 5)**, dando así un valor Z = 1.96.

Para la probabilidad de éxito y de rechazo, se tiene igual probabilidad de ser aceptado o rechazado **p = 0.5, q=0.5** por que q = 1-0.5 = 0.5. Es decir existe la posibilidad de que acepten responder a la encuesta o que se abstengan de hacerlo.

Una vez establecidos los valores necesarios en la formula se procede a la determinación del tamaño de la muestra que se utilizara, la cual será de:

$$n= \frac{(1.96^2*0.5*0.5*125)}{\{(125-1)*0.05^2\}+\{1.96^2*0.5*0.5\}}.$$

n= **94.498**, aproximadamente 95 docentes el tamaño de la muestra

Es decir que el número de docentes pertenecientes a las Universidad privadas en total a encuestar será de **95**.

En cada universidad, el tamaño de la muestra será de:

n= N de cada universidad* 0.76, que es la proporción entre el total de docentes de universidades privadas y la muestra a ser encuestada.

A continuación se detallan la cantidad de docentes a encuestar en cada universidad:

UNIVERSIDAD	POBLACIÓN	n
UCA	11	9
UFG	9	7
UTEC	12	9
UPES	6	5
UAE	7	5
UEES	9	7
ULS	6	5
UDB	14	11
UCAD	9	7
UNAB	7	6
USAM	7	5
UMA	5	4
UGB	7	5
UNIVO	6	3
UNICAES	7	5
USO	3	2
Total	**125**	**95**

Tabla No 19: Detalle del total de docentes de universidades privadas a encuestar

III. SECTOR PROFESIONAL

En cuanto al sector profesional, se tomó como muestra a profesionales del área de informática, que hayan fungido como peritos en el área de la informática forense y que hayan utilizado herramientas de software teniendo como objetivo el obtener evidencias digitales con el propósito de ser utilizadas por los operadores de la justicia en El Salvador.

PERITOS INFORMÁTICOS

Para poder conocer el nivel de uso que se les da a las herramientas de software para la informática forense en El Salvador es importante recopilar información del sector profesional encargado de su aplicación.

- ✓ **Población:**

En este sentido, la población de peritos informáticos en el país es desconocida ya que al no existir una entidad o academia que se dedique a su formación no se posen datos estadísticos (profesionales graduados o capacitados, cantidad de cursos impartidos por año, etc.) que puedan ser utilizados para determinar el tamaño de la población a investigar.

Sin embargo, el código procesal penal permite que cualquier profesional en informática con conocimientos en la materia pueda actuar como peritos en los procesos legales.

Por este motivo la información será recopilada de distintas fuentes: peritos informáticos independientes que han actuado en distintos procesos penales, peritos de la División técnica científica de la Policía Nacional Civil **(DPTC)** además se contactara a la Asociación de Ciencias Forenses de El Salvador **(ACFES),** organización que aglutina diferentes tipos de peritos forenses.

- ✓ **Muestra Poblacional:**

Debido a las condiciones descritas en el apartado anterior el tipo de muestreo a realizar es un determinístico dirigido o intencional.

La consulta de fuentes en este sector específico se realizará tal como se detalla en la tabla presentada a continuación:

FUENTE	CANTIDAD DE PERITOS
División técnica científica de la Policía Nacional Civil	4 peritos
Peritos independientes	6 peritos
ACFES(Asociación de Ciencias Forenses de El Salvador)	2 peritos

Tabla No 20: Detalles de los peritos a ser consultados

El tamaño total de la muestra será de 12 peritos informáticos para el sector profesional en Informática forense.

B. DISEÑO DE LAS HERRAMIENTAS DE RECOLECCIÓN DE DATOS

Se ha decidido hacer uso de encuestas como la principal herramienta para la recolección de datos. Las preguntas han sido diseñadas con el objetivo de poder obtener datos específicos que permitan a los investigadores poder hacer análisis sobre situaciones o hechos para sacar conclusiones de los mismos.

Se ha elaborado una encuesta para cada uno de los sectores en estudio (legal, educativo y profesional) ya que cada uno de ellos posee características de interés para nuestra investigación.

En general, todas las encuestas están formados por un encabezado, por el objetivo de la realización de la medición (se especifica el objetivo según el sector donde es aplicada), el nombre del proyecto a realizar con su respectiva nota de confidencialidad además de incluir las instrucciones necesarias para su correcta contestación.

Las preguntas diseñadas para cada tipo de encuestas tienen como objetivo principal la recopilación de la mayor cantidad de información que permita la recopilación de la información necesaria para realizar la comprobación de las hipótesis, responder las preguntas de la investigación y el cumplimiento de los objetivos del estudio. Para su elaboración su ha tenido en cuenta la situación problemática descubierta gracias al estudio o investigación exploratoria hecha en la etapa anterior.

La mayor parte de estas preguntas son cerradas, de opción múltiples y en caso de ser necesario se coloca la opción de “otros” seguido por un “especifique”, esto se hace con el fin de obtener respuestas adicionales a las que han sido propuestas.

Además, existen preguntas abiertas que tienen como objetivo recoger opiniones de los encuestados sobre situaciones o temas de interés.

I. DISEÑO DEL INSTRUMENTO RECOLECTOR DE DATOS PARA EL SECTOR LEGAL

El principal objetivo de este instrumento es el de conocer el grado de conocimiento de los elementos incluidos dentro del sector legal (jueces, fiscales, abogados) respecto a la informática forense, sus herramientas y la evidencia digital.

Al estar interesados por conocer la situación actual del uso de las herramientas de software para la informática forense en El Salvador es importante conocer de las opiniones y puntos de vista de los aplicadores de la justicia (los jueces, la parte acusadora representada por la Fiscalía General y la parte defensora representada por la Procuraduría General) ya que son estos los que utilizan el resultado (evidencia digital) obtenido por el uso de dichas herramientas

Consultar el **Anexo #6** para poder ver el formato final del instrumento recolector de datos dirigido al sector legal y el **Anexo #7** para ver la codificación de las respuestas del instrumento utilizado.

A continuación se presentan las preguntas a realizar al sector legal y el objetivo que se pretende con cada una de ellas

Pregunta 1

¿Sabe usted qué es la Informática Forense?

Objetivo: Determinar si las personas encuestadas conocen la definición de informática forense. Esto permitirá establecer el nivel de conocimiento de la informática forense.

Pregunta 2

¿Sabe usted qué son los delitos informáticos?

Objetivo: Determinar si las personas conocen la definición de delitos informáticos. Esto permitirá conocer que tan difundido esta el termino delitos informáticos en el sector legal.

Pregunta 3

¿Sabe usted qué son las herramientas de informática forense?

Objetivo: Conocer si están conscientes de la existencia de las herramientas de informática forense. Permitirá saber el nivel de popularidad de estas herramientas.

Pregunta 4

¿Sabe qué es la evidencia digital, también conocida como prueba científica?

Objetivo: Saber el nivel de conocimiento que tienen los encuestados respecto a la evidencia digital. El grado de conocimiento de la evidencia digital, estará ligado a si conocen el campo de acción de la informática forense y si conocen acerca de los delitos informáticos. Es importante determinar si las personas del sector legal tiene conocimiento de la evidencia digital, dado que de este conocimiento depende mucho la importancia que le den a este tipo de evidencia y por tanto, al darle importancia, valorarán la utilización de las herramientas que la informática forense utiliza para la obtención de este tipo de evidencia.

Pregunta 5

¿Ha tenido a su cargo algún juicio de delito informático donde se haya presentado evidencia digital?

Objetivo: Conocer la frecuencia con que las personas encuestadas han tenido contacto con los delitos informáticos, con la informática forense y sus aspectos en general. El objetivo de esta pregunta es conocer que tan práctico es el conocimiento que tiene en la resolución de delitos informáticos, la informática forense y la evidencia digital recopilada mediantes las herramientas de software que ésta utiliza.

Pregunta 6

¿Qué tipo de delitos ha tratado?

Objetivo: Conocer cuáles son los delitos informáticos a los cuales se enfrentan más frecuentemente. Esta pregunta permitirá obtener los problemas de delitos informáticos a los cuales se enfrentan principalmente los del sector legal y con ello realizar las propuestas de herramientas de informática forense.

Pregunta 7

¿Considera que la evidencia digital válida puede ser determinante en el esclarecimiento de un delito informático?

Objetivo: Saber si, para las personas encuestadas, la evidencia digital es determinante para la resolución de un delito informático. Con las respuestas a esta pregunta se permitirá determinar el nivel de confianza en la evidencia digital.

Pregunta 8

Si respondió si a la respuesta anterior, ¿En qué porcentaje influye la validez evidencia digital para la resolución favorable de un delito informático?

Objetivo: Conocer el nivel de importancia que las personas encuestadas del sector legal le dan a la evidencia digital en los juicios de delitos informáticos.

Pregunta 9

¿Según su criterio cuales de los siguientes factores hacen válida la evidencia digital?

Objetivo: Conocer los criterios que según las personas encuestadas hacen, desde el punto de vista legal, valida la evidencia digital.

Pregunta 10

¿Según su criterio, cuales son los principales obstáculos que impiden que los delitos informáticos tengan una resolución favorable?

Objetivo: Conocer la opinión del sector legal respecto a cuáles son los principales impedimentos con los que se enfrentan en los juicios de delitos informáticos y que evitan la resolución de este tipo de delitos.

Pregunta 11

¿Considera usted que los peritos informáticos tienen los conocimientos técnicos y científicos para realizar sus labores y permitir la obtención de evidencia digital válida?

Objetivo: Conocer si, desde el punto de vista legal, los peritos informáticos son considerados como personas aptas para la obtención de evidencia digital valida.

Pregunta 12

¿Cree que la aplicación de la informática forense en los casos de delitos informáticos trae ventajas en la resolución de delitos informáticos?

Objetivo: Conocer si desde el punto de vista legal, la utilización de la informática forense y sus herramientas es considerada como una ventaja para la resolución de delitos informáticos

II. DISEÑO DEL INSTRUMENTO RECOLECTOR DE DATOS PARA EL SECTOR EDUCATIVO

El objetivo general de la encuesta es conocer y medir el uso por parte de docentes universitarios de herramientas de software utilizadas en la informática forense y definir la necesidad y disposición de impartir conocimientos sobre las mismas.

Para el diseño de este instrumento de recolección de datos se tomaron en cuenta las preguntas de la investigación planteadas en el anteproyecto.

Tomando en cuenta que los docentes universitarios son de gran importancia ya que ellos son los encargados de impartir conocimientos sobre las diferentes disciplinas y tecnologías que actualmente posee la informática.

Consultar el **Anexo #8** para ver el formato final del instrumento recolector de datos dirigido al sector educativo y el **Anexo #9** que contiene la codificación de las respuestas.

A continuación se presentan las preguntas a realizar al sector educativo y el objetivo que se pretende con cada una de ellas:

Pregunta No. 1

¿Ha recibido alguna capacitación sobre herramientas de software que se utilizan en la informática forense?

Objetivo: Conocer si los docentes universitarios han recibido capacitaciones sobre herramientas de software que se utilizan en la informática forense y por consiguiente poseen conocimientos sobre las mismas, además definir si los docentes tienen conocimientos de la informática forense y sus herramientas.

Pregunta No. 2

¿Ha utilizado software que se aplica en la informática forense?

Objetivo: Conocer si los docentes universitarios han utilizado algún tipo de herramientas de software aplicables en informática forense.

Pregunta No.3

SI respondió que si a la pregunta anterior, ¿Con que frecuencia lo utiliza o ha utilizado?

Objetivo: Medir la frecuencia del uso que le han dado a este tipo de herramientas con el fin de conocer su nivel de utilización entre docentes universitarios.

Pregunta 4.

¿Cuál del siguiente software aplicable en la informática forense ha utilizado?

Objetivo: Conocer específicamente que software(s) que se aplican en la informática forense han utilizado los docentes.

Pregunta 5.

¿Considera necesario que los nuevos profesionales posean conocimientos enfocados a este tipo de herramientas?

Objetivo: Conocer si es necesario que los nuevos profesionales en el área informática posean conocimientos sobre las herramientas de software para la informática forense y además saber los motivos por los cuales consideran necesarios este tipo de conocimientos.

Pregunta 6.

Como docente, ¿estaría en la disposición de impartir conocimientos referentes a las herramientas de software de informática forense que ayuden al desarrollo de esta rama de la informática y colaboren al esclarecimiento de delitos informáticos?

Objetivo: Conocer el grado de disposición por parte de docentes universitarios para impartir conocimientos sobre herramientas de software aplicables en la informática forense y los motivos que conllevan a esta disposición.

Pregunta 7

¿Estaría dispuesto a ser capacitado en informática forense y sus herramientas de software?

Objetivo: Conocer si los actuales docentes universitarios en las áreas de la informática estarían dispuestos a ser capacitados en informática forense y la utilización de herramientas de software que apoyan a esta rama de la informática y conocer las razones que motivan esta disposición.

Pregunta 8

¿Considera que es necesaria la introducción de una materia en la(s) carreras(s) relacionada(s) a la informática en que se capacite en herramientas de software para informática forense ampliando así el campo de acción de los profesionales?

Objetivo: Conocer si los docentes universitarios consideran que es necesario que se impartan materias relacionadas a la informática forense en donde se capacite en herramientas de software a los futuros profesionales.

Pregunta 9

¿Qué factor considera que facilitaría la enseñanza en el área de la informática forense y la aplicación de sus herramientas?

Objetivo: Conocer el factor o los factores que los docentes universitarios consideran ayudarían a facilitar la enseñanza de la informática forense y la aplicación de sus herramientas de software.

Pregunta 10.

¿Cuál sería la principal ventaja de conocer como se utilizan las herramientas de software para informática Forense?

Objetivo: Conocer la ventaja o las principales ventajas que el conocimiento en la aplicación de herramientas de software para informática forense brinda a los poseedores de este conocimiento.

III. DISEÑO DEL INSTRUMENTO RECOLECTOR DE DATOS PARA EL SECTOR PROFESIONAL

Este instrumento tiene como finalidad la obtención de información por parte de los profesionales que interactúan de forma directa con las herramientas de software para la informática forense y de esta forma poder establecer cuál es la situación actual en El Salvador.

Consultar el **Anexo #10** para poder ver el formato final del instrumento recolector de datos dirigido al sector legal y el **Anexo #11** para ver la codificación de las respuestas del instrumento.

A continuación se presentan las preguntas a realizar al sector profesional y el objetivo que se pretende con cada una de ellas:

Pregunta 1

¿De qué forma inició sus conocimientos en el campo de la informática forense?

Objetivo: Conocer en qué forma las personas que prestan servicios como peritos en el área de informática forense se iniciaron en este campo.

Pregunta 2

De la siguiente clasificación ¿Cuáles son los tipos de herramientas de informática forense que ha utilizado?

Objetivo: En base a la clasificación presentada, conocer los tipos y frecuencias de las herramientas para la informática forense que han sido utilizadas por los peritos.

Pregunta 3

De la siguiente clasificación ¿Sobre qué tipo de herramientas tiene mayor conocimiento?

Objetivo: Determinar si los peritos informáticos poseen mayores conocimientos en las herramientas de software propietario que los que poseen sobre las herramientas de software libre.

Pregunta 4

¿Cuáles son las herramientas de software para la informática forense que ha utilizado con mayor frecuencia y el uso que les ha dado?

Objetivo: Conocer de forma específica las herramientas de software para la informática forense utilizadas por los peritos informáticos y las aplicaciones que se les dan.

Pregunta 5

¿Conoce la existencia de entidades o instituciones que ofrezcan certificaciones en el campo de la informática forense en El Salvador?

Objetivo: Determinar si los peritos poseen conocimientos acerca de instituciones en El Salvador que ofrezcan certificaciones en el área de informática forense.

Pregunta 6

¿En qué casos de delitos informáticos ha participado como perito forense?

Objetivo: Conocer los tipos de delitos en los que se requiere con mayor frecuencia la intervención de los peritos informáticos para la obtención de evidencia digital.

Pregunta 7

¿Cuáles son los factores que dificultan la adquisición de nuevos conocimientos sobre las herramientas de software para la informática forense?

Objetivo: Identificar cuáles son los factores que dificultan a los peritos informáticos la obtención y actualización de los conocimientos acerca de las herramientas de software para la informática forense.

Pregunta 8

¿Cómo considera los resultados obtenidos por las herramientas de software libre para la informática forense en comparación con los obtenidos por medio de las herramientas de software propietario?

Objetivo: Conocer el nivel de confianza que los peritos le dan a los resultados obtenidos mediante la aplicación de software libre para la informática forense.

Pregunta 9

Desde su punto de vista ¿Cuáles son los factores que dificultan la implementación de software libre para la informática forense?

Objetivo: Identificar cuáles son los factores que impiden o dificultan la implementación de las herramientas de software libre para la informática forense en El Salvador.

Pregunta 10

Ha recibido alguna capacitación sobre las herramientas de software para la informática forense

Objetivo: Conocer si los peritos informáticos se han sometido a capacitaciones en el área de la informática forense y a la vez identificar cuáles son los temas más comunes impartidos en dichas capacitaciones

Pregunta 11

Considera que la creación de una entidad o academia que se encargue de la formación, capacitación y certificación de peritos informáticos influiría de forma positiva en la persecución de los delitos informáticos.

Objetivo: Conocer si los peritos informáticos consideran que la creación de instituciones o academias destinadas a la formación, capacitación y certificación de los profesionales en el área de informática forense impactaría de forma positiva en la persecución de los delitos informáticos.

Pregunta 12

Considera importante que las instituciones de educación superior incluyeran en sus planes de estudio materias relacionadas con la práctica de la informática forense y sus herramientas.

Objetivo: Identificar la importancia de incluir materias relacionadas a la informática forense por parte de las instituciones de educación superior en sus respectivos planes de estudio.

C. TABULACIÓN Y ANÁLISIS DE LOS RESULTADOS OBTENIDOS

I. SECTOR LEGAL

JUECES

El análisis que se presenta a continuación es el resultado de las respuestas a las encuestas realizadas en 42 Juzgados de Instrucción.

1. ¿Sabe usted qué es la Informática Forense?

RESPUESTA	TOTAL	PORCENTAJE
SI	26	61.90%
NO	16	38.10%
TOTAL	**42**	100.00%

Tabla No 21: Resultados pregunta 1, Sector Legal, Jueces

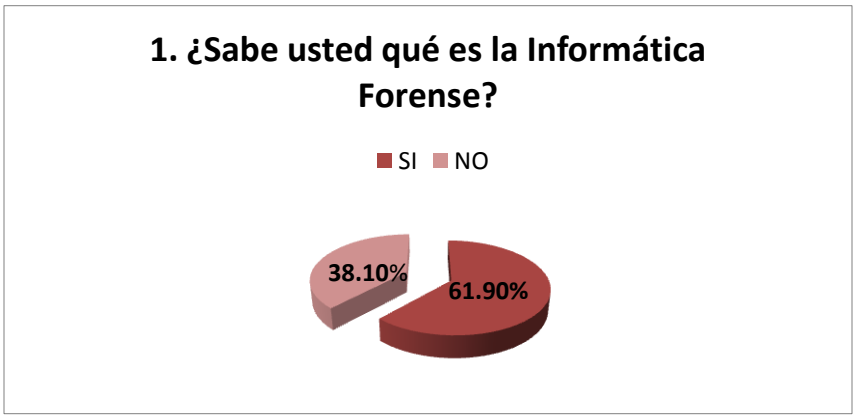

Figura No. 7: Resultados pregunta 1, Sector Legal, Jueces

Lectura

De los 42 jueces encuestados, el 61.90% (26) dijo saber que es la informática forense y un 38.10% (16) dijo no saberlo.

Análisis

De acuerdo a los resultados correspondientes a esta pregunta, se puede concluir que la informática forense en El Salvador es un término que está siendo conocido por los jueces, sin embargo, el conocimiento que tienen de esta no es tan generalizado como debería ser, demostrando que esta es una ciencia que aún está en desarrollo en este país. El que un poco más de la mitad de los jueces sean los que saben que es la informática forense plantea un reto para esta disciplina: demostrarles a los encargados de administrar justicia en los tribunales que la informática forense puede traer muchas ventajas en la resolución de los delitos informáticos y hacerlos conocedores de esta ciencia.

2. ¿Sabe usted qué son los delitos informáticos?

RESPUESTA	TOTAL	PORCENTAJE
SI	42	100.00%
NO	0	0.00%
TOTAL	**42**	**100.00%**

Tabla No 22: Resultados pregunta 2, Sector Legal, Jueces

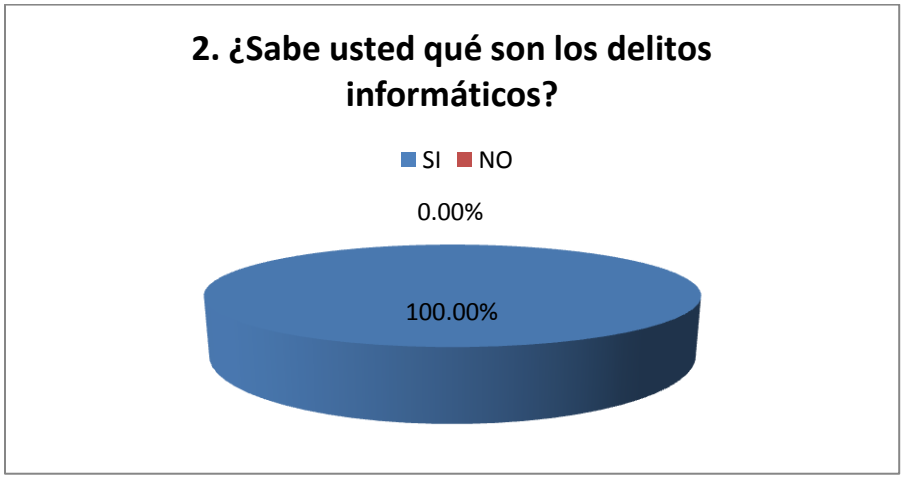

Figura No. 8: Resultados pregunta 2, Sector Legal, Jueces

Lectura

De los 42 jueces que fueron encuestados, el 100% dijo conocer lo que son los delitos informáticos.

Análisis

Esto es bueno, dado que a pesar que en El Salvador no existe un marco legal que defina formalmente qué son los delitos informáticos los jueces están consientes que estos tipos de delitos existen y que necesitan ser regulados. La necesidad de castigo a este tipo de delitos puede servir como base para impulsar el desarrollo de la informática forense en nuestro país.

3. ¿Sabe usted qué son las herramientas de informática forense?

RESPUESTA	TOTAL	PORCENTAJE
SI	22	52.38%
NO	20	47.62%
TOTAL	**42**	**100.00%**

Tabla No 23: Resultados pregunta 3, Sector Legal, Jueces

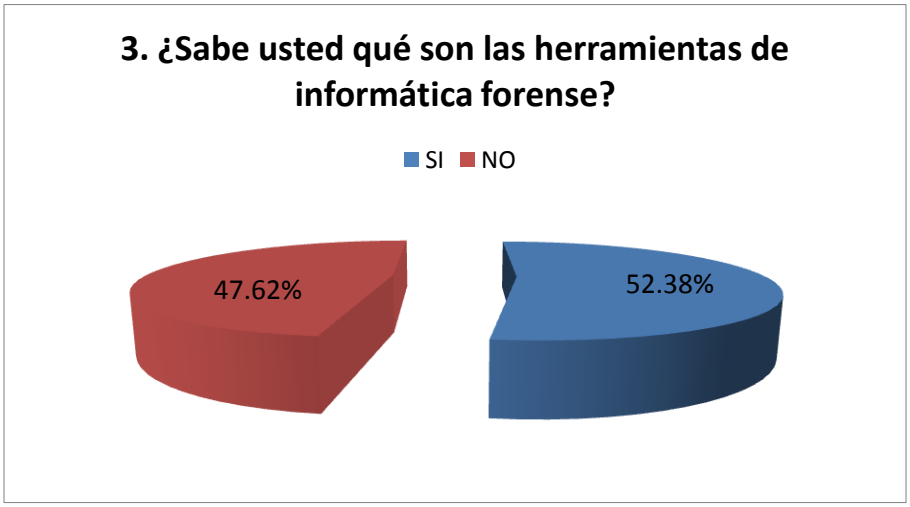

Figura No. 9: Resultados pregunta 3, Sector Legal, Jueces

Lectura

De los 42 jueces entrevistados, 52.38% de los jueces conoce que son las herramientas de informática forense y el 47.62% restante dijo no conocer que son estas herramientas.

Análisis

Este sector no está interesado en lo que son las herramientas de informática forense, sin embargo se demuestra que a pesar de no ser su campo de acción los jueces están conscientes de la existencia de herramientas que ayudan a obtener evidencia digital en los casos de delitos informáticos. El que un poco más de la mitad de la población de jueces conozca lo que son las herramientas de informática forense permite demostrar que sus principios y su aplicación están tomando importancia dentro del ámbito legal, esto debido a que cada vez más las tecnologías de información y comunicación son más necesarias para la realización de funciones de apoyo en labores cotidianas.

El nivel de conocimiento que tengan de las herramientas de informáticas forense, les permitirá definir con más información si aceptan o no la evidencia presentada como válida.

4. ¿Sabe qué es la evidencia digital, también conocida como prueba científica?

RESPUESTA	TOTAL	PORCENTAJE
SI	31	73.81%
NO	11	26.19%
TOTAL	**42**	**100.00%**

Tabla No 24: Resultados pregunta 4, Sector Legal, Jueces

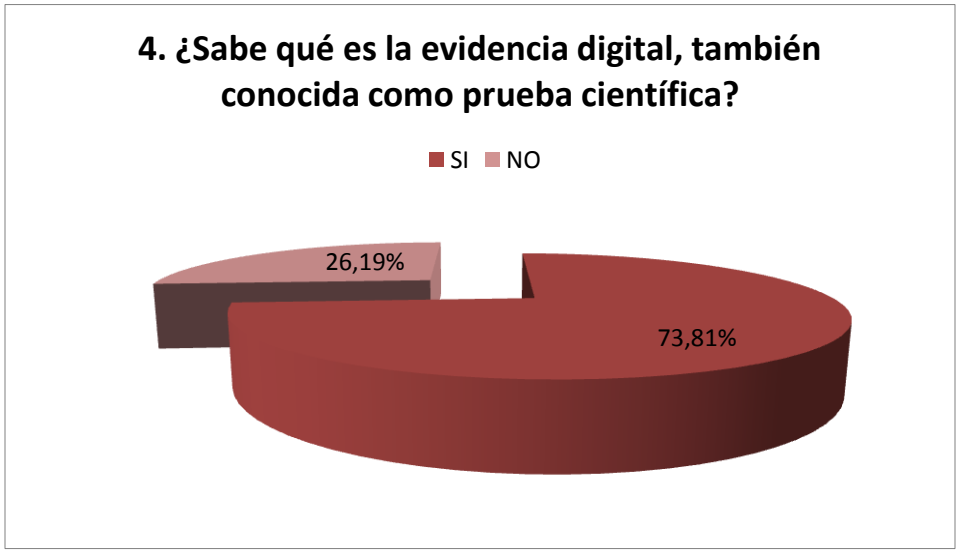

Figura No. 10: Resultados pregunta 4, Sector Legal, Jueces

Lectura

Un 73.81% de jueces conoce lo que la evidencia digital representa, mientras que un 26.19% dijo desconocerlo.

Análisis

La evidencia digital es la que demuestra la comisión de un delito y se obtienen mediante la aplicación de las herramientas de informática forense. De la validez que ésta tenga depende la importancia en la resolución de los delitos informáticos. Los jueces son los encargados de determinar si permiten o no que la evidencia digital sea tomada en cuenta. El conocimiento de este tipo de evidencia permite que estos la tomen en serio a la hora de la realización de los juicios. Cuando la conocen y la aceptan permiten que la informática forense se desarrolle. Sin embargo, para que la acepten deben tener confianza en que fue obtenida de forma tal que representa lo que ha pasado y no ha sido alterada, es decir, que tenga validez como tal.

Los resultados a esta pregunta nos permiten llegar a la conclusión de que la evidencia digital está siendo del conocimiento de los jueces debido a la importancia que puede representar para el esclarecimiento de los casos de delitos informáticos.

5. ¿Ha tenido a su cargo algún juicio de delito informático donde se haya presentado evidencia digital? (Si su respuesta es Si pase a la siguiente pregunta si es No pase a la pregunta 7)

RESPUESTA	TOTAL	PORCENTAJE
SI	19	45.24%
NO	23	54.76%
TOTAL	**42**	**100.00%**

Tabla No 25: Resultados pregunta 5, Sector Legal, Jueces

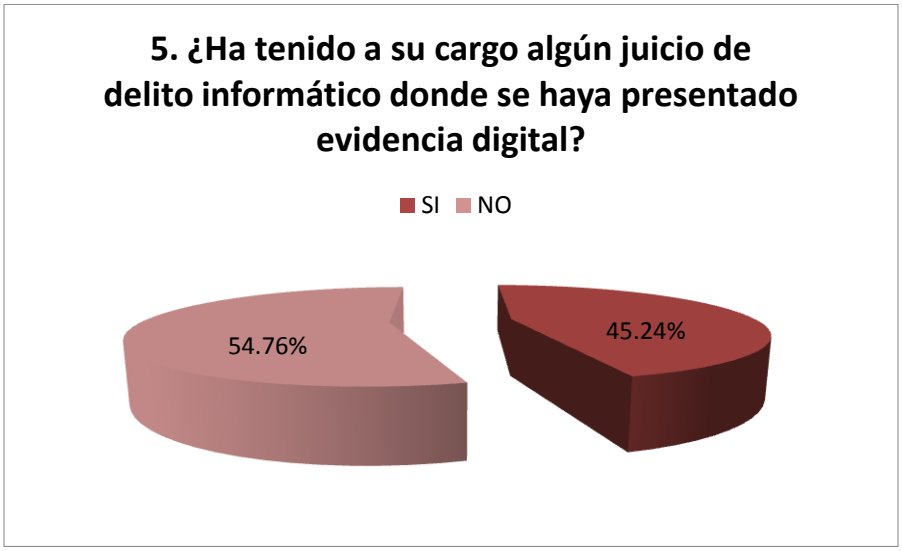

Figura No. 11: Resultados pregunta 5, Sector Legal, Jueces

Lectura

De los 42 jueces que fueron encuestados, 19 (45.24%) de ellos dijo haber tenido bajo su cargo un delito informático en el que se haya presentado evidencia digital, el restante 54.74% dijo que no.

Análisis

Los resultados anteriores, según comentaban los encuestados son debido a que no existe una tipificación de delito informático y a que no ha existido la posibilidad de que la parte acusadora ha presentado evidencia digital dado que no ha sido posible obtenerla, tratando los delitos informáticos como delitos comunes. Otro de los factores que manifestaban es que en muchos de los casos de delitos informáticos ha sido imposible obtener evidencia digital que se considere contundente.

El resultado de esto puede ser que la evidencia digital que no se presenta aunque haya sido recabada no es considerada como válida, dado que no permite esclarecer los delitos informáticos.

6. De los siguientes ¿Qué tipo de delitos ha tratado? (El total de respuestas difiere del total de encuestados porque podían elegir más de una opción y la pregunta solo fue contestada por los que respondieron si a la pregunta anterior)

RESPUESTA	TOTAL	PORCENTAJE
Pornografía Infantil	11	9.57%
Violación a la privacidad.	15	13.04%
Clonación de tarjetas electrónica.	24	20.87%
Piratería	25	21.74%
Fraude Electrónico	19	16.52%
Estafas.	15	13.04%
Otros	6	5.22%
TOTAL	**115**	**100.00%**

Tabla No 26: Resultados pregunta 6, Sector Legal, Jueces

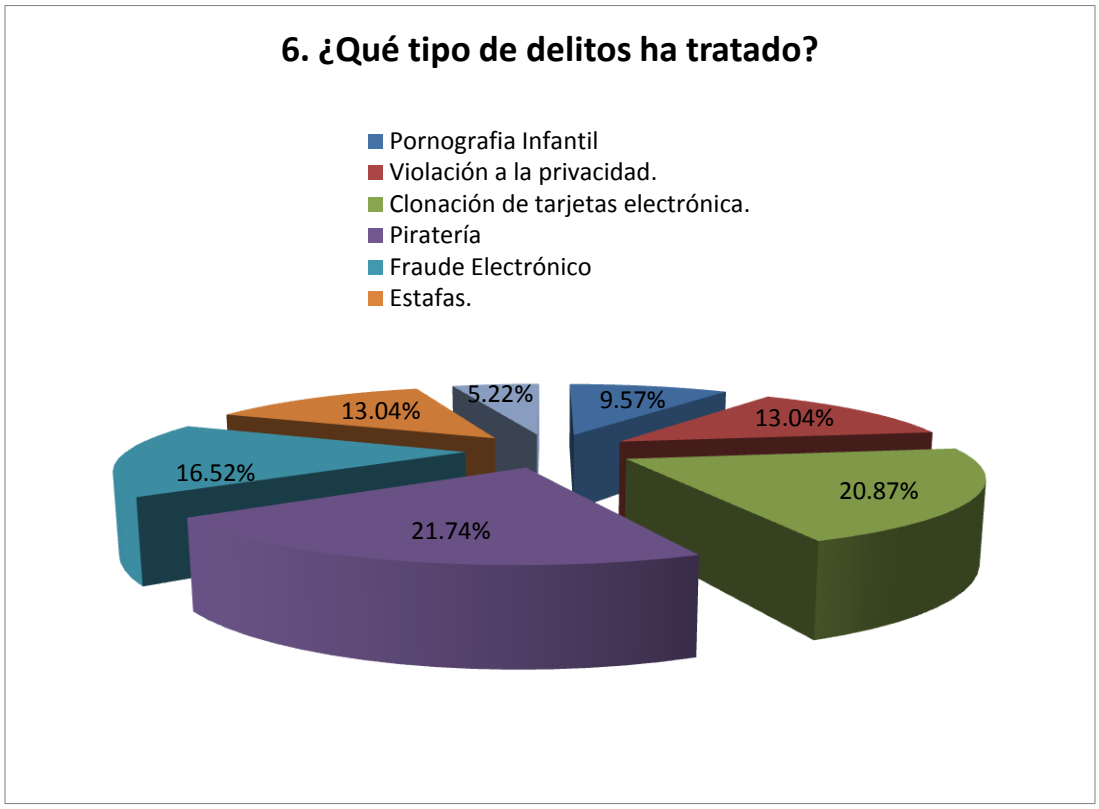

Figura No. 12: Resultados pregunta 6, Sector Legal, Jueces

Análisis

De los principales delitos que los jueces han tenido que tratar, resalta en primer lugar la piratería con un 21.74% de las respuestas, la clonación de tarjetas electrónicas con un 20.87% se ubica en segundo lugar, en tercero se encuentra el fraude electrónico con un 16.52% y en cuarto la violación a la privacidad con un 13.04%. Entre otros delitos están los de estafas con un 13.04%, la pornografía infantil con un 9.57% y un 5.22% dijo que otros delitos. Los resultados de esta pregunta demuestran cuales son los delitos que ocurren frecuentemente en el país, brindando así un panorama hacia donde deben estar orientadas las herramientas y los esfuerzos de la informática forense para evitar que estos delitos se sigan cometiendo y queden impunes.

Estos resultados permiten saber cuál es la situación actual en El Salvador en cuanto a delitos informáticos se refiere y nos permitirá realizar propuestas de herramientas que permitan obtener la evidencia digital de este tipo de delitos y por ende, esclarecer los delitos informáticos.

Dentro de la piratería, resalta principalmente la copia ilícita de materiales multimedia como películas y música, sin embargo, también incluye la copia ilegal de software.

Con respecto a lo del fraude electrónico, se puede dar el caso de phishing, en el cual alguien simula ser una entidad que no es, por ejemplo, paginas que simulan ser de un banco y no lo son y piden al usuario información bancaria como números de PIN, números de cuenta, etc.

Los delitos de violación a la privacidad pueden englobar aquellos como intervención de correos electrónicos, desvíos de información o sniffing.

7. ¿Considera que la evidencia digital válida puede ser determinante en el esclarecimiento de un delito informático?

RESPUESTA	TOTAL	PORCENTAJE
SI	38	90.48%
No	4	9.52%
TOTAL	**42**	**100.00%**

Tabla No 27: Resultados pregunta 7, Sector Legal, Jueces

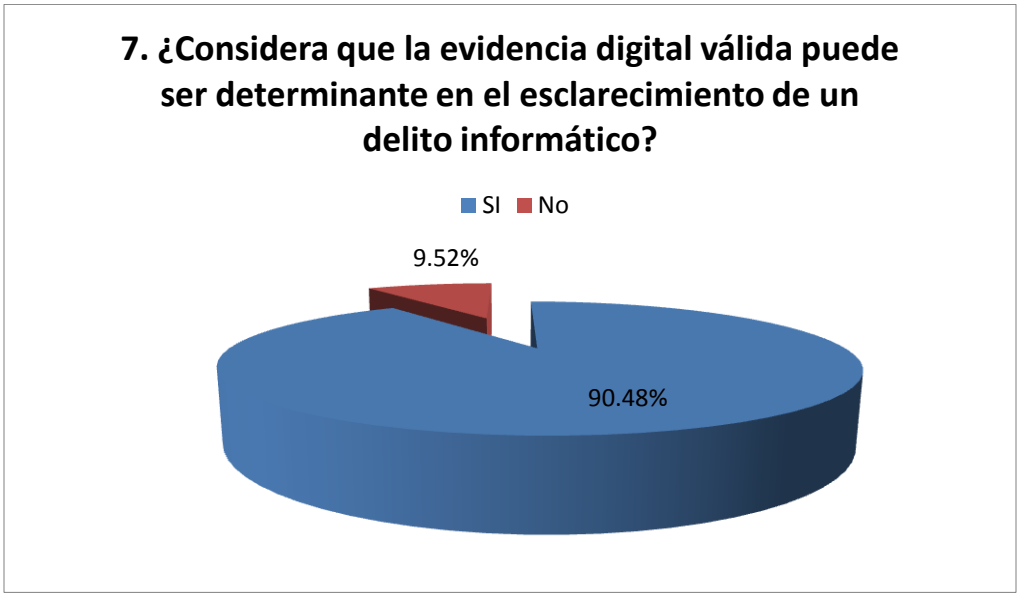

Figura No. 13: Resultados pregunta 7, Sector Legal, Jueces

Lectura

De los 42 jueces encuestados, 38 (90.48%) dijo que la evidencia digital puede ser determinante en el esclarecimiento de los delitos informáticos y 4, es decir el 9.52% dijo que no.

Análisis

Los resultados demuestran que los jueces consideran que la evidencia digital puede resultar probatoria para la resolución y el esclarecimiento de los delitos informáticos. Esto demuestra la importancia que le dan los jueces a la evidencia digital y la necesidad de poderla obtener correctamente para que sea válida. Por supuesto, lo determinante que pueda resultar la evidencia digital depende del nivel de validez que a juicio del juez se considera que tenga, es decir, que tanto cumple con los criterios de validez.

8. Si respondió si a la respuesta anterior, ¿En qué porcentaje influye la validez evidencia digital para la resolución favorable de un delito informático?

RESPUESTA	TOTAL	PORCENTAJE
0 – 24%	1	2.63%
25 – 49%	3	7.89%
50 – 74 %	23	60.53%
75 – 100%	11	28.95%
TOTAL	**38**	**100.00%**

Tabla No 28: Resultados pregunta 8, Sector Legal, Jueces

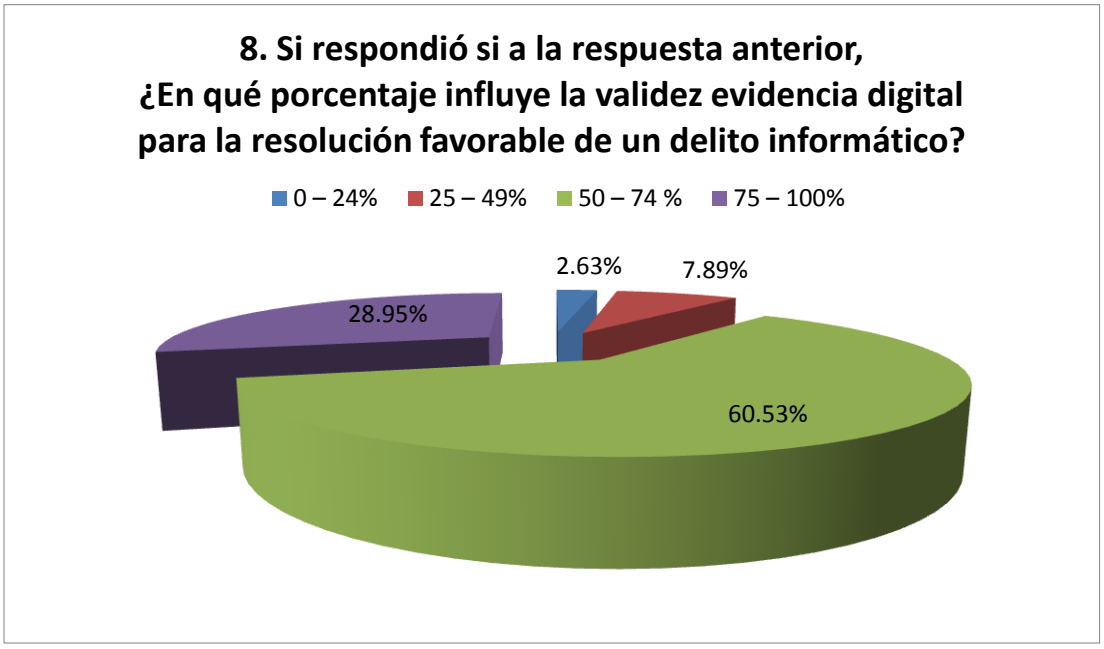

Figura No. 14: Resultados pregunta 8, Sector Legal, Jueces

Lectura

De los 38 jueces que consideraron que la evidencia digital puede ser determinante en el esclarecimiento de un delito informático el 60.53% consideró que la validez de esta evidencia digital influye en el proceso en un rango del 50 – 74 % y el 28.95% (11 jueces) consideraron que la evidencia digital puede ser influyente en un rango del 75 – 100%.

Análisis

Es decir que del total de encuestados, 34 de los 38 consideran que la evidencia digital valida puede influir en el proceso judicial del 50 al 100% y solo 4 consideró que puede ser determinante en menos de ese rango. El análisis a estas resultado demuestra que la evidencia digital valida tiene un gran valor para los jueces quienes al fin son los que deciden si aceptarla o no. Y demuestra también la necesidad de que la evidencia digital que se obtenga en los juicios de delitos informáticos tenga el valor como para servir en el esclarecimiento de los delitos informáticos. Debido a lo determinante que puede ser este tipo de evidencia para los jueces, es necesario que esta refleje lo que realmente ocurrió y no dé lugar a ambigüedades de responsabilidad del delito.

9. Según su criterio ¿Cuales de los siguientes factores hacen válida la evidencia digital? (El total de respuestas difiere del total de encuestados porque podían elegir más de una opción)

RESPUESTA	TOTAL	PORCENTAJE
La forma en que fue recolectada.	26	19.26%
El tipo de herramienta que se utilizó.	20	14.81%
La capacidad técnica del que obtuvo la evidencia digital.	35	25.93%
La cadena de custodia.	24	17.78%
El marco legal que la soporta.	8	5.93%
El nivel de conocimiento en la aplicación de las herramientas del perito que obtuvo la evidencia digital.	15	11.11%
Otros.	2	5.19%
TOTAL	**135**	**100.00%**

Tabla No 29: Resultados pregunta 9, Sector Legal, Jueces

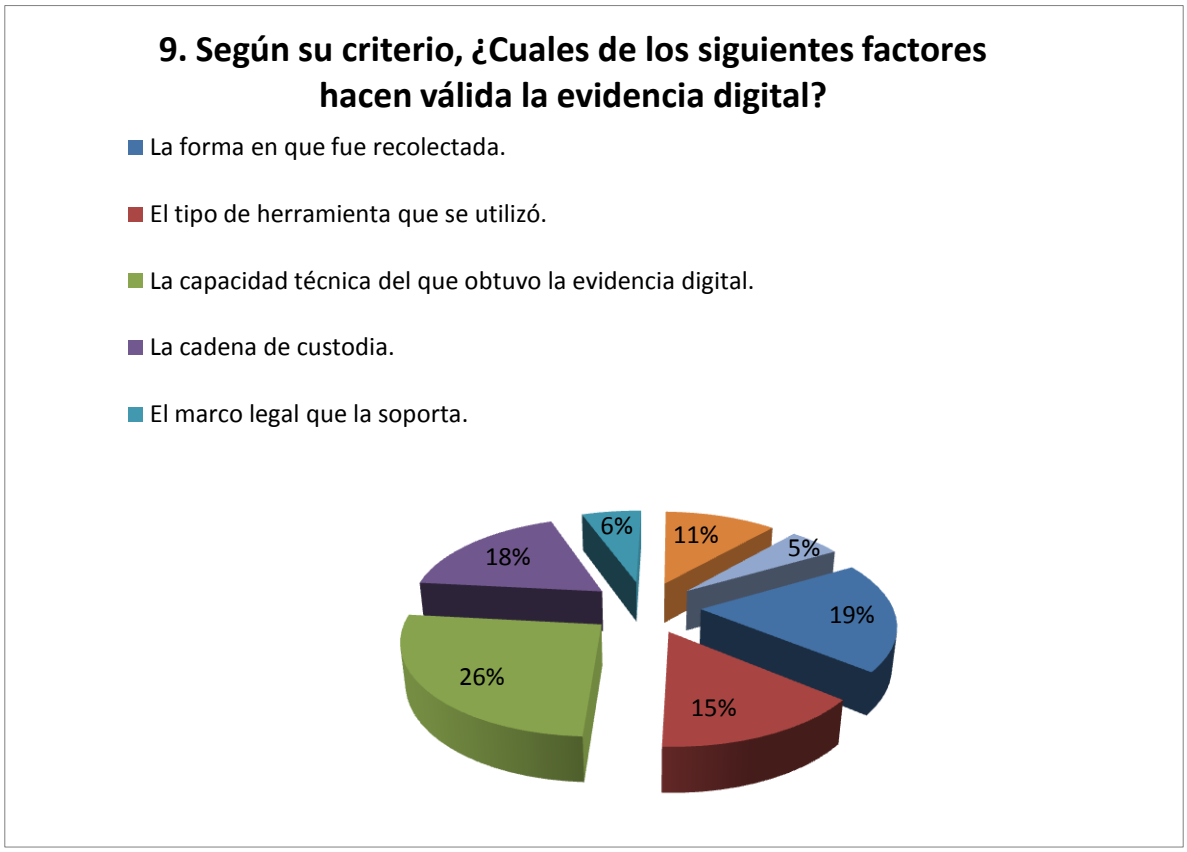

Figura No. 15: Resultados pregunta 9, Sector Legal, Jueces

Análisis

Entre los factores que más resaltan a la hora de considerar valida la evidencia digital resaltó la capacidad técnica de la persona que obtuvo la evidencia digital, es decir el perito. Esto demuestra la necesidad de garantizar que las personas que realizan labores de peritos informáticos tengan los conocimientos necesarios para realizar sus labores, volviendo al hecho de hacer necesarias las capacitaciones en el área informática y aumentar sus conocimientos en la utilización de las herramientas de informáticas forense.

Otro factor de gran importancia es la forma en que fue recolectada la evidencia, esto quiere decir que la persona encargada de realizar esta operación debe estar capacitada con una serie de conocimientos que garanticen el correcto uso de las herramientas ya que una mala aplicación de las mismas puede derivar en una contaminación de la evidencia.

El tercer factor que resaltaron es la cadena de custodia. Mediante una cadena de custodia adecuada se garantiza que la evidencia digital que fue recolectada se conserve tal y como fue encontrada, garantizando así su integridad y por ende su validez. Por tanto, se debe buscar los mecanismos para garantizar que la cadena de custodia no altere la evidencia obtenida, esto implica conocimientos en la conservación y organización de los medios en los que está almacenada la evidencia digital.

Como se puede ver en los resultados, los tres primeros elementos están relacionados a la habilidad del perito para obtener la evidencia digital, y según los jueces, esta determina una buena cantidad de la validez que le puedan ofrecer a este tipo de evidencia.

10. ¿Según su criterio, cuales son los principales obstáculos que impiden que los delitos informáticos tengan una resolución favorable? (El total de respuestas difiere del total de encuestados porque podían elegir más de una opción)

RESPUESTA	TOTAL	PORCENTAJE
Marco legal con vacios	4	3.31%
Capacidad técnica de los peritos	69	57.02%
Probar mediante la evidencia la comisión del delito.	34	28.10%
Valor probatorio de la prueba	6	4.96%
Falta de herramientas especializadas	8	6.61%
TOTAL	**121**	**100.00%**

Tabla No 30: Resultados pregunta 10, Sector Legal, Jueces

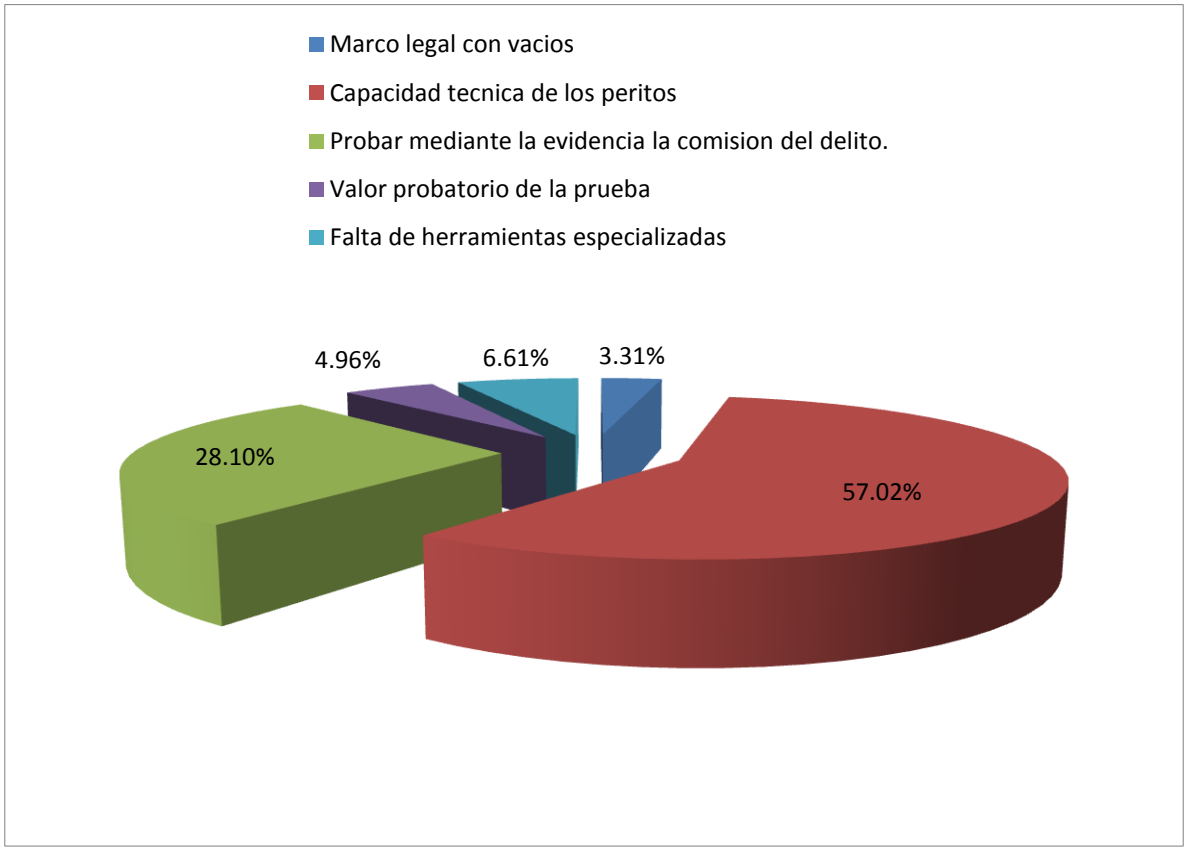

Figura No. 16: Resultados pregunta 10, Sector Legal, Jueces

Análisis

Los principales obstáculos que evitan la resolución de delitos informáticos de forma favorable, según los resultados de las encuestas son los siguientes:

En primer lugar, con un 57.02% está la falta de capacidad técnica de los peritos. Esto demuestra que a criterio de los jueces, los delitos informáticos no se resuelven favorablemente debido a que la poca capacidad de técnica de los peritos impide obtener evidencia digital que sea contundente a la hora de definir culpables.

En segundo lugar, está el probar que la persona ha cometido ese delito, a veces se puede obtener la evidencia digital pero no se puede demostrar que se cometió el delito. Este puede ser el resultado de una incorrecta o insuficiente aplicación de los principios de informática forense.

En tercer lugar se considera que las herramientas con que cuentan los peritos no permiten recabar la evidencia digital que se presenta en la variedad de ambientes posibles. Esta respuesta según comentaban es que a la hora de presentar evidencia digital, los fiscales se han quejado de que los peritos no pueden obtener la evidencia por falta de herramientas adecuadas.

En cuarto lugar está el marco legal que no soporta, según los jueces la evidencia digital y no establece los requisitos que esta debe cumplir dejando a discreción del juez si la toma como valida o no.

En conclusión, se puede decir que los jueces aceptarán la evidencia digital si la persona que la obtuvo demuestra tener los requisitos técnicos para demostrar que es válida y que la forma en que la recolectó fue correcta. A juicio de los jueces, el principal obstáculo está relacionado con la capacidad técnica y científica de los peritos y a los conocimientos en los usos de las herramientas, demostrando que es necesario contar principalmente con personal altamente capacitado en la disciplina de la informática forense.

11. ¿Considera usted que los peritos informáticos, tienen los conocimientos técnicos y científicos para realizar sus labores y permitir la obtención de evidencia digital válida?

RESPUESTA	TOTAL	PORCENTAJE
SI	28	66.67%
NO	14	33.33%
TOTAL	**42**	**100.00%**

Tabla No 31: Resultados pregunta 11, Sector Legal, Jueces

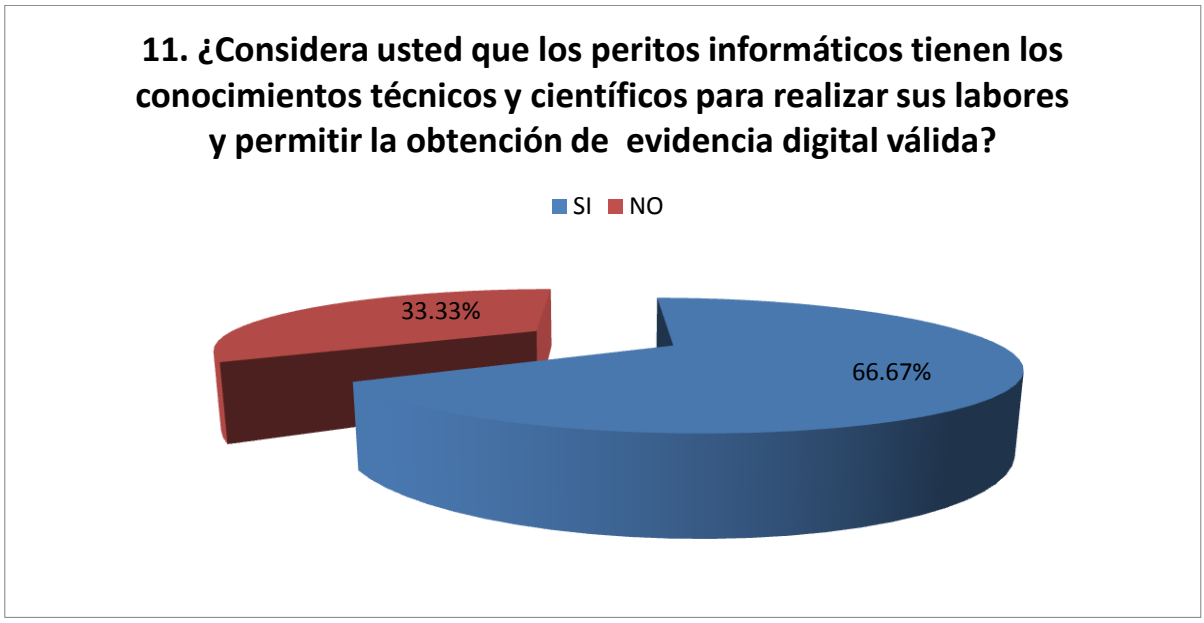

Figura No. 17: Resultados pregunta 11, Sector Legal, Jueces

Lectura

El 66.67% de los jueces considera que los peritos informáticos no tienen los conocimientos técnicos y científicos para obtener evidencia digital válida. Solo un 33.33% de los jueces consideró que estos si los tienen.

Análisis

Cuando un juez considera que la personas que obtuvo la evidencia digital no cumple con los requisitos técnicos que se requiere para ello, desestima la evidencia. De aquí surge la necesidad de dotar a los peritos informáticos de los conocimientos y herramientas necesarias para realizar su trabajo de manera eficiente y aceptable legalmente.

El que los jueces consideren que no se cuenta con conocimientos necesarios puede estar ligado a que en nuestro país no hay peritos certificados en cuanto a conocimientos, y los conocimientos que los peritos adquieren lo hacen de forma autodidacta.

12. ¿Cree que la aplicación de la informática forense en los casos de delitos informáticos trae ventajas en la resolución de delitos informáticos?

PREGUNTA	TOTAL	PORCENTAJE
SI	39	92.86%
NO	3	7.14%
TOTAL	**42**	**100.00%**

Tabla No 32: Resultados pregunta 12, Sector Legal, Jueces

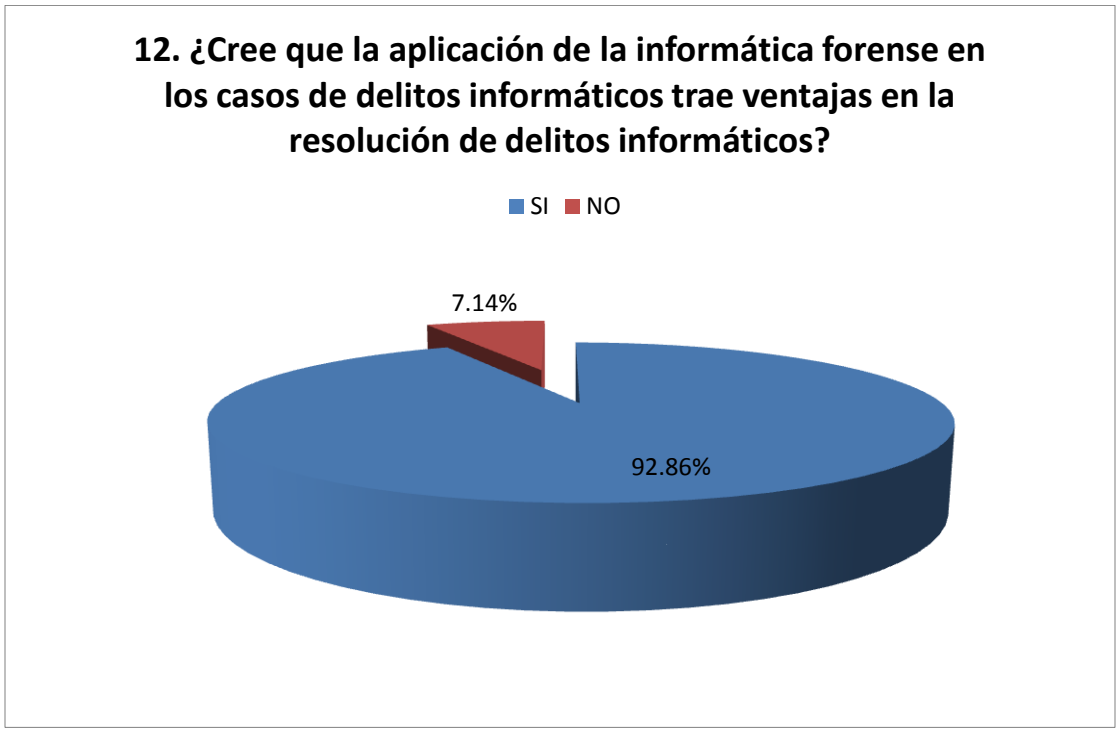

Figura No. 18: Resultados pregunta 12, Sector Legal, Jueces

Lectura

De los 42 jueces encuestados, 39 (92.86%) considera que la informática forense puede traer de alguna forma ventajas en la resolución de los delitos informáticos y solo 3 (7.14%) considero que no.

Análisis

Esto demuestra la confianza que los jueces tienen en los procedimientos de informática forense y que estos consideran que cuando se aplican correctamente se pueden resolver delitos. Los resultados a estas preguntas se fundamentan en los resultados de que los jueces han tenido en los casos de delitos informáticos que se ha aplicado la informática forense y al conocimiento de la disciplina que han obtenido mediante sus investigaciones.

Para poder acceder al resto de las tabulaciones y análisis correspondientes a las poblaciones que conforman el SECTOR LEGAL ver el CD adjunto, Apartado "Tabulaciones y Análisis", opción "Sector Legal".

ANÁLISIS GENERAL PARA LA POBLACIÓN DEL SECTOR LEGAL

Se obtuvieron 246 respuestas de profesionales del sector legal entre ellos 184 abogados, 42 jueces y 20 fiscales.

De las 246 personas encuestadas 155 saben que es la informática forense entre ellos 117 abogados 26 jueces y 12 fiscales lo cual nos permite ver que la cantidad de personas del sector legal que conocen que es la informática forense es superior a la mitad de los encuestados cabe mencionar que los mayores porcentajes se encontraron en los jueces y fiscales aunque también la cantidad de abogados es considerable; además se les pregunto si sabían que son los delitos informáticos y los resultados fueron que 199 de las personas encuestadas si saben que son los delitos informáticos de estos 145 abogados 42 jueces y 12 fiscales aumentando la cantidad de personas que si saben que son en la muestra de abogados de 117 que conocen el termino de informática forense a 145 que saben que son los delitos informáticos lo cual puede ser muestra de que no se conoce el termino como tal en el sector de abogados; notamos que en general las personas parte de la muestra del sector legal conocen que es la informática forense y los delitos informáticos tanto los encargados de acusar así como de defender y juzgar estos tipos de delitos.

Se consulto además sobre si sabían que son las herramientas de informática forense obteniendo las siguientes respuestas según muestra contestaron que si 37 abogados, 22 jueces y 12 fiscales encuestados dando un total de 71 personas de 246 lo cual refleja un desconocimiento de parte del sector legal sobre que son las herramientas de informática forense lo cual puede afectar la credibilidad que tengan en los resultados obtenidos a partir de los peritajes informáticos; además se les consulto sobre si saben que es la evidencia digital y los resultados fueron los siguientes contestaron que si 105 abogados 31 jueces y 19 fiscales logramos observar claramente que las cantidades son mayor a la mitad de cada muestra y cabe mencionar que la que manifestó tener un mayor índice de conocimiento de fue la muestra de fiscales donde un 95% de los fiscales encuestados dijo saber que es la evidencia digital; el sector legal tiene conocimientos de forma general sobre lo que son los delitos informáticos pero expresaron ciertas deficiencias en conocimientos específicos sobre las herramientas de informática forense y la evidencia digital.

De las 246 personas encuestadas han tenido a su cargo juicios en los que se han auxiliado de evidencia digital 85 de los 184 abogados, 19 de los 42 jueces y 15 de los 20 fiscales encuestados logramos notar que los fiscales son los que en su mayoría han formado parte de procesos en los cuales se ha utilizado la evidencia digital como medio probatorio; como complemento a esta pregunta se consulto en que tipos de casos de delitos informáticos habían fungido como defensores, acusadores o jueces y se obtuvo que los delitos con mayor incidencia han sido la piratería, la clonación de tarjetas electrónicas y el fraude electrónico en un menor grado se encuentra la pornografía infantil, la violación a la privacidad y las estafas en consonancia con las noticias que se encuentran en los medios de comunicación nacionales.

De la muestra del sector legal 197 personas consideran que la evidencia digital valida puede ser determinante en el esclarecimiento de un delito informático un alto índice considerando que su conocimiento es enfocado en el actuar legal y no en la informática forense ya que no existen juzgados especializados para tratar este tipo de crímenes además se les consulto acerca de qué

porcentaje influye la validez de la evidencia digital en la resolución favorable de un delito informático y los resultados fueron los siguientes 123 personas consideran que el porcentaje se encuentra entre 50%- 74% considerando un porcentaje alto de influencia de la evidencia digital valida en un delito informático.

Se consulto sobre los factores que hacen valida la evidencia digital y los 4 principales factores que se definen a partir de la preguntas son los siguientes: La capacidad técnica del que obtuvo la evidencia digital , el marco legal que la soporta., la forma en que fue recolectada y el nivel de conocimiento de las herramientas utilizadas por los peritos informáticos notamos que son puntos fundamentales para que la evidencia digital sea válida el conocimiento y la pericia técnica de los peritos y el marco legal en que esta se soporta ya que en el país existen vacios legales para la persecución de los delitos informáticos; además se consulto sobre los principales obstáculos que impiden que los delitos informáticos tengan una resolución favorable y se obtuvo el siguiente resultado: El principal obstáculo es la capacidad técnica de los peritos seguido por el valor probatorio de la prueba, la falta de herramientas especializadas y el marco legal que los soporta notamos que son similares los factores que validan la evidencia digital como los obstáculos que tienen la solución de los delitos informáticos tomando en cuenta la capacidad de los peritos y su conocimiento y las herramientas que utilizan acompañados por un marco legal que legitime el proceder de los mismos

Además se consulto a los encuestados del sector legal si consideraban que los peritos informáticos poseen los conocimientos técnicos y científicos para realizar sus labores y obtener evidencia digital valida a lo cual las respuestas fueron las siguientes 128 de las personas encuestadas consideran que los peritos no poseen el conocimiento necesario para obtener evidencia digital valida lo cual implica que la mayoría de profesionales del sector legal encuestados están cocientes que el nivel de conocimientos de los peritos es limitado y a su vez esto puede entorpecer las investigaciones en los delitos informáticos

Por último se les consulto si consideraban que la aplicación de la informática forense trae ventajas en la resolución de los delitos informáticos y los resultados fueron los siguientes: 211 personas consideran que si trae ventajas la aplicación de la informática forense en el país tomando en cuenta que la mayoría considera que los peritos no están lo suficientemente capacitados para desempeñar su trabajo pero a la vez ven el beneficio que el trabajo de esto trae a los encargados de impartir justicia en el país.

Como conclusión, En el país la población del sector legal entiéndase abogados jueces y fiscales consideran que la informática forense es una rama de la informática que apoya sus labores de justicia a su vez se concluye que no existe la suficiente capacitación para los peritos consecuentemente no poseen los conocimiento necesarios para realizar los peritajes de manera optima.

Para poder acceder a las tabulaciones y análisis correspondientes a las poblaciones que conforman el SECTOR EDUCATIVO ver el CD adjunto, Apartado "Tabulaciones y Análisis", opción "Sector Educativo".

ANÁLISIS GENERAL PARA LA POBLACIÓN DEL SECTOR EDUCATIVO

Se obtuvieron 125 respuestas de docentes universitarios distribuidos de la siguiente mantera: 30 docentes de la Universidad de El Salvador la única universidad pública del país y 95 docentes de 16 diferentes universidades que ofertan carreras Informáticas en el país; los dos grupos conformando la muestra para la investigación del sector educativo; los docentes tomados para la muestras son los que imparten materias de las carreras informáticas en las universidades seleccionadas.

Se consulto inicialmente a los docentes sobre si habían recibido capacitaciones sobre herramientas de software de informática forense, en la universidad pública y en las privadas el porcentaje de docentes que habían recibido capacitaciones fue similar 10% en la universidad de El Salvador y 10.53 % en las universidades privadas equivalente a 13 docentes de los 125 encuestados del total de la población esto nos permite ver que los docentes capacitados en este tipo de herramientas son un número limitado pero a la vez se cuenta con personal dentro de las universidades que podrían impartir conocimientos sobre este tipo de herramientas; además se les pregunto si habían utilizado herramientas de informática forense, en la Universidad de El Salvador el 36.67% contesto que si y en las universidades privadas el 67.37% contesto que sí, es notorio que en las universidades privadas hacen un mayor uso de este tipo de herramientas y su uso no es exclusivo para peritajes ya que los docentes los han utilizado en sus actividades diarias el total de los 125 docentes que han utilizado este tipo de herramientas es de 75.

Entre los tipos de herramientas utilizadas por los docentes encuestados tenemos herramientas para recuperación de datos los 75 docentes que han utilizado herramientas de informática forense seguidas por la recuperación de passwords utilizadas por 21 personas, la desencriptación de archivos utilizadas por 20 personas, la verificación de integridad de datos utilizada por 20 personas y las copias de backups de datos bits a bits por 18 personas también manifestaron haber utilizado herramientas de análisis de puertos y de trafico de red entre otros; con respecto a la frecuencia de utilización de los software los docentes en su mayoría con 49 de las 75 respuestas contestaron que los utilizan ocasionalmente o cuando surge la necesidad lo cual nos permite ver que aunque no se utilicen constantemente los docentes hacen uso de ellos cuando les son útiles.

Entre las herramientas que los docentes han utilizado se encuentran Norton Ghost el cual ha sido utilizado por 29 docentes de los 75 que han utilizado herramientas de informática forense seguido por OnTrackEasy Recovery por 21 docentes para realizar copias bit a bit y recuperar datos eliminados respectivamente además han utilizado Produkey, WinHex, Safeback, TestDisk Getdataback, Recuva, WireShark, entre otros; se les pregunto si consideraban necesario que los nuevos profesionales posean conocimientos enfocados a este tipo de herramientas a lo cual 107 de los 125 respondieron que si notando así el nivel de importancia que los docentes dan a este tipo de conocimientos que promueven el desarrollo de la informática forense en el país como complemento a la pregunta anterior se pregunto si estarían dispuestos a impartir conocimientos enfocados a este tipo de herramientas a lo cual 106 de los 125 docentes respondieron que si y entre los motivos por los cuales lo harían se encuentran: el Colaborar con la formación académica en primer lugar seguido de apoyar por colaborar con la justicia y apoyar el desarrollo de la

informática, los docentes consideran que este tipo de conocimientos apoyara la formación académica de los estudiantes y aumentara sus campos de acción en el quehacer profesional;

Se quiso conocer el interés y la disposición de los docentes para ser capacitados en informática forense y sus herramientas de software y de los 125 docentes encuestados 111 estarían en la disposición lo cual denota un interés generalizado de los docentes por conocer sobre esta nueva aplicación de las tecnologías de información y el apoyo que esta da a la justicia para la persecución de delitos informáticos; en consonancia con lo anterior se les consulto si consideraban necesario que se introdujera en las carreras informáticas materias enfocadas a las herramientas de informática forense 113 docentes consideran que si es necesario que se impartan materias enfocadas a la informática forense en las carreras informáticas en las universidades.

Se les consulto también sobre qué factores facilitarían la enseñanza en el área de informática forense y la aplicación de sus herramientas la mayoría de docentes opina que debe haber promoción por parte de las instituciones de educación superior es considerado el principal factor para los docentes seguido por la promoción de software libre para informática forense, la promoción por parte del gobierno y la creación de una academia capacitadora y laboratorios forenses en el país apoyando de esta manera el desarrollo de la informática forense y preparando a los nuevos profesionales para desempeñarse en esta área de la informática ; además se les pregunto cuales serian las principales ventajas de poseer conocimientos sobre estas herramientas y la mayoría de docentes contesto que sería estar preparado para desempeñarse como perito informático seguido de que aumenta la competitividad de los profesionales y supone un valor agregado para los mismos en su desarrollo profesional.

Como conclusión, En el país existe una carencia de fuentes de capacitación en informática forense, y consideran que se debe promover el conocimiento en estas aéreas de la informática a través de materias y capacitaciones en las universidades además un 60% de los docentes encuestados hacen uso actualmente de herramientas de informática forense y aunque el número de docentes que han recibido capacitaciones sobre estas herramientas es de 10 implica que es muy poca la gente capacitada para impartir conocimientos sobre estas herramientas.

Para poder acceder a las tabulaciones y análisis correspondientes al SECTOR PROFESIONAL ver el CD adjunto, Apartado "Tabulaciones y Análisis", opción "Sector Profesional".

ANÁLISIS GENERAL PARA LA POBLACIÓN DEL SECTOR PROFESIONAL

Se obtuvieron 12 respuestas de peritos nacionales incluyendo 4 contactados a través de la División Policía Técnica Científica, 6 peritos independientes que actúan al ser requeridos por la fiscalía y 2 peritos contactados a través de la Asociación de Ciencias Forenses de El Salvador.

Los profesionales encuestados iniciaron sus conocimientos en la informática forense a través de capacitaciones en el país o en el extranjero y de forma autodidacta la distribución de las respuestas se dio de la siguiente manera 6 peritos iniciaron sus conocimientos en la informática forense de manera autodidacta 4 lo iniciaron en capacitaciones en el país y 2 fueron capacitados fuera del país las capacitaciones en el país fueron a través las instituciones encargadas de realizar los análisis forenses en delitos informáticos con la colaboración de peritos internacionales que apoyaron estas capacitaciones esta área de la informática es prácticamente nueva en el país por lo cual no tiene un alto nivel de desarrollo y pueden existir muchos vacios en los análisis realizados por los peritos informáticos.

Entre las herramientas utilizadas por los peritos encuestados tenemos herramientas para recuperación de datos los 12 peritos las han utilizados seguidas por las herramientas de monitoreo de computadoras utilizadas por 6 de los 12 peritos encuestados dejando en último lugar herramientas de marcado de documentos y herramientas de hardware utilizadas únicamente por 4 de los peritos encuestados también mencionaron entre las otras herramientas utilizadas herramientas para análisis de redes backups de información y recuperación de números de licencia de software propietario; se consulto a los peritos sobre qué tipo de herramientas tenían mayor nivel de conocimientos y 7 de los 12 manifestaron tener mayor conocimiento sobre herramientas de software propietario y 5 de software libre por lo cual es notorio que aunque tienen conocimientos de los 2 tipos de herramientas es en mayor grado del software propietario pudiendo esto deberse a falta de capacitaciones en herramientas de software libre para informática forense.

Además, se consulto a los peritos sobre las herramientas de software para informática forense que han utilizado con mayor frecuencia y el uso que se les ha dado entre los software utilizados por los peritos tenemos los siguientes: Helix, Safeback, Norton Ghost, Produkey, Network Miner, Recover My Files, Alien Registry Viewer Smart Data Recovery y WinHex dándonos una idea real de los tipos de software utilizados por los peritos informáticos en el país; también se les consulto sobre si conocían sobre la existencia de alguna entidad certificadora en informática forense en el país ya que fue una de las principales carencias expuestas por personas relacionadas a la aplicación de la informática forense y el total de peritos manifestó no conocer por lo cual es notoria la inexistencia de una entidad capacitadora y certificadora en el área.

Tomando en cuenta la variedad de delitos informáticos que se comenten en el país se consulto a los peritos sobre en qué casos de delitos habían participado como peritos informáticos dando como resultado una mayor participación de los mismos en el análisis de equipo implicado en piratería de software en primer lugar seguido por pornografía infantil y el fraude comercial y en últimos lugares los delitos de clonación de tarjetas electrónicas y robo de información confidencial en concordancia con los delitos que se pueden observar a diario en los medios de comunicación

como flagelos de la económica y la justicia en el país; enfocándonos en el objetivo del conocimiento de estas herramientas se les consulto a los peritos cuales consideraban eran los factores que afectaban el adquirir conocimientos sobre este tipo de herramientas, 12 contestaron que la falta de instituciones capacitadoras y 7 que el costo de las herramientas observando que el factor principal y determinante es la falta de instituciones que impartan conocimientos en el área de la informática forense en el país.

En consonancia con el segundo factor mencionado anteriormente el cual es el costo de las herramientas se consulto a los 12 peritos como consideraban los resultados obtenidos por las herramientas de software libre para informática forense en comparación con las de software propietario obteniendo como resultado que 9 de los 12 consideran que son de igual calidad, 2 consideran que es de mayor calidad y uno considera que son de menor calidad logrando ver con esto que se podría fomentar el uso de herramientas de software libre para informática forense dado que no se requeriría una inversión en software y según el criterio de 11 de los 12 peritos los resultados son de igual calidad o superior que las de software propietario.

Considerando que el nivel de conocimiento es menor en herramientas de software libre se consulto a los peritos sobre cuáles son los factores que dificultan la implementación de software libre en la informática forense y 9 de los 12 contestaron que no existe difusión de sus características y ventajas, 8 que no hay fuentes de capacitación con respecto a su uso y 1 considera que la falta de credibilidad en sus resultados logrando ver nuevamente que la falta de entidades capacitadoras es uno de los principales factores y la falta de difusión de las características y ventajas del uso del mismo, ya que de tener una difusión mayor y fuentes de capacitación podrían implementarse en mayor medida herramientas de software libre para informática forense.

De los 12 peritos informáticos solo 2 manifestaron no haber recibido capacitaciones sobre las herramientas de software que se aplican en la informática forense dándonos esto una visión real de la necesidad de las capacitaciones sobre estas herramientas para los profesionales que desempeñan sus labores como peritos informáticos para que puedan estar preparados idóneamente en el momento de realizar un peritaje en algún caso de delito informático.

Se pregunto a los peritos si la creación de una academia influiría positivamente en la persecución de delitos informáticos y 10 contestaron que si haciendo ver de nuevo la necesidad apremiante de constante capacitación y actualización sobre todo en el área de tecnologías de información que evoluciona constantemente a un ritmo acelerado; además el 100% de los peritos encuestados consideran que las instituciones de educación superior entiéndanse universidades deberían incluir materias en sus planes de estudio que capacitaran a los estudiantes en informática forense y sus herramientas; es cierto El salvador aun esta iniciándose en esta área pero es de importancia preponderante el acelerado desarrollo en la misma ya que los criminales aprovechan la tecnología para cometer delitos y mientras más avanza la tecnología los métodos de delinquir son más sofisticados por lo cual debe estarse preparado no solo como profesional sino como país para afrontar esta realidad.

Para terminar se consultó a los peritos en que porcentaje consideraban que el conocimiento sobre las herramientas de informática forense influía en la obtención de evidencia digital valida y 8 de ellos consideran que afecta en un 51-75% 2 consideran que entre un 26% -50% y 2 que en un 76-100% viendo que 10 de ellos consideran que influye entre un 50-100% notamos la importancia que para ellos tiene el poseer los conocimientos necesarios para poder obtener la evidencia digital

de una manera adecuada y pueda ser considerada válida por los fiscales que apoyan las investigaciones.

Como conclusión, En el país existe una carencia de fuentes de capacitación en informática forense, y el principal obstáculo para los peritos es este ya que si no se poseen los conocimientos de diferentes herramientas de informática forense pueden entorpecer la obtención de evidencias a la hora de realizar los peritajes.

D. MATRIZ DE PUNTOS DE ANÁLISIS

La tabla presentada a continuación proporciona un resumen de los puntos coincidentes presentes en los análisis realizados a los distintos sectores en estudio:

Poblaciones / Criterios	Jueces	Abogados	Peritos	Fiscales	Docentes
Conocimiento sobre IF[29].	60%	57%	100%	60%	9%
Conocimiento de evidencia digital	70%	59%	100%	95%	----
Delitos informáticos con mayor auge	Piratería	Piratería	Piratería	Piratería	-----
Conocimiento sobre herramientas.	50%	79%	100%	60%	9%
Falta de Instituciones Capacitadoras	----	----	100%	----	91%

Tabla No 33: Matriz de puntos Coincidentes

Como resultado de los análisis se puede determinar el grado de conocimiento sobre la informática forense y los elementos que están involucrados en un delito informático y la aplicación de las herramientas idóneas para obtener la evidencia digital, como puntos de coincidencia las operadores de justicia involucrados y los elementos presentados muestran que nuestro país no posee la capacidad actualmente para hacer frente a los delitos informáticos. Los fiscales, abogados y jueces no poseen el conocimiento de cómo tratar la evidencia digital.

[29] IF: Informática Forense.

E. RESPUESTAS A LAS PREGUNTAS DE LA INVESTIGACIÓN

En base a los datos recopilados se procede a responder las preguntas planteadas para la investigación realizada.

I. COMUNIDAD EDUCATIVA

- ✓ **¿Cuentan las instituciones de educación superior con personal para enseñar herramientas de informática forense?**

Como demuestran los resultados de las respuestas a la pregunta 6 de la encuesta, 106 de los 125 docentes universitarios, contestaron estar dispuestos a impartir conocimientos sobre informática forense y sus herramientas.

Los resultados a la pregunta 7 demuestran que el 111 de los 125 encuestados de las Universidades, estarían dispuestos a ser capacitados.

En conclusión, como respuesta a esta pregunta de investigación podemos decir que existe personal dispuesto a enseñar respecto a la informática forense y a ser capacitado en esta área; los docentes han utilizado herramientas de informática forense pero sus conocimientos han sido adquiridos de forma autodidacta. Esto hacer notar la necesidad de capacitarlos a través de personal certificado para que posteriormente puedan enseñar respecto a la informática forense y a sus herramientas.

- ✓ **¿Qué factores son los que impiden o facilitan la enseñanza de la informática forense y sus herramientas como disciplina?**

De acuerdo a los datos recopilados en las encuestas realizadas a los docentes, entre los factores que impiden que la informática forense sea enseñada como disciplina están en primer lugar, que no tienen conocimientos certificados referente a la informática forense, en segundo lugar, los recursos para la enseñando de las informática forense tales como herramientas de software y no cuentan con el equipo de cómputo necesario.

Entre los factores que pueden facilitar la enseñanza están la promoción por parte de las instituciones de educación superior, la promoción del software libre para la informática forense y la promoción por parte del gobierno. Entre otros factores están la disposición de los docentes para enseñar informática forense y ser capacitados en esta área y el conocimiento personal que han adquirido mediante la aplicación experimental de cierto tipo de herramientas de software de informática forense. Además están conscientes de los beneficios que la aplicación de la informática forense puede traer a la resolución de delitos informáticos.

La respuesta a esta pregunta de investigación fue brindada por los resultados de las respuestas a la pregunta 9 de la encuesta realizada a los docentes universitarios.

- ✓ **¿Qué factores influyen para que las instituciones de educación superior no brinden conocimientos relacionados con la informática forense y las herramientas de software que se utilizan?**

Dentro de los factores que influyen en que las instituciones de educación superior no brinden conocimientos en la informática forense en el país es que esta ciencia está aún en desarrollo y por tanto, muchos de los docentes no conocen las ventajas que puede traer en la resolución de delitos

informáticos. Otro factor lo constituye el personal que no tiene los conocimientos necesario para poder enseñar informática forense de manera profesional, además el costo de las herramientas y del equipo de laboratorio que se necesita para poder enseñar la aplicación de las herramientas de informática forense.

En resumen los principales factores que impiden que las instituciones de educación superior no brinden estos conocimientos están el conocimiento y el factor económico respecto a la aplicación esta disciplina.

II. SECTOR LEGAL

- ✓ **¿Existe un marco legal que soporte la utilización de herramientas de informática forense?**

El marco legal salvadoreño carece de soporte para la informática forense. No se encuentra en la legislación salvadoreña la definición jurídica de delito informático ni los procedimientos que se deben realizar en los procesos legales de este tipo de delitos. Tampoco se determina si la evidencia digital puede ser tomada como válida ni siquiera se define los criterios que la hacen válida dejando a criterio de juez si toma la evidencia como valedera en los procesos legales o la desestima. Estos puntos fueron expresados por los jueces, fiscales y abogados que fueron encuestados.

III. SECTOR PROFESIONAL

- ✓ **¿Cuáles son las herramientas de informática forense que se utilizan en El Salvador?**

Entre el software de informática forense que han utilizado los peritos en El Salvador a partir de los resultados de las encuestas se encuentran:

- Produkey: herramienta para obtención de números de licencia llamada.
- Safeback: herramienta para realizar backups bit a bit.
- Smart Data Recovery: herramienta para recuperación de datos.
- Norton Ghost: herramienta para realizar backups.
- Winhex: completo editor hexadecimal.
- Recover My Files: herramienta para recuperar datos.
- Network Miner: analizador de redes.
- Alien Registry Viewer: analizador de registros.
- Helix: suite para informática forense.

Como se puede observar, las principales herramientas que se utilizan son la de recuperación de datos. Estos resultados fueron obtenidos de las respuestas a la pregunta #4 de la encuesta realizada a los peritos informáticos.

- ✓ **¿Cuál es el nivel de uso de las herramientas de informática forense en El Salvador?**

El nivel de uso de las herramientas de informática forense en el sector profesional es relativamente bajo, haciendo referencia a la cantidad y variedad de las mismas, el número limitado de herramientas mencionadas por los peritos demuestra el bajo nivel de uso, esto se debe a una diversidad de factores como lo es el costo de adquisición de las herramientas de

informática forense, el poco conocimiento que se tiene de este tipo de herramientas afectado principalmente por la falta de instituciones capacitadoras y el tipo de delitos que se dan en nuestro país.

- ✓ **¿Cómo se clasifican las herramientas de informática forense son utilizadas en El Salvador?**

Las herramientas de informática forense que se utilizan en nuestro país pueden ser clasificadas de la siguiente forma:

a. Clasificación según el tipo de herramientas:

1. Herramientas para la recuperación de datos
2. Herramientas para el monitoreo de ordenadores
3. Herramientas de marcado de documentos
4. Herramientas de hardware
5. Otros: herramientas para recuperar números de licencia de software propietario, etc.

b. Con respecto a licencia de uso:

1. Herramientas de software propietario 58.33%
2. Herramientas de software libre 41.67%

La mayor cantidad de herramientas de informática forense son del recuperación de datos, este es el trabajo principal del perito, y para ello utiliza principalmente herramientas de software propietario. Los resultados fueron obtenidos de la pregunta #2 y la #3 de la encuesta del sector profesional.

- ✓ **¿Qué nivel de incidencia tienen las herramientas de informática forense en la resolución de delitos informáticos?**

El nivel de incidencia de las herramientas de informática forense en la resolución de delitos informáticos está ligado a los diferentes delitos que se cometen comúnmente en el país y a su vez está relacionado al conocimiento de los peritos de las diferentes herramientas y su aplicación, como a la validez que se da a la evidencia digital por parte de los operadores de justicia, dependiendo esto del papel que desempeñen ya sea como defensores, acusadores o jueces relacionando estos factores logramos concluir que este nivel es alto aunque se ve afectado por la subjetividad o la conveniencia de los profesionales del sector legal.

- ✓ **¿Cómo ayudan las herramientas de informática forense a obtener evidencia digital confiable?**

Las herramientas de informática forense permiten a los peritos obtener evidencia digital que compruebe la comisión de los delitos. La aplicación de este tipo de herramientas se hace necesaria debido a los diferentes ambientes en que puede estar este tipo de evidencia.

Las herramientas de informática forense permiten obtener la evidencia digital de una manera que no se vea afectada o contaminada por el perito que la esta accediendo al momento de extraerla de algún dispositivo. Por tanto, las herramientas de software permiten que la evidencia digital no sea manipulada erróneamente y logran esclarecer situaciones en las que exista algún tipo de duda, aumentando el nivel de confiabilidad en su extracción.

- ✓ **¿Tiene el recurso humano el suficiente conocimiento en la aplicación de las herramientas de informática forense?**

Los peritos informáticos encuestados consideran que los conocimientos que tienen en la aplicación de las herramientas informáticas son buenos, sin embargo, están conscientes de que hay mucho que aprender y saber.

Los conocimientos en las herramientas de informática forense que poseen les permiten desarrollar sus peritajes bajo los ambientes más comunes, sin embargo, dado que la evidencia digital puede estar en muchos ambientes, han comentado que siempre existe la necesidad de aumentar ese conocimiento. En resumen, los peritos informáticos consideran que si tienen los conocimientos necesario para los tipo de delitos que ocurren comúnmente en nuestro país.

Cabe recalcar, que están conscientes de que este conocimiento es en gran parte adquirido autodidácticamente y que eso representa un problema ante los jueces que requieren como criterio de validez la certificación de los conocimientos de los peritos informáticos.

IV. TODOS LOS SECTORES

- ✓ **¿Qué factores afectan el nivel de uso de las herramientas de informática forense, tanto positiva como negativamente?**

Después de encuestar a los sectores involucrados, se han identificado los siguientes factores que pueden beneficiar el uso de las herramientas de informática forense:

- El deseo de aprender nuevos conocimientos.
- El deseo de los profesionales docentes de aprender y enseñar respecto a la informática forense.
- La confianza que el sector legal deposita en la evidencia digital valida como factor determinante en la resolución de delitos informáticos.
- Nivel de comisión de delitos informáticos en aumento debido al uso generalizado de las TICs en la sociedad salvadoreña.
- Avance en el desarrollo y aplicación de la informática forense mediante herramientas de software libre.

Entre los factores que pueden afectar el nivel de uso de las herramientas de informática forense se tiene:

- Marco legal que no considera la evidencia digital ni define los criterios de validez de esta.
- Peritos informáticos sin respaldo de sus conocimientos en la aplicación de la informática forense.
- Falta de entidades que capaciten a los profesionales y docentes en el uso de las herramientas de software de informática forense.
- Alto costo económico de las herramientas de informática forense.

- ✓ **¿Se cuenta con el recurso humano, tecnológico, financiero, educativo para hacer del uso de las herramientas de informática forense una disciplina difundida?**

Después de haber obtenido datos de los diferentes sectores involucrados en la informática forense se puede concluir que no se cuenta ni con el recurso humano, ni tecnológico, ni financiero, ni educativo para hacer el uso de las herramientas una disciplina ampliamente difundida.

La enseñanza de la informática forense requiere personal capacitado por expertos en la utilización de las herramientas de software, además de laboratorios y herramientas donde se practique en casos reales la aplicación de estas herramientas.

El sector profesional, al igual que el educativo, carece de herramientas y laboratorio tecnológicos para aplicar las herramientas de informática forense. El poco recurso económico y conocimiento certificado impide que estos peritos informáticos estén en constante capacitación acerca de la informática forense.

- ✓ **¿Qué ventajas o desventajas trae la utilización de herramientas de software en la informática forense a las personas o instituciones que las utilizan?**

Bajo un entorno ideal, la informática forense permitiría entre otras cosa:

- Obtener evidencia digital determinante en los procesos judiciales referentes a delitos informáticos.
- Acelerar la justicia en este tipo de delitos.
- Crear una sociedad con conocimientos en informática forense.

Entre las desventajas están:

- Aplicación de las herramientas de informática forense para recuperación de documentos confidenciales.

F. COMPROBACIÓN DE HIPÓTESIS

Para comenzar la comprobación de hipótesis, como primer paso, recordaremos cual es el enunciado del problema y las hipótesis bajo las cuales hemos basado nuestro estudio.

Enunciado del problema

¿En qué medida, la falta de aplicación de las herramientas de software para la informática forense influye en la evidencia digital presentada en los procesos judiciales?

Hipótesis de estudio

Estas son las hipótesis bajo las cuales hemos basado nuestra investigación.

Hipótesis de Investigación.

"El poco conocimiento de las herramientas de informática forense y su aplicación en casos prácticos impide obtener evidencia digital valida que ayude a la resolución de delitos informáticos de forma contundente en 60%".

Hipótesis nula.

"El poco conocimiento sobre la aplicación de las herramientas de informática forense a casos prácticos no constituye un impedimento para obtener evidencia digital válida".

Hipótesis alternativas.

Otras explicaciones al fenómeno de las herramientas de informática forense en El Salvador, estaría dado por las siguientes hipótesis alternativas:

1. "El factor económico constituye un impedimento para la obtención de evidencia digital válida en un 50% de los casos"
2. "Las nula enseñanza de las instituciones de educación superior impide que la aplicación de las herramientas informáticas se convierta en una disciplina ampliamente difundida".
3. "La validez de la evidencia digital está influida negativamente por la metodología utilizada para su recolección en el 75% de los casos".
4. "La utilización de las herramientas de informática forense está ligada, principalmente, la definición de metodologías para su aplicación, en un 45%".

Como segundo paso, tenemos que definir las relaciones entre las diferentes variables de la hipótesis de investigación, su conceptualización, los valores que cada una de ellas puede tomar y la forma de medir su valor tomado. A este proceso se le denomina operalización de variables.

La operalización de las variables nos permite ver la definición conceptual de las variables, los valores de estas, ya sean cuantitativos o cualitativos, la forma de medir estas variables y el instrumento utilizada para recopilar información respecto a estas variables.

Por ejemplo, la variable independiente "Aplicación de las herramientas de Informáticas forense a casos prácticos" se puede considerar que tiene dos dimensiones de medición ya sea "buena aplicación" o "mala aplicación". El que tome uno u otro valor depende de los resultados que muestren los indicadores para cada dimensión a medir. La operalización de variables para nuestra hipótesis de investigación quedaría de la siguiente manera:

OPERALIZACIÓN DE LAS VARIABLES

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	INSTRUMENTOS
Independiente: Aplicación de las herramientas de Informáticas forense a casos prácticos.	Aplicación de las distintas herramientas de informática forense adecuándose al ambiente en que la evidencia digital se encuentra.	Buena aplicación.	1. Herramienta adecuada al ambiente. 2. Uso de tecnología. 3. Recurso humano calificado en la aplicación de las herramientas. 4. Manejo de técnicas y conocimientos científicos. 5. Recursos económicos, humanos y tecnológicos adecuados.	Encuestas
		Mala aplicación	1. Desconocimiento de los diferentes tipos de herramientas de informática forense. 2. Desconocimiento de los principios físicos de lectura, escritura y borrado de información. 3. Desconocimiento de las técnicas de informática forense 4. Falta de recurso humano capacitado. 5. Falta de recursos tecnológicos 6. Recursos tecnológicos obsoletos o inaplicables a la realidad nacional.	Encuestas
Dependiente: Evidencia digital válida.	Evidencia digital almacenada en medios físicos que permita demostrar que es lo que ha ocurrido correctamente y permita esclarecer los hechos de delitos informáticos y que tenga valor legal en los procesos legales de estos tipos de delitos.	Evidencia digital con características de validez y aceptación legal.	1. Manejo adecuado de las metodologías de recolección de evidencia digital. 2. Interpretación adecuada de las leyes.	Encuestas

Tabla No 34: Operalización de las variables a utilizar.

El método estadístico a utilizar para la comprobación de la prueba de hipótesis de investigación será la prueba de Chi cuadrado.

Prueba de Chi cuadrado.

La prueba de Chi cuadrado es una técnica estadística para evaluar hipótesis acerca de la relación entre dos variables cualitativas. Se simboliza con X^2 y sirve para probar hipótesis correlacionales. Es decir, la prueba de Chi cuadrado sirve para determinar si los datos obtenidos de una muestran presentan variaciones estadísticamente significativas respecto a la hipótesis nulas Ho.

Recordemos que la hipótesis nula representa en términos generales la negación de la hipótesis de investigación. De acuerdo a la hipótesis nula, las variaciones en las variables independientes **no tienen correspondencia** con las variaciones que pudiere haber de la variable dependiente. Es decir que existe independencia estadística. Este es el supuesto principal en el que se basa la prueba de Chi cuadrado.

Procedimiento para el cálculo de Chi cuadrada.

El procedimiento de la Chi cuadrada se calcula a través de una tabla de contingencia o tabulación cruzada, que es una tabla de dos dimensiones y cada dimensión contiene una variable. A su vez, cada variable se subdivide en dos o más categorías.

En la tabla de contingencia se anotan las frecuencias observadas en la muestra de investigación. Posteriormente se calculan las frecuencias esperadas para cada celda.

En esencia, la Chi cuadrada es una comparación entre la "tabla de frecuencias observadas" y la "tabla de frecuencias esperadas", la cual constituye la tabla que esperaríamos encontrar si las variables fueran estadísticamente independientes o no estuvieran relacionadas.

La Chi cuadrada es una prueba que parte del supuesto de "no relación entre variables" y el investigador evalúa si en su caso es cierto o no, analizando si sus frecuencias observadas son diferentes de lo que pudiera esperarse en caso de ausencia de correlación. La lógica es así: "Si no hay relación entre las variables, debe de tenerse una tabla así (la de las frecuencias esperadas). Si hay una relación, la tabla que obtengamos como resultado en nuestra investigación debe ser muy diferente respecto a la tabla de frecuencias esperadas".

Para la aplicación del Chi cuadrado es necesario establecer el nivel de significancia (**α**) a utilizar y los grados de libertad de nuestra muestra.

El nivel de significancia es un valor de certeza que fija el investigador "a priori". De certeza respecto a no equivocarse. Por ejemplo, si se dice que el nivel de significancia es del 95%, se está diciendo que se desea tener un nivel de certeza del 95% y 5% de error en los datos.

La frecuencia esperada de cada celda, casilla o recuadro, se calcula mediante la siguiente fórmula aplicada a la tabla de frecuencias observadas:

$$fe = \frac{(Total\ de\ renglón)(Total\ de\ columna)}{N}$$

Donde "N" es el número total de frecuencias observadas.

Una vez obtenidas las frecuencias esperadas, se aplica la siguiente fórmula de Chi cuadrada:

$$x^2 = \sum \frac{(O-E)^2}{E}$$

Donde:

"O" es la frecuencia observada en cada celda.

"E" es la frecuencia esperada en cada celda.

Es decir, se calcula para cada celda la diferencia entre la frecuencia observada y la esperada, esta diferencia se eleva al cuadrado y se divide entre la frecuencia esperada. Finalmente se suman estos resultados y la sumatoria es el valor de X^2 obtenida.

Interpretación de la Chi cuadrada.

La Chi cuadrada proviene de una distribución muestral, denominada distribución X^2, y los resultados obtenidos en la muestra están identificados por los grados de libertad. Esto es, para saber si un valor de X^2 es o no significativo, debemos calcular los grados de libertad. Estos se obtienen mediante la siguiente fórmula:

$$Gl = (r-1)(c-1)$$

En donde "r" es el número de renglones o filas de la tabla de contingencia y "c" el número de columnas. Recordemos que la tabla de contingencia se forma de los valores de las frecuencias observadas y de los esperados. Acudimos con los grados de libertad que nos corresponden a la tabla de distribución Chi cuadrada **(Ver Anexo 12)**, eligiendo nuestro nivel de confianza (.05 ó .01). Si nuestro valor calculado de Chi cuadrada (**X^2**) es igual o superior al de la tabla **(X^2_t)**, decimos que las variables están relacionadas (X^2 fue significativa), o lo que es lo mismo, aceptamos la hipótesis de investigación, de lo contrario, aceptamos la hipótesis nula.

Poblaciones

Las poblaciones que fueron objetos de estudio y de las cuales se recopilaron los datos para la comprobación de hipótesis son las siguientes:

POBLACIÓN	ENCUESTADOS
Peritos informáticos.	12
Abogados	184
Jueces	42
Fiscales	20
TOTAL ENCUESTADOS	**258**

Tabla No 35: Cantidad de personas encuestadas por población

Otra de las poblaciones que fueron encuestadas lo constituyó el sector educativo, sin embargo no fue tomado en cuenta debido a que no participan en la aplicación de la informática forense y sus herramientas de forma directa.

Aplicación de la comprobación de la hipótesis mediante la Chi cuadrada.

Para realizar el procedimiento de comprobación de hipótesis, partiremos de la siguiente tabla de valores observados:

OBSERVADOS	SI	NO	TOTAL
Aplicación de las herramientas de Informáticas forense a casos prácticos (VI).	167	91	258
Dependiente: Evidencia digital válida (VD).	118	128	246
TOTAL	285	219	504

Tabla No 36: Valores Observados

Estos valores observados fueron obtenidos mediante la aplicación de los instrumentos de recolección de datos a las diferentes poblaciones.

Los valores para la variable independiente (VI) fueron tomados de la pregunta número 1 de la encuesta que fue realizada a los jueces, fiscales, abogados **(Véase el Anexo #6)** y del resultado de las preguntas 4 y 6 de la encuesta realizada a los peritos **(Véase Anexo #10)** donde expresan utilizar diferentes herramientas y haber participado en peritajes informáticos en casos de delitos informáticos.

Los valores de la variable dependiente fueron tomados de las respuestas a la pregunta número 11 hechas a los jueces, abogados y fiscales. **(Véase el Anexo #6)**

A partir de la tabla de valores observados, calculamos la siguiente tabla de valores esperados:

ESPERADOS	SI	NO
Aplicación de las herramientas de Informáticas forense a casos prácticos (VI).	**145.8928**	**112.1071**
Dependiente: Evidencia digital válida (VD).	139.1071	106.8928

Tabla No 37: Valores Observados

Para calcular los valores esperados, nos auxiliaremos de la tabla de valores observados. Por ejemplo, los valores esperados para la variable independiente fueron calculados de la siguiente forma:

Valores “SI” esperados = 258 *285 /504 = **145.8928**

Valores “NO” esperados = 258 * 219/504 = **112.1071**

Donde 258 es el total de respuestas para variable independiente, 285 y 219 son el total de respuestas “SI” y “NO” respectivamente y 504 es el total de la sumatoria de las filas o las columnas.

El mismo procedimiento se repitió para los valores esperados de la variable dependiente.

Aplicando la fórmula de Chi cuadrada vista anteriormente

$$x^2 = \sum \frac{(O-E)^2}{E}$$

Y sustituyendo los datos, tenemos:

$$X^2 = \frac{(167-145.8928)^2}{145.8928} + \frac{(91-112.1071)^2}{112.1071} + \frac{(118-139.1071)^2}{139.1071} + \frac{(128-106.8928)^2}{106.8928}$$

$$X^2 = 3.0537 + 3.9739 + \ 3.2026 + 4.1678$$

$$X^2 = 14.3980$$

El valor de Chi cuadrada para nuestros valores (X^2) es de **14.3980.** Ahora necesitamos obtener el valor de Chi cuadrado en la tabla de distribución.

Para obtener el valor del Chi cuadrado de la tabla, se toma en cuenta lo siguiente:

- El nivel de confianza alfa (α) será de 95%, por lo tanto el valor de alfa es de 0.05. Es decir que buscamos que nuestro nivel de certeza sea 95% con 5% de error.
- Los grados de libertad están dado por la siguiente fórmula:

$$Gl = (r-1)(c-1)$$

Por tanto los grados de libertad son:

Gl = (2 - 1)(2 – 1) = 1.

Entonces, con e = 0.05 (Nivel de significancia de 95 %) y 1 grado de libertad, el valor de la distribución de Chi cuadrado en la tabla **(X^2_t)** es de **3.84.** Para mayor información, véase el **anexo 8 con la tabla de distribución X^2**.

Dado que X^2(14.3980) es mayor a X^2_t (3.84), es decir, el valor de X^2 encontrado es mayor que el de la tabla de la distribución, se <u>acepta la hipótesis de investigación</u> para un nivel de confianza de 95% con 1 grado de libertad y se rechaza la hipótesis nula.

CAPÍTULO IV

DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

CAPÍTULO IV: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

A. INTRODUCCIÓN

Dentro de los casos de delitos informáticos en el país es preciso presentar evidencia digital y las herramientas que apoyan la obtención de la misma son las herramientas aplicables en la informática forense. Para los operadores de justicia, entiéndase jueces, abogados o fiscales involucrados en el tratamiento de estos delitos, es determinante el conocimiento científico de los peritos para la obtención de las pruebas que puedan incriminar al delincuente.

Los informes periciales del análisis de la evidencia se les proporcionan a fiscales y abogados que son las partes acusatorias y defensoras respectivamente en un juicio, dando lugar a que el juez según lo expuesto de las pruebas presentadas tome su decisión para dictaminar la sentencia.

El primer paso a llevar a cabo para la realización del diagnóstico consiste en la elaboración de un conjunto de indicadores que tienen como finalidad convertir la información recolectada mediante las encuestas a los sectores involucrados en la informática forense, en un valor cuantificable y medible que permitirá llevar a cabo un análisis sobre características relevantes de las variables que son objeto de estudio.

Una vez identificado y definidos los indicadores a utilizar, se procede a realizar la evaluación de cada uno de ellos utilizando los datos obtenidos en la investigación realizada. En base a esta evaluación obtendremos valores que nos proporcionaran el estado de la situación actual del uso de este tipo de herramientas.

Para conocer el estado de la aplicación de herramientas de software que se utilizan en la informática forense en El Salvador, se utilizo la información recolectada de las población de jueces, abogados, fiscales, peritos informáticos y Universidades; dando como resultado el siguiente diagnóstico.

B. CREACIÓN DE INDICADORES PARA LA INVESTIGACIÓN

I. CONCEPTO DE INDICADOR

Los indicadores son utilizados para poder medir con claridad los resultados obtenidos con la aplicación de programas, procesos o acciones específicas, con el fin de obtener el diagnóstico de una situación, comparar las características de una población o para evaluar las variaciones de un evento. Estos son desarrollados mediante la recolección de datos y se expresan a través de fórmulas matemáticas, tablas o gráficas.

Entre las definiciones encontradas podemos mencionar:

- ✓ Un indicador es un valor mesurable que permite seguir la evolución de un proceso para identificar el logro de un objetivo.
- ✓ Medida sustitutiva de información que permite calificar un concepto abstracto. Se mide en porcentajes, tasas y razones para permitir comparaciones.
- ✓ Conjetura o señal que posibilita el conocimiento de algo que ha existido o va a ocurrir.

Aunque no existe una definición oficial de lo que es un indicador por parte de un organismo internacional, es posible detectar dos elementos básicos que los caracterizan[30]:

1. Es una estadística, un hecho, una medida, una serie estadística (en otras palabras cuantitativa) o alguna forma de evidencia o percepción (en otras palabras cualitativa).
2. Su propósito es el de clarificar y definir objetivos, establecer direcciones presentes y futuras con respecto a metas, evaluar programas específicos, demostrar progresos, medir cambios en una condición especifica o situación a través del tiempo, determinar el impacto de programas, etc.

II. CARACTERÍSTICAS DE LOS INDICADORES

Entre sus características más importantes tenemos:

- ✓ Estar inscrito en un marco teórico o conceptual, que le permita asociarse firmemente con el evento al que el investigador pretende dar forma.
- ✓ Ser específicos, es decir, estar vinculados con los fenómenos económicos, sociales, culturales o de otra naturaleza sobre los que se pretende actuar; por lo anterior, se debe contar con objetivos y metas claros.
- ✓ Ser explícitos, de tal forma que su nombre sea suficiente para entender si se trata de un valor absoluto o relativo, de una tasa, una razón, un índice, etc.
- ✓ Estar disponibles para varios años, con el fin de que se pueda observar el comportamiento del fenómeno a través del tiempo.
- ✓ Los indicadores no son exclusivos de una acción específica; uno puede servir para estimar el impacto de dos o más hechos.

---

[30] Organización de las Naciones Unidas (ONU). *Integrated and coordinated implementation and follow-up of major.* United Nations conferences and summits. Nueva York, Estados Unidos de América, 10 y 11 de mayo de 1999

- ✓ Ser claro, de fácil comprensión para los miembros de la comunidad, de forma que no haya duda o confusión acerca de su significado.
- ✓ Que la recolección de la información permita construir el mismo indicador de la misma manera y bajo condiciones similares, de modo que las comparaciones sean válidas.
- ✓ Técnicamente debe ser sólido, es decir, válido, confiable y comparable, así como factible, en términos de que su medición tenga un costo razonable.
- ✓ Ser sensible a cambios en el fenómeno, tanto para mejorar como para empeorar.

III. TIPOS DE INDICADORES

Existen por lo menos dos criterios para poder realizar una clasificación de los indicadores:

1. ***A partir de la dimensión o valoración de la realidad económica, social, política o humana que se pretende expresar.***

   Dependiendo del campo de conocimiento que se pretende analizar, se habla de indicadores económicos, sociales, ambientales, etc. Si bien el fin último de todos ellos es ser un insumo para evaluar la cercanía o lejanía hacia las metas de bienestar económico, social y de conservación del medio ambiente, en lo que varían es en las unidades de medida que utilizan: mientras que los indicadores económicos lo hacen en unidades monetarias y/o productos, los sociales lo hacen en personas; y los ambientales, principalmente, en recursos naturales.

2. ***Partiendo del tipo de medida o procedimiento estadístico necesario para su obtención.***

   Si consideramos la forma como se obtiene la información para construirlos, se puede diferenciar entre los indicadores objetivos y subjetivos. Los primeros se basan en evidencias externas independientes del informante, suponiendo que los métodos de captación, procesamiento y divulgación de la información son objetivos. Los segundos son juicios, casi siempre en modo y en concepto, y reflejan percepciones y opiniones de la población con respecto a su situación.

IV. SELECCIÓN DEL TIPO DE INDICADOR A UTILIZAR

Para la presente investigación se ha decidido elaborar indicadores de tipo social por las siguientes razones:

- ✓ Los indicadores serán utilizados para poder medir el nivel de uso dado a las herramientas de software para la informática forense.
- ✓ A parte de medir la utilización de las herramientas se pretende corroborar la validez dada a la evidencia digital obtenida y que es utilizada en la resolución de los delitos informáticos.
- ✓ Los delitos informáticos son fenómenos que tienen incidencia directa en diferentes áreas de la sociedad salvadoreña, los indicadores elaborados buscan ser herramientas que puedan medir el nivel de evolución del uso de las herramientas de software en el combate de los mismos.

En el marco de desarrollo social, es de gran importancia utilizar este tipo de indicadores ya que aportan evidencia empírica para la realización de diagnósticos, implementación de políticas públicas, formulación de programas y proyectos. A pesar de su importancia, los indicadores sociales han sido menos explorados que los económicos y técnico-productivos, esto debido a que se refieren a fenómenos más complejos y, por ende, de difícil medición.

Los indicadores empleados en proyectos sociales, usualmente son cuantitativos, sin embargo es posible emplear indicadores cualitativos para obtener un acercamiento más preciso a los logros del proyecto

Los indicadores pueden ser clasificados según su objetivo de la siguiente manera:

1. **Indicadores de actividades**. Se refieren a las actividades vinculadas con la ejecución o forma en que el trabajo es realizado para elaborar los productos (bienes y/o servicios), incluyen actividades o prácticas de trabajo tales como procedimientos de compra, procesos tecnológicos y de administración financiera.
2. **Indicadores de Producto**: miden las características o cualidades de los bienes o servicios creados o resultantes por las acciones realizadas mediante el uso de los insumos.
3. **Indicadores de Impacto**: miden el efecto que los resultados obtenidos provocan en otras variables o situaciones ajenas sobre las que no se actúa en forma directa.

V. CRITERIOS PARA LA SELECCIÓN DE INDICADORES SOCIALES

Con el objetivo de garantizar la validez de los indicadores sociales a desarrollar, se tienen que tomar en cuenta ciertos criterios, en ese sentido la Organización de las Naciones Unidas[31] define los presentados a continuación:

- ✓ Los indicadores sociales deben adecuarse y medir el aspecto de la preocupación social que quiere medir.
- ✓ El sistema de indicadores propuestos debe ser mínimo en cuanto al número, de tal manera que cada uno de los indicadores integrantes recoja el mayor volumen de información posible.
- ✓ El sistema de indicadores debe estar perfectamente coordinado, pues solo así se puede ofrecer una visión completa del fenómeno que se trata de describir.
- ✓ Los indicadores sociales se elaborarán a partir de series estadísticas fiables.
- ✓ Los indicadores sociales deben de estar disponibles en un plazo de tiempo corto.
- ✓ Los indicadores deben de ser viables, esto es, de inmediata aplicación o en el futuro más cercano.

[31] ONU, 1975: Sistemas de Estadísticas Sociales y Demográficas (SESD). Proyecto de normas sobre los indicadores sociales.

VI. METODOLOGÍA UTILIZADA EN LA CREACIÓN DE LOS INDICADORES

Para la elaboración de los indicadores se tomaron como base los resultados obtenidos en las encuestas realizadas a las distintas poblaciones seleccionadas, estos indicadores serán utilizados en la realización del diagnóstico de la situación actual del uso de las herramientas de software para la informática forense en El Salvador y además podrán servir en futuras investigaciones que busquen determinar el comportamiento de dicho fenómeno.

En la siguiente figura se presenta la metodología a utilizar:

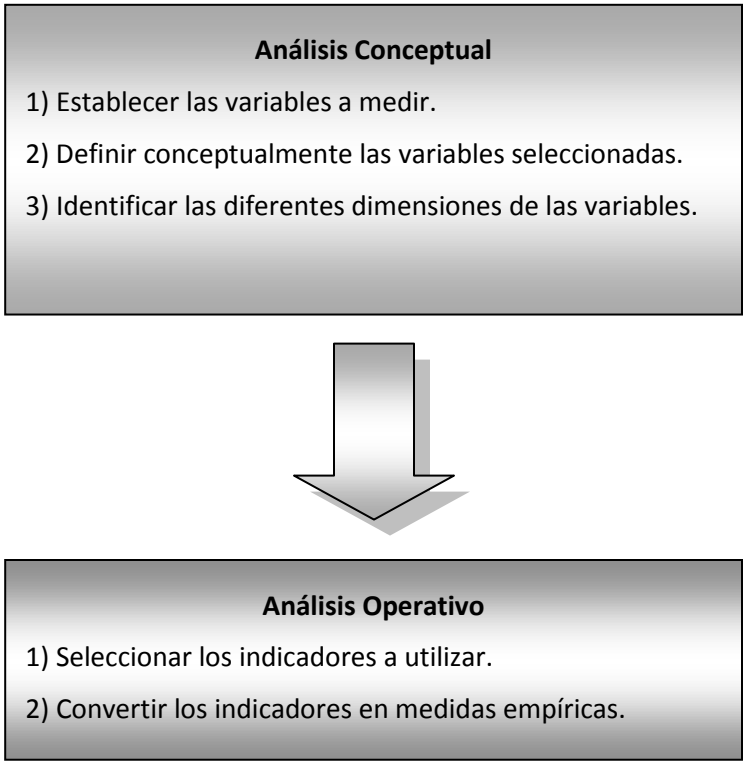

Figura No. 19: Metodología para la elaboración de indicadores.

El proceso de creación de los indicadores está dividido en dos grandes etapas:

1. **Análisis Conceptual**, en donde se define lo que se va a medir.
2. **Análisis Operativo**, en donde se realiza la operacionalización de lo que se va a medir.

ANÁLISIS CONCEPTUAL

Los fenómenos sociales no pueden ser medidos de forma directa debido a su nivel de abstracción y complejidad. Para que un hecho o fenómeno social deje de ser una simple observación y se convierta en un objeto de estudio, es necesario asociarle un concepto o variable que pueda ser objeto de medición.

Una vez seleccionados estos conceptos es necesario proporcionarles una definición teórica, es decir explicar su significado en términos lo más simple posible.

La definición teórica posee las siguientes funciones[32]:

- ✓ Asociar una etiqueta al concepto o variable.
- ✓ Extraer de la definición teórica de la variable sus posibles dimensiones, pues sucede con excesiva frecuencia que un concepto en sociología se describe, y en consecuencia se deberá medir, a partir de las dimensiones que lo componen.
- ✓ La definición teórica nos ofrece información adicional sobre el tipo de indicadores más afines para medir el concepto o variable.

El análisis conceptual nos permite exponer y aclarar los términos en los que se va a aplicar el concepto o variable y en consecuencia indicamos los aspectos que queremos conocer del mismo al momento de realizar el acercamiento. Hasta este momento, el análisis realizado es exclusivamente en un plano teórico.

Esta fase se presenta como la más importante y relevante ya que es la que determina la validez y significación del proceso de medición al que hemos sometido un hecho o fenómeno social.

ANÁLISIS OPERATIVO

El concepto o las dimensiones del concepto para poder ser medibles se operacionalizan. Es en este proceso cuando a las variables teóricas de un hecho o fenómeno social se les aplica mediciones empíricas, convirtiéndolas en variables prácticas. Por lo tanto podemos decir que un indicador es una medición operativa de las dimensiones de un concepto dado.

Cuando ya se tienen debidamente identificadas las dimensiones que representan un concepto hay que realizar una selección de los indicadores adecuados. La elección de los indicadores depende fundamentalmente de los objetivos y las necesidades de la investigación.

Una vez identificado el conjunto de indicadores que desde el punto de vista del investigador y en función de los objetivos de la investigación son los adecuados para cuantificar el hecho social se procede a llevar a cabo la operacionalización de los mismos, es decir pasar el concepto teórico a un lenguaje científico.

[32] Juan Díez Medrano, Catedrático del Departamento de Teoría Sociológica, Facultad de Ciencias Económicas y Empresariales, Universidad de Barcelona.

VII. APLICACIÓN DE LA METODOLOGÍA PARA LA CREACIÓN DE INDICADORES

En este apartado se llevará a cabo la aplicación de la metodología expuesta en el punto anterior con el objetivo de construir los indicadores para la investigación.

ANÁLISIS CONCEPTUAL

Para la realización de los indicadores se han identificados cuatro variables que serán sujetas de medición, siendo estas:

1. Evidencia digital.
2. Herramientas de software para la informática forense.
3. Recurso humano.
4. Delitos informáticos.

Una vez identificados los conceptos o variables se procede a relacionar cada una de ellas con una definición teórica:

1. ***Evidencia digital:*** cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal. La evidencia digital debe cumplir una serie de criterios para poder tener una validez jurídica y es utilizada por los diferentes operadores del sistema judicial.

2. ***Herramientas de software para la informática forense:*** conjunto de herramientas que tienen como finalidad ayudar a la informática forense en el descubrimiento y la interpretación de la información almacenada en medios magnéticos con el objetivo de establecer los hechos. Este tipo de herramientas pueden ser de licencia libre o de licencia comercial.

3. ***Recurso humano:*** conjunto de personas que interactúan con las herramientas de software para la informática forense, ya sea desde un punto de vista didáctico o para la obtención de la evidencia digital a ser presentada en los procesos judiciales.

4. ***Delito informático:*** actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)[33].

[33] Julio Téllez Valdés, Investigador titular "B" de tiempo completo en el Instituto de Investigaciones Jurídicas de la UNAM.

A continuación, se extraen las distintas dimensiones que conforman y describen los conceptos presentados anteriormente, para facilitar su comprensión se hará uso de la siguiente tabla:

CONCEPTO	DIMENSIONES
Evidencia digital.	1. Utilizada en la resolución de delitos informáticos.
	2. Validez dada a la evidencia digital.
	3. Conocimientos que le den credibilidad a la evidencia digital.
Herramientas de software para la informática forense.	1. Se pueden clasificar según su tipo de licenciamiento.
	2. Se pueden clasificar según su utilidad.
	3. Uso dado a las herramientas de software para la informática forense.
Recurso humano.	1. Personal capacitado en las instituciones de educación superior.
	2. Peritos informáticos con capacitados en el uso de las herramientas de software para la informática forense.
Delitos informáticos.	1. Conocimiento por parte de los operadores de justicia.
	2. Interacción de los operadores de justicia.

Tabla No 38: Conceptos a utilizar para la creación de los indicadores

A continuación se presenta el formato a ser utilizado para la descripción de los indicadores creados para la presente investigación:

NOMBRE DEL INDICADOR	
Tipo	
Objetivo	
Forma de cálculo	
Unidad de medida	
Fuente de la información a utilizar	
Interpretación	
Frecuencia	

Tabla No 39: Formato de presentación de los indicadores creados

Para un mejor entendimiento, se procede a la descripción de cada uno de los elementos que conforman el formato para la presentación de indicadores:

- ✓ **Tipo:** se definirá si el indicador elaborado corresponde a un indicador de actividad, producto o de impacto.
- ✓ **Objetivo:** describe la finalidad con la que fue creado el indicador.
- ✓ **Forma de cálculo:** representación matemática a utilizar para la obtención del indicador.
- ✓ **Unidad de medida:** indica la unidad en que estará dado el valor del indicador obtenido mediante la aplicación de su respectiva formula.
- ✓ **Fuente de la información a utilizar:** especifica de donde se obtendrán los datos a utilizar para la obtención del valor del indicador.
- ✓ **Interpretación:** la forma en que será explicado el significado del valor obtenido para el indicador.
- ✓ **Frecuencia:** indica el tiempo sugerido en el que el valor de cada indicador tendría que ser actualizado a través de una nueva medición.

ANÁLISIS OPERATIVO

Con las variables identificadas y descritas conceptualmente, se procede a la creación de los indicadores a utilizar. Como paso final se realiza la representación matemática de los mismos utilizando expresiones de agregación simple que tienen como objeto la obtención de los indicadores a partir de la agregación de variables o dimensiones que participan en la observación. La unidad de medida obtenida en este tipo de indicadores es la de un porcentaje (%).

- Indicadores relacionados con la evidencia digital:

IMPORTANCIA DADA A LA EVIDENCIA DIGITAL (IED).	
Tipo	Producto.
Objetivo	Conocer el nivel de importancia dado a la evidencia digital que es presentada en los procesos judiciales en El Salvador.
Forma de cálculo	$$IED = \frac{\left(\begin{array}{c}\sum \text{de jueces, abogados y fiscales} \\ \text{que consideran determinate la evidencia digital} \\ \text{en los procesos judiciales}\end{array}\right)}{\left(\sum \text{dejueces ,abogados y fiscales}\right)} \text{ x } 100$$
Unidad de medida	Porcentaje (%).
Fuente de la información a utilizar	La información será obtenida mediante las encuestas realizadas a los operadores de justicia de El Salvador; específicamente 42 jueces, 184 abogados y 20 fiscales.
Interpretación	Malo Regular Bueno 0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100% Mientras el valor obtenido para este indicador se encuentre más cercano al 100% reflejará que los operadores de la justicia en El Salvador lo consideran un elemento contundente para la resolución de los delitos informáticos. En caso contrario, mientras más se aleje, refleja la poca importancia dada a este elemento.
Frecuencia	Anual.

Tabla No 40: Descripción del indicador IED

<table>
<tr><th colspan="2">VALIDEZ DADA A LA EVIDENCIA DIGITAL (VED).</th></tr>
<tr><td>Tipo</td><td>Producto.</td></tr>
<tr><td>Objetivo</td><td>Conocer si los aplicadores de justicia en El Salvador consideran que los peritos informáticos poseen los suficientes conocimientos para lograr la obtención de evidencia digital válida.</td></tr>
<tr><td>Forma de cálculo</td><td>$$VED = \frac{\left(\begin{array}{c}\sum \text{ de jueces, abogados y fiscales} \\ \text{que consideran que los peritos poseen} \\ \text{conocimientos suficientes para obtener evidencia} \\ \text{digital válida}\end{array}\right)}{\left(\sum \text{dejueces,abogados y fiscales}\right)} \text{ x 100}$$</td></tr>
<tr><td>Unidad de medida</td><td>Porcentaje (%).</td></tr>
<tr><td>Fuente de la información a utilizar</td><td>La información será obtenida mediante las encuestas realizadas a los operadores de justicia de El Salvador; específicamente 42 jueces, 184 abogados y 20 fiscales.</td></tr>
<tr><td>Interpretación</td><td>Malo Regular Bueno
<table><tr><td>0%</td><td>10%</td><td>20%</td><td>30%</td><td>40%</td><td>50%</td><td>60%</td><td>70%</td><td>80%</td><td>90%</td><td>100%</td></tr></table>
Si el valor de este indicador se acerca al 100% quiere decir que los aplicadores de justicia consideran que la validez de la evidencia digital presentada se encuentra respaldada por los conocimientos de los peritos informáticos. En caso contrario, si el valor se aleja del 100% nos indica que los aplicadores de justicia consideran que los conocimientos de los peritos no son los suficientes para poder garantizar la obtención de evidencia digital válida.</td></tr>
<tr><td>Frecuencia</td><td>Anual.</td></tr>
</table>

Tabla No 41: Descripción del indicador VED

- Indicadores relacionados con las herramientas de software para la informática forense:

CONOCIMIENTO SOBRE HERRAMIENTAS DE SOFTWARE LIBRE (CSL).	
Tipo	Actividad.
Objetivo	Identificar el porcentaje de peritos que tienen mayor conocimiento sobre las herramientas de software libre para la obtención de evidencia digital.
Forma de cálculo	$$CSL = \frac{(\sum \boldsymbol{peritos\ que\ tienen\ mayor\ conocimiento\ sobre\ software\ libre\ para\ informatica\ forense})}{(\sum \boldsymbol{total\ de\ peritos})} \boldsymbol{x100}$$
Unidad de medida	Porcentaje (%).
Fuente de la información a utilizar	La información será obtenida mediante las encuestas realizadas a 12 peritos informáticos.
Interpretación	Bajo Medio Alto **0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%** Mientras el valor obtenido para este indicador se encuentre más cercano al 100% reflejará que los peritos informáticos realizan un mayor uso de ese tipo de herramientas. Si dicho valor se aleja indica que los peritos no hacen uso de herramientas de software libre para la obtención de la evidencia digital. Este indicador ayudará a conocer en qué forma evolucionan el conocimiento sobre este tipo de herramientas.
Frecuencia	Anual.

Tabla No 42: Descripción del indicador CSL

<table>
<tr><th colspan="2">CONOCIMIENTOS SOBRE HERRAMIENTAS DE SOFTWARE PROPIETARIO (CSP).</th></tr>
<tr><td>Tipo</td><td>Actividad.</td></tr>
<tr><td>Objetivo</td><td>Identificar el porcentaje de peritos que tienen mayor conocimiento sobre las herramientas de software propietario para la obtención de evidencia digital.</td></tr>
<tr><td>Forma de cálculo</td><td>$$CSP = \frac{(\sum \textbf{peritos que tienen mayor conocimiento sobre software propietario para informatica forense})}{(\sum \textbf{total de peritos})} x100$$</td></tr>
<tr><td>Unidad de medida</td><td>Porcentaje (%).</td></tr>
<tr><td>Fuente de la información a utilizar</td><td>La información será obtenida mediante las encuestas realizadas a 12 peritos informáticos.</td></tr>
<tr><td>Interpretación</td><td>Bajo Medio Alto
<table><tr><td>0%</td><td>10%</td><td>20%</td><td>30%</td><td>40%</td><td>50%</td><td>60%</td><td>70%</td><td>80%</td><td>90%</td><td>100%</td></tr></table>
Mientras el valor obtenido para este indicador se encuentre más cercano al 100% reflejará que los peritos informáticos realizan un mayor uso de este tipo de herramientas. Si dicho valor se acerca al 0% indica que los peritos no hacen uso de herramientas de software propietario para la obtención de la evidencia digital. Este indicador ayudará a conocer en qué forma evoluciona el conocimiento sobre este tipo de herramientas.</td></tr>
<tr><td>Frecuencia</td><td>Anual.</td></tr>
</table>

Tabla No 43: Descripción del indicador CSP

<table>
<tr><th colspan="2">USO DE LAS HERRAMIENTAS DE SOFTWARE PARA LA INFORMÁTICA FORENSE POR PARTE DE LOS DOCENTES UNIVERSITARIOS (UDU).</th></tr>
<tr><td>Tipo</td><td>Actividad.</td></tr>
<tr><td>Objetivo</td><td>Identificar el nivel de uso que se les da a las herramientas de software libre por parte de los docentes universitarios que imparten asignaturas en carreras relacionadas con la informática.</td></tr>
<tr><td>Forma de cálculo</td><td>$$UDU = \frac{(\sum \textbf{\textit{de docentes que han utilizado herramientas de software para la informática forense}})}{(\sum \textbf{\textit{del total de docentes}})} x100$$</td></tr>
<tr><td>Unidad de medida</td><td>Porcentaje (%).</td></tr>
<tr><td>Fuente de la información a utilizar</td><td>La información será obtenida mediante las encuestas realizadas a 125 docentes universitarios que imparten asignaturas en carreras relacionadas a la informática.</td></tr>
<tr><td>Interpretación</td><td>Bajo Medio Alto
<table><tr><td>0%</td><td>10%</td><td>20%</td><td>30%</td><td>40%</td><td>50%</td><td>60%</td><td>70%</td><td>80%</td><td>90%</td><td>100%</td></tr></table>
Mientras el valor de este indicador este más cercano al 100% refleja el hecho de que los docentes han hecho uso de este tipo de herramientas y por lo tanto están familiarizados con su aplicación. Si este valor se aleja del 100% nos indica que los docentes no han utilizado estas herramientas.</td></tr>
<tr><td>Frecuencia</td><td>Anual.</td></tr>
</table>

Tabla No 44: Descripción del indicador UDU

<table>
<tr><th colspan="2">USO DE HERRAMIENTAS DE INFORMÁTICA FORENSE (USIF).</th></tr>
<tr><td>Tipo</td><td>Actividad.</td></tr>
<tr><td>Objetivo</td><td>Identificar el nivel de uso por tipo de herramientas de software para informática forense por parte de los peritos informáticos para la obtención de la evidencia digital.</td></tr>
<tr><td>Forma de cálculo</td><td>$$\boldsymbol{USIF = \frac{(\sum de\ peritos\ que\ utilizan\ herramienta\ X)}{(\sum total\ de\ peritos\ )} x100}$$</td></tr>
<tr><td>Unidad de medida</td><td>Porcentaje (%).</td></tr>
<tr><td>Fuente de
la información
a utilizar</td><td>La información será obtenida mediante las encuestas realizadas a 12 peritos informáticos.</td></tr>
<tr><td>Interpretación</td><td>Bajo Medio Alto
<table><tr><td>0%</td><td>10%</td><td>20%</td><td>30%</td><td>40%</td><td>50%</td><td>60%</td><td>70%</td><td>80%</td><td>90%</td><td>100%</td></tr></table>
Mientras el valor obtenido para este indicador se encuentre más cercano al 100% reflejará que los peritos informáticos realizan un mayor uso de ese tipo de herramientas. Si dicho valor se aleja indica que los peritos hacen poco uso de herramientas de software de este tipo para la obtención de la evidencia digital. Este indicador ayudará a conocer en qué forma aumenta o disminuye el uso de herramientas de software para Informática Forense.</td></tr>
<tr><td>Frecuencia</td><td>Anual.</td></tr>
</table>

Tabla No 45: Descripción del indicador USIF

- Indicadores relacionados al recurso humano:

<table>
<tr><th colspan="2">PERSONAL DOCENTE CAPACITADO (PDC).</th></tr>
<tr><td>Tipo</td><td>Actividad.</td></tr>
<tr><td>Objetivo</td><td>Conocer si los docentes que imparten materias relacionadas a la informática en Universidades han sido capacitados en el uso de las herramientas de software para la informática forense.</td></tr>
<tr><td>Forma de cálculo</td><td>$$PDC = \frac{(\sum del\ total\ de\ docentes\ capacitados)}{(\sum total\ de\ docentes)}$$ x 100</td></tr>
<tr><td>Unidad de medida</td><td>Porcentaje (%).</td></tr>
<tr><td>Fuente de la información a utilizar</td><td>La información será obtenida mediante las encuestas realizadas a 125 docentes universitarios que imparten asignaturas en carreras relacionadas a la informática.</td></tr>
<tr><td>Interpretación</td><td>Malo Regular Bueno
<table><tr><td>0%</td><td>10%</td><td>20%</td><td>30%</td><td>40%</td><td>50%</td><td>60%</td><td>70%</td><td>80%</td><td>90%</td><td>100%</td></tr></table>
Mientras el valor obtenido para este indicador se encuentre más cercano al 100% reflejará que los docentes han sido capacitados en el uso de las herramientas de software para la informática forense lo que facilita el proceso de enseñanza de las mismas. Si el valor obtenido se acerca al 0% indica que los docentes no poseen conocimientos frutos de capacitaciones.</td></tr>
<tr><td>Frecuencia</td><td>Anual.</td></tr>
</table>

Tabla No 46: Descripción del indicador PDC

<table>
<tr><th colspan="2">PERITOS INFORMÁTICOS CAPACITADOS (PIC).</th></tr>
<tr><td>Tipo</td><td>Actividad.</td></tr>
<tr><td>Objetivo</td><td>Identificar el porcentaje de peritos informáticos que han recibido capacitaciones en el uso de las herramientas de software para la informática forense.</td></tr>
<tr><td>Forma de cálculo</td><td>$$PIC = \frac{(\sum del\ total\ de\ peritos\ capacitados)}{(\sum total\ de\ peritos)}$$ x 100</td></tr>
<tr><td>Unidad de medida</td><td>Porcentaje (%).</td></tr>
<tr><td>Fuente de la información a utilizar</td><td>La información será obtenida mediante las encuestas realizadas a 12 peritos que utilizan las herramientas para la informática forense en la obtención de loa evidencia digital.</td></tr>
<tr><td>Interpretación</td><td>Malo Regular Bueno
<table><tr><td>0%</td><td>10%</td><td>20%</td><td>30%</td><td>40%</td><td>50%</td><td>60%</td><td>70%</td><td>80%</td><td>90%</td><td>100%</td></tr></table>
Mientras el valor obtenido para este indicador se encuentre más cercano al 100% reflejará que la gran mayoría de los peritos informáticos han recibido capacitaciones en el uso de este tipo de herramientas lo que origina evidencia digital de mayor calidad ya que fue obtenida mediante la aplicación de conocimientos específicos. Si este valor se acerca al 0% indica que la mayoría de los peritos poseen conocimientos que no han sido adquiridos por medio de capacitaciones.</td></tr>
<tr><td>Frecuencia</td><td>Anual.</td></tr>
</table>

Tabla No 47: Descripción del indicador PIC

- Indicadores relacionados a los delitos informáticos:

CONOCIMIENTO SOBRE DELITOS INFORMÁTICOS POR PARTE DE LOS OPERADORES DE JUSTICIA EN EL SALVADOR (CDI).	
Tipo	Actividad.
Objetivo	Identificar el porcentaje de operadores de justicia en El Salvador que poseen conocimientos acerca de los delitos informáticos.
Forma de cálculo	$$CDI = \frac{(\sum \textit{del total de operadores de justicia que tienen conocimientos sobre delitos informáticos})}{(\sum \textit{total de operadores de justicia})} \textbf{ x 100}$$
Unidad de medida	Porcentaje (%).
Fuente de la información a utilizar	La información será obtenida mediante las encuestas realizadas a los operadores de justicia de El Salvador; específicamente 42 jueces, 184 abogados y 20 fiscales.
Interpretación	Malo Regular Bueno **0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%** Si su valor se encuentra cercano al 100% nos indica que los operadores de justicia en El Salvador poseen conocimientos acerca de los que son los delitos informáticos. En cambio, si este valor es cercano al 0% nos indica que no poseen conocimientos acerca de lo que son los delitos informáticos.
Frecuencia	Anual.

Tabla No 48: Descripción del indicador CDI

<table>
<tr><th colspan="2">INTERACCIÓN DE LOS DELITOS INFORMÁTICOS CON LOS OPERADORES DE JUSTICIA (ODI).</th></tr>
<tr><td>Tipo</td><td>Impacto.</td></tr>
<tr><td>Objetivo</td><td>Identificar el porcentaje de operadores de justicia que han tenido a su cargo procesos penales en los que han sido tratados delitos informáticos.</td></tr>
<tr><td>Forma de cálculo</td><td>$$ODI = \frac{(\sum \textit{de abogados, fiscales y jueces que han tratado juicios relacionados a delitos informáticos})}{(\sum \textit{total de operadores de justicia})}$$ x 100</td></tr>
<tr><td>Unidad de medida</td><td>Porcentaje (%).</td></tr>
<tr><td>Fuente de la información a utilizar</td><td>La información será obtenida mediante las encuestas realizadas a los operadores de justicia de El Salvador; específicamente 42 jueces, 184 abogados y 20 fiscales.</td></tr>
<tr><td>Interpretación</td><td>Malo Regular Bueno
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Mientras el valor de este indicador se aproxime al 100% refleja que la mayoría de operadores de justicia han estado involucrados en procesos judiciales que involucran a delitos informáticos, en cambio si el valor se aleja del 100% los delitos informáticos son poco comunes para los involucrados en los procedimientos judiciales.</td></tr>
<tr><td>Frecuencia</td><td>Anual.</td></tr>
</table>

Tabla No 49: Descripción del indicador ODI

Los indicadores antes presentados serán utilizados para la realización de un diagnóstico acerca de la situación actual del uso de las herramientas de software para la informática forense descubierta durante el transcurso de la presente investigación.

C. APLICACIÓN DE LOS INDICADORES

Una vez definido el conjunto de indicadores procedemos a su correspondiente aplicación haciendo uso de los datos obtenidos durante la investigación. Con el propósito de presentar la evaluación realizada se hará uso del siguiente formato:

NOMBRE DEL INDICADOR	
Forma de cálculo	
Evaluación	
Valor obtenido	
Clasificación	

Tabla No 50: Formato para la presentación de la evaluación de los indicadores

En donde :

- ✓ **Forma de cálculo:** expresión matemática utilizada para la obtencion del valor del indicador.
- ✓ **Evaluación:** sustitución de cada termino que conforma la expresión matemática por su correspondiente valor, en base a los datos recolectados.
- ✓ **Valor obtenido:** valor númerico del indicador, expresado en terminos porcentuales.
- ✓ **Clasificación:** Representación en la escala propuesta del resultado obtenido.

En base al resultado obtenido se llevará a cabo una interpretación del indicador aplicado. Como paso final y tomando en cuenta el análisis conceptual utilizado para la elaboración de los indicadores, se hará un diagnóstico para cada variable o concepto que fueron identificados en el analisis conceptual, los cuales son:

1. Evidencia digital.
2. Herramientas de software para la informática forense.
3. Recurso humano.
4. Delito informático.

I. INDICADORES RELACIONADOS A LA EVIDENCIA DIGITAL

IMPORTANCIA DADA A LA EVIDENCIA DIGITAL (IED).	
Forma de cálculo	$$IVD = \frac{\left(\begin{array}{c}\sum \text{de jueces,abogados y fiscales} \\ \text{que consideran determinate la evidencia digital} \\ \text{en los procesos judiciales}\end{array}\right)}{\left(\sum \text{dejueces,abogados y fiscales}\right)} \text{ x 100}$$
Evaluación	$$IVD = \frac{(193)}{(246)} \text{ x 100}$$
Valor obtenido	**78.45 %**
Clasificación	Malo — Regular — Bueno 0% | 10% | 20% | 30% | 40% | 50% | 60% | 70% | **80%** | 90% | 100%

Tabla No 51: Evaluación del indicador IED

Según el resultado del indicador "Importancia dada a la evidencia digital", el **78.45%** de los operadores de justicia en El Salvador consideran determinante el valor de la evidencia digital al momento de resolver un delito informático.

Para los abogados, fiscales y jueces la presentación de este tipo de evidencia es de suma importancia ya que representa una prueba científica mediante la cual se pueden determinar responsabilidades o confirmar la existencia de ilícitos. En base al resultado obtenido éste puede ser catalogado como "Bueno" según la escala utilizada.

VALIDEZ DADA A LA EVIDENCIA DIGITAL (VED).	
Forma de cálculo	$$VED = \frac{\left(\begin{array}{c}\sum \text{ de jueces,abogados y fiscales} \\ \text{que consideran que los peritos poseen} \\ \text{conocimientos suficientes para obtener evidencia} \\ \text{digital válida}\end{array}\right)}{\left(\sum \text{de jueces, abogados y fiscales}\right)} \text{ x 100}$$
Evaluación	$$VED = \frac{(118)}{(246)} \text{ x 100}$$
Valor obtenido	**47.96 %**
Interpretación	Malo Regular Bueno 0% 10% 20% 30% 40% **50%** 60% 70% 80% 90% 100%

Tabla No 52: Evaluación del indicador VED

Al realizar la evaluación del indicador "Validez dada a la evidencia digital", obtenemos que un **47.96%** de los abogados, jueces y fiscales consideran que los peritos poseen los suficientes conocimientos que les permitan la obtención de una evidencia digital que pueda ser considerada como válida en los procesos judiciales.

Resulta preocupante el hecho de que menos de la mitad de los operadores de justicia consideren que los peritos informáticos tienen los conocimientos necesarios para la correcta aplicación de las metodologías y herramientas de la informática forense, por esta razón el resultado obtenido para el indicador es de un nivel regular-malo.

Con respecto a la evidencia digital y en base a los resultados obtenidos en los indicadores IED y VED podemos establecer que los operadores de justicia reconocen la importancia de la misma en la resolución de los delitos informáticos, pero menos de la mitad de ellos consideran que en la actualidad los peritos informáticos poseen conocimientos capaces de proveer evidencia digital valida. Mientras más confianza se tenga en las habilidades técnicas y científicas de los peritos, mayor será la credibilidad de la evidencia presentada por estos profesionales.

II. INDICADORES RELACIONADOS A LAS HERRAMIENTAS DE SOFTWARE

<table>
<tr><th colspan="2">CONOCIMIENTO SOBRE HERRAMIENTAS DE SOFTWARE LIBRE (CSL).</th></tr>
<tr><td>Forma de cálculo</td><td>$$CSL = \frac{(\sum \textit{peritos que tienen mayor conocimiento sobre software libre para informatica forense})}{(\sum \textit{total de peritos})} x100$$</td></tr>
<tr><td>Evaluación</td><td>$$CSL = \frac{(5)}{(12)}$$ x 100</td></tr>
<tr><td>Valor obtenido</td><td>41.67 %</td></tr>
<tr><td>Clasificación</td><td>Bajo Medio Alto
0% | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100%</td></tr>
</table>

Tabla No 53: Evaluación del indicador CSL

Según el indicador "Conocimientos sobre herramientas de software libre", el **41.67%** de los peritos tienen mayor conocimiento sobre herramientas de software libre para la informática forense lo cual indica que un porcentaje alto ha optado por las alternativas de software libre debido principalmente a los costos de las herramientas de software propietario para informática forense.

El resultado sobre conocimientos sobre las herramientas de software libre para informática forense es de un nivel medio - bajo debido a que los peritos optan por alternativas realistas conforme al medio ambiente donde se desenvuelven. Además existen casos en que los peritos deben poseer las herramientas para la informática forense ya que las instituciones no las proporcionan.

CONOCIMIENTO SOBRE HERRAMIENTAS DE SOFTWARE PROPIETARIO (CSP).	
Forma de cálculo	$$CSP = \frac{(\sum \textbf{peritos que tienen mayor conocimiento sobre software propietario para informatica forense})}{(\sum \textbf{total de peritos})} x100$$
Evaluación	$CSP = \frac{(7)}{(12)}$ **x 100**
Valor obtenido	**58.33 %**
Clasificación	Bajo — Medio — Alto 0% | 10% | 20% | 30% | 40% | 50% | **60%** | 70% | 80% | 90% | 100%

Tabla No 54: Evaluación del indicador CSP

Según el resultado del indicador "Conocimientos sobre herramientas de software propietario", un **58.33**% de peritos poseen mayor conocimiento sobre herramientas de software propietario; el resultado es superior a la mitad de peritos que prefieren invertir en herramientas con suficiente documentación y capacitaciones accesibles aunque sea fuera del país.

El porcentaje que indica un mayor conocimiento sobre herramientas de software libre para informática forense es de un nivel medio – alto, esto debido a que los peritos optan por alternativas con suficiente documentación para auto capacitarse en la aplicación de las mismas obteniendo así los conocimientos necesarios para la obtención de evidencia digital.

USO DE LAS HERRAMIENTAS DE SOFTWARE PARA LA INFORMÁTICA FORENSE POR PARTE DE LOS DOCENTES UNIVERSITARIOS (UDU).	
Forma de cálculo	$$UDU = \frac{(\sum \textit{de docentes que han utilizado herramientas de software para la informática forense})}{(\sum \textit{del total de docentes})} x100$$
Evaluación	$$UDU = \frac{(75)}{(125)}$$ **x 100**
Valor obtenido	**60.00%**
Clasificación	Bajo — Medio — Alto 0% | 10% | 20% | 30% | 40% | 50% | **60%** | 70% | 80% | 90% | 100%

Tabla No 55: Evaluación del indicador UDU

El conocimiento acerca de las herramientas utilizadas por los docentes ha sido adquirido principalmente de manera autodidacta ya que solo el **10.40**% de los docentes ha recibido capacitaciones acerca de la informática forense y sus herramientas de software.

El indicador "Uso de las herramientas de software para la informática forense por parte de los docentes universitarios" dio como resultado un **60**% de los docentes han utilizado o utilizan herramientas aplicables en la informática forense.

La aplicación por parte de docentes de software utilizable en la informática forense se clasifica en un grado medio – alto tomando en cuenta que la mayoría de docentes utilizan este tipo de herramientas enfocado a la utilidad de las mismas en situaciones a las que se enfrenta el profesional informático.

Dentro de las herramientas de software para informática forense se encuentran varios tipos, el diagnóstico se realizará aplicando el indicador a cada tipo de herramientas y utilizando las respuestas obtenidas por parte de los peritos.

El nivel de uso de las herramientas está ligado directamente a la calidad de los peritajes realizados en los casos de delitos informáticos, por lo cual el alto o bajo nivel de uso afecta de manera determinante la obtención de evidencia digital.

<table>
<tr><th colspan="2">USO DE LAS HERRAMIENTAS DE INFORMÁTICA FORENSE (USIF) PARA RECUPERACIÓN DE DATOS ELIMINADOS.</th></tr>
<tr><td>Forma de cálculo</td><td>$$USIF = \frac{(\sum \textbf{de peritos que utilizan herramientas para recuperacion de datos eliminados})}{(\sum \textbf{total de peritos})} x100$$</td></tr>
<tr><td>Evaluación</td><td>$$USIF = \frac{(12)}{(12)}$$ x 100</td></tr>
<tr><td>Valor obtenido</td><td>100.00 %</td></tr>
<tr><td>Clasificación</td><td>Bajo Medio Alto
0% | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100%</td></tr>
</table>

Tabla No 56: Evaluación del indicador USIF (1)

El indicador “Uso de las herramientas de software para la informática forense” dio como resultado un 100% en herramientas para la recuperación de datos lo cual implica que todos los peritos han utilizado o utilizan herramientas para recuperar datos de los medios comprometidos en los delitos.

El nivel de uso por parte de peritos de herramientas para recuperación de datos se clasifica en un grado Alto ya que esto garantiza que si algún archivo que pueda ser catalogado como evidencia digital fue eliminado podrá ser recuperado.

USO DE LAS HERRAMIENTAS DE INFORMÁTICA FORENSE (USIF) PARA COPIAS DE DATOS BIT A BIT.	
Forma de cálculo	$$USIF = \frac{(\sum \textbf{de peritos que utilizan herramientas para copias de datos bit a bit})}{(\sum \textbf{total de peritos})} x100$$
Evaluación	$$USIF = \frac{(2)}{(12)}$$ **x 100**
Valor obtenido	**16.67%**
Clasificación	Bajo Medio Alto 0% 10% **20%** 30% 40% 50% 60% 70% 80% 90% 100%

Tabla No 57: Evaluación del indicador USIF (2)

El indicador "Uso de las herramientas de software para la informática forense" dio como resultado un 16.67% en herramientas para copia de datos bit a bit, lo cual implica que un pequeño porcentaje utiliza herramientas para realizar copias de los medios investigados.

El nivel de uso por parte de los peritos de herramientas de copiado de datos bit a bit se clasifica en un grado bajo ya que si no se realizan copias de los medios pueden contaminarse afectando esto la evidencia y perdiendo su valor a nivel legal.

USO DE LAS HERRAMIENTAS DE INFORMÁTICA FORENSE (USIF) PARA RECUPERACIÓN DE NÚMEROS DE LICENCIA	
Forma de cálculo	$$USIF = \frac{(\sum \textbf{de peritos que utilizan herramientas para recuperacion de numeros de licencia})}{(\sum \textbf{total de peritos})} x100$$
Evaluación	$$USIF = \frac{(2)}{(12)}$$ **x 100**
Valor obtenido	**16.67 %**
Clasificación	Bajo Medio Alto 0% 10% **20%** 30% 40% 50% 60% 70% 80% 90% 100%

Tabla No 58: Evaluación del indicador USIF (3)

El indicador "Uso de las herramientas de software para la informática forense" dio como resultado un **16.67**% en herramientas para la recuperación de números de licencia, lo cual implica que una pequeña parte de los peritos utiliza herramientas para comprobar el número de licencia de software propietario en casos de piratería de software.

El nivel de uso por parte de los peritos de herramientas para recuperación de números de licencia se clasifica en un grado bajo ya que la recuperación de estos números permitiría comprobar si el software instalado en los equipos concuerda con los números de licencia de los certificados de autenticidad.

USO DE LAS HERRAMIENTAS DE INFORMÁTICA FORENSE (USIF) PARA MONITOREO DE COMPUTADORAS	
Forma de cálculo	$$USIF = \frac{(\sum \textbf{de peritos que utilizan herramientas para monitoreo de computadoras})}{(\sum \textbf{total de peritos})} x100$$
Evaluación	$$USIF = \frac{(6)}{(12)}$$ **x 100**
Valor obtenido	**50.00 %**
Clasificación	Bajo Medio Alto 0% 10% 20% 30% 40% **50%** 60% 70% 80% 90% 100%

Tabla No 59: Evaluación del indicador USIF (4)

El indicador "Uso de las herramientas de software para la informática forense" dio como resultado un **50%** en herramientas para monitoreo de computadoras, lo cual implica que la mitad de peritos ha utilizado o utilizan herramientas para registrar las acciones en equipos comprometidos en delitos informáticos.

El nivel de uso por parte de los peritos de las herramientas de monitoreo de computadoras se clasifica en un grado medio ya que este tipo de software permite obtener detalles de las acciones realizadas en equipos de cómputo.

USO DE LAS HERRAMIENTAS DE INFORMÁTICA FORENSE (USIF) PARA CALCULO DE HASH.	
Forma de cálculo	$$USIF = \frac{(\sum \textbf{de peritos que utilizan herramientas para calculo de hash})}{(\sum \textbf{total de peritos})} x100$$
Evaluación	$$USIF = \frac{0}{(12)}$$ **x 100**
Valor obtenido	**0.00 %**
Clasificación	Bajo Medio Alto **0%** 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

Tabla No 60: Evaluación del indicador USIF (5)

El indicador "Uso de las herramientas de software para la informática forense" dio como resultado un **0%** en herramientas para cálculo de numero Hash, lo cual implica que ningún perito utiliza herramientas para calcular el número Hash que ayuda a garantizar la integridad de los datos de los medios donde se busca la evidencia.

El nivel de uso por parte de los peritos de herramientas para cálculo de hash se clasifica en un grado bajo debido a que ningún perito manifestó utilizarlas aunque estas son una de las principales herramientas para garantizar la integridad de datos y a su vez la validez de la evidencia digital.

<table>
<tr><th colspan="2">USO DE LAS HERRAMIENTAS DE INFORMÁTICA FORENSE (USIF) PARA MARCADO DE DOCUMENTOS.</th></tr>
<tr><td>Forma de cálculo</td><td>$$USIF = \frac{(\sum \textbf{de peritos que utilizan herramientas de marcado de documentos})}{(\sum \textbf{total de peritos})} x100$$</td></tr>
<tr><td>Evaluación</td><td>$$USIF = \frac{(4)}{(12)}$$ x 100</td></tr>
<tr><td>Valor obtenido</td><td>33.33 %</td></tr>
<tr><td>Clasificación</td><td>Bajo Medio Alto
0% | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100%</td></tr>
</table>

Tabla No 61: Evaluación del indicador USIF (6)

El indicador “Uso de las herramientas de software para la informática forense” dio como resultado un **33.33%** en herramientas para marcado de documentos, lo cual implica que la tercera parte de los peritos han utilizado o utilizan herramientas para marcar archivos para posterior rastreo.

El nivel de uso por parte de los peritos de herramientas de marcado de documentos se clasifica en un grado bajo ya que solamente la tercera parte los utiliza y el uso de estos ayuda al rastreo de archivos en investigaciones.

USO DE LAS HERRAMIENTAS DE INFORMÁTICA FORENSE (USIF) PARA RECUPERACIÓN DE CONTRASEÑAS DE ARCHIVOS PROTEGIDOS.	
Forma de cálculo	$$USIF = \frac{(\sum \textbf{de peritos que utilizan herramientas para recuperacion de contraseñas de archivos protegidos})}{(\sum \textbf{total de peritos})} x100$$
Evaluación	$USIF = \frac{(1)}{(12)}$ **x 100**
Valor obtenido	**8.33 %**
Clasificación	Bajo — Medio — Bueno 0% | **10%** | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100%

Tabla No 62: Evaluación del indicador USIF (7)

El indicador "Uso de las herramientas de software para la informática forense" dio como resultado un **8.33%** en herramientas para la recuperación de contraseñas, lo cual implica una mínima cantidad de peritos han utilizado o utilizan herramientas que les permitan recuperar contraseñas de archivos protegidos en los análisis forenses.

El nivel de uso por parte de los peritos de herramientas de recuperación de contraseñas se clasifica en un grado bajo ya que la cantidad de peritos que los utilizan es mínima y estos ayudan a acceder al contenido de los archivos.

Como análisis general, en el país el nivel de uso de herramientas aplicables a la informática forense es malo o bajo debido a que la poca aplicación de las mismas afecta los resultados de los análisis realizados por los peritos informáticos y la obtención de evidencia digital que los operadores de justicia puedan considerar valida. Este nivel bajo de uso indica el poco desarrollo que existe sobre la informática forense y las debilidades de las mismas para enfrentar la variedad y creciente cantidad de delitos informáticos que se cometen en el país.

III. INDICADORES RELACIONADOS AL RECURSO HUMANO

PERSONAL DOCENTE CAPACITADO (PDC).	
Forma de cálculo	$PDC = \frac{(\sum del\ total\ de\ docentes\ capacitados)}{(\sum total\ de\ docentes)}$ **x 100**
Evaluación	$PDC = \frac{(13)}{(125)}$ **x 100**
Valor obtenido	**10.4 %**
Interpretación	Bajo Medio Alto 0% **10%** 20% 30% 40% 50% 60% 70% 80% 90% 100%

Tabla No 63: Evaluación indicador PDC

Al realizar la evaluación del indicador "Personal docente capacitado" obtenemos un valor de **10.4%**. Podemos apreciar que la mayoría del personal docente de las instituciones de educación superior que imparten asignaturas relacionadas con las carreras informáticas no han recibido ningún tipo de capacitación acerca del uso de las herramientas de software para la informática forense.

El resultado de este indicador es catalogado como bajo. Un personal docente debidamente capacitado facilitaría el proceso de enseñanza en el uso de las herramientas de software y en el área de la informática forense en general, ya que contaría con sólidos conocimientos que servirían de base al momento de establecer los puntos a ser tratados durante el aprendizaje de los estudiantes.

<table>
<tr><th colspan="2">PERITOS INFORMÁTICOS CAPACITADOS (PIC)</th></tr>
<tr><td>Forma de cálculo</td><td>$$PIC = \frac{(\sum del\ total\ de\ peritos\ capacitados)}{(\sum total\ de\ peritos)}$$ x 100</td></tr>
<tr><td>Evaluación</td><td>$$PIC = \frac{(10)}{(12)}$$ x 100</td></tr>
<tr><td>Valor obtenido</td><td>83.33 %</td></tr>
<tr><td>Interpretación</td><td>Malo Regular Bueno
<table><tr><td>0%</td><td>10%</td><td>20%</td><td>30%</td><td>40%</td><td>50%</td><td>60%</td><td>70%</td><td>80%</td><td>90%</td><td>100%</td></tr></table></td></tr>
</table>

Tabla No 64: Evaluación del indicador PIC

Al hacer la evaluación del indicador "Peritos Informáticos Capacitados" obtenemos que un 80% de los peritos informáticos ha recibido capacitación sobre el uso de alguna herramienta de software para la informática forense.

El resultado obtenido para este indicador es catalogado como bueno, aunque esto no quiere decir que los peritos sean expertos en el uso de todas las herramientas de software, sino que en algún momento de su carrera, ya sea por necesidad o por la búsqueda de nuevos conocimientos han recibido capacitaciones.

Con respecto al Recurso Humano, uno de los principales problemas presentes en nuestro país es la falta de una institución que sea la encargada de la formación de este tipo de profesionales o por lo menos que se encargue de otorgar las certificaciones necesarias que garanticen que los profesionales de la informática tengan conocimientos sobre el uso de este tipo de herramientas.

IV. INDICADORES RELACIONADOS A LOS DELITOS INFORMÁTICOS

<table>
<tr><th colspan="2">CONOCIMIENTO SOBRE DELITOS INFORMÁTICOS POR PARTE DE LOS OPERADORES DE JUSTICIA EN EL SALVADOR(CDI)</th></tr>
<tr><td>Forma de cálculo</td><td>$$CDI = \frac{(\sum \textit{del total de operadores de justicia que tienen conocimientos sobre delitos informáticos})}{(\sum \textit{total de operadores de justicia})}$$ x 100</td></tr>
<tr><td>Evaluación</td><td>$$CDI = \frac{(205)}{(246)}$$ x 100</td></tr>
<tr><td>Valor obtenido</td><td>83.33 %</td></tr>
<tr><td>Interpretación</td><td>Malo Regular Bueno
<table><tr><td>0%</td><td>10%</td><td>20%</td><td>30%</td><td>40%</td><td>50%</td><td>60%</td><td>70%</td><td>80%</td><td>90%</td><td>100%</td></tr></table></td></tr>
</table>

Tabla No 65: Evaluación del indicador CDI

Al realizar la evaluación de este indicador obtenemos como resultado que un **83.33%** de los operadores de justicia conocen acerca de los delitos informáticos. Debido a que este tipo de delitos ha ido en aumento, los operadores de justicia se han visto en la necesidad de adquirir o actualizar sus conocimientos y de esta forma estar preparados para poder tratar casos de este tipo.

El resultado de este indicador puede ser calificado como bueno ya que un alto porcentaje de abogados, jueces y fiscales han adquirido este tipo de conocimiento, para la sociedad esto es muy importante ya que se cuenta con un sistema judicial cuyos operadores han ido mejorando sus capacidades ante la necesidad de hacerle frente al auge de los delitos informáticos.

INTERACCIÓN DE LOS DELITOS INFORMÁTICOS CON LOS OPERADORES DE JUSTICIA (ODI).	
Forma de cálculo	$PIC = \frac{(\sum \textit{de abogados, fiscales y jueces que han tratado juicios relacionados a delitos informáticos})}{(\sum \textit{total de operadores de justicia})}$ **x 100**
Evaluación	$PIC = \frac{(119)}{(246)}$ **x 100**
Valor obtenido	**48.37%**
Interpretación	Malo — Regular — Bueno 0% | 10% | 20% | 30% | 40% | **50%** | 60% | 70% | 80% | 90% | 100%

Tabla No 66: Evaluación del indicador ODI

La evaluación de este indicador dio como resultado que el **48.37%** de los operadores de justicia han estado involucrados en procesos judiciales en los que han sido tratados delitos informáticos, un poco menos de la mitad han tenido una interacción directa con este tipo de ilícitos.

Este valor puede ser catalogado con un nivel de regular, en la actualidad la incidencia de los delitos informáticos abarca casi a la mitad de los operadores de justicia, siendo estos los que conocen de primera mano los delitos informáticos y el valor de la evidencia digital presentada en la resolución de estos procesos judiciales.

Con respecto a los delitos informáticos y utilizando los valores obtenidos para los indicadores presentados anteriormente (CDI y ODI) podemos concluir que no todo el conocimiento que poseen los abogados, fiscales o jueces es por la interacción directa sino que una parte de este conocimiento puede ser adquirido a través de los medios de comunicación o de forma autodidacta.

D. ELABORACIÓN DEL DIAGNÓSTICO

I. DIAGNÓSTICO CONCERNIENTE AL SECTOR LEGAL

FUENTES DE INFORMACION Y DATOS PARA EL DIAGNÓSTICO

- ✓ 20 encuestas realizadas a fiscales
- ✓ 184 encuestas realizadas a abogados de la Procuraduría General de la República
- ✓ 42 encuestas realizadas a jueces de instrucción
- ✓ Indicador IDE(Importancia dada a la Evidencia Digital)
- ✓ Indicador VED(Validez dada a la Evidencia Digital)
- ✓ Indicador ODI(Interacción de los operadores de Justicia en Delitos Informáticos)
- ✓ Indicador CDI (Conocimiento de los Operadores de Justicia de los Delitos Informáticos)

PUNTOS DE DIAGNÓSTICO

- ❖ Importancia dada a la Evidencia Digital
- ❖ Validez dada a la Evidencia digital
- ❖ Interacción de los operadores de Justicia en Delitos Informáticos
- ❖ Conocimiento de los Operadores de Justicia de los Delitos Informáticos
- ❖ Conocimientos de Evidencia digital por parte de los operadores de justicia
- ❖ Factores que validan la Evidencia Digital

DIAGNÓSTICO ACERCA DE LA IMPORTANCIA DADA A LA EVIDENCIA DIGITAL

El 78.45% de los encuestados del sector justicia consideran determinante la evidencia digital lo cual implica que aunque no existe un marco legal que la soporte consideran que esta puede ser determinante para la resolución de casos de delitos informáticos.

Lo anterior da un buen punto de partida en caso que se creen leyes que apoyen la investigación en casos de delitos informáticos.

DIAGNÓSTICO ACERCA DE LA VALIDEZ DADA A LA EVIDENCIA DIGITAL

El 47.96% de los encuestados del sector justicia considera que los conocimientos de los peritos son suficientes para considerar la evidencia digital recolectada como valida lo cual denota que los operadores de justicia tienen una percepción realista acerca del conocimientos especializado de los peritos informáticos.

Este resultado indica que debe trabajarse en la capacitación y certificación de los peritos informáticos para aumentar la confianza de los operadores de justicia en los mismos.

DIAGNÓSTICO ACERCA DE LA INTERACCIÓN DE LOS OPERADORES DE JUSTICIA EN DELITOS INFORMÁTICOS

El 48.37% de los operadores de justicia encuestados han participado en procesos judiciales que implican delitos informáticos ya sea como jueces, fiscales o defensores esto indica un grado significativo ya que prácticamente la mitad de ellos están familiarizados con este tipo de delitos.

Es considerado de importancia la cantidad de operadores de justicia que han participado en este tipo de procesos judiciales ya que da una pauta de conocimiento acerca de los mismos, esto ayuda a que el sector justicia apoye la creación de leyes que soporten la evidencia digital.

DIAGNÓSTICO ACERCA DEL CONOCIMIENTO DE LOS OPERADORES DE JUSTICIA DE LOS DELITOS INFORMÁTICOS

El 83.33% de los operadores de justicia conocen que son los delitos informáticos esto es un punto a favor del desarrollo de la informática forense en el país porque son ellos los encargados de aplicar las leyes que correspondan en la persecución de los mismos.

El alto grado de conocimiento de los delitos informáticos por parte de los operadores de justicia además indica que se comenten en el país muchos delitos informáticos de tal forma que casi la totalidad de los encuestados conoce de ellos.

DIAGNÓSTICO ACERCA DE CONOCIMIENTOS DE EVIDENCIA DIGITAL POR PARTE DE LOS OPERADORES DE JUSTICIA

El 63.01% de los encuestados del sector legal, conocen que es la evidencia digital, es un porcentaje mayor al de operadores de justicia, que ha interactuado en procesos judiciales de delitos informáticos y menor a los que saben que son los delitos informáticos lo cual implica que existe un interés por parte de los operadores de justicia acerca de los aspectos legales que implica la informática forense.

El apoyo por parte del sector legal en la informática forense en caso de fomentar el desarrollo de la misma sería bastante grande debido al interés de ellos sobre el tema.

DIAGNÓSTICO ACERCA DE LOS FACTORES QUE VALIDAN LA EVIDENCIA DIGITAL

Para los operadores de justicia los factores que validan la evidencia digital en un proceso judicial principalmente son:

La capacidad técnica del perito, esta es de suma importancia ya que un perito capacitado y metódico al realizar el análisis forense garantiza que no contaminara la evidencia a la hora de obtenerla.

El marco legal que la soporta, aunque no existe en el país un marco legal para delitos informáticos, los operadores de justicia se apoyan de las leyes existentes para los procesos judiciales de este tipo de delitos.

Hay que fomentar el desarrollo de la informática forense en el país promoviendo profesionales especializados y certificados, así como apoyando la creación de leyes que garanticen hacer justicia en este tipo de delitos.

II. DIAGNÓSTICO CONCERNIENTE AL SECTOR EDUCATIVO

FUENTES DE INFORMACION Y DATOS PARA EL DIAGNOSTICO

- ✓ 95 encuestas realizadas a docentes de universidades privadas
- ✓ 30 encuestas realizadas a docentes de la universidad de el salvador
- ✓ Indicador PDC(Personal Docente Capacitado)
- ✓ Indicador UDU (Uso de las herramientas de software para la informática forense por parte de los docentes universitarios)

PUNTOS DE DIAGNÓSTICO

- ❖ Capacitación de personal docente
- ❖ Aplicación de herramientas de software para informática forense por docentes universitarios de carreras informáticas
- ❖ Importancia dada por los docentes al conocimientos sobre herramientas de software por parte de nuevos profesionales informáticos
- ❖ Disposición de personal docente a ser capacitados e impartir conocimientos sobre informática forense

DIAGNOSTICO ACERCA DE LA CAPACITACIÓN DE PERSONAL DOCENTE EN LAS UNIVERSIDADES DEL PAIS

El porcentaje de personal docente capacitado es de 10.40% a partir de este número es notorio que en las Instituciones de Educación Superior del País no existe suficiente recurso humano capacitado en el área de informática forense, debido principalmente a la falta de cultura e interés en esta área de aplicación de la informática por parte de las autoridades Universitarias

La capacitación de personal docente traería grandes beneficios a la sociedad enfocado al proceso de transmisión de conocimiento maestro-alumno aumentando a mediano plazo la capacidad de los profesionales en esta área realizar peritajes en casos de delitos informáticos. La capacitación de los nuevos profesionales en informática forense aumentaría a largo plazo la resolución favorable en casos de delitos informáticos promoviendo el desarrollo de la misma en pro del crecimiento en el área de tecnologías de información en el país.

DIAGNOSTICO ACERCA DE LA APLICACIÓN DE HERRAMIENTAS DE SOFTWARE PARA INFORMÁTICA FORENSE POR DOCENTES UNIVERSITARIOS DE CARRERAS INFORMÁTICAS

El porcentaje de personal docente que aplica herramientas de software para informática forense es de 60.00% a partir de este número es notorio que la mayoría de los docentes universitarios en las carreras informáticas que se imparten en la universidades del País, aplican este tipo de software en sus actividades profesionales y no necesariamente realizando un peritaje en algún delito informático; es importante resaltar que los docentes se interesan por estos tipos de software y aun sin haber recibido capacitaciones han aprendido de forma autodidacta acerca de cómo se utilizan los mismos.

La aplicación por parte de personal docente es un buen punto de partida en el caso que se deseara capacitarlos, debido a que ya tienen cierto conocimiento sobre las herramientas en cuestión y tomando en cuenta la variedad que existen de estas y su aplicación por parte de los docentes lo cual volvería estos conocimientos complementarios entre sí para la capacitación de docentes y facilitaría la transmisión de los mismos a los futuros profesionales.

DIAGNOSTICO ACERCA DE LA IMPORTANCIA DADA POR LOS DOCENTES AL CONOCIMIENTO SOBRE HERRAMIENTAS DE SOFTWARE PARA INFORMATICA FORENSE POR PARTE DE NUEVOS PROFESIONALES INFORMÁTICOS

El porcentaje de personal docente que considera importante y que se debería de impartir conocimientos sobre herramientas de software para informática forense a los futuros profesionales es de 85.6% lo cual confirma que la mayoría de docentes universitarios de carreras relacionadas a las tecnologías de información reconocen la importancia de este tipo de conocimientos para fomentar el desarrollo de esta área de aplicación de la informática y a su vez aumentar la aplicación de estas herramientas que ayuden directamente en la resolución de casos de delitos informáticos apoyando al sector Justicia de nuestro país.

Los docentes consideran además que este tipo de conocimientos aumentarían el valor de los profesionales en informática tomando en cuenta que se volverían más competitivos y estarían preparados para apoyar a los fiscales realizando peritajes informáticos, La importancia que dan a este tipo de conocimientos se ve además considerada en que consideran que debe realizarse promoción de estos por parte de las instituciones de educación superior y del gobierno.

La importancia de este tipo de conocimientos tiene su origen en los beneficios que traen a los profesionales en Informática y a la sociedad en general debido a las ventajas directas de la aplicación de las herramientas en la resolución de delitos informáticos.

DIAGNOSTICO ACERCA DE LA DISPOSICIÓN DE PERSONAL DOCENTE A SER CAPACITADOS E IMPARTIR CONOCIMIENTOS SOBRE INFORMÁTICA FORENSE

El porcentaje de personal docente dispuesto a ser capacitado es de 88.9% y el dispuesto a impartir conocimientos sobre informática forense es de 84.8% es evidente el alto porcentaje de docentes que están en disposición de colaborar y formar parte practica en el desarrollo de la informática forense en el país tomando en cuenta que ellos serian los principales encargados de su difusión a través de las clases teórico-practicas que dan a sus alumnos.

Poseer personal docente capacitado en informática forense no solo aumentara el nivel de desarrollo de las Tecnologías de Información sino que será una base solida como apoyo al sector justicia del país a través de la formación de peritos informáticos.

III. DIAGNÓSTICO CONCERNIENTE AL SECTOR PROFESIONAL

FUENTES DE INFORMACION Y DATOS PARA EL DIAGNÓSTICO

- ✓ 12 encuestas realizadas a peritos informáticos del país
- ✓ Indicador PIC(Peritos Informáticos Capacitados)
- ✓ Indicador USIF (Uso de las herramientas de Informática Forense)
- ✓ Indicador CSP(Conocimiento sobre herramientas de Software Propietario)
- ✓ Indicador CSL(Conocimiento sobre herramientas de Software Libre)

PUNTOS DE DIAGNÓSTICO

- ❖ Capacitación de Peritos Informáticos
- ❖ Uso de las Herramientas de Informática Forense
- ❖ Conocimientos sobre herramientas de Software para informática forense libres o propietarias
- ❖ Existencia de Instituciones Capacitadoras en Informática Forense
- ❖ Delitos tratados en mayor grado por los Peritos Informáticos
- ❖ Percepción del rendimiento de software libre aplicable en informática forense y dificultades para su implementación
- ❖ Importancia de Capacitación en Informática Forense en Universidades y limitantes para adquirir nuevos conocimientos sobre herramientas de Informática Forense.

DIAGNÓSTICO ACERCA DE LA CAPACITACIÓN DE PERITOS INFORMATICOS EN EL PAIS

En referencia a este punto un 80% de los peritos informáticos ha recibido capacitación sobre el uso de alguna herramienta de software para la informática forense.

Los peritos no son especialistas en el uso de todas las herramientas de software, sino que en algún momento de su carrera, ya sea por necesidad o por la búsqueda de nuevos conocimientos han recibido capacitaciones.

Con respecto al Recurso Humano, uno de los principales problemas presentes en nuestro país es la falta de una institución que sea la encargada otorgar las certificaciones que garanticen que los profesionales de la informática tengan conocimientos sobre el uso de este tipo de herramientas.

La capacitación constante y certificación de conocimientos de los peritos ayudaría al desarrollo de la informática forense en el país y fomentaría la creación de laboratorios especializados en esta área para la resolución de delitos informáticos como aliado directo de las autoridades de justicia del país.

DIAGNÓSTICO ACERCA DE EL USO DE LAS HERRAMIENTAS DE INFORMATICA FORENSE

Los peritos informáticos que practican análisis forenses en el país tienen conocimientos sobre diversas herramientas de software para informática forense principalmente acerca de las herramientas útiles en los tipos de delitos más tratados por los mismos pero la falta de promoción de la informática forense en el país limita a su vez la expansión de este conocimiento por parte de los peritos.

En el país el nivel de uso de herramientas aplicables a la informática forense es malo o bajo debido a que el poco conocimiento de las mismas afecta los resultados de los análisis realizados por los peritos informáticos y la obtención de evidencia digital que los operadores de justicia puedan considerar valida. Este nivel bajo de uso indica las debilidades de las mismas para enfrentar la variedad y creciente cantidad de delitos informáticos que se cometen en el país.

DIAGNÓSTICO ACERCA DE CONOCIMIENTOS SOBRE HERRAMEINTAS DE SOFTWARE LIBRE Y PROPIETARIO POR PARTE DE PERITOS INFORMATICOS

Los peritos manifestaron tener mayor conocimiento sobre herramientas de software propietario para informática forense con un 58.33% y un 41.67% de los peritos tienen mayor conocimiento sobre herramientas de software libre para la informática forense lo cual indica que la mayoría de peritos posee más conocimientos sobre herramientas de software propietario para informática forense.

El resultado sobre conocimientos sobre las herramientas de software para informática forense es confirma que los peritos optan por alternativas realistas conforme al medio ambiente donde se desenvuelven. Además existen casos en que los peritos deben poseer las herramientas para la informática forense ya que las instituciones no las proporcionan. Además optan por alternativas con suficiente documentación para auto capacitarse en la aplicación de las mismas obteniendo así los conocimientos necesarios para la obtención de evidencia digital.

DIAGNÓSTICO ACERCA DE LA EXISTENCIA DE INSTITUCIONES CAPACITADORAS EN INFORMÁTICA FORENSE

La totalidad de peritos informáticos manifestaron no conocer la existencia de instituciones capacitadoras en informática forense en el país.

La inexistencia de este tipo de instituciones denota la falta interés por parte de la sociedad y de las instituciones educativas en esta área de aplicación de la informática lo cual conlleva a limitar el desarrollo de la misma y dificultar la expansión de conocimientos referentes a esta disciplina que sería de gran beneficio social.

No existe en el país una entidad que capacite y certifique peritos informáticos por lo cual los conocimientos de los peritos informáticos al no estar certificados pueden ser menospreciados por las autoridades o las personas.

DIAGNÓSTICO ACERCA DE LOS DELITOS TRATADOS EN MAYOR GRADO POR LOS PERITOS INFORMATICOS

En el país se cometen una variedad de delitos informáticos los peritos encuestados manifestaron que el tipo de delito informático mas tratado por ellos es la piratería tanto de software como de contenidos multimedia seguido por la pornografía infantil y el fraude electrónico.

El delito tratado en mayor grado el cual es la piratería deja grandes pérdidas económicas a empresas de producción de video, y producciones musicales así como a las empresas de desarrollo de software, además el estado deja de percibir grandes cantidades de dinero debido a la evasión fiscal que este delito implica; los otros delitos que han tratado todos buscan el mismo fin hacerse de beneficios materiales o económicos a través de acciones fuera de la ley resultando afectada la sociedad con estos tipos de flagelos.

EL promover la informática forense ayudaría a la resolución de los casos de delitos informáticos y podría verse una disminución en los índices de los mismos ya que esto promovería leyes más drásticas para los delincuentes informáticos.

DIAGNÓSTICO ACERCA DEL RENDIMIENTO DE SOFTWARE LIBRE APLICABLE EN INFORMÁTICA FORENSE Y DIFICULTADES PARA SU IMPLEMENTACIÓN SEGÚN LOS PERITOS

De los peritos encuestados el 75% considera que los resultados de software libre para informática forense es igual o de mejor calidad que los de software propietario; Esto implica que los peritos

consideran en un grado excelente a las herramientas de software libre en contraste con el conocimiento ya que la mayoría conoce más sobre herramientas de software propietario.

Dentro de las dificultades que existen para la implementación de herramientas de software libre para informática forense están que no existe difusión acerca de sus características y ventajas y la falta de instituciones que capaciten a los profesionales en esta área. Lo anterior es un indicador acerca de los puntos que deben reforzarse para poder aplicar herramientas de software libre para informática forense en el país

DIAGNÓSTICO ACERCA DE LA IMPORTANCIA DE LAS CAPACITACIÓNES EN INFORMÁTICA FORENSE EN UNIVERSIDADES Y LIMITANTES PARA ADQUIRIR NUEVOS CONOCIMIENTOS SOBRE HERRAMIENTAS DE INFORMÁTICA FORENSE.

Todos los peritos encuestados consideran que deben impartirse conocimientos sobre informática forense en las instituciones de educación superior y el hecho de que no se impartan es la causa principal de que se dificulte la adquisición de nuevos conocimientos sobre este tipo de herramientas de software

El implementar la informática forense en la currÍcula de las carreras informáticas en el País, aumentaría los campos de acción de los nuevos profesionales y promovería el desarrollo de la informática, a la vez que apoyaría a las Autoridades para perseguir delincuentes informáticos.

IV. DIAGNÓSTICO GENERALIZADO

Para la realización de los indicadores se han identificado cuatro variables que serán sujetas de medición, siendo estas:

1. Evidencia digital.
2. Herramientas de software utilizadas en la informática forense.
3. Recurso humano.
4. Delitos informáticos.

A continuación se presenta un cuadro resumen de los indicadores y sus valores para cada una de las variables y se incluye su análisis:

EVIDENCIA DIGITAL		
Indicador	**Valor obtenido**	**Interpretación**
Importancia dada a la evidencia digital (IED)	78.45 %	Bueno
Validez dada a la evidencia digital (VED)	47.96 %	Regular.

Tabla No 67: Indicadores relacionados a la evidencia digital

HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE			
No.	**Indicador**	**Valor obtenido**	**Interpretación**
1	Conocimiento sobre las herramientas de software libre (CSL)	41.67 %	Medio – bajo
2	Conocimiento sobre las herramientas de software propietario (CSP)	58.33 %	Medio – alto
3	Uso de las herramientas de software para la informática forense por parte de los docentes universitarios (UDU).	60.00 %	Medio – alto
4	Uso de las herramientas de informática forense para recuperación de datos eliminados (USIF).	100.00 %	Alto
5	Uso de las herramientas de informática forense para copias de datos de bit a bit.	16.67 %	Bajo
6	Uso de las herramientas de informática forense para recuperación de números de licencias.	16.67 %	Bajo
7	Uso de las herramientas de informática forense para monitoreo de computadoras.	50.00 %	Medio
8	Uso de las herramientas de informática forense para calculo	0.00 %	Bajo

	de hash.		
9	Uso de las herramientas de informática forense para marcado de documento.	33.33 %	Bajo
10	Uso de las herramientas de informática forense para recuperación de contraseñas de archivos protegidos.	8.33 %	Bajo

Tabla No 68: Indicadores relacionados a las herramientas de software

RECURSO HUMANO		
Indicador	**Valor obtenido**	**Interpretación**
Personal docente capacitado (PDC).	10.40 %	Bajo
Peritos informáticos capacitados (PIC).	83.33 %	Bueno

Tabla No 69: Indicadores relacionados al Recurso Humano

DELITO INFORMÁTICO		
Indicador	**Valor obtenido**	**Interpretación**
Conocimiento sobre los delitos informáticos por parte de los operadores de justicia (CDI).	83.33 %	Bueno
Interacción entre los delitos informáticos y los operadores de justicia (ODI).	48.37 %	Regular

Tabla No 70: Indicadores relacionados a los delitos informáticos

Al evaluar el diagnóstico brindado por cada una de las variables a través de los indicadores, se llega al siguiente diagnóstico que nos demuestra la realidad relacionada con la informática forense en nuestro país:

En El Salvador, los operadores de justicia están conscientes de la existencia de los delitos informáticos y de alguna forma u otra han recibido información relacionada con ellos. Sin embargo, debido a que **nuestro marco legal no tipifica lo que es un delito informático**, en la mayoría de casos estos son tratados como delitos comunes por lo que al consultarse sobre la interacción que estos han tenido con los delitos, el indicador ODI demuestra que solo el 48.37 % de los encuestados ha tenido casos que tienen que ver con los delitos informáticos en sí.

Los encargados de presentar los requerimientos en los tribunales son los abogados, jueces y fiscales, estos últimos son ayudados por los peritos informáticos en la recolección de la evidencia para determinar los culpables de los delitos. La evidencia digital se convierte, por tanto, en una parte muy importante en el desarrollo de los juicios de delitos informáticos tal y como lo demuestra el indicador IED, un 78.45 % de encuestados que dijeron considerar importante la evidencia digital. Sin embargo, a pesar de esa importancia brindada a la evidencia digital, solo un 47.96% (Indicador VED) consideran que la evidencia presentada es válida demostrando la desconfianza que existen en este tipo de evidencia.

Esta desconfianza esta relacionada con la validez de la evidencia digital. Por supuesto, la validez de la evidencia digital incluye muchos factores tales como recurso humano y tecnológico, sin embargo, los indicadores relacionados con el recurso humano demuestran que el principal factor que afecta la validez de la evidencia digital es el poco conocimiento y capacitaciones que los peritos informáticos tienen en la aplicación de las herramientas de informática forense. El indicador CDI refleja que los peritos informáticos han recibido capacitaciones respecto a la utilización de las herramientas de informática forense con un 83.33 % pero entra en contraste con el tipo de herramientas que los peritos informáticos conocen (indicadores de software de informática forense). Estos indicadores demuestran que los peritos informáticos no aplican o no tienen conocimiento sobre las herramientas que deben utilizarse en los procedimientos de recuperación de la evidencia y que permiten garantizar su integridad de la evidencia. El poco conocimiento queda reflejado, por ejemplo, en que indicadores relacionados con las herramientas de copias de bit a bit y de cálculo de hash caigan dentro de un nivel bajo cuando son de vital importancia en el desarrollo de las pericias de informática forense.

Los resultados del análisis y tabulación de datos demuestran que la principal causa del poco conocimiento de los peritos o profesionales relacionados a la informática forense radica en que en nuestro país no existe personal, academias o instituciones que capaciten en temas relacionados a esta disciplina. Entre los factores que brindan una razón para la carencia de instituciones de enseñanza está relacionada a los pocos conocimientos de los docentes que imparten materias relacionadas con la informática y los altos costos para la construcción de laboratorios de informática forense.

En cuanto al marco legal salvadoreño existe una deuda, debido a que no tipifica lo que son los delitos informáticos ni define que características debe tener la evidencia para ser considerada válida. Debido a esto, cada juez de cada tribunal o cámara es quien decide si la evidencia se acepta o se rechaza basada en apreciaciones personales en la mayoría de casos.

En el sector educativo, no existen los recursos necesarios para iniciar la enseñanza de la informática forense en nuestro país. Dentro de esta carencia de recursos está principalmente la de docente con conocimientos certificados en informática forense que puedan enseñar esta disciplina, esta realidad es reflejada por el indicador PDC con un 10.40 % de personal docente capacitado.

En conclusión se puede señalar que existen debilidades y huecos legales en el marco salvadoreño al no tipificar los delitos informáticos ni que es la evidencia digital valida, los conocimientos de los peritos, en su mayoría de casos no son certificados y por ende, su trabajo pierde credibilidad, los docentes no están capacitados para brindar conocimientos respecto a informática forense y los peritos no cuentan con los recursos necesarios para actualizar sus conocimientos respecto a la inf0ormática forense.

Por el lado bueno, existe buen conocimiento respecto a la informática forense en los operadores de justicia, los docentes tiene voluntad de ayudar o capacitar a personas en el área de informática forense y los peritos informáticos buscan herramientas alternativas a las propietarias lo que le permite hacerse de herramientas de informática forense y aprender su funcionamiento y aplicación de forma autodidacta. Cabe recalcar, que todos los sectores que fueron encuestados mencionaron creer que la informática forense es de suma importancia y que puede traer muchos beneficios a la sociedad salvadoreña si se convirtiera en una disciplina en nuestro país.

CAPÍTULO V

ESTUDIO DE LAS HERRAMIENTAS DE SOFTWARE PARA LA INFORMÁTICA FORENSE

CAPÍTULO V: ESTUDIO DE LAS HERRAMIENTAS DE SOFTWARE PARA LA INFORMÁTICA FORENSE

A. SELECCIÓN DE LAS HERRAMIENTAS DE SOFTWARE A SER ESTUDIADAS

Para la selección de las herramientas que serán objeto de estudio se realizó, inicialmente, una investigación general, dando como resultado un total de 61 herramientas aplicables en la informática forense **(ver Anexo #13)**, que se encuentran agrupadas según su utilidad:

- ✓ **Herramientas para el cálculo de hash.**

  Hash se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, o medio de almacenamiento para resumir o identificar un dato a través de la probabilidad, utilizando una función hash o algoritmo hash. Un hash es el resultado de dicha función o algoritmo.[34]

- ✓ **Herramientas para copias de datos bit a bit.**

  El copiado bit a bit consiste en realizar una copia íntegra de un medio o disco incluyendo su espacio libre pudiendo operar con la copia con las mismas características que con la original.

- ✓ **Herramientas para recuperación de datos.**

  El objetivo de este tipo de herramientas es la recuperación de ficheros o archivos eliminados en un medio o disco.

- ✓ **Kits de herramientas para la informática forense.**

  Estos son conjuntos de herramientas recopilados para las funciones aplicables en un análisis forense o peritaje informático.

- ✓ **Herramientas para la recuperación de números de licencias.**

  Estas herramientas realizan una búsqueda en los registros del sistema operativo y una desencriptación de datos para brindar los números de licencias con que fueron instalados software específico en medios o discos.

- ✓ **Herramientas para la recuperación de contraseñas.**

  Estas herramientas recuperan contraseñas de archivos protegidos para poder acceder al contenido de los mismos.

[34] Fuente de la definición: http://es.wikipedia.org/wiki/Hash

Luego, sobre estas 61 herramientas se realizó una selección final que tuvo como objetivo identificar las que serían estudiadas en la presente investigación. Para la realización de la selección se tomaron en cuenta los criterios presentados en la siguiente tabla:

NO.	NOMBRE	DESCRIPCIÓN
1	**Utilidad**	Fin con el que se utiliza la herramienta en la Informática Forense.
2	**Adaptabilidad**	No necesita complementos para instalarse o utilizarse en los equipos.
3	**Mantenimiento**	Se estudiarán herramientas que cuenten con actualizaciones permanentes, ya que la evolución de la informática es constante.
4	**Portabilidad**	No es necesaria su instalación sobre el sistema operativo o puede ejecutarse en diferentes plataformas de hardware.
5	**Accesibilidad**	Que esté disponible su obtención para el respectivo estudio.
6	**Documentación**	Se estudiarán herramientas de las que exista documentación suficiente para obtener la información necesaria.
7	**Estabilidad**	Robustez de la aplicación en cuanto a operatividad en la plataforma que vaya a ser utilizada.

Tabla No 71: Criterios de selección de herramientas para informática forense

Además se tomo en cuenta las herramientas que actualmente se utilizan en mayor grado en el país para realizar comparaciones posteriores y herramientas que no se están utilizando en el país y la accesibilidad a las mismas

En el **Anexo #14** se muestra la matriz de los criterios y las herramientas que nos llevaron a la siguiente selección:

- ✓ Herramientas para el cálculo de Hash.
  - CRCDropper
  - HashX
  - HyperHasher
  - MD5SUM

- ✓ Herramientas para copias de datos bit a bit.
  - Norton Ghost
  - HDClone
  - CloneZilla
  - Drive Clone

- ✓ Herramientas para recuperación de datos.
    - Smart Data Recovery
    - Pandora Recovery
    - NTFS Undelete
    - Recover My Files

- ✓ Kits de herramientas para la informática forense.
    - ENCASE Forensic
    - HELIX
    - C.A.I.N.E.
    - DEFT Linux

- ✓ Herramientas para la recuperación de números de licencias.
    - Produkey
    - Magical Jelly Bean Key Finder
    - LicenseCrawler
    - Product Key Explorer

- ✓ Herramientas para la recuperación de contraseñas.
    - Advanced Office Password Recovery
    - Office Password Recovery Magic
    - Advanced RAR Password Recovery
    - RAR Password Unlocker
    - Advanced PDF Password Recovery
    - PDF Password Cracker

B. INVESTIGACIÓN DE LAS HERRAMIENTAS SELECCIONADAS

Con la finalidad de presentar la información recopilada sobre cada una de las herramientas seleccionadas en una forma sencilla y ordenada, se hará uso de una ficha técnica en la que estarán descritas sus principales características. El diseño de la ficha a utilizar se muestra en la **Figura No.81**:

Ficha de Herramienta de Software para Informática Forense **Nombre:** *xxxxxxxxx*	
Numero de Ficha: #	**Página # de #**
Objetivo de la herramienta:	***Sistemas Operativos sobre los que funciona:***
Uso(s) en la Informática Forense:	
Tipo de instalación:	
Tipo de licenciamiento:	
Costo de la herramienta:	
Pagina web del fabricante:	
Características:	
Requerimientos de hardware:	***Requerimientos de software:***

Figura No. 20: Formato de la ficha resumen propuesta para cada herramienta

Como parte de la investigación hecha a las herramientas seleccionadas, se ha elaborado para cada una de ellas un manual de instalación (en caso de ser necesario) y un manual de usuario básico en el que se describen los pasos a seguir para la realización de las principales funciones que estas poseen.

Para poder acceder a dichos manuales, utilizar el CD adjunto, Apartado "Manuales de las Herramientas Estudiadas".

I. HERRAMIENTAS PARA EL CÁLCULO DE HASH

<table>
<tr><td colspan="2">Ficha de Herramienta de Software para Informática Forense
Nombre: CRCDropper</td></tr>
<tr><td colspan="2">Numero de Ficha: 1 Página 1 de 1</td></tr>
<tr><td>Objetivo de la herramienta:</td><td>Sistemas operativos sobre los que funciona:</td></tr>
<tr><td>Calculo de hash CRC32, MD2, MD4, MD5, SHA1 y CRC16.</td><td>Windows 95 / Windows 98 / Windows ME / Windows 2000 / Windows XP / Windows Vista.</td></tr>
<tr><td colspan="2">Uso(s) en la Informática Forense:</td></tr>
<tr><td colspan="2">Comprobar las copias de respaldo o seguridad realizadas mediante el cálculo de hash CRC32, MD2, MD4, MD5, SHA1 o CRC16.</td></tr>
<tr><td colspan="2">Tipo de instalación: Instalación en el sistema operativo</td></tr>
<tr><td colspan="2">Tipo de licenciamiento: Freeware</td></tr>
<tr><td colspan="2">Costo de la herramienta: $ 0.00</td></tr>
<tr><td colspan="2">Pagina web del fabricante: http://www.goat1000.com/crcdropper.php</td></tr>
<tr><td colspan="2">Características:</td></tr>
<tr><td colspan="2">• Calculo de hash de tipo CRC32, MD2, MD5, MD4, SHA1 y CRC16.
• Funciona solo bajo sistema operativo Windows.
• Liviano.
• Soporta drag and drop.
• Capacidad para trabajar con archivos múltiples.</td></tr>
<tr><td>Requerimientos de hardware:</td><td>Requerimientos de software:</td></tr>
<tr><td>• Procesador a 300 MHz o superior.
• 64 MB de RAM
• 1 MB disponible en disco duro.
• Monitor VGA
• Ratón PS/2 o USB</td><td>• Microsoft Windows 95 o superior.</td></tr>
</table>

Ficha de Herramienta de Software para Informática Forense **Nombre:** *HashX*	
Numero de Ficha: 2	**Página 1 de 1**
Objetivo de la Herramienta:	***Sistemas Operativos sobre los que Funciona:***
Calcular algoritmos hash CRC32, MD2, MD4, MD5, SHA1, SHA2-256, SHA2-384, SHA2-512	Windows 95 / Windows 98 / Windows ME / Windows 2000 / Windows XP / Windows Vista.
Uso(s) en la Informática Forense:	
La herramienta puede ser utilizada para calcular algoritmos hash sobre las copias de respaldo realizadas a discos duros, archivos o particiones para comprobar su integridad e igualdad de los originales con las copias.	
Tipo de Instalación: Instalación en el sistema operativo	
Tipo de Licenciamiento: Freeware	
Costo de la Herramienta: $ 0.00	
Pagina Web del Fabricante: http://www.boilingbit.com/products/hashx/default.html	
Características:	
• Soporte *drag and drop*. • Se puede elegir el formato del resultado a desplegar. • Se puede copiar el resultado al portapapeles. • Compara el resultado del hash con una cadena dada.	
Requerimientos de Hardware:	***Requerimientos de Software:***
• Procesador de 300Mhz o superior • 64 MB RAM o superior. • 1.1 MB disponible en disco duro. • Monitor VGA	• Microsoft Windows 95 o superior.

Ficha de Herramienta de Software para Informática Forense **Nombre:** *Hyper Hasher*	
Numero de Ficha: 3	**Página 1 de 1**
Objetivo de la Herramienta:	***Sistemas Operativos sobre los que Funciona:***
Calcular hash para comprobación de exactitud de copias de respaldo.	Windows 95 / Windows 98 / Windows ME / Windows 2000 / Windows XP / Windows Vista.
Uso(s) en la Informática Forense:	
La herramienta puede ser utilizada para aplicar algoritmos hash a las copias de respaldo de datos realizados para comprobar su exactitud con el original. Si las copias son exactas, se puede manipular la copia como si se estuviera trabajando en la original.	
Tipo de Instalación: Instalación en el sistema operativo	
Tipo de Licenciamiento: Propietario	
Costo de la Herramienta: $ 10.00	
Pagina Web del Fabricante:	
Características:	
• Calculo de algoritmos de hash MD2, MD4, MD5, SHA-1, SHA-256, SHA-384, SHA-512, HAVAL, Tiger, Panama, RIPEMD-160, FCS-16, FCS-32, GHash-32-3, GHash-32-5, GOST, Size32-Hash, emule/edonkey. • Calculo de sumas de comprobación como CRC16, CRC16-CCITT, CRC32, Adler32. • Interfaz configurable. • Integración con la consola de comandos de Windows. • Soporta guardar las configuraciones del programa. • Puede comparar dos archivos. • Permite escribir los resultados en un archivo.	
Requerimientos de Hardware:	***Requerimientos de Software:***
• Procesador a 666 MHz o superior. • 64 MB de RAM • Monitor o adaptador de video VGA.	• Windows 95 o superior. • .NET Framework 2.0

Ficha de Herramienta de Software para Informática Forense **Nombre:** *md5sum*	
Numero de Ficha: 4	**Página 1 de 1**
Objetivo de la Herramienta:	***Sistemas Operativos sobre los que Funciona:***
Calcular el hash MD5.	Sistemas operativos GNU/Linux tales como Debian, Red Hat, SuSe, Fedora, etc.
Uso(s) en la Informática Forense:	
Calcular y verifica el hash MD5 a una copia de respaldo para compararla con el hash MD5 del original y determinar si las copias son exactas o ha habida alteración.	
Tipo de Instalación: Instalación en el sistema operativo	
Tipo de Licenciamiento: GNU GPL	
Costo de la Herramienta: $ 0.00	
Pagina Web del Fabricante: http://www.gnu.org/software/software.html	
Características:	
• Liviano • Calcula el hash MD5 de un archivo, partición o disco completo. • El programa viene integrado dentro de un paquete instalado en los sistemas base de los sistemas operativos GNU/Linux denominado coreutils (desarrollado por la Free Software Fundation). • Permite la lectura de archivos en formato binario. • Realiza la comprobación de hash MD5 en archivos comparando el generado con el original del archivo. • Permite leer los ficheros en formato texto.	
Requerimientos de Hardware:	***Requerimientos de Software:***
• Procesador a 300 MHz o superior. • Monitor VGA • Teclado PS/2 o USB.	• Necesita el paquete *coreutils* debido a que es una utilidad de este.

Para poder acceder al resto de las fichas elaboradas, utilizar el CD adjunto, Apartado "Fichas de Herramientas".

C. PROPUESTAS DE HERRAMIENTAS

Para la propuesta de herramientas se realizará una jerarquización de las herramientas estudiadas anteriormente. Para la jerarquización de las herramientas estudiadas se realizará lo siguiente.

1. Definir qué criterios son los que nos interesan medir de las herramientas que necesitamos comparar.

2. Para todas las herramientas seleccionadas, medir el nivel de cumplimiento de cada criterio.

3. Comparar cada herramienta del mismo tipo entre sí para determinar cuáles son las que obtienen mejores puntuaciones en los criterios definidos. Para ello se utilizará la tabla de criterios. Las puntuaciones serán dadas describiendo que tanto se apega la herramienta al criterio seleccionado.

4. Establecer la jerarquía de propuestas. No se va a proponer solo una, sino que se propondrá una jerarquía de los mayores puntajes a los menores.

I. CRITERIOS A TOMAR EN CUENTA

Los criterios a tomar en cuenta para la comparación de las herramientas serán:

1. **Portabilidad:** Capacidad de la herramienta para ser utilizada tanto en un entorno de hardware y software determinado como en otro, conservando la funcionalidad de esta. Se refiere al nivel en que la misma herramienta puede ser utilizada en diferentes entornos (combinaciones de hardware y software) donde se pueda encontrar la evidencia. Este criterio también incluye la facilidad de instalación con que las herramientas puedan instalarse en los entornos en que puede funcionar.

2. **Requerimientos de hardware y software para su instalación o funcionamiento:** Alguna de las herramientas que se han propuesto se necesitan instalar en el sistema operativo y pueden exigir cierto tipo de hardware o software para alcanzar la funcionalidad principal para las que fueron diseñadas. Este criterio servirá para determinar si las aplicaciones pueden ser instaladas o no en computadoras "comunes" y no sea necesario adquirir nueva hardware o software para ello.

3. **Confiabilidad de los resultados**: Para que una herramienta sea confiable en los resultados que proporciona, es necesario comparar el resultado de ésta con lo de las otras herramientas del mismo tipo y si son similares, podemos tomarlo como confiable, pero si no, se considerará no confiable. Por ejemplo, con las herramientas de hash, el resultado

de cálculo del mismo tipo de hash al mismo archivo debe dar igual para todas las herramientas.

4. **Costo de adquisición de la herramienta**: Algunas de las herramientas seleccionadas pueden tener costo que puede ser significativo. Por supuesto, si existen herramientas que realicen la misma funcionalidad pero el costo de adquisición es menor o nulo esta sería una alternativa viable comparada con la de costo mayor.

5. **Variedad de funciones de apoyo**: Algunas herramientas además de cumplir con la función principal para la que fueron diseñadas, tienen funciones "complementos" que pueden servir de utilidad a la hora de desarrollar el trabajo del perito. Este criterio se toma en cuenta dado que la variedad de funciones de estas herramientas puede permitir al perito informático realizar el trabajo de una manera más fácil.

6. **Facilidad de uso y aplicación:** Facilidad con que la herramienta puede ser aplicada para obtener el fin de esta. Esta facilidad de uso está relacionada al nivel de entendimiento del programa y su funcionabilidad, la facilidad de control y uso por parte del usuario y el esfuerzo necesario para aprender a utilizarla, en esto intervienen criterios como la interfaz del programa y la forma en que ésta va guiando al usuario a través del proceso de ejecución de las operaciones para las que las herramientas fue diseñadas y la ayuda en pantalla.

7. **Costo de implementación:** El costo de implementación es el valor adicional que se necesita invertir para proveer el entorno necesario para que la herramienta funcione correctamente. Es de hacer notar que si la herramienta necesita algún hardware o software especial para ser puesta a punto para ser utilizada, esto incrementará los costos. Esto constituye un factor muy importante a tomar en cuenta.

8. **Funcionalidad de la documentación:** Descripción de la funcionalidad de las herramientas y la forma de utilizar las características mediante la guía del manual de usuario. Este criterio evalúa que tan útil es la información presentada en los manuales de usuario de la herramienta. La ayuda brindada por el manual de usuario al perito es muy importante para que este pueda resolver sus dudas en la utilización de la herramienta y puede explotar al cien por ciento la funcionalidad de ésta.

9. **Mayor capacidad operativa:** Este criterio se refiere a que si dos herramientas realizan la misma función, se debe seleccionar las herramientas que tenga mayor capacidad para realizar dicha función. Por ejemplo seleccionar la herramienta que haga copias de bit a bit pero que pueda trabajar con discos de mayor tamaño.

10. **Soporte para la herramienta:** Es necesario que las herramientas seleccionadas tengan soporte para solventar problemas que puedan surgir con esta y actualizaciones que los fabricantes ponen a disposición para asegurar el correcto funcionamiento de la herramienta.

II. CARACTERÍSTICAS A EVALUAR

El método utilizado para ponderar las herramientas y lograr jerarquizarlas está basado en el método de criterios ponderados. Mediante este método, se definen los criterios que las herramientas deben cumplir y se le asigna un puntaje de acuerdo al peso del factor. El peso del factor depende de la importancia del factor. Los criterios y subcriterios tomados en cuenta y su ponderación son los siguientes:

- **Adaptabilidad al entorno: (15pts)**

    1. No requiere de sistema operativo. (10pts)
    2. Requiere de sistema operativo, pero funciona sobre más de uno. (5pts)
    3. Soporta más de una arquitectura de computadora. (5pts)

    El primero y el segundo criterio son excluyentes, si una herramienta cumple con el primero, no puede cumplir con el segundo y viceversa.

- **Requerimientos de hardware o software para su instalación (10pts).**

    1. No requiere hardware especial. (6pts)
    2. No requiere software especial (4pts)

- **Confiabilidad de resultados: (15pts).**

    1. Los resultados son iguales a los anteriores (15pts).

- **Costo de adquisición de la herramienta: (5pts).**

    1. No existe costo para la herramienta. (**5pts**).

- **Variedad de funciones: (10pts)**

    1. Tiene de una a dos funciones más que el objetivo principal con que fue desarrollada la herramienta. (5pts)
    2. Tiene más de dos funciones del objetivo principal (10pts).

- **Facilidad de uso y aplicación (10pts)**

    1. Tiene interfaz gráfica amigable. (5pts)
    2. Presenta ayuda en pantalla. (5pts)

- **Costo de implementación (5pts)**

    1. No es necesario realizar inversión para que la implementación de la herramienta sea completamente funcional. (5pts)

- **Funcionalidad de la documentación (10pts)**

    1. Existe documentación asociada con el programa (3pts)
    2. La documentación describe las operaciones clara y completamente (7pts).

- **Capacidad operativa (15pts)**

    1. Soporta lo más común del hardware en el mercado (8pts)
    2. Tiene soporte para elementos de hardware especiales o puede operar sobre ellos (7pts).

- **Soporte para la herramienta (5pts).**

    1. Tiene desarrollo y actualizaciones constantes de las herramientas (5pts).

III. CRITERIOS PARA LA SELECCIÓN DE SUITES

- **Adaptabilidad al entorno: (20pts)**

    1. No requiere de sistema operativo. (10pts)
    2. Requiere de sistema operativo, pero funciona sobre más de uno. (5pts)
    3. Soporta más de una arquitectura de computadora. (5pts)

- **Requerimientos de hardware o software para su instalación (20pts)**

    1. No requiere hardware especial. (10pts)
    2. No requiere software especial (10pts)

- **Variedad de funciones: (20pts)**

    1. Tiene de una a dos funciones más que el objetivo principal. (8pts)
    2. Tiene más de dos funciones del objetivo principal (12pts).

- **Funcionalidad de la documentación (15pts)**

    1. Existe documentación asociada con el programa (5pts)

    2. La documentación describe las operaciones clara y completamente (10pts).

- **Capacidad operativa: (15pts)**

    1. Soporta la mayoría o lo más común del hardware en el mercado (10pts)

    2. Tiene soporte para elementos de hardware especiales o puede operar sobre ellos (5pts).

- **Soporte para la herramienta. (10pts)**

    1. Desarrollo y actualizaciones de las herramientas (10pts).

Los criterios de comparación han sido elegidos en base a la norma ISO 9126-1998 que define los criterios y subcriterios que debe tener un software para ser considerado de calidad. La norma está orientada al desarrollo de software, por lo tanto, no todos son aplicables, siendo necesarios tomar solo los que consideramos importantes para la jerarquización de las herramientas de informática forense estudiadas.

Las ponderaciones dadas a cada uno de los criterios y subcriterios fueron definidas en consenso por el grupo de trabajo, basados en las investigaciones hechas con los profesionales que utilizan las herramientas y mediante el conocimiento que se ha adquirido de estas a través su estudio.

El mayor puntaje que una herramienta puede alcanzar será de 100, esta es el total de la sumatoria de cada puntaje máximo.

IV. COMPARACIONES DE LAS HERRAMIENTAS EN BASE A LOS CRITERIOS

HERRAMIENTAS PARA EL CÁLCULO DE HASH																	
HERRAMIENTA	**CRITERIO 1**			**CRITERIO 2**		**CRITERIO 3**	**CRITERIO 4**	**CRITERIO 5**		**CRITERIO 6**		**CRITERIO 7**	**CRITERIO 8**		**CRITERIO 9**		**CRITERIO 10**
	A	**B**	**C**	**A**	**B**	**A**	**A**	**A**	**B**	**A**	**B**	**A**	**A**	**B**	**A**	**B**	**A**
CRCDropper	No	No	No	Si	Si	Si	No	No	No	Si	No	No	No	No	Si	No	Si
HashX	No	No	No	Si	Si	Si	No	Si	No	Si	No	No	No	No	Si	No	Si
Hyper Hasher	No	No	No	Si	Si	Si	No	Si	No	Si	No	No	Si	Si	Si	No	Si
Md5sum	No	Si	No	Si	Si	Si	Sí	No	No	No	No	No	Si	Si	Si	Si	Si

Tabla No 72: Comparación de herramientas para calculo de hash

HERRAMIENTAS PARA COPIA DE MEDIOS																	
HERRAMIENTA	**CRITERIO 1**			**CRITERIO 2**		**CRITERIO 3**	**CRITERIO 4**	**CRITERIO 5**		**CRITERIO 6**		**CRITERIO 7**	**CRITERIO 8**		**CRITERIO 9**		**CRITERIO 10**
	A	**B**	**C**	**A**	**B**	**A**	**A**	**A**	**B**	**A**	**B**	**A**	**A**	**B**	**A**	**B**	**A**
Norton Ghost	No	No	No	Si	No	Si	Si	No	Si	Si	Si	No	Si	Si	Si	Si	Si
HDClone	Si	No	No	No	No	Si	Si	No	No	Si	Si	No	Si	Si	Si	Si	Si
DriveClone Pro	No	No	No	No	No	Si	Si	No	Si	Si	Si	No	Si	Si	Si	No	Si
CloneZilla	Si	No	No	No	No	Si	No	Si	No	Si	No	No	No	No	Si	Si	Si

Tabla No 73: Comparación de herramientas para copia de medios

HERRAMIENTAS PARA RECUPERACION DE CONTRASEÑAS																	
HERRAMIENTA	**CRITERIO 1**			**CRITERIO 2**		**CRITERIO 3**	**CRITERIO 4**	**CRITERIO 5**		**CRITERIO 6**		**CRITERIO 7**	**CRITERIO 8**		**CRITERIO 9**		**CRITERIO 10**
	A	**B**	**C**	**A**	**B**	**A**	**A**	**A**	**B**	**A**	**B**	**A**	**A**	**B**	**A**	**B**	**A**
Advanced Office Password Recovery	No	No	No	Si	Si	Si	No	No	No	Si	Si	Si	Si	Si	Si	No	Si
Office Password Recovery Magic	No	No	No	Si	Si	Si	No	No	No	Si	Si	Si	Si	Si	Si	No	Si
Advanced RAR password recovery.	No	No	No	Si	Si	Si	No	No	No	Si	Si	Si	Si	Si	Si	No	Si
RAR password unlocker	No	No	No	Si	Si	Si	No	No	No	Si	Si	Si	Si	Si	Si	No	Si
PDF Password Cracker	No	No	No	Si	Si	Si	No	No	No	Si	Si	Si	No	No	Si	No	Si
Advanced PDF password recovery.	No	No	No	Si	Si	Si	No	No	No	Si	Si	Si	Si	Si	Si	No	Si

Tabla No 74: Comparación de herramientas para recuperación de contraseñas

KITS DE HERRAMIENTAS PARA INFORMATICA FORENSE												
HERRAMIENTA	**CRITERIO 1**			**CRITERIO 2**		**CRITERIO 3**		**CRITERIO 4**		**CRITERIO 5**		**CRITERIO 6**
	A	**B**	**C**	**A**	**B**	**A**		**A**	**B**	**A**	**B**	**A**
C.A.I.N.E.	Si	No	Si	Si	Si	Si	Si	Si	No	Si	No	Si
DEFT Linux	Si	No	Si	Si	Si	Si	Si	No	No	Si	No	Si
HELIX	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
ENCASE	Si	No	Si	Si	Si	Si	Si	Si	No	Si	Si	Si

Tabla No 75: Comparación de Kits para informática Forense

HERRAMIENTAS PARA RECUPERACION DE NUMEROS DE LICENCIA																	
HERRAMIENTA	**CRITERIO 1**			**CRITERIO 2**		**CRITERIO 3**	**CRITERIO 4**	**CRITERIO 5**		**CRITERIO 6**		**CRITERIO 7**	**CRITERIO 8**		**CRITERIO 9**		**CRITERIO 10**
	A	**B**	**C**	**A**	**B**	**A**	**A**	**A**	**B**	**A**	**B**	**A**	**A**	**B**	**A**	**B**	**A**
Produkey	No	No	Si	Si	Si	Si	Si	Si	No	Si	No	Si	No	Si	Si	No	No
LicenseCrawler	No	No	Si	Si	Si	Si	Si	No	No	Si	No	Si	Si	No	Si	No	No
Magical Jelly Bean Key Finder	No	No	Si	Si	No	Si	Si	Si	No	Si	No	Si	No	Si	Si	No	Si
Product Key Explorer	No	No	Si	Si	No	Si	No	Si	No	Si	No	No	Si	No	Si	No	No

Tabla No 76: Comparación de herramientas para recuperación de números de licencia

HERRAMIENTAS PARA RECUPERACION DE DATOS ELIMINADOS																	
HERRAMIENTA	**CRITERIO 1**			**CRITERIO 2**		**CRITERIO 3**	**CRITERIO 4**	**CRITERIO 5**		**CRITERIO 6**		**CRITERIO 7**	**CRITERIO 8**		**CRITERIO 9**		**CRITERIO 10**
	A	**B**	**C**	**A**	**B**	**A**	**A**	**A**	**B**	**A**	**B**	**A**	**A**	**B**	**A**	**B**	**A**
Smart Data Recovery	No	No	No	Si	Si	Si	No	Si	No	Si	No	No	Si	No	Si	No	Si
Pandora Recovery	No	No	No	Si	Si	Si	Si	Si	No	No	Si	Si	No	Si	Si	No	No
NTFS Undelete	No	No	No	Si	Si	Si	Si	Si	No	Si	No	No	Si	No	Si	No	Si
Recover My Files	No	No	No	Si	Si	Si	No	Si	No	No	Si	Si	Si	Si	Si	No	Si

Tabla No 77: Comparación de herramientas para recuperación de datos eliminados

V. PUNTUACIONES DE HERRAMIENTAS SEGÚN PONDERACIONES DE CRITERIOS

A continuación se presenta los puntajes obtenidos para cada herramienta. Recordemos que el criterio de puntuación está basado en el método de los factores ponderados como se explicó en la sección anterior.

HERRAMIENTAS PARA EL CÁLCULO DE HASH (PUNTAJES)											
HERRAMIENTA	**CRITERIOS**										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**TOTAL**
CRCDropper	0	10	15	5	0	5	5	0	8	5	53
HashX	0	10	15	5	5	5	5	0	8	5	58
Hyper Hasher	0	10	15	0	5	5	5	10	8	5	63
Md5sum	5	10	15	5	0	0	5	10	15	5	70

Tabla No 78: Puntuaciones de herramientas para calculo de Hash

HERRAMIENTAS PARA COPIA DE MEDIOS (PUNTAJES)											
HERRAMIENTA	**CRITERIOS**										**TOTAL**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Norton Ghost	0	6	15	0	10	10	5	10	15	5	86
HDClone	10	10	15	0	0	10	5	10	15	5	80
DriveClone Pro	0	10	15	0	10	10	5	10	8	5	73
CloneZilla	10	10	15	5	5	5	5	0	15	5	75

Tabla No 79: Puntuaciones de herramientas para copia de Medios

HERRAMIENTAS PARA RECUPERACION DE CONTRASEÑAS (PUNTAJES)											
HERRAMIENTA	**CRITERIO**										**TOTAL**
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
Advanced Office Password Recovery	0	10	15	0	0	10	5	10	8	5	63
Office Password Recovery Magic	0	10	15	0	0	10	5	10	8	5	63
Advanced RAR password recovery.	0	10	15	0	0	10	5	10	8	5	63
RAR password unlocker	0	10	15	0	0	10	5	10	8	5	63
PDF Password Cracker	0	10	15	0	0	10	5	0	8	5	53
Advanced PDF password recovery.	0	10	15	0	0	10	5	10	8	5	63

Tabla No 80: Puntuaciones de herramientas para recuperación de contraseñas

HERRAMIENTAS PARA RECUPERACION DE NUMEROS DE LICENCIA (PUNTAJES)											
HERRAMIENTA	**CRITERIOS**										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**TOTAL**
Produkey	5	10	15	5	5	5	5	7	8	0	65
LicenseCrawler	5	10	15	5	0	5	5	3	8	0	56
Magical Jelly Bean Key Finder	5	10	15	5	5	5	5	7	8	5	70
Product Key Explorer	5	10	15	0	5	5	0	3	8	0	51

Tabla No 81: Puntuaciones de herramientas para recuperación de números de licencia

HERRAMIENTAS PARA RECUPERACION DE DATOS (PUNTAJES)											
HERRAMIENTA	**CRITERIOS**										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**TOTAL**
Smart Data Recovery	0	10	15	0	5	5	0	3	8	5	51
Pandora Recovery	0	10	15	5	5	10	5	7	8	0	65
NTFS Undelete	0	10	15	5	5	5	0	3	8	5	56
Recover My Files	0	10	15	0	5	10	5	10	8	5	68

Tabla No 82: Puntuaciones de herramientas para recuperación de datos eliminados

KITS DE HERRAMIENTAS PARA INFORMATICA FORENSE (PUNTAJES)							
HERRAMIENTA	**CRITERIOS**						
	1	**2**	**3**	**4**	**5**	**6**	**TOTAL**
C.A.I.N.E.	15	20	20	5	10	10	80
DEFT Linux	15	20	20	0	10	10	75
HELIX	15	20	20	15	15	10	95
ENCASE	15	20	20	5	15	10	85

Tabla No 83: Puntuaciones de Kits de herramientas para informática forense

VI. JERARQUIZACIÓN DE LAS HERRAMIENTAS

Las propuestas de las herramientas de software se han realizado mediante los criterios definidos para evaluar su funcionamiento y características que poseen cada una de las herramientas pertenecientes a una determinada categoría en estudio.

Para establecer como evaluar las herramientas de software con respecto a los criterios, se realizó una ponderación para poder cuantificar el funcionamiento y las características de cada herramienta con respecto a otra.

Como las herramientas de software de cada categoría son similares, se decidió darle prioridad a la herramienta que representará una ventaja con respecto a otra, ya sea por factores como el costo de adquisición, la capacidad operativa, la funcionalidad ó el soporte y la documentación.

Para poder seleccionar la herramienta de software de una determinada categoría, que será sugerida para ser utilizada primordialmente, se analizó el resultado de la evaluación de cada herramienta con respecto a los criterios; y en base a los resultados se estableció una jerarquía para cada categoría.

A continuación se presenta cada categoría de las herramientas de software para la informática forense que fueron investigadas y en las cuales se encuentran definidas las jerarquías de las herramientas que son sugeridas utilizar prioritariamente.

Herramientas para recuperación de números de licencia

1. Magical Jelly Bean Key Finder
2. Produkey
3. LicenseCrawler
4. Product Key Explorer

Herramientas para recuperación de datos

1. Recover My Files
2. Pandora Recovery
3. NTFS Undelete
4. Smart Data Recovery

Kits de herramientas para informática forense

1. HELIX
2. Encase Forensic
3. C.A.I.N.E.
4. DEFT Linux

Herramientas para el cálculo de hash.

1. Md5sum.
2. hyper Hasher.
3. HashX.
4. CRCDropper.

Herramientas para copias de discos.

1. Norton Ghost
2. HDClone
3. CloneZilla
4. DriveClone Pro

Herramientas para la recuperación de contraseñas

Las herramientas seleccionadas se han limitado al tipo de archivos en los que podría encontrarse la evidencia digital tales como documentos de Office y documentos compresos en formato WinRAR. Por supuesto que existen tantas herramientas para recuperar contraseñas como tipos de archivos existan, haciendo imposible el estudio de todas ellas.

- Advanced Office Password Recovery, Office Password Recover Magic si se trata de obtener claves de documentos elaborados en cualquier programa de la paquetería de Microsoft Office.
- Advanced RAR password recovery, RAR password unlocker si se intenta obtener claves de documentos que han sido compresos con WinRAR.

CAPÍTULO VI

PROPUESTA DE LABORATORIO PARA INFORMÁTICA FORENSE

CAPÍTULO VI: PROPUESTA DE LABORATORIO PARA INFORMÁTICA FORENSE

Una de los principales activos para los peritajes informáticos son los laboratorios para informática forense y las herramientas con que estos cuentan para realizar los análisis.

En nuestro país no se cuenta con laboratorios especializados para realizar los peritajes informáticos por lo cual investigamos sobre los requerimientos de un laboratorio para informática forense y hacemos la siguiente propuesta basados en los requerimientos planteados por Leopoldo Sebastián Gómez[35].

A. DESCRIPCIÓN DE REQUERIMIENTOS

Se plantean 9 puntos principales para el establecimiento de un laboratorio forense, los cuales se exponen a continuación:

- ✓ **Servidor del laboratorio:** La utilidad de este radica en ser el principal centro de almacenamiento de evidencia digital y reportes técnicos generados a partir de los peritajes realizados sobre los medios comprometidos.

- ✓ **Red interna de laboratorio de tipo Gigabit Ethernet:** Esta apoya los procedimientos de transmisión de datos entre estaciones de trabajo y el servidor central del laboratorio esta red es una intranet que no tiene acceso a ningún tipo de red pública.

- ✓ **Protectores contra escritura (Write Blockers) & Duplicadores:** El objetivo de estos es proteger los medios contra escritura para garantizar la integridad de los datos en los medios o copias de medios y duplicadores que realizan copias bit a bit de los medios comprometidos.

- ✓ **Telefonía celular:** Este apartado especifica herramientas que apoyen el análisis o peritaje forense sobre aparatos de telefonía celular para mantener la integridad de datos y realizar recopilación de evidencia en los aparatos

- ✓ **Equipo Informático Forense Móvil:** Este es equipo que se utiliza para recolectar evidencia en allanamientos ya sea digital o material en caso que sea necesario secuestrar los medios.

---

[35] Abogado (UCaSal-Argentina), Lic. En Ciencias de la Computación (UNS-Argentina), Magister en Ingeniería del Software (ITBA-Argentina), Posgraduado en Gestión y Calidad del Software (UPC-España), Master en Ingeniería del Software (UPM-España). Perito Informático Oficial – Poder Judicial – Argentina.

- ✓ **Equipo Informático Forense para Laboratorio (Forensic Workstation):** Estas son las estaciones de trabajo que se tienen en el laboratorio en donde se realizan las copias de los medios comprometidos y se recupera la evidencia digital.

- ✓ **Periféricos del Laboratorio:** Este consta de los periféricos utilizados en el laboratorio para la generación de reportes o para captura de imágenes ya sean escáneres o cámaras digitales.

- ✓ **Software Forense:** Es el software especializado para la obtención de evidencia digital contando con diferentes tipos como kits para informática forense o herramientas individuales que cumplen funciones aplicables en esta rama de la informática.

- ✓ **Entrenamiento Forense:** Uno de los principales puntos para el establecimiento de un laboratorio para informática forense es que los peritos que realicen sus análisis en el estén capacitados en la utilización de las herramientas de hardware y software que este posee para poder realizar análisis oportunos en un tiempo adecuado.

B. PROPUESTA PARA LA IMPLEMENTACIÓN

A continuación se exponen los requerimientos para la implementación de un laboratorio en informática forense:

SERVIDOR DE LABORATORIO

- ✓ **Requerimientos mínimos:**

Este servidor actuará funcionalmente equiparado a un NAS para el almacenamiento de evidencia digital, casuística y reportes técnicos. Asimismo, se utilizará para la ejecución de máquinas virtuales y para operaciones que demanden tiempo de cómputo intensivo. Deberá tener un espacio de almacenamiento de 4,5 Tb en discos SAS, los que se dividirán en dos zonas (grupos lógicos).

La primera zona se implementará como un RAID-1E de 1,5 Tb (o sea que ya utilizó 3 de los 4,5). Este repositorio se utilizará para almacenar información de los casos trabajados (ej. informes técnicos, dictámenes) y selectivamente alguna evidencia digital que sea conveniente resguardar porque puede ser objeto de un peritaje posterior.

La segunda zona tendrá un RAID-0 de 750 Gb (o sea 1,5 Tb que quedaban de los 4,5) y se utilizará principalmente como repositorio de trabajo temporal, para actividades forenses específicas: ej. carving e indexados.

- ✓ **Recomendaciones:**

a) Se estima que $ 20.000 son suficientes para un Laboratorio de Informática Forense que comienza sus actividades. Puede adquirirse un Servidor Blade, con una o dos hojas Blade como máximo. Estos equipos son escalables.

b) El servidor deberá tener preferentemente un S.O. que brinde servicios de Terminal Server para inicio de sesiones remotas. Se recomienda Windows Server 2008.

c) Se requieren UPS acordes al Servidor del Laboratorio.

RED INTERNA DE LABORATORIO DE TIPO GIGABIT ETHERNET

✓ **Requerimientos Mínimos:**

Red local aislada y de uso exclusivo del Laboratorio, Gigabit Ethernet.

✓ **Recomendaciones:**

Se estima en función de los puestos de trabajo se requieren pero no supone mayores costos. (Rack + Switch + Placas de Red para cada puesto + Cableado Estructurado + Red eléctrica separada para conexión de para equipos informáticos).

PROTECTORES CONTRA ESCRITURA (WRITE BLOCKERS) & DUPLICADORES

✓ **Requerimientos Mínimos:**

a) Tableau T8 (U$ 269,15 por unidad)

b) Tableau TD1 (U$ 1314 por unidad)

c) Disk Jockey Pro Forensic Kit (U$ 657,85 por unidad)

✓ **Recomendaciones:**

Se debe estimar U$ 5000 en este rubro para una suite de productos de trabajo típicos.

TELEFONÍA CELULAR

✓ **Requerimientos Mínimos:**

a) Caja de Faraday para el Laboratorio (U$ 1495 por unidad)

b) Bolsas de Faraday (U$ 30 por unidad)

c) Device Seizure Toolbox (U$ 750 por unidad)

d) Lector de memorias + Cargador externo (U$ 50)

e) CSI Stick (U$ 299 por unidad)

✓ **Recomendaciones:**

a) Se debe estimar U$ 4000 en este rubro para una suite de productos de trabajo típicos.

b) Existen Forensic Kits de Hardware + Software que disminuyen sensiblemente los costos de adquisición. Ej. Device Seizure Field Kit de Paraben (U$ 3495).

EQUIPO INFORMÁTICO FORENSE MÓVIL

- ✓ **Requerimientos mínimos:**

Se debe prever una notebook, una impresora portátil y otros materiales típicos para el trabajo de campo (ej. allanamientos), al que se sumará eventualmente parte del equipo forense del punto 3 y 4.

- ✓ **Recomendaciones:**

a) Se debe estimar U$ 3000 por notebook que requiera para procedimientos judiciales, U$s 300 por impresora portátil, y U$ 500 para otros elementos operativos (caja de herramientas, pinzas, destornilladores, cables de datos, etc.). No se debe gastar más dinero en este ítem porque la mayor parte del trabajo se realiza en el Laboratorio.

b) En caso de realizar un procedimiento judicial se debe planificar el trabajo de campo ya que es probable que se requieran elementos de almacenamiento de evidencia digital adicionales.

EQUIPO INFORMÁTICO FORENSE PARA LABORATORIO (FORENSIC WORKSTATION)

- ✓ **Requerimientos mínimos:**

Memoria RAM de 4 GB o superior, Monitor LCD 22", RAID-0 de 750 GB o superior, placa de red Ethernet Gigabit, Sistema Operativo Windows Vista Ultimate.

- ✓ **Recomendaciones:**

a) Se debe estimar U$ 3.500 por puesto de trabajo.

b) Los equipos deben tener las interfaces para conexión de dispositivos externos, ej. USB, P-ATA, S-ATA, FIREWIRE, etc.

c) También se debe contemplar que en gran parte de los casos la evidencia digital se almacena temporariamente en el RAID-0 del Laboratorio que actúa como repositorio compartido. Puede aprovecharse la potencia de cómputo de las hojas Blade del Servidor del Laboratorio, estableciendo una sesión remota mediante Terminal Services.

PERIFÉRICOS DEL LABORATORIO

- ✓ **Requerimientos mínimos:**

Impresora laser con conexión a red de buen rendimiento en Blanco y Negro, y una impresora color de un costo que no sea elevado ya que tendrá menor uso. Cámara digital de costo moderado.

- ✓ **Recomendaciones:**

Se debe estimar U$ 6.000 para estos periféricos.

SOFTWARE FORENSE

- ✓ **Requerimientos mínimos:**

Puede utilizarse software gratuito como Helix, Liveview!, FTK Imager, etc.

- ✓ **Recomendaciones:**

a) EnCase: 1 Licencia por puesto de trabajo U$ 3000 + PLSP por 3 años U$ 3000.00

b) Device Seizure: depende del número de casos que deban trabajarse (como mínimo 1 Licencia, U$ 1095 + Suscripción por 1 año U$ 220).

c) Mount Image Pro: depende del número de casos que deban trabajarse (como mínimo 1 licencia, U$ 299).

d) VMware Workstation: 1 Licencia por puesto de trabajo U$ 189.00

ENTRENAMIENTO FORENSE

- ✓ **Recomendaciones:**

a) Capacitación in situ: el instructor viaja a la institución e imparte un curso especializado con un programa predefinido. Se resuelven casos prácticos y se exponen dictámenes de peritajes informáticos. El personal del laboratorio local queda capacitado en todos los aspectos esenciales sobre metodología de trabajo forense, técnicas de investigación de delitos con tecnología informática, y uso de hardware y software forense.

CAPÍTULO VII

RESOLUCIÓN DE CASO SIMULADO DE DELITO INFORMÁTICO

CAPÍTULO VII: RESOLUCIÓN DE CASO SIMULADO DE DELITO INFORMÁTICO

A. FLUJOGRAMA DEL PROCEDIMIENTO DE ANALISIS

A continuación se presenta la siguiente figura, en la cual se presentan los pasos a seguir durante el desarrollo de la investigación pericial:

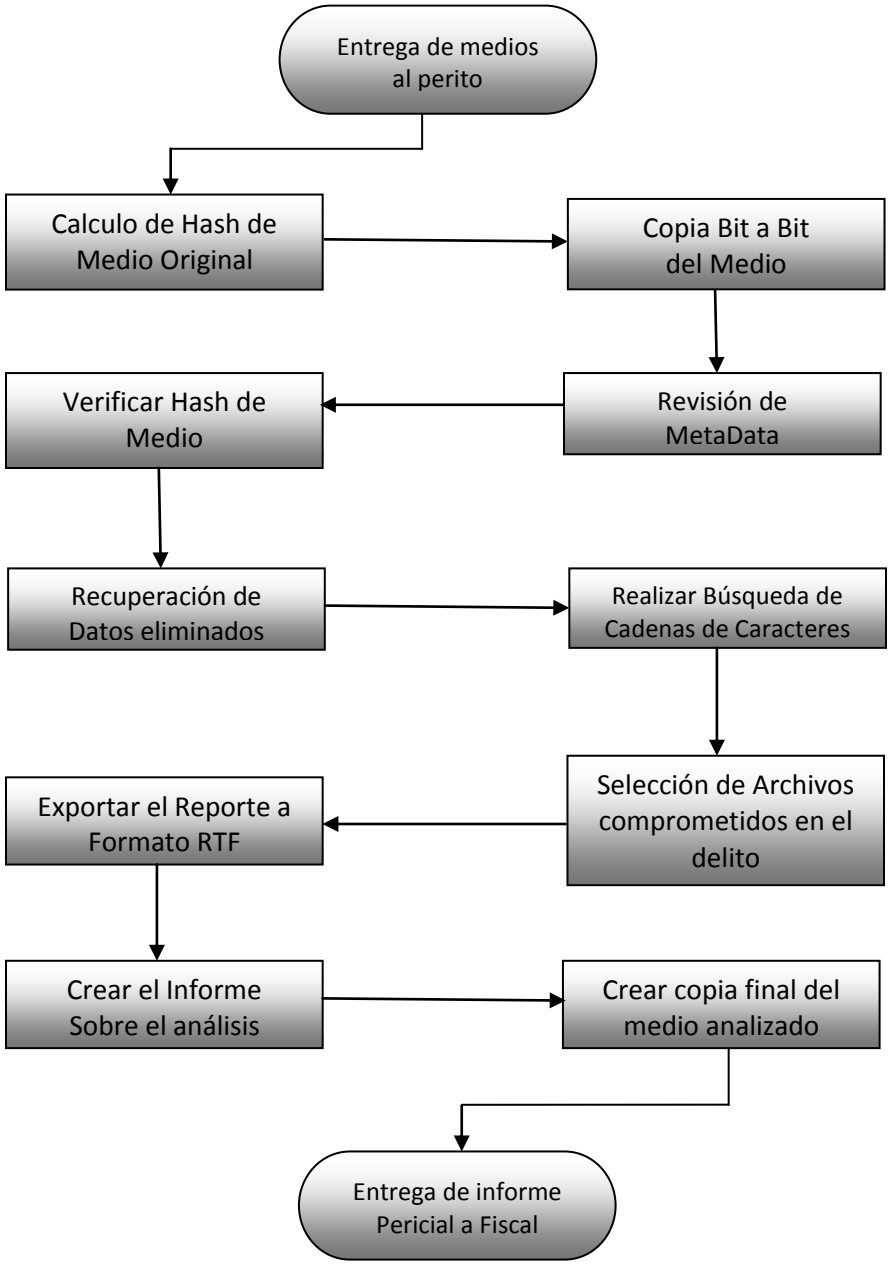

Figura No. 21: Figura correspondiente al flujograma del procedimiento de análisis

B. DESCRIPCIÓN DE LA SITUACIÓN

Tipo de delito:

Pornografía Infantil.

Situación previa:

Se descubrió que en el país existe una red de distribución de pornografía infantil un agente de interpol se ha infiltrado en esta red para lograr capturar a los participes de la misma y disminuir los efectos de este flagelo a la sociedad salvadoreña.

El agente de interpol especialista en informática forense se ha suscrito al foro en internet donde se ponen en contacto los distribuidores de este tipo de contenidos.

En la red se distribuyen videos e imágenes de menores de edad teniendo relaciones sexuales y mostrando sus cuerpos desnudos.

El objetivo de la captura de estas personas es eliminar esa fuente de distribución de contenidos ilegales

El agente ha logrado entrar en contacto con la cabeza de la red de distribución se ha rastreado el origen de los datos transmitidos a través de internet y se conoce el lugar de residencia del sospechoso.

La policía el perito informático y el fiscal del caso con una orden de allanamiento irrumpen en la vivienda del sospechoso para lo cual se secuestran los medios electrónicos y ópticos de almacenamiento para su respectivo análisis por parte del perito en el laboratorio forense en búsqueda de evidencia digital para poder incriminar al sospechoso.

Luego del allanamiento se entrego al perito el material confiscado:

Medios Ópticos: 10 DVDS de datos y

Medios Magnéticos: 1 Disco Duro

Medios Electrónicos: 1 memoria SD de 128 mb

Peritaje:

En el laboratorio de informática forense se realizo el respectivo análisis del disco duro y de los 10 Dvd de datos y no se encontró ningún archivo comprometedor

Se realizo el análisis de la memoria SD en el cual se encontraron archivos relacionados a la red de distribución de pornografía infantil entre ellos videos documentos e imágenes.

A continuación se expone los procedimientos que se siguieron para el análisis de este medio de almacenamiento.

El software forense a utilizar en este caso es EnCase Forensic Version 4.20

Para poder acceder a la resolución del presente caso, utilizar el CD adjunto, Apartado "Resolución de caso simulado", opción "Peritaje informático".

CONCLUSIONES

CONCLUSIONES

A. EN BASE A LOS OBJETIVOS DE LA INVESTIGACIÓN

- ✓ En El Salvador se utilizan herramientas para informática forense dependiendo de la necesidad que tengan los peritos. Entre ellas se aplican herramientas para recuperación de datos eliminados, recuperación de números de licencia, recuperación de contraseñas, Kits de herramientas para Informática forense; estas apoyan la resolución de casos de delitos informáticos.

- ✓ El nivel de uso de herramientas de informática forense en El Salvador está clasificado en un nivel bajo debido a que en general los peritos utilizan en promedio un 32.14% de la variedad investigada de las mismas existiendo casos, de tipos de herramientas no utilizadas en el país.

- ✓ La aplicación de las herramientas de informática forense y el conocimiento que los peritos poseen sobre las mismas son determinantes en la recolección de la evidencia digital y en la validez dada por los jueces en a la misma, para comprobar que se ha cometido un ilícito en los tribunales de justicia.

- ✓ Los factores que influyen en la utilización de herramientas de informática forense son económicos, educativos y legales debido a que se considera que existe un bajo conocimiento y una baja aplicación por falta de recursos, falta de instituciones capacitadoras y falta de un marco legal que apoye su aplicación y valide la evidencia obtenida a través de ellas.

- ✓ La utilización de herramientas de software para informática forense tiene ventajas enfocadas al beneficio que trae la obtención rápida y oportuna de evidencia digital en casos de delitos informáticos que de no aplicarse requerirían más tiempo, esfuerzo e inversión.

- ✓ Los peritos no poseen los conocimientos necesarios ni cuentan con las herramientas adecuadas para realizar los análisis forenses sobre los medios comprometidos en delitos informáticos.

- ✓ En El Salvador no existe un marco legal que tipifique los delitos informáticos y apoye su persecución por parte de las autoridades y que a la vez soporte la validez de la evidencia digital en este tipo de casos.

B. EN BASE A LA INVESTIGACIÓN DE CAMPO

- ✓ Para el sector legal la informática forense trae ventajas en la resolución de los delitos informáticos en El Salvador. Sin embargo, considera que los profesionales no tienen los conocimientos técnicos y científicos necesarios para la aplicación para la obtención de evidencia digital válida, desestimando por esta razón, en muchas de las ocasiones, la evidencia digital resultante de la aplicación de esta disciplina.

- ✓ Dentro de los factores que hacen válida la evidencia digital está la capacidad de quien obtuvo la evidencia, la cadena de custodia que se le aplicó a la evidencia, la utilización de las herramientas adecuadas para su recuperación y el marco legal que brinda el soporte jurídico a ésta. El sector legal considera que si la evidencia digital cumple con los requisitos anteriores, esta puede ser determinante en un porcentaje superior al 50% en la resolución de los delitos informáticos.

- ✓ Los delitos informáticos a los que se enfrenta el sector legal son principalmente la piratería, clonación de tarjetas y fraude electrónicos. Para poder esclarecer estos tipos de delitos los peritos hacen uso de las herramientas de software para informática forense.

- ✓ En El Salvador la enseñanza de la informática forense y la utilización de sus herramientas son nulas debido a que no existen entidades capacitadoras, sin embargo, se cuenta con personal dispuesto a incursionar en esta área. Aunque es de considerar que dicho personal debe ser capacitado, para que posteriormente pueda difundir el conocimiento de una forma certificada o respaldada en cuanto a los conocimientos que transmitan.

- ✓ El marco legal salvadoreño no cuenta con una forma de tratar los delitos informáticos, ni define que criterios debe cumplir la evidencia digital para ser tomada como válida. Estos deben ser puntos muy importantes a tomar en cuenta para que la informática forense se desarrolle en nuestro país, tomando en cuenta siempre al sector educativo.

- ✓ Entre los principales obstáculos a la hora de adquirir conocimientos de informática forense están la falta de entidades de enseñanza en El Salvador, lo que deriva en el factor económico por el pago de las capacitaciones, esto debido a que tienen que emigrar al extranjero para obtener los conocimientos de profesionales certificados en este tema.

- ✓ El desarrollo de la informática forense, en el sector profesional, se ha desarrollado principalmente mediante software privativo, dejando de lado el software libre. Esto es así porque generalmente, las empresas que venden el software privativo brindan soporte en cuanto a la utilización de este. Sin embargo, también se ha demostrado que el software libre está tomando una buena porción del campo de las herramientas utilizadas en la informática forense, esto debido al bajo costo que representa su adquisición y a los buenos resultados que se han obtenido mediante este tipo de software.

- ✓ Los resultados obtenidos mediante la aplicación de software privativo y libre son considerados por la mayoría de peritos informáticos como iguales, quedando entonces al conocimiento que tengan en la aplicación de las herramientas y al costo como elección de las herramientas a utilizar.

- ✓ Los datos recopilados de los diferentes sectores que están involucrados en la informática forense, ya sea directa o indirectamente, permite demostrar que el que muchos de los casos de delitos informáticos no llegue a una resolución favorable, está relacionado al poco conocimiento que los peritos informáticos tienen en la recuperación de evidencia digital con validez, haciendo necesario capacitar a los profesionales en la aplicación de la informática forense y así poder esclarecer un mayor porcentaje de los delitos informáticos.

- ✓ La tendencia que sigue la informática forense en el país es hacia al crecimiento. A medida que pasa el tiempo, los jueces, fiscales y abogados conocen cada vez más de la informática forense. Esto representa un buen punto ya que a medida que la informática forense se desarrolla y es tomada en cuenta en los diferentes sectores que componen el sistema judicial, profesional y educativo, permitirá resolver los delitos informáticos que también van en aumento debido al uso generalizado que se hace de las tecnologías de información y comunicación.

- ✓ El sector educativo tiene un papel importante en el desarrollo de la informática forense, en especial las instituciones de educación superior. Al final de la investigación se muestra la necesidad de que estas incluyan en sus materias, la informática forense. Si bien es cierto que no sacarían profesionales especializados en esta área, brindarían el impulso inicial para que muchos profesionales de informática se dediquen a la aplicación de la informática forense.

C. EN BASE AL DIAGNÓSTICO

- ✓ Los peritos informáticos tienen mayor conocimiento sobre herramientas de software propietario para informática forense ya que el 58.33% de ellos lo manifestó y justificaron esto en que existen más fuentes de documentación y de capacitación que para herramientas de Software Libre.

- ✓ Los peritos informáticos optan también por las alternativas de software libre para informática forense debido a que existen ocasiones en que las instituciones o los interesados no proporcionan las herramientas para realizar los respectivos peritajes y este tipo de herramientas les permiten realizar sus análisis forenses en equipos informáticos sin incurrir en costos extras, aunque el aprendizaje de estas requiera un mayor tiempo debido a las pocas fuentes de documentación.

- ✓ Los docentes universitarios utilizan herramientas aplicables en la informática forense debido a que estas tienen diversas aplicaciones en las actividades de los profesionales informáticos del país, permitiendo esto, que los mismos posean conocimientos que suponen un valor agregado.

- ✓ El nivel de uso de herramientas de software para informática forense se ve influenciado principalmente por la poca cultura en el área de la informática forense en el país, el poco apoyo a esta rama de la informática por parte de las instituciones de gobierno relacionadas a la aplicación de la misma, la falta de personal capacitado en el área en las instituciones de educación superior del país y el poco interés por parte de las autoridades de las mismas sobre el tema.

- ✓ La herramienta más utilizada por los peritos es la de recuperación de datos. El 100% de los peritos las han utilizado denotando esto que las personas que cometen delitos informáticos intentan eliminar las pruebas que puedan incriminarlos en caso de ser descubiertos.

- ✓ El esclarecimiento de los delitos informáticos depende en gran medida de la evidencia digital presentada durante los procesos judiciales. La validez de la evidencia esta en un buen grado respaldada por los conocimientos técnicos y científicos que tengan los peritos que recuperan este tipo de evidencia.

- ✓ Debido a que en nuestra legislación no existe una tipificación específica para los delitos informáticos la validez de la evidencia digital depende de la apreciación personal de los jueces.

- ✓ Un factor determinante que afecta el conocimiento del recurso humano (docentes y peritos) que utiliza las herramientas de software para la informática forense es la falta de una entidad o academia en el país que se encargue de la formación de profesionales en esta área de la informática. En nuestro país, no se cuenta con una institución que se encargue de brindar estos conocimientos técnico – científicos a los peritos.

- ✓ Los kits de herramientas de software para la informática forense ofrecen un entorno de trabajo asistido que proporciona al investigador interfaces amigables y que lo guían durante los pasos que componen un estudio informático forense.

- ✓ La correcta utilización de las herramientas de copias de bits a bits y de las herramientas para el cálculo de Hash ayudan a garantizar la validez de la evidencia digital.

RECOMENDACIONES

RECOMENDACIONES

A. A LAS INSTITUCIONES RELACIONADAS CON LA PERSECUCIÓN DE LOS DELITOS INFORMÁTICOS

- ✓ Debe fomentarse a nivel de gobierno el desarrollo de la informática forense para poder contar con peritos capacitados e instituciones capacitadoras sobre esta aplicación de la informática y sus herramientas.

- ✓ La Fiscalía General de la República debería crear una unidad especializada para la persecución de los delitos informáticos teniendo esta personal capacitado en el área técnica informática exclusiva para este tipo de casos.

- ✓ La Policía Nacional Civil debería invertir en el establecimiento de un laboratorio para informática forense en el cual sean tratados los delitos informáticos

- ✓ Debería crearse y establecerse un marco legal que respalde la persecución de delitos informáticos y la validez de la evidencia digital en los Tribunales de Justicia.

- ✓ Fomentar o promover la capacitación de los peritos informáticos o profesionales en el área, procurando mantener una actualización constante ya que el delincuente informático se va actualizando en las formas de delinquir y el perito debe estar en capacidad de obtener evidencias sin importar la tecnología utilizada.

- ✓ Capacitar a los elementos policiales que participan de allanamientos en casos de delitos informáticos, para el debido trato con los medios de almacenamiento, procurando así evitar la contaminación de la evidencia.

- ✓ Si el recurso económico es una limitante deberían considerar opciones libres de software para informática forense, ya que existen alternativas con funcionalidades equivalentes a las de software que requiere licenciamiento.

B. A LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

- ✓ Considerar la utilidad de la Informática forense y los beneficios que esta trae a la sociedad promoviendo la capacitación del personal docente de las mismas.

- ✓ Impartir conocimientos sobre la informática forense y sus herramientas de software a los futuros profesionales, para mantenerse actualizados y apoyar a los encargados de ejercer justicia en la persecución de delitos informáticos.

- ✓ Realizar un análisis del beneficio que la implementación de materias referentes a la informática forense traería al desarrollo tecnológico del país y a la resolución de delitos informáticos.

- ✓ Fomentar los trabajos de investigación ya que estos contribuyen al desarrollo e implementación de Tecnologías de Información en el País, que traen beneficios a la sociedad en general.

- ✓ Incluir en las carreras relacionadas al derecho un área referente a la informática forense, ya que la proliferación de delitos informáticos en el país, esta plateando nuevas formas de delinquir por lo cual los abogados tienen que conocer cómo hacerles frente desde el comienzo de su formación como profesionales.

- ✓ Promover alianzas con las Instituciones de Gobierno encargadas de perseguir los delitos informáticos para conjuntamente trabajar en los análisis de los medios comprometidos para la resolución de este tipo de delitos y fomentar el desarrollo de la Informática forense en el País.

- ✓ Promover la Capacitación del personal docente en la Informática Forense y sus herramientas de software para contar con recurso humano que tenga conocimientos en el área.

REFERENCIA BIBLIOGRÁFICA

REFERENCIA BIBLIOGRÁFICA

A. LIBROS

1. Sistemas Operativos, Una Visión aplicada;
   Jesús Carretero;
   McGraw- Hill Primera edición México, 2001.
2. Metodología de la investigación;
   Roberto Sampieri;
   Editorial Mc. Graw Hill, segunda edición, Mexico, 1998.
3. Forensic Discovery;
   Wietse, Venema;
   Editorial Adison-Wesley, Second Edition, United States, 2004.
4. Derecho Informático:
   Téllez Valdez, Julio;
   Editorial McGraw Hill Interamericana Tercera Edición México, 2004.

B. PÁGINAS WEB

1. "Información sobre Informática Forense"
   <http://www.microsoft.com/spain/empresas/legal/forensic.mspx>; Febrero/2009.
2. "Información sobre herramientas para recuperar datos de discos duros"
   <http://inza.wordpress.com/2006/11/28/herramientas-de-informatica-forense-para-recuperar-datos-de-disco-duro/>; Febrero/2009.
3. "Información sobre derecho informático y delitos informáticos en El Salvador"
   <http://www.monografias.com/trabajos11/inin/inin.shtml#deli>; Febrero/2009.
4. "Información sobre comercialización de datos"
   <http://indatasv.blogspot.com/2008_02_01_archive.html>; Febrero/2009.
5. "Información sobre herramientas de Informática Forense" <http://www.ordenadores-y-portatiles.com/herramientas-informatica-forense.html>; Febrero/2009.

6. "Información sobre piratería" <http://www.elfaro.net/secciones/Noticias/20080204/noticias2_20080204.asp>; Febrero/2009.

7. López, Oscar; "INFORMÁTICA FORENSE : GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS, Bogotá Colombia" (documento web), 2002 <http://www.criminalistaenred.com.ar/Informatica_F.html>;6/Abr/2009.

8. *Microsoft; "¿Qué es la informática forense o Forensic? España ,"* (documento web), 2009 <http://www.microsoft.com/spain/empresas/legal/forensic.mspx>; 6/Abr/2009.

9. Aguilar, Luis;" ¿Qué es un forense informático?, México"(documento web)2006 <http:/ /www.eluniversal.com.mx>; 6/Abr/2009.

10. Internet Solutions, "Informática Forense Colombia" (documento web)2005 <http://www.internet-solutions.com.co/ser_infor_foren.php>; 6/Abr/2009.

11. Wikipedia;"Medios de almacenamiento España" ; (documento web)2009 <http://es.wikipedia.org/wiki/Medios_de_almacenamiento>; 7/Abr/2009.

12. Asobancaria; "Informática Forense y la banca, Bogotá Colombia"(documento web)2004 <www.asobancaria.com/upload/docs/docPag1993_1.pdf>; 7/Abr/2009.

13. Bilbao,Joseba ;"Sistemas de Ficheros, Madrid España"(documento web)2006 <http://memnon.ii.uam.es/descargas_web/cursos_verano/20060701/Joseba_Bilbao/Sistemas_ficheros.pdf> ; 7/Abr/2009.

14. Cano, Jeimy;"Evidencia digital, Buenos Aires Argentina "(documento web)2006 <http://virusprot.com/Archivos/Eviden-GECTI03.pdf>; 7/Abr/2009.

15. Landaverde, Melvin; "Delitos Informáticos El Salvador" (documento web)2000 <http://www.monografias.com/trabajos6/delin/delin.shtml?monosearch>; 7/Abr/2009

16. Kioskea; "Sistema operativo"; (documento web); 2008. <http://es.kioskea.net/contents/systemes/sysintro.php3>; Marzo/2009.

17. Bob Rankin; "Encriptación"; (documento web); Octubre/1997. <http://www.bbs.ingedigit.com.ve/articulos/encriptacion.html>; Marzo/2009.

18. "Como funciona la encriptación"; (documento web); <http://www.ordenadores-y-portatiles.com/encriptacion.html>; Marzo/2009.

19. Julián Inza; "Herramientas de informática forense para recuperar datos de disco duro"; (documento web); Marzo/2009. <http://inza.wordpress.com/2006/11/28/herramientas-de-informatica-forense-para-recuperar-datos-de-disco-duro/> ; Marzo/2009.

20. D. Jeimy J. Cano; "INFORMÁTICA FORENSE, LIDERANDO LAS INVESTIGACIONES"; (documento web); Septiembre/2001; <http://www.virusprot.com/Col8.html> ; Marzo/2009.

21. Jeimy J. Cano; "Introducción a la Informática Forense"; (Documento pdf); 2006. <www.acis.org.co/fileadmin/Revista_96/dos.pdf>; Marzo/2009.

22. "Herramientas en la informática forense"; <http://www.ordenadores-y-portatiles.com/herramientas-informatica-forense.html>; Marzo/2009.

23. ROSSEL, SEBASTIÁN; "EL DISEÑO DE INVESTIGACIÓN" (documento web),2005 <http://deepistemologiaymetodologia.blogspot.com/2005/05/el-diseo-de-investigacin.html>;Junio/2009

24. Austin, Tomás; "EL DISEÑO DE INVESTIGACIÓN" (documento web),2009 <http://www.angelfire.com/emo/tomaustin/Met/guiacuatrodise_o.htm>;Junio/2009

25. Fuentes, Marcelo Adrián; "EL DISEÑO DE INVESTIGACIÓN" (documento web),2000 <http://www.educar-argentina.com.ar/OCT2000/educ30.htm>;Junio/2009

26. Prof. Lino Pastene O.; "El Planteamiento del Problema. Diseños de Investigación" (Diapositiva) <http://www.slideshare.net/lpastene/diseos-de-investigacin>;Junio/2009

27. Guillermo Maza; "Determinación del tamaño de la muestra". Tabla de Z 2009. <http://seminarioclourdes.blogspot.com/2009/07/tabla-de-areas-bajo-la-curva-normal.html>;Junio/2009

28. Cursos, "Investigación y Recursos en Inteligencia Artificial". Tablas Estadísticas Chi Cuadrado 2009 <http://www.wiphala.net/research/manual/statistic/chi_cuadrado.html>;Junio/2009

29. "Documento digital sobre indicadores Organización de las Naciones Unidas". <http://www.scribd.com/doc/7469823/Que-son-los-indicadores>;Octubre/2009

30. "Documento digital sobre indicadores sociales en América Latina". <http://www.eclac.org/publicaciones/xml/0/23000/lcl2383e.pdf>;Octubre/2009

31. "Documento electrónico sobre delitos informáticos". <http://www.calp.org.ar/Info/producciones/delinfo.doc>;Octubre/2009

32. "Enciclopedia en línea contenido relacionado al Hash". <http://es.wikipedia.org/wiki/Hash>;Octubre/2009

33. "Documento sobre evaluación de software" <http://www.lisi.usb.ve/publicaciones/03%20evaluacion/evaluacion_09.pdf>; Octubre/2009

34. "Documento de propuesta de equipo para la implementación de un laboratorio de informática forense" <http://sebastiangomez.sytes.net/papers/GILIF.pdf>;Octubre/2009

35. "Documento de internet que demuestra como esta compuesto un informe pericial " <http://www.delitosinformaticos.info/peritaje_informatico/informe_pericial.html>; Octubre/2009

C. OTROS DOCUMENTOS

1. Trabajo de Graduación: “Análisis y Diagnostico de la Informática Forense en El Salvador” UES FIA EISI 2008.
   DOCENTE DIRECTOR Ing. Julio Alberto Portillo
   Presentado por :
   Belloso Urbina, Ramiro Alexander
   Mancia Rivera, Mirna Noemy
   Morán Bautista, Oscar José
   Olmedo Portillo, Guadalupe Beatriz

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

A

Antijurídico: comportamiento contrario a Derecho.

Apócrifo/a: Falso, supuesto o fingido.

Atípico: Que no encaja en un tipo o modelo.

Autenticidad: satisfacer a una corte en que los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa (por ejemplo la fecha).

B

Bolsa de Faraday: dispositivo en forma de bolsa que provoca que el campo electromagnético en el interior de un conductor en equilibrio sea nulo, anulando el efecto de los campos externos.

Bomba lógica: programa informático que se instala en un ordenador y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción; como por ejemplo borrar información del disco duro.

Boot: En informática, la secuencia de arranque, (boot o booting en inglés) es el proceso que inicia el sistema operativo cuando el usuario enciende una computadora. Se encarga de la inicialización del sistema y de los dispositivos.

Byte: un byte es la unidad fundamental de datos en los ordenadores personales, un byte son ocho bits contiguos. El byte es también la unidad de medida básica para memoria, almacenando el equivalente a un carácter.

C

Caja de Faraday: dispositivo en forma de caja que provoca que el campo electromagnético en el interior de un conductor en equilibrio sea nulo, anulando el efecto de los campos externos.

Campo magnético: es una región del espacio en la cual una carga eléctrica puntual de valor q que se desplaza a una velocidad V, sufre los efectos de una fuerza que es perpendicular y proporcional tanto a la velocidad como al campo, llamada inducción magnética o densidad de flujo magnético.

Carving: proceso cuya misión es recuperar ficheros en un escenario forense basando el análisis en contenidos y no en metadatos.

Checksum: Una suma de verificación o checksum es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corruptos. Es empleado para comunicaciones (internet, comunicación de dispositivos, etc.) tanto como para datos almacenados (archivos compresos, discos portátiles, etc.).

Ciencias forenses: se definen como el conjunto de disciplinas cuyo objeto común es el de la materialización de la prueba a efectos judiciales mediante una metodología científica. Cualquier ciencia se convierte en forense en el momento que sirve al procedimiento judicial.

Cifrar: escribir un mensaje en clave.

Cluster: es un conjunto contiguo de pistas de sectores que componen la unidad más pequeña de almacenamiento de un disco. Los archivos se almacenan en uno o varios clústeres, dependiendo de su Tamaño de unidad de asignación. Sin embargo, si el archivo es más pequeño que un clúster, éste lo ocupa completo.

Concepto atípico: concepto que no encaja en un tipo o modelo.

Concepto típico: característico o representativo de un tipo o modelo, del que reproduce las características.

Controlador de disco: conjunto de circuitos integrados que tienen como función organizar la lectura y escritura en las unidades de disco en una computadora.

CRC: La comprobación de redundancia cíclica (CRC) es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida.

D

Delincuente informático: persona que utiliza medios electrónicos automatizados (informáticos) para realizar acciones ilícitas en contra de alguna persona o grupo de personas.

Delito: es definido como una conducta, acción u omisión típica (tipificada por la ley), antijurídica (contraria a Derecho), culpable y punible. Supone una conducta infraccional del Derecho penal, es decir, una acción u omisión tipificada y penada por la ley.

Derecho: orden normativo e institucional de la conducta humana en sociedad inspirado en postulados de justicia, cuya base son las relaciones sociales existentes que determinan su contenido y carácter. En otras palabras, es el conjunto de normas que regulan la convivencia social y permiten resolver los conflictos interpersonales.

Descriptor de archivo: Generalmente, un descriptor de archivo es una clave a una estructura de datos residente en el núcleo, que contiene detalles de todos los ficheros abiertos. En POSIX, esta estructura de datos se llama "tabla de descriptores de ficheros", y cada proceso tiene la suya.

Disco virtual: emula a un disco duro de ordenador y gracias a la conexión a Internet, permite el acceso desde cualquier lugar.

Drag and drop: expresión informática (arrastrar y soltar), que se refiere a la acción de mover con el ratón objetos de una ventana a otra o entre partes de una misma ventana.

E

Encriptacion: Es el proceso mediante el cual una rutina es codificada de tal manera que no pueda ser interpretada fácilmente. Es una medida de seguridad utilizada para que al momento de transmitir la información ésta no pueda ser interceptada por intrusos. Existe además un proceso

de desencriptación a través del cual la información puede ser interpretada una vez que llega a su lugar de origen.

Escalable: propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para extender el margen de operaciones sin perder calidad, o bien manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.

Espacio Unallocated: espacio disponible no asignado en disco que no se asigna a ningun volumen. El tipo de volumen que puede crear el espacio no asignado depende del tipo de disco. En los discos básicos, puede usar el espacio no asignado para crear o ampliar las particiones primarias. En los discos dinámicos, puede utilizar el espacio no asignado para crear volúmenes dinámicos.

Evidencia digital: el término abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor. Desde el punto de vista del derecho probatorio, puede ser comparable con "un documento" como prueba legal.

Evidencia digital confiable: entendemos que la evidencia digital es confiable cuando viene de fuentes que son creíbles y verificables. Es decir una prueba digital seria confiable siempre y cuando el sistema que la haya producido no haya sido violado y este en correcto funcionamiento al momento de recibir, almacenar o generar la prueba.

F

Fraude Electrónico: el fraude electrónico es una de tantas maneras que utilizan los espías cibernéticos para obtener información confidencial, especialmente de cuentas e instituciones bancarias. Engañan a los usuarios y los estafan a través de Internet.

Freeware: tipo de software de computadora que se distribuye sin costo, disponible para su uso y por tiempo ilimitado, siendo una variante gratuita del shareware. A veces se incluye el código fuente, pero no es lo usual.

Firmware: es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria de tipo no volátil (ROM, EEPROM, flash,...), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

Formato binario: es un formato para datos usado por las aplicaciones de computadores.

G

GB: un gigabyte es una unidad de medida informática cuyo símbolo es el GB, y puede equivalerse a 2^{30} bytes o a 10^{9} bytes, según el uso.

GNU/Linux: es uno de los términos empleados para referirse al sistema operativo libre similar a Unix que utiliza el núcleo Linux y herramientas de sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo el código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU) y otras licencias libres.

Gusano: Un gusano informático (también llamados IWorm por su apocope en inglés, I de Internet, Worm de gusano) es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

H

Hacker: es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar hackeo y hackear a las obras propias de un hacker.

Hash: es un valor numérico de longitud fija que identifica datos de forma unívoca. Los valores hash se utilizan para comprobar la integridad de los datos que se envían a través de canales no seguros. Puede compararse el valor hash de los datos recibidos con el valor hash de los datos que se enviaron para determinar si se alteraron los datos.

Hojas Blade: servidores de tipo hoja.

I

Indexado: En informática, tiene como propósito la elaboración de un índice que contenga de forma ordenada la información, esto con la finalidad de obtener resultados de forma sustancialmente más rápida y relevante al momento de realizar una búsqueda.

Indicador: medida sustitutiva de información que permite calificar un concepto abstracto. Se mide en porcentajes, tasas y razones para permitir comparaciones.

Item: Cada uno de los elementos que forman parte de un dato.

L

Licenciamiento Freewere: licencia de uso del software freeware, que permite su redistribución pero con algunas restricciones, como no modificar la aplicación en sí, ni venderla, y dar cuenta de su autor. También puede desautorizar el uso en una compañía con fines comerciales o en una entidad gubernamental, o bien, requerir pagos si se le va a dar uso comercial.

Licenciamiento GNU: la licencia de documentación libre de GNU (GNU Free Documentation License o GFDL) es una licencia copyleft para contenido libre, diseñada por la Fundación del Software Libre (FSF) para el proyecto GNU. Esta licencia, a diferencia de otras, asegura que el material licenciado bajo la misma esté disponible de forma completamente libre, pudiendo ser copiado, redistribuido, modificado e incluso vendido siempre y cuando el material se mantenga bajo los términos de esta misma licencia (GNU GFDL).

Litigación civil: controversias jurídicas de carácter civil.

liveCD: (traducido en ocasiones como CD vivo o CD autónomo), es un sistema operativo (normalmente acompañado de un conjunto de aplicaciones) almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de archivos.

M

Malware: (del inglés malicious software, también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano a un spyware.

Maquina virtual: en informática una máquina virtual es un software que emula a un ordenador y puede ejecutar programas como si fuese un ordenador real. Este software en un principio fue definido como "un duplicado eficiente y aislado de una máquina física". La acepción del término actualmente incluye a máquinas virtuales que no tienen ninguna equivalencia directa con ningún hardware real.

MD5: En criptografía, MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

Memoria Flash: La memoria flash es una forma desarrollada de la memoria EEPROM que permite que múltiples posiciones de memoria sean escritas o borradas en una misma operación de programación mediante impulsos eléctricos, frente a las anteriores que sólo permite escribir o borrar una única celda cada vez. Por ello, flash permite funcionar a velocidades muy superiores cuando los sistemas emplean lectura y escritura en diferentes puntos de esta memoria al mismo tiempo.

Meta-archivo: El metaarchivo de Windows (Windows Metafile, WMF) es un formato de archivo gráfico en sistemas Microsoft Windows, diseñado originalmente a principios de los años 1990 y que no se utiliza tan frecuentemente desde la aparición de Internet y formatos más comunes como GIF, JPEG, PNG y SVG. Es un formato de gráficos vectoriales que permite también la inclusión de mapas de bits.

Meta-datos: o sobre-datos, son datos que describen otros datos. En general, un grupo de metadatos se refiere a un grupo de datos, llamado recurso. El concepto de metadatos es análogo al uso de índices para localizar objetos en vez de datos.

Muestreo aleatorio simple: Es la extracción de una muestra de una población finita, en el que el proceso de extracción es tal que garantiza a cada uno de los elementos de la población la misma oportunidad de ser incluidos en dicha muestra. Esta condición garantiza la representatividad de la muestra porque si en la población un determinado porcentaje de individuos presenta la característica A, la extracción aleatoria garantiza matemáticamente que por término medio se obtendrá el mismo porcentaje de datos muestrales con esa característica.

Muestreo estratificado: Consiste en la división previa de la población de estudio en grupos o clases que se suponen homogéneos respecto a característica a estudiar. A cada uno de estos estratos se le asignaría una cuota que determinaría el número de miembros del mismo que

compondrán la muestra. Dentro de cada estrato se suele usar la técnica de muestreo sistemático, ya que con aquella suelen ser las técnicas más usadas en la practica.

Muestreo por conglomerados: Técnica similar al muestreo por estadios múltiples, se utiliza cuando la población se encuentra dividida, de manera natural, en grupos que se supone que contienen toda la variabilidad de la población, es decir, la representan fielmente respecto a la característica a elegir, pueden seleccionarse sólo algunos de estos grupos o conglomerados para la realización del estudio.

Muestreo sistemático: Se utiliza cuando el universo o población es de gran tamaño, o ha de extenderse en el tiempo. Primero hay que identificar las unidades y relacionarlas con el calendario (cuando proceda). Luego hay que calcular una constante, que se denomina coeficiente de elevación K= N/n; donde N es el tamaño del universo y n el tamaño de la muestra. Determinar en qué fecha se producirá la primera extracción, para ello hay que elegir al azar un número entre 1 y K; de ahí en adelante tomar uno de cada K a intervalos regulares. Ocasionalmente, es conveniente tener en cuenta la periodicidad del fenómeno.

N

NAS: (del inglés Network Attached Storage) es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (Servidor) con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

Nodo-i: En informática, un inodo, nodo-i, nodo índice o i-node en inglés es una estructura de datos propia de los sistemas de archivos tradicionalmente empleados en los sistemas operativos tipo UNIX como es el caso de Linux. Un inodo contiene las características (permisos, fechas, ubicación, pero NO el nombre) de un archivo regular, directorio, o cualquier otro objeto que pueda contener el sistema de ficheros.

O

Operadores de justicia: profesionales del sector judicial que participan como acusadores o defensores, tales como abogados, fiscales y jueces.

Operacionalización: es el procedimiento por el cual se pasa de variables generales a indicadores, es el proceso de medición en las ciencias sociales.

P

Partición: en informática, es el nombre genérico que recibe cada división presente en una sola unidad física de almacenamiento de datos. Toda partición tiene su propio sistema de archivos (formato); generalmente, casi cualquier sistema operativo interpreta, utiliza y manipula cada partición como un disco físico independiente, a pesar de que dichas particiones estén en un solo disco físico.

Peritaje informático: Se conoce como peritaje informático a los estudios e investigaciones orientados a la obtención de una prueba informática de aplicación en un asunto judicial para que sirva a un juez para decidir sobre la culpabilidad o inocencia de una de las partes.

Peritar: Evaluar, analizar o estudiar un asunto en calidad de perito o especialista.

Policarbonato: El policarbonato es un grupo de termoplásticos fácil de trabajar, moldear y termoformar, y son utilizados ampliamente en la manufactura moderna. El nombre "policarbonato" se basa en que se trata de polímeros que presentan grupos funcionales unidos por grupos carbonato en una larga cadena molecular.

Prosecución: continuación, reanudación, persecución, acoso, seguimiento.

Puntero: Un puntero (o apuntador) es una variable que referencia una región de memoria; en otras palabras es una variable cuyo valor es una dirección de memoria. Si se tiene una variable ' p ' de tipo puntero que contiene una dirección de memoria en la que se encuentra almacenado un valor ' v ' se dice que ' p ' apunta a ' v'.

R

RAID-0: Un RAID 0 (también llamado conjunto dividido o volumen dividido), distribuye los datos equitativamente entre dos o más discos sin información de paridad que proporcione redundancia. El RAID 0 se usa normalmente para incrementar el rendimiento, aunque también puede utilizarse como forma de crear un pequeño número de grandes discos virtuales a partir de un gran número de pequeños discos físicos.

RAID-1: Un RAID 1 crea una copia exacta (o espejo) de un conjunto de datos en dos o más discos. Esto resulta útil cuando el rendimiento en lectura es más importante que la capacidad. Un conjunto RAID 1 sólo puede ser tan grande como el más pequeño de sus discos. Un RAID 1 clásico consiste en dos discos en espejo, lo que incrementa exponencialmente la fiabilidad respecto a un solo disco; es decir, la probabilidad de fallo del conjunto es igual al producto de las probabilidades de fallo de cada uno de los discos (pues para que el conjunto falle es necesario que lo hagan todos sus discos).

Red Gigabit Ethernet: también conocida como GigaE, es una ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet (También llamado 100-Base/T).

Respaldo incremental: a diferencia de los respaldos completos, los respaldos incrementales primero revisan para ver si la fecha de modificación de un archivo es más reciente que la fecha de su último respaldo. Si no lo es, significa que el archivo no ha sido modificado desde su último respaldo y por tanto se puede saltar esta vez. Por otro lado, si la fecha de modificación es más reciente, el archivo ha sido modificado y se debería copiar. Los respaldos incrementales son utilizados en conjunto con respaldos regulares completos (por ejemplo, un respaldo semanal completo, con respaldos incrementales diarios).

S

SAS: tecnología de transferencia de información punto a punto que se creó para solucionar alguno de los inconvenientes de su predecesora: SCSI.

SATA: interfaz de transferencia de datos entre la placa base y algunos dispositivos de almacenamiento.

SCSI: acrónimo inglés Small Computers System Interface (Sistema de Interfaz para Pequeñas Computadoras), es un interfaz estándar para la transferencia de datos entre distintos dispositivos del bus de la computadora.

Sistema de archivos: Los sistemas de archivos (filesystem en inglés), estructuran la información guardada en una unidad de almacenamiento (normalmente un disco duro de una computadora), que luego será representada ya sea textual o gráficamente utilizando un gestor de archivos. La mayoría de los sistemas operativos poseen su propio sistema de archivos.

Swap: En informática, el espacio de intercambio es una zona del disco (un fichero o partición) que se usa para guardar las imágenes de los procesos que no han de mantenerse en memoria física. A este espacio se le suele llamar swap, del inglés "intercambiar".

T

Tabla de partición: La tabla de particiones está alojada en el MBR (del inglés Master Boot Record) a partir del byte 446 del MBR y ocupa 64 bytes, conteniendo 4 registros de 16 bytes, los cuales definen las particiones primarias. En ellos se almacena toda la información básica sobre la partición: si es arrancable, si no lo es, el formato, el tamaño y el sector de inicio.

TB: Un terabyte es una unidad de medida de almacenamiento de datos cuyo símbolo es TB y puede equivaler a 1024 GB.

Terminal Server: una computadora específica que permite conectar varios módems de uno de sus lados y una conexión a una red LAD o a otro servidor del otro lado. La mayoría de estos servidores proveen servicios PPP y SLIP si están conectados a Internet. Este servidor contesta llamadas en los módems y las transfiere a los nodos adecuados.

Teleproceso: se refiere al procesamiento de datos provenientes de terminales en una unidad central. Esta palabra aparece a finales de la década de 1960 y se deriva de telecomunicación en proceso de datos.

Típico: Característico o representativo de un tipo o modelo, del que reproduce las características.

U

Unidad Iomega: la unidad Iomega Zip, llamada también unidad Zip, es un dispositivo o periférico de almacenamiento, que utiliza discos Zip como soporte de almacenamiento; dichos soportes son del tipo magneto-óptico, extraíbles de media capacidad, lanzada por Iomega en 1994. La primera versión tenía una capacidad de 100 MB, pero versiones posteriores lo ampliaron a 250 y 750 MB.

Unidad Jazz: es un sistema de almacenamiento masivo removible creado por Iomega y lanzado inicialmente en 1997.

V

Variable: una variable es un elemento de una fórmula, proposición o algoritmo que puede adquirir o ser sustituido por un valor cualquiera (siempre dentro de su universo).

Virus: Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos.

W

WWrite Blockers: son dispositivos que permiten la adquisición de información en un disco sin crear la posibilidad de dañar accidentalmente el contenido del disco.

ANEXOS

ANEXOS

ANEXO #1: MODELO DE ENTREVISTA PRELIMINAR

1. ¿Utilizan herramientas como apoyo a las investigaciones Forenses en el área informática?

2. ¿Qué Tipos de Herramientas Utilizan?

3. ¿Desde cuándo utilizan herramientas de software para informática forense?

4. ¿Cuáles son los principales obstáculos al utilizar las herramientas?

5. ¿Considera que los conocimientos que posee son suficientes para realizan un Peritaje informático? Si, No y porque

6. ¿Cuales Considera que son las debilidades que se tiene con respecto a la utilización de herramientas que se utilizan en los peritajes informáticos?

7. ¿Existen instituciones que los capaciten en el uso de esas herramientas?

8. ¿Si no existen como realizan su capacitación?

9. ¿Poseen el equipo informático de hardware para utilizar las herramientas de software mas actualizadas para informática forense?

10. ¿Qué elementos considera necesarios para que exista desarrollo en el área de Informática Forense?

11. ¿Cómo considera que se encuentra la aplicación de Herramientas de informática Forense en El Salvador? Porque

12. ¿Considera que la legislación Salvadoreña se encuentra Fortalecida para la persecución de delitos Informáticos? ¿Si no que cree que hace falta?

13. ¿La inexistencia de leyes para delitos informáticos tiene incidencia en el desarrollo de la informática forense en el país? ¿De qué manera?

ANEXO #2: PLANES DE ESTUDIO DE UNIVERSIDADES CONSULTADAS

NÚMERO	UNIVERSIDAD	CARRERA
1	Universidad de El Salvador	Ingeniería de Sistemas Informáticos
2	Universidad Centroamericana José Simeón Cañas	Licenciatura en Ciencias de la Computación
3	Universidad Francisco Gavidia	Ingeniería en Ciencias de la Computación
4	Universidad Tecnológica	Ingeniería en Sistemas y Computación
		Licenciatura en Informática
5	Universidad Politécnica de El Salvador	Ingeniería en Ciencias de la Computación
6	Universidad Albert Einstein	Ingeniería en Computación
7	Universidad Evangélica de El Salvador	Ingeniería en Sistemas Comp-{-utacionales
8	Universidad Luterana Salvadoreña	Licenciatura en Ciencias de la Computación
9	Universidad Don Bosco	Ingeniería en Ciencias de la Computación
10	Universidad Cristiana de las Asambleas de Dios	Ingeniería en Ciencias de la Computación
11	Universidad Dr. Andrés Bello	Licenciatura en Computación
12	Universidad Gerardo Barrios	Ingeniería en Sistemas y Redes Informáticas
13	Universidad de Sonsonate	Ingeniería en Sistemas Computacionales
14	Universidad Salvadoreña Alberto Masferrer	Licenciatura en Ciencias de la Computación
15	Universidad Dr. José Matías Delgado	Licenciatura en Gerencia Informática
16	Universidad Católica de El Salvador	Ingeniería en Sistemas Informáticos
17	Universidad de Oriente	Ingeniería Informática

Para poder ver en detalle los planes de estudio de estas universidades, utilizar el CD adjunto, Apartado "Anexos", opción "Planes de Estudio".

ANEXO #3: DEFINICIONES DE DELITO INFORMÁTICO

FUENTE	DEFINICIÓN
Julio Téllez Valdés	"Actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".
Carlos Sarzana Tratadista penal Italiano	"Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".
Rafael Fernández Calvo Miembro de Asociación de Técnicos de Informática de España.	"La realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la constitución española".
Código penal Colombiano	"Puede comprender tanto aquellas conductas que recaen sobre herramientas informáticas propiamente tales, llámense programas, ordenadores, etc.; como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como son la intimidad, el patrimonio económico, la fe pública, etc".
María de la Luz Lima Malvado Doctora en Derecho por el Instituto Nacional de Ciencias Penales.	"En un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

ANEXO #4: TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR LA ORGANIZACIÓN DE LAS NACIONES UNIDAS (O.N.U.)

Fraudes cometidos mediante manipulación de computadoras.

a) Manipulación de los datos de entrada: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

b) La manipulación de programas: es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c) Manipulación de los datos de salida: se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para decodificar información electrónica en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

d) Fraude efectuado por manipulación informática: aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina técnica del salchichón en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones informáticas.

a) Como objeto: cuando se alteran datos de los documentos almacenados en forma computarizada.

b) Como instrumentos: las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Daños o modificaciones de programas o datos computarizados.

a) Sabotaje informático: es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

> *i) Virus:* es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
>
> *ii) Gusanos:* se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus. Por ejemplo, un programa gusano que eventualmente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.
>
> *iii) Bomba lógica o cronológica:* exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

b) Acceso no autorizado a servicios y sistemas informáticos: se produce por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

> i) Piratas informáticos o hackers: el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a diversos medios de ingreso. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

c) Reproducción no autorizada de programas informáticos de protección legal: ésta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

ANEXO #5: TABLA ÁREAS BAJO LA CURVA NORMAL TIPIFICADA DE 0 A Z PARA DETERMINAR EL NIVEL DE CONFIANZA Y EL COEFICIENTE DE CONFIABILIDAD

z	0	1	2	3	4	5	6	7	8	9
0.0	0.0000	0.0040	0.0080	0.0120	0.0160	0.0199	0.0239	0.0279	0.0319	0.0359
0.1	0.0398	0.0438	0.0478	0.0517	0.0557	0.0596	0.0636	0.0675	0.0714	0.0753
0.2	0.0793	0.0832	0.0871	0.0910	0.0948	0.0987	0.1026	0.1064	0.1103	0.1141
0.3	0.1179	0.1217	0.1255	0.1293	0.1331	0.1368	0.1406	0.1443	0.1480	0.1517
0.4	0.1554	0.1591	0.1628	0.1664	0.1700	0.1736	0.1772	0.1808	0.1844	0.1879
0.5	0.1915	0.1950	0.1985	0.2019	0.2054	0.2088	0.2123	0.2157	0.2190	0.2224
0.6	0.2257	0.2291	0.2324	0.2357	0.2389	0.2422	0.2454	0.2486	0.2517	0.2549
0.7	0.2580	0.2611	0.2642	0.2673	0.2703	0.2734	0.2764	0.2793	0.2823	0.2652
0.8	0.2881	0.2910	0.2939	0.2967	0.2995	0.3023	0.3051	0.3078	0.3106	0.3133
0.9	0.3159	0.3186	0.3212	0.3238	0.3264	0.3289	0.3315	0.3340	0.3364	0.3389
1.0	0.3413	0.3438	0.3461	0.3485	0.3508	0.3531	0.3554	0.3577	0.3599	0.3621
1.1	0.3643	0.3665	0.3686	0.3708	0.3729	0.3749	0.3770	0.3790	0.3810	0.3830
1.2	0.3849	0.3869	0.3888	0.3907	0.3925	0.3944	0.3962	0.3980	0.3997	0.4015
1.3	0.4032	0.4049	0.4066	0.4082	0.4099	0.4115	0.4131	0.4147	0.4162	0.4177
1.4	0.4192	0.4207	0.4222	0.4236	0.4251	0.4265	0.4279	0.4292	0.4306	0.4319
1.5	0.4332	0.4345	0.4357	0.4370	0.4382	0.4394	0.4406	0.4418	0.4429	0.4441
1.6	0.4452	0.4463	0.4474	0.4485	0.4495	0.4505	0.4515	0.4525	0.4535	0.4545
1.7	0.4554	0.4564	0.4573	0.4582	0.4591	0.4599	0.4608	0.4616	0.4685	0.4633
1.8	0.4641	0.4649	0.4656	0.4664	0.4671	0.4678	0.4686	0.4693	0.4699	0.4706
1.9	0.4713	0.4719	0.4726	0.4732	0.4738	0.4744	0.4750	0.4756	0.4762	0.4767
2.0	0.4773	0.4778	0.4783	0.4788	0.4793	0.4798	0.4803	0.4808	0.4812	0.4817
2.1	0.4821	0.4826	0.4830	0.4834	0.4838	0.4842	0.4846	0.4850	0.4854	0.4857
2.2	0.4861	0.4865	0.4868	0.4871	0.4875	0.4878	0.4881	0.4884	0.4887	0.4890
2.3	0.4893	0.4896	0.4898	0.4901	0.4904	0.4906	0.4909	0.4911	0.4913	0.4916
2.4	0.4918	0.4920	0.4922	0.4925	0.4927	0.4929	0.4931	0.4932	0.4934	0.4936
2.5	0.4938	0.4940	0.4941	0.4943	0.4945	0.4946	0.4948	0.4949	0.4951	0.4952
2.6	0.4953	0.4955	0.4956	0.4957	0.4959	0.4960	0.4961	0.4962	0.4963	0.4964
2.7	0.4965	0.4966	0.4967	0.4968	0.4969	0.4970	0.4971	0.4972	0.4973	0.4974
2.8	0.4975	0.4975	0.4976	0.4977	0.4978	0.4978	0.4979	0.4980	0.4980	0.4981
2.9	0.4981	0.4982	0.4983	0.4984	0.4984	0.4985	0.4985	0.4985	0.4986	0.4986
3.0	0.4987	0.4987	0.4987	0.4988	0.4988	0.4989	0.4989	0.4989	0.4990	0.4990
3.1	0.4990	0.4991	0.4991	0.4991	0.4992	0.4992	0.4992	0.4992	0.4993	0.4993
3.2	0.4993	0.4993	0.4994	0.4994	0.4994	0.4994	0.4994	0.4995	0.4995	0.4995
3.3	0.4995	0.4995	0.4995	0.4996	0.4996	0.4996	0.4996	0.4996	0.4996	0.4997
3.4	0.4997	0.4997	0.4997	0.4997	0.4997	0.4997	0.4997	0.4997	0.4997	0.4998
3.5	0.4998	0.4998	0.4998	0.4998	0.4998	0.4998	0.4998	0.4998	0.4998	0.4998
3.6	0.4998	0.4998	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999
3.7	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999
3.8	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999	0.4999
3.9	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000

Para un nivel de confianza del 95%, Z = 1.96

ANEXO #6: MODELO DE ENCUESTAS PARA EL SECTOR LEGAL

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

Objetivo: Conocer el grado de conocimiento de los elementos incluidos dentro del sector legal (jueces, fiscales, abogados) respecto a la informática forense, sus herramientas y la evidencia digital.

Los datos obtenidos a través de esta encuesta serán utilizados únicamente con objetivos académicos, para el trabajo de graduación: **"INVESTIGACIÓN DE LAS HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE EN EL SALVADOR".**

1. **¿Sabe usted qué es la Informática Forense?**

   Sí ☐ No ☐

2. **¿Sabe usted qué son los delitos informáticos?**

   Si ☐ No ☐

3. **¿Sabe usted qué son las herramientas de informática forense?**

   Sí ☐ No ☐

4. **¿Sabe qué es la evidencia digital, también conocida como prueba científica?**

   Sí ☐ No ☐

5. **¿Ha tenido a su cargo algún juicio de delito informático donde se haya presentado evidencia digital? (Si su respuesta es Si pase a la siguiente pregunta si es No pase a la pregunta 7)**

   Sí ☐ No ☐

6. **¿Qué tipo de delitos ha tratado?**

Pornografía infantil.		**Piratería.**	
Violación a la privacidad.		**Fraude Electrónico.**	
Clonación de tarjetas electrónica.		**Estafas.**	
Otros.		**Especifique:**	

7. **¿Considera que la evidencia digital válida puede ser determinante en el esclarecimiento de un delito informático?**

   Sí ☐ No ☐

8. **Si respondió si a la respuesta anterior, ¿En qué porcentaje influye la validez evidencia digital para la resolución favorable de un delito informático?**

0 – 24%		25 – 49%	
50 – 74 %		75 – 100%	

9. **¿Según su criterio cuales de los siguientes factores hacen válida la evidencia digital?**

La forma en que fue recolectada.	
El tipo de herramienta que se utilizó.	
La capacidad técnica del que obtuvo la evidencia digital.	
La cadena de custodia.	
El marco legal que la soporta.	
El nivel de conocimiento en la aplicación de las herramientas del perito que obtuvo la evidencia digital.	
Otros. Especifique:	

10. **¿Según su criterio, cuales son los principales obstáculos que impiden que los delitos informáticos tengan una resolución favorable?**

    _____
    _____
    _____
    _____

11. **¿Considera usted que los peritos informáticos tienen los conocimientos técnicos y científicos para realizar sus labores y permitir la obtención de evidencia digital válida?**

    Sí ☐ No ☐

12. **¿Cree que la aplicación de la informática forense en los casos de delitos informáticos trae ventajas en la resolución de delitos informáticos?**

    Sí ☐ No ☐

ANEXO #7: MODELO DE CODIFICACIÓN DE LAS ENCUESTAS PARA EL SECTOR LEGAL

PREGUNTA	**¿Sabe usted qué es la informática forense?**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Sabe usted qué son los delitos informáticos?**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Sabe usted qué son las herramientas de informática forense?**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Sabe qué es la evidencia digital, también conocida como prueba científica?**	
	RESPUESTA	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Ha tenido a su cargo algún juicio de delito informático donde se haya presentado evidencia digital?**	
	RESPUESTA	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Qué tipo de delitos ha tratado?**	
	RESPUESTA	**CÓDIGO**
	Pornografía infantil.	1
	Violación a la privacidad.	2
	Clonación de tarjetas electrónicas.	3
	Piratería.	4
	Fraude electrónico.	5
	Otros	6
PREGUNTA	**¿Considera que la evidencia digital válida puede ser determinante en el esclarecimiento de un delito informático?**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**Si respondió si a la respuesta anterior, ¿En qué porcentaje influye la validez evidencia digital para la resolución favorable de un delito informático?**	
	RESPUESTA	**CÓDIGO**
	0 – 24%	1
	25 – 49 %	2
	50 – 74%	3
	75 – 100	4

PREGUNTA	**¿Según su criterio cuales de los siguientes factores hacen válida la evidencia digital?**	
	RESPUESTA	**CÓDIGO**
	La forma en que fue recolectada.	1
	El tipo de herramienta que se utilizó.	2
	La capacidad técnica del que obtuvo la evidencia digital.	3
	La cadena de custodia.	4
	El marco legal que la soporta.	5
	El nivel de conocimiento en la aplicación de las herramientas del perito que obtuvo la evidencia digital.	6
	Otros. Especifique:	7
PREGUNTA	**¿Según su criterio, cuales son los principales obstáculos que impiden que los delitos informáticos tengan una resolución favorable?**	
	RESPUESTAS	**CÓDIGO**
PREGUNTA	**¿Considera usted que los peritos informáticos tienen los conocimientos técnicos y científicos para realizar sus labores y permitir la obtención de evidencia digital válida?**	
	REPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Cree que la aplicación de la informática forense en los casos de delitos informáticos trae ventajas en la resolución de delitos informáticos?**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2

ANEXO #8: MODELO DE ENCUESTAS PARA EL SECTOR EDUCATIVO

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

Objetivo: Conocer y medir el uso por parte de docentes universitarios de herramientas de software utilizadas en la informática forense y definir la necesidad y disposición de impartir conocimientos sobre las mismas.

Los datos obtenidos a través de este instrumento serán utilizados únicamente con objetivos académicos, para el trabajo de graduación: **"INVESTIGACIÓN DE LAS HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE EN EL SALVADOR".**

Por favor conteste las preguntas que se formulan a continuación marcando con una X las respuestas Si o No o marcando las casillas de las opciones que apliquen.

1. **¿Ha recibido alguna capacitación sobre herramientas de software que se utilizan en la informática forense?**
   Si □ No □

2. **¿Ha utilizado software que se aplica en la informática forense?**
   Si □ No □

Si su respuesta es sí marque una X cuales de los mencionados a continuación. Si es no pase a la pregunta 5.

Recuperación de archivos eliminados		Recuperación de números de Licencia	
Copias de backup de datos bit a bit		Verificación de Integridad de datos	
Monitoreo o control de computadoras		Otros:	
Marcado de documentos			
Recuperación de Passwords			
Desencriptación de Archivos			

3. **¿Con que frecuencia lo utiliza o ha utilizado?**

Semanalmente		**Anualmente**	
Mensualmente		Otros:	
Trimestralmente			
Semestralmente			

4. **¿Cuáles de los siguientes software aplicables en la informática forense ha utilizado? Marcar con una X.**

Encase		Norton Ghost	
Safeback		OnTrack Easy Recovery	
Produkey		Fire	
Helix		Sleuthkit	
C.A.I.N.E		Otros:	
WinHex			
Forensic Toolkit			

5. **¿Considera necesario que los nuevos profesionales posean conocimientos enfocados a este tipo de herramientas?**

   Si □ No □

   Si su respuesta es Si ¿Por qué?_____
   _____

6. **Como docente, ¿estaría en la disposición de impartir conocimientos referentes a las herramientas de software de informática forense que ayuden al desarrollo de esta rama de la informática y colaboren al esclarecimiento de delitos informáticos?**

   Si □ No □

   Si su respuesta fue Si marque con una X el motivo o los motivos:

Colaborar con la formación académica		Otros:	
Apoyar el desarrollo de la Informática			
Colaborar con la justicia			

7. **¿Estaría dispuesto a ser capacitado en informática forense y sus herramientas de software?**

   Si □ No □

   Si su respuesta es Si ¿Por qué?_____
   _____

8. **¿Considera que es necesaria la introducción de una materia en la(s) carreras(s) relacionada(s) a la informática en que se capacite en herramientas de software para informática forense ampliando así el campo de acción de los profesionales?**

   Si □ No □

9. Que factor considera que facilitaría la enseñanza en el área de la informática forense y la aplicación de sus herramientas.

Promoción por parte del Gobierno		Mayor recurso económico para el desarrollo de la Informática	
Promoción por parte de las instituciones de educación superior		Creación de academia capacitadora y laboratorios forenses en el país.	
Promoción de software libre para informática forense		Otros:	

10. ¿Cuál sería la principal ventaja de conocer como se utilizan las herramientas de software para informática Forense?

Valor Agregado		Poseer conocimiento para compartirlo	
Estar preparado para desempeñarse como Perito informático		Otra:	
Aumentar la competitividad de los profesionales			
Estar preparado para actuar en casos de detectar un posible delito informático			

ANEXO #9: MODELO DE CODIFICACIÓN DE LAS ENCUESTAS PARA EL SECTOR EDUCATIVO

PREGUNTA	¿Ha recibido alguna capacitación sobre herramientas de software que se utilizan en la informática forense?	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Ha utilizado software que se aplica en la informática forense.**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**Si su respuesta es sí marque una X cuales de los mencionados a continuación. Si es no pase a la pregunta 5.**	
	RESPUESTAS	**CÓDIGO**
	Recuperación de archivos eliminados.	1
	Copias de backup de datos bit a bit.	2
	Monitoreo o control de computadoras.	3
	Marcado de documentos.	4
	Recuperación de Passwords.	5
	Desencriptación de Archivos.	6
	Recuperación de números de Licencia.	7
	Verificación de Integridad de datos.	8
	Otros.	9
PREGUNTA	**¿Con que frecuencia lo utiliza o ha utilizado?**	
	RESPUESTA	**CÓDIGO**
	Semanalmente.	1
	Mensualmente.	2
	Trimestralmente.	3
	Semestralmente.	4
	Anualmente.	5
	Otros.	6
PREGUNTA	**¿Cuales de los siguientes software aplicables en la informática forense ha utilizado?**	
	RESPUESTA	**CÓDIGO**
	Encase	1
	Safeback	2
	Produkey	3
	Helix	4
	C.A.I.N.E	5
	WinHex	6
	Forensic Toolkit	7
	Norton Ghost	8
	OnTrack Easy Recovery	9
	Fire	10
	Sleuthkit	11
	Otros.	12

PREGUNTA	**¿Considera necesario que los nuevos profesionales posean conocimientos enfocados a este tipo de herramientas?**	
	RESPUESTA	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**Como docente, ¿estaría en la disposición de impartir conocimientos referentes a las herramientas de software de informática forense que ayuden al desarrollo de esta rama de la informática y colaboren al esclarecimiento de delitos informáticos?**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**Si su respuesta fue Si marque con una X el motivo o los motivos.**	
	RESPUESTA	**CÓDIGO**
	Colaborar con la formación académica.	1
	Apoyar el desarrollo de la Informática.	2
	Colaborar con la justicia.	3
	Otros.	4
PREGUNTA	**¿Estaría dispuesto a ser capacitado en informática forense y sus herramientas de software?**	
	RESPUESTA	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Considera que es necesaria la introducción de una materia en la(s) carreras(s) relacionada(s) a la informática en que se capacite en herramientas de software para informática forense ampliando así el campo de acción de los profesionales?**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**Que factor considera que facilitaría la enseñanza en el área de la informática forense y la aplicación de sus herramientas.**	
	REPUESTAS	**CÓDIGO**
	Promoción por parte del Gobierno	1
	Promoción por parte de las instituciones de educación superior	2
	Promoción de software libre para informática forense	3
	Mayor recurso económico para el desarrollo de la Informática	4
	Creación de academia capacitadora y laboratorios forenses en el país.	5
	Otros.	6
PREGUNTA	**¿Cuál sería la principal ventaja de conocer como se utilizan las herramientas de software para informática Forense?**	
	RESPUESTAS	**CÓDIGO**
	Valor Agregado.	1
	Estar preparado para desempeñarse como Perito informático.	2
	Aumentar la competitividad de los profesionales.	3
	Estar preparado para actuar en caso de detectar un posible delito informático.	4
	Poseer conocimiento para compartirlo.	5
	Otra.	6

ANEXO #10: MODELO DE ENCUESTAS PARA EL SECTOR PROFESIONAL

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

Objetivo: Conocer y medir el uso de las herramientas de software utilizadas en la informática forense por los peritos informáticos en El Salvador.

Los datos obtenidos a través de este instrumento serán utilizados únicamente con objetivos académicos, para el trabajo de graduación: **"INVESTIGACIÓN DE LAS HERRAMIENTAS DE SOFTWARE UTILIZADAS EN LA INFORMÁTICA FORENSE EN EL SALVADOR"**.

Por favor conteste las preguntas que se formulan a continuación marcando con una X las respuestas Si o No o marcando las casillas de las opciones que apliquen.

1. **De qué forma inició sus conocimientos en el campo de la informática forense**

   De manera autodidacta ☐

   Capacitaciones recibidas en el país ☐
   Donde la recibió:
   _____

   Capacitaciones recibidas en el extranjero ☐
   Donde la recibió:
   _____

   Otros ☐
   Especifique:
   _____
   _____

2. **De la siguiente clasificación ¿Cuáles son los tipos de herramientas de informática forense que ha utilizado?**

   Herramientas para la recuperación de datos ☐
   Herramientas para el monitoreo de computadoras ☐
   Herramientas de marcado de documentos ☐
   Herramientas de hardware ☐
   Otros:
   _____
   _____

3. **De la siguiente clasificación ¿Sobre qué tipo de herramientas tiene mayor conocimiento?**

   Herramientas de software propietario ☐ Herramientas de software libre ☐

4. **¿Cuáles son las herramientas de software para la informática forense que ha utilizado con mayor frecuencia y cual el uso que les ha dado?**

Nombre de la herramienta	Uso

5. **¿Conoce la existencia de entidades o instituciones que ofrezcan certificaciones en el campo de la informática forense en El Salvador?**
   Si ☐ No ☐

   Si su respuesta es "Si", especifique cuales conoce:

   _____
   _____

6. **¿En qué casos de delitos informáticos ha participado como perito forense?**
   a. Pornografía infantil ☐
   b. Piratería ☐
   c. Fraude comercial ☐
   d. Clonación de tarjetas de crédito ☐
   e. Robo de información confidencial ☐
   f. Financiamiento del crimen ☐
   g. Otros ☐

   Si su respuesta es "otros", especifique:

   _____
   _____

7. ¿Cuáles son los factores que dificultan la adquisición de nuevos conocimientos sobre las herramientas de software para la informática forense?

Costo de las herramientas □
Falta de lugares que ofrezcan capacitaciones □
Se consideran innecesarias □
Otros □
Si su respuesta es "otros", especifique:

_____
_____

8. ¿Cómo considera los resultados obtenidos por las herramientas de software libre para la informática forense en comparación con los obtenidos por medio de las herramientas de software propietario?

Menor calidad □ igual calidad □ mejor calidad □

9. Desde su punto de vista ¿Cuáles son los factores que dificultan la implementación de software libre para la informática forense?

Falta de compatibilidad con el equipo tecnológico existente □
Falta de fuentes de capacitación con respecto a su uso □
Falta de credibilidad de sus resultados □
Poca difusión de sus características y ventajas □
Otros □
Si su respuesta es "otros", especifique:

_____
_____

10. ¿Ha recibido alguna capacitación sobre las herramientas de software para la informática forense?

Si □ No □

Si su respuesta es "si" ¿Que tema se trato en dicha capacitación?

_____
_____

11. ¿Considera que la creación de una entidad o academia que se encargue de la formación, capacitación y certificación de peritos informáticos influiría de forma positiva en la persecución de los delitos informáticos?

Si □ No □

12. ¿Considera importante que las instituciones de educación superior incluyeran en sus planes de estudio materias relacionadas con la práctica de la informática forense y sus herramientas?

Si □ No □

13. ¿En qué porcentaje considera que el bajo nivel conocimiento sobre las herramientas que se utilizan en informática forense afecte la obtención de una evidencia digital valida?

0%-25%		26-50%	
51%-75%		76%-100%	

ANEXO #11: MODELO DE CODIFICACIÓN DE LAS ENCUESTAS PARA EL SECTOR PROFESIONAL

PREGUNTA	**¿De qué forma inició sus conocimientos en el campo de la informática forense?**	
	RESPUESTAS	**CÓDIGO**
	De manera autodidacta.	1
	Capacitaciones recibidas en el país.	2
	Capacitaciones recibidas en el extranjero.	3
	Otros.	4
PREGUNTA	**De la siguiente clasificación ¿Cuáles son los tipos de herramientas de informática forense que ha utilizado?**	
	RESPUESTAS	**CÓDIGO**
	Herramientas para la recuperación de datos	1
	Herramientas para el monitoreo de computadoras	2
	Herramientas de marcado de documentos	3
	Herramientas de hardware	4
	Otros	5
PREGUNTA	**De la siguiente clasificación ¿Sobre qué tipo de herramientas tiene mayor conocimiento?**	
	RESPUESTAS	**CÓDIGO**
	Herramientas de software propietario	1
	Herramientas de software libre	2
PREGUNTA	**¿Cuáles son las herramientas de software para la informática forense que ha utilizado con mayor frecuencia y cual el uso que les ha dado?**	
	RESPUESTA	**CÓDIGO**
	Herramienta	1
	Herramienta	2
PREGUNTA	**¿Conoce la existencia de entidades o instituciones que ofrezcan certificaciones en el campo de la informática forense en El Salvador?**	
	RESPUESTA	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿En qué casos de delitos informáticos ha participado como perito forense?**	
	RESPUESTA	**CÓDIGO**
	Pornografía infantil.	1
	Piratería	2
	Fraude comercial	3
	Clonación de tarjetas de crédito	4
	Robo de información confidencial	5
	Financiamiento del crimen	6
	Otros	7
PREGUNTA	**¿Cuáles son los factores que dificultan la adquisición de nuevos conocimientos sobre las herramientas de software para la informática forense?**	
	RESPUESTAS	**CÓDIGO**
	Costo de las herramientas.	1
	Falta de lugares que ofrezcan capacitaciones.	2
	Se consideran innecesarias.	3
	Otros.	4

PREGUNTA	**¿Cómo considera los resultados obtenidos por las herramientas de software libre para la informática forense en comparación con los obtenidos por medio de las herramientas de software propietario?**	
	RESPUESTA	**CÓDIGO**
	menor calidad	1
	igual calidad	2
	mejor calidad	3
PREGUNTA	**Desde su punto de vista ¿Cuáles son los factores que dificultan la implementación de software libre para la informática forense?**	
	RESPUESTA	**CÓDIGO**
	Falta de compatibilidad con el equipo tecnológico existente	1
	Falta de fuentes de capacitación con respecto a su uso	2
	Falta de credibilidad de sus resultados	3
	La cadena de custodia.	4
	Poca difusión de sus características y ventajas	5
	Otros	6
PREGUNTA	**¿Ha recibido alguna capacitación sobre las herramientas de software para la informática forense?**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Considera que la creación de una entidad o academia que se encargue de la formación, capacitación y certificación de peritos informáticos influiría de forma positiva en la persecución de los delitos informáticos?**	
	REPUESTAS	**CÓDIGO**
	SI	1
	NO	2
PREGUNTA	**¿Considera importante que las instituciones de educación superior incluyeran en sus planes de estudio materias relacionadas con la práctica de la informática forense y sus herramientas?**	
	RESPUESTAS	**CÓDIGO**
	SI	1
	NO	2

ANEXO #12: TABLA DE DISTRIBUCIÓN CHI CUADRADO

	PROBABILIDAD DE UN VALOR SUPERIOR - *ALFA* (α)				
Grados libertad	**0,1**	**0,05**	**0,025**	**0,01**	**0,005**
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,60
3	6,25	7,81	9,35	11,34	12,84
4	7,78	9,49	11,14	13,28	14,86
5	9,24	11,07	12,83	15,09	16,75
6	10,64	12,59	14,45	16,81	18,55
7	12,02	14,07	16,01	18,48	20,28
8	13,36	15,51	17,53	20,09	21,95
9	14,68	16,92	19,02	21,67	23,59
10	15,99	18,31	20,48	23,21	25,19
11	17,28	19,68	21,92	24,73	26,76
12	18,55	21,03	23,34	26,22	28,30
13	19,81	22,36	24,74	27,69	29,82
14	21,06	23,68	26,12	29,14	31,32
15	22,31	25,00	27,49	30,58	32,80
16	23,54	26,30	28,85	32,00	34,27
17	24,77	27,59	30,19	33,41	35,72
18	25,99	28,87	31,53	34,81	37,16
19	27,20	30,14	32,85	36,19	38,58
20	28,41	31,41	34,17	37,57	40,00
21	29,62	32,67	35,48	38,93	41,40
22	30,81	33,92	36,78	40,29	42,80
23	32,01	35,17	38,08	41,64	44,18
24	33,20	36,42	39,36	42,98	45,56
25	34,38	37,65	40,65	44,31	46,93
26	35,56	38,89	41,92	45,64	48,29
27	36,74	40,11	43,19	46,96	49,65
28	37,92	41,34	44,46	48,28	50,99
29	39,09	42,56	45,72	49,59	52,34
30	40,26	43,77	46,98	50,89	53,67
40	51,81	55,76	59,34	63,69	66,77
50	63,17	67,50	71,42	76,15	79,49
60	74,40	79,08	83,30	88,38	91,95
70	85,53	90,53	95,02	100,43	104,21
80	96,58	101,88	106,63	112,33	116,32
90	107,57	113,15	118,14	124,12	128,30
100	118,50	124,34	129,56	135,81	140,17

ANEXO #13: HERRAMIENTAS SELECCIONADAS PRELIMINARMENTE

NOMBRE DE LA HERRAMIENTA	TIPO DE HERRAMIENTA	TIPO DE LICENCIAMIENTO	PRECIO ($)	ENLACE
µHash	**Cálculo de Hash**	Libre	0.00	http://uhash.mivanov.org/download/0.3/uHash.zip
Hyper Hasher	**Cálculo de Hash**	Propietario	10.00	http://www.hyperhasher.com/
FileVerifier++	**Cálculo de Hash**	Libre	0.00	http://www.programmingunlimited.net/siteexec/content.cgi?page=fv
FlexTk	**Cálculo de Hash**	Propietario	125.00	http://flexense.com/flextk/
Encrypt Easy	**Cálculo de Hash**	Propietario	29.00	http://www.encrypt-easy.com/
HashX	**Cálculo de Hash**	Libre	0.00	http://www.boilingbit.com/
HashOnClick	**Cálculo de Hash**	Libre	0.00	http://www.2brightsparks.com/freeware/freeware-hub.html
digestIt	**Cálculo de Hash**	Libre	0.00	http://www.colonywest.us/

CRCDropper drag and drop CRC32/hash calculator.	**Cálculo de Hash**	Libre	0.00	http://www.goat1000.com/crcdropper.php
md5sum	**Cálculo de Hash**	Libre	0.00	Repositorios GNU/Linux Debian
X-Ways Replica	**Copias de datos bit a bit**	Propietario	500.00	http://www.x-ways.net/winhex/index-m.html
Herramienta dd para linux	**Copias de datos bit a bit**	Libre	0.00	http://ss64.com/bash/dd.html
Clonezilla-Live	**Copias de datos bit a bit**	Libre	0.00	http://clonezilla.org/
Norton Ghost 14	**Copias de datos bit a bit**	Propietario	69.99	http://www.symantec.com/es/mx/norton/ghost
DriveClone	**Copias de datos bit a bit**	Libre	0.00	http://www.farstone.com
HDClone Pro Edition 3.7.3	**Copias de datos bit a bit**	Propietario	83.59	http://www.miray.de/products/sat.hdclone.html

DriveClone Pro 6	**Copias de datos bit a bit**	Propietario	49.99	http://www.farstone.com/software/driveclone-pro.htm
DriveImage XML	**Copias de datos bit a bit**	Propietario	100.00	http://www.runtime.org/driveimage-xml.htm
SelfImage 1.2.1.92	**Copias de datos bit a bit**	Libre	0.00	http://winbytes.net/selfimage_download/
Iolo Search and Recover	**Recuperación de datos**	Propietario	19.95	http://www.iolo.com/sr/5/
File Scavenger	**Recuperación de datos**	Propietario	49.00	http://www.quetek.com/prod02.htm
Recover My Files	**Recuperación de datos**	Propietario	69.95	http://www.recovermyfiles.com/
Smart Data Recovery	**Recuperación de datos**	Propietario	49.95	http://www.smartpctools.com/es/data_recovery/index.html

TestDisk	**Recuperación de datos**	Libre	0.00	http://www.cgsecurity.org/wiki/TestDisk
Pandora Recovery	**Recuperación de datos**	Libre	0.00	http://www.pandorarecovery.com/
Eaesus Deleted File Recovery	**Recuperación de datos**	Libre	0.00	http://www.easeus-deletedrecovery.com/
NTFS Undelete	**Recuperación de datos**	Libre	0.00	http://www.ntfsundelete.com/downloads/
Recuva	**Recuperación de datos**	Libre	0.00	http://www.recuva.com/
PC Inspector File Recovery	**Recuperación de datos**	Libre	0.00	http://www.pcinspector.de/
Encase Forensic	**Kits de herramientas**	Propietario	3,000.00	http://www.guidancesoftware.com/computer-forensics-ediscovery-software-digital-evidence.htm
Forensic Toolkit	**Kits de herramientas**	Propietario	3,835.00	http://www.digitalintelligence.com/software/accessdata/forensictoolkit2/

CAINE	**Kits de herramientas**	Libre	0.00	http://www.caine-live.net/
HELIX PRO	**Kits de herramientas**	Libre	0.00	http://www.e-fense.com/helix3pro.php
Windows NT Forensic Utility Suite	**Kits de herramientas**	Propietario	No Disponible	http://www.forensics-intl.com/suite9.html
Coroner´s Toolkit	**Kits de herramientas**	Libre	0.00	http://www.porcupine.org/forensics/tct.html
DEFT Linux	**Kits de herramientas**	Libre	0.00	http://www.deftlinux.net/
LicenseCrawler	**Recuperación de números de licencia**	Libre	0.00	http://www.klinzmann.name/
Product Key Explorer	**Recuperación de números de licencia**	Propietario	29.50	http://www.product-key-explorer.com/productkey-explorer-features.html
Produkey	**Recuperación de números de licencia**	Libre	0.00	http://www.nirsoft.net/utils/product_cd_key_viewer.html

Magical Jelly Bean Keyfinder	**Recuperación de números de licencia**	Libre	0.00	http://magicaljellybean.com/keyfinder/
PDF Unlocker	**Recuperación de contraseñas**	Propietario	24.00	http://www.pdf-unlocker.com/get-pdf-restriction-remover.html
Advanced PDF Password Recovery Professional	**Recuperación de contraseñas**	Propietario	24.00	http://www.elcomsoft.com/apdfpr.html
PDF Password Remover	**Recuperación de contraseñas**	Propietario	29.00	http://www.verypdf.com/pwdremover/
PDF Password Cracker	**Recuperación de contraseñas**	Propietario	24.95	http://www.crackpdf.com/
Office Password Recovery Magic	**Recuperación de contraseñas**	Propietario	47.99	http://www.password-recovery-magic.com/office_password_recovery/index.htm
Advanced Office Password Recovery	**Recuperación de contraseñas**	Propietario	199.00	http://www.elcomsoft.com/aopr.html

Advanced Office Password Breaker	**Recuperación de contraseñas**	Propietario	199.00	http://www.elcomsoft.com/aopb.html
Advanced Rar password Recovery	**Recuperación de contraseñas**	Propietario	60.00	http://www.elcomsoft.com/arpr.html
Rar Password Cracker	**Recuperación de contraseñas**	Propietario	30.00	http://www.rarpasswordcracker.com/
Rar password Recovery	**Recuperación de contraseñas**	Propietario	29.95	http://www.intelore.com/rar_password_recovery.php
Rar Password Unlocker	**Recuperación de contraseñas**	Propietario	19.95	http://www.passwordunlocker.com/products/rpu.html

ANEXO #14: MATRIZ CRITERIOS-HERRAMIENTAS

HERRAMIENTA	UTILIDAD	ADAPTABILIDAD	MANTENIMIENTO	PORTABILIDAD	ACCESIBILIDAD	DOCUMENTACIÓN	ESTABILIDAD
• µHash	Calculo de Hash	Si	Si	No	No	Si	Si
• Hyper Hasher	Calculo de Hash	Si	Si	No	Si	Si	Si
• FileVerifier++	Calculo de Hash	Si	Si	No	No	Si	Si
• FlexTk	Calculo de Hash	Si	Si	No	No	Si	Si
• Encrypt Easy	Calculo de Hash	Si	Si	No	No	Si	Si
• HashX	Calculo de Hash	Si	Si	No	No	Si	Si
• HashOnClick	Calculo de Hash	Si	Si	No	No	Si	Si
• digestIt	Calculo de Hash	Si	Si	No	No	Si	Si
• CRCDropper	Calculo de Hash	Si	Si	No	Si	Si	Si
• md5sum	Calculo de Hash	Si	Si	No	No	Si	Si
• µHash	Calculo de Hash	Si	Si	No	No	Si	Si
• Hyper Hasher	Calculo de Hash	Si	Si	No	No	Si	Si
• FileVerifier++	Calculo de Hash	Si	Si	No	No	Si	Si
• FlexTk	Calculo de Hash	Si	Si	No	No	Si	Si

• Encrypt Easy	Calculo de Hash	Si	Si	No	No	Si	Si
• HashX	Calculo de Hash	Si	Si	No	Si	Si	Si
• HashOnClick	Calculo de Hash	Si	Si	No	No	Si	Si
• digestIt	Calculo de Hash	Si	Si	No	No	Si	Si
• CRCDropper	Calculo de Hash	Si	Si	No	No	Si	Si
• md5sum	Calculo de Hash	Si	Si	No	Si	Si	Si
• X-Ways Replica	Copias bit a bit	Si	Si	No	No	Si	Si
• dd linux	Copias bit a bit	Si	Si	No	No	Si	Si
• Clonezilla-Live	Copias bit a bit	Si	Si	Si	Si	Si	Si
• Norton Ghost 14	Copias bit a bit	Si	Si	No	Si	Si	Si
• PC Inspector clone maxx	Copias bit a bit	Si	Si	No	No	Si	Si
• HDClone	Copias bit a bit	Si	Si	No	Si	Si	Si
• DriveClone Pro 6	Copias bit a bit	Si	Si	No	Si	Si	Si
• DriveImage XML	Copias bit a bit	Si	Si	No	No	Si	Si
• SelfImage 1.2.1.92	Copias bit a bit	Si	Si	No	No	Si	Si

• Iolo Search and Recover	Recuperacion de datos	Si	Si	No	No	Si	Si
• File Scavenger	Recuperacion de datos	Si	Si	No	No	Si	Si
• Recover My Files	Recuperacion de datos	Si	Si	No	SI	Si	Si
• Smart Data Recovery	Recuperacion de datos	Si	Si	No	Si	Si	Si
• TestDisk	Recuperacion de datos	Si	Si	No	No	Si	Si
• Pandora Recovery	Recuperacion de datos	Si	Si	No	Si	Si	Si
• Eaesus Deleted File Recovery	Recuperacion de datos	Si	Si	No	No	Si	Si
• NTFS Undelete	Recuperacion de datos	Si	Si	No	Si	Si	Si
• Recuva	Recuperacion de datos	Si	Si	No	No	Si	Si
• Autopsy Forensic Browser	Kit Informatica Forense	Si	Si	No	No	Si	Si
• Encase Forensic	Kit Informatica Forense	Si	Si	SI	Si	Si	Si
• Forensic Toolkit	Kit Informatica Forense	Si	Si	SI	No	Si	Si

• CAINE	Kit Informatica Forense	Si	Si	SI	Si	Si	Si
• HELIX PRO	Kit Informatica Forense	Si	Si	SI	Si	Si	Si
• Windows NT Forensic Utility Suite	Kit Informatica Forense	Si	Si	No	No	Si	Si
• Coroner´s Toolkit	Kit Informatica Forense	Si	Si	No	No	Si	Si
• DEFT	Kit Informatica Forense	Si	Si	Si	Si	Si	Si
• LicenseCrawler	Recuperacion de Seriales	Si	Si	Si	Si	Si	Si
• Product Key Explorer	Recuperacion de Seriales	Si	Si	No	Si	Si	Si
• Produkey	Recuperacion de Seriales	Si	Si	Si	Si	Si	Si
• Magical Jelly Bean Keyfinder	Recuperacion de Seriales	Si	Si	Si	Si	Si	Si
• PDF Unlocker	Recuperacion de Password	Si	Si	No	Si	Si	Si
• Advanced PDF Password Recovery	Recuperacion de Password	Si	Si	No	Si	Si	Si
• PDF Password Remover	Recuperacion de Password	Si	Si	No	Si	Si	Si
• PDF Password Cracker	Recuperacion de Password	Si	Si	No	Si	Si	Si
• Office Password Recovery Magic	Recuperacion de Password	Si	Si	No	Si	Si	Si

• Advanced Office Password Recovery	Recuperacion de Password	Si	Si	No	Si	Si	Si
• Advanced Office Password Breaker	Recuperacion de Password	Si	Si	No	Si	Si	Si
• Advanced Rar password Recovery	Recuperacion de Password	Si	Si	No	Si	Si	Si
• Rar Password Cracker	Recuperacion de Password	Si	Si	No	Si	Si	Si
• Rar password Recovery	Recuperacion de Password	Si	Si	No	Si	Si	Si
• Rar Password Unlocker	Recuperacion de Password	Si	Si	No	Si	Si	Si