Universidad De El Salvador

Facultad De Ingenieria Y Arquitectura

Escuela De Ingenieria De Sistemas Informaticos

Trabajo De Graduación

"Estudio Y Análisis Sobre La Informática Forense En El Salvador"

Presentado Por

Belloso Urbina, Ramiro Alexander	Bu01001
Mancia Rivera, Mirna Noemy	Mr00005
Morán Bautista, Oscar José	Mb01031
Olmedo Portillo, Guadalupe Beatriz	Op00002

Docente Director Ing. Julio Alberto Portillo.

Cuidad Universitaria, Noviembre De 2008

INDICE

INDICE DE TABLAS, FIGURAS Y GRÁFICOS

TABLAS

FIGURAS

GRÁFICO

INTRODUCCIÓN

INTRODUCCIÓN

Las nuevas tecnologías y el desarrollo del mercado relacionado con los dispositivos que permiten acceder a las nuevas comunicaciones han revolucionado el mundo, permitiendo llevar a otro nivel los negocios, las transacciones, la administración de las entidades, comunicaciones y el almacenamiento de información en lugares físicamente alejados de las empresas. Esta evolucion tecnologica tambien es aprovechada por personas malintencionadas quienes utilizan la gama de herramientas tecnologicas para fines incorrectos, como lo es la realizacion de un crimen de indole informatico, valiendose muchas veces de que la información queda almacenada en forma digital pudiendo sustraerla y manipularla de manera erronea. Cuando pasa una situacion de este tipo se presenta un problema, debido a que las computadoras guardan la información que puede servir como evidencia de forma tal que no puede ser recolectada por medios comunes, si no que se requiere la utilización de mecanismos diferentes a los tradicionales. Es de aquí que surge la informática forense como una ciencia relativamente nueva, que permite el esclarecimiento de este tipo de delitos por medio de su aplicación.

El Salvador experimenta una amplia variedad de delitos informáticos, siendo este uno de los problemas que empieza a afectar a la ciudadanía y que tienen lugar en todo el mundo. Este tipo de delitos no excluyen a nadie, afecta a todos los sectores que conforman nuestro pais desde empresarios a ciudadanos, como todo tipo de violencia afecta las posibilidades de desarrollo del país.

Por esta razón, surge el estudio y análisis sobre la informática forense en El Salvador como el resultado de una reflexión y análisis que se llevo a cabo en la materia de Auditoria de Sistemas Informáticos, el cual es retomado por la escuela de Ingeniería de Sistemas Informáticos, como se puede constatar según carta anexa (***Anexos N° 1)***, debido a la importancia que esta temática tiene y el impacto que ésta puede llegar a causar dentro de la sociedad salvadoreña y en especifico en los procesos judiciales.

La informática forense involucra la participación de profesionales de las tecnologías de la información y de los profesionales del derecho debido a que los resultados obtenidos por medio de la aplicación de informática forense está sujeto al análisis judicial.

El Estudio y Análisis sobre la informatica forense en El Salvador permite dar a conocer cual es la situacion actual de esta especializacion en nuestro pais, para obtener esta informacion fue necesario como primer punto hacer una investigacion preliminar sobre la informatica forense y todos los elementos que estan involucrados en su proceso de aplicación. A continuación se muestra en detalle las partes por las cuales esta comprendido el presente proyecto de graduación, desde la fase teórica hasta la fase practica de la informática forense.

El **Capitulo Uno** de este estudio trata todo lo referente al aspecto teorico de esta ciencia, donde se hace incapie de la importancia de su aplicación, se conocera en que consiste los delitos informaticos, ya que son estos la causa para la aplicación de la informatica forense, ademas de presentar el marco teorico de la investigacion donde se mostrara que tipo de investigacion se realizara. Ademas se da a conocer las entidades involucradas en la aplicación de la informatica forense en nuestro pais, las cuales son las reponsables de evitar que tipos de delitos de carácter tecnologico sigan realizandose.

Dentro del **Capitulo Dos**, se puede observar la metodologia que se utiliza para el desarrollo del estudio, es aquí donde se plasma la justificacion del estudio, sus objetivos, el planteamiento del problema a solucionar, definicion de las poblaciones a encuestar y determinacion de muestras.

Para el desarrollo de la presente investigación, una parte muy importante fue la definición y planteamiento del problema o lo que es lo mismo el objeto de estudio de la misma, es por esto que se elaboro y se presenta la problemática que se tiene en nuestro país con respecto a la informatica forense, la cual se analizo por medio de la formulación y análisis del problema planteado, así como también se definio el por qué de la investigación y cuál es el objetivo que se pretendio alcanzar con la realizacion de este proyecto.

La recoleccion, tabulacion y analisis de datos esta comprendido en el **Capitulo Tres**, esta parte muestra la tabulacion de los datos obtenidos por medio de encuestas, ademas se presentan los analisis de las correspondientes interrogantes hechas a las poblaciones involucradas en el estudio y se comprueba la hipotesis generada al inicio de la investigacion, la cual indica si se cumple o no la suposicion.

Para la obtencion de la informacion y presentacion de la situacion actual de este estudio se hizo uso de métodos, técnicas e instrumentos de recolección de datos que permitieron contar con informacion confiable y que son los elementos que ayudaron a desarrollar una investigacion clara y eficiente. La información obtenida por medio de una investigación debe ser comprobada estadísticamente para ver su grado de confiabilidad y asi poder determinar cual es su error muestral, es por estar razon que se llevo a cabo el procedimiento de comprobación de la hipótesis general de esta investigación a través de la prueba estadística Chi cuadrado y asi comprobar la validez de la informacion recolectada.

Los análisis presentados de cada una de las poblaciones estudiadas dan a conocer el nivel de aplicación que se tiene de la informática forense en el país por las instituciones involucradas en el esclarecimiento de delitos informáticos, la información que ayudo a la elaboración de dicho análisis fue obtenida por medio de herramientas de medición validadas, las cuales permitieron obtener resultados precisos y confiables.

Además de obtener informacion sobre la situacion actual de la informatica forense en nuestro pais, se considero de gran utilidad diseñar indicadores que ayuden para medir el grado de avance de ésta atravez del tiempo, estos estan comprendidos en el **Capitulo Cuatro,** donde su principal funcion es monitorear el comportamiento de las diversas manifestaciones del desarrollo que tiene la informática forense en El Salvador. Del mismo modo, su propósito es servir de herramienta de análisis para la formulación de políticas públicas dirigidas a la prevención y a la transformación de la violencia en el País.

La presentacion de indicadores con sus respectivos resultados y analisis son retomados en el diagnostico que se elaboro con respecto a la aplicación de la informatica forense en El Salvador, con este diagnostico se presenta la situacion actual en la que se encuentra la informatica forense en nuestro pais.

Como punto final se presentan los elementos que estan compuestos dentro de la informatica forense, estos son tratados en el **Capitulo Cinco,** donde se muestran metodologías para la aplicación de informática forense utilizadas por expertos de paises internacionales como: España, Uruguay,

Colombia, Argentina entre otros, esto para tener una mejor comprension de que es lo que se debe de hacer en un proceso de analisis forense.

También se muestra una serie de herramientas informáticas que son utilizadas para realizar análisis de informática forense, se expone una breve descripción de su funcionamiento, requerimientos de hardware y software, incluso el costo que cada una de estas tiene tomando como base las recomendaciones brindadas por peritos internaciones expertos en el tema. De la mano con estas herramientas se plasma una guía sobre la demostración del uso de una de ellas.

Las herramientas no lo son todo para el profesional en informática forense, también debe de conocer procedimientos, metodologías que le permitan hacer un buen trabajo, por lo cual se presentan técnicas y estándares internacionales que explican con detalle la forma adecuada de obtener y tratar la evidencia digital de la escena del crimen.

Se presentan ejemplos de formatos de cadena de custodia utilizados para la recolección de la evidencia digital y de peritajes informáticos forenses como resultado del análisis realizado a la evidencia, se incluyen propuestas de formatos tanto de cadena de custodia como de peritajes informáticos.

Como un agregado a esta investigación se encuentra una propuesta de temario para capacitaciones en informática forense, orientada a estudiantes y profesionales de las áreas de la informática y del derecho, teniendo presente que las instituciones de educación superior son las encargadas de instruir a futuros profesionales en estas áreas por tal razón debe brindarse el conocimiento sobre la informática forense.

Finalmente se presentan las conclusiones y recomendaciones a las que se llegó con la investigación de campo realizada sobre el proyecto "Estudio y Análisis sobre la Informática forense en El Salvador".

ESTE DOCUMENTO VA ACOMPAÑADO DE UN CD.

El cual contiene el documento impreso en digital, de igual manera presenta una serie de elemento que complementaran al documento impreso para facilitar la comprension de la informacion presentada en El Estudio y Analisis sobre la Informatica Forense en El Salvador.

OBJETIVOS DEL PROYECTO

OBJETIVOS DEL ESTUDIO

GENERAL

- Realizar el estudio y análisis sobre la informática forense en El Salvador y presentar el diagnostico de la situación actual de ésta, determinando así su incidencia en los procesos judiciales.

ESPECÍFICOS

- Definir la población y muestra de los elementos involucrados en el estudio.
- Diseñar los instrumentos para la recolección de datos que serán distribuidos en la población y muestra para recabar los datos que serán posteriormente utilizados en la elaboración del análisis.
- Recopilar y tabular los datos extraídos de los instrumentos de recolección para realizar la interpretación y análisis de éstos presentando la información obtenida.
- Explicar los procedimientos actuales utilizados por instituciones encargadas de velar por la seguridad de la sociedad.
- Plantear y comprobar las hipótesis que se establecen en el estudio sobre la informática forense en El Salvador.
- Elaborar indicadores que revelen la realidad de la informática forense de EL Salvador para poder cuantificar el desarrollo de ésta en los procesos judiciales y ser además un insumo que se utilice como base para observar las tendencias y los cambios a través del tiempo que la informática forense vaya experimentando.
- Presentar metodologías y herramientas utilizadas para la aplicación de la informática forense en base a la información obtenida a través de peritos.
- Mostrar ejemplos de formatos tanto de peritajes informáticos forenses como de cadenas de custodia utilizados en la recolección de la evidencia digital.
- Presentar las conclusiones y recomendaciones a las cuales se llego después de la realización del análisis de las encuestas dirigidas a las poblaciones involucradas en la utilización de la informática forense y en la resolución de casos por delitos informáticos.

IMPORTANCIA

IMPORTANCIA

La importancia del proyecto se ha centrado en el elemento que ha influido en la realización de delitos informáticos a nivel mundial sin ser El Salvador excluido, este es el creciente uso de Internet por parte de las empresas y personas.

Desde sus inicios se ha tenido un uso incorrecto de internet por parte de individuos que han demostrado la existencia de debilidades en las instituciones por no contar con tecnologia adecuada para hacer frente a la forma de proceder de estos.

Por tal razón se realiza el estudio sobre la informática forense en El Salvador para sentar un precedente de lo que es esta especializacion que está en desarrollo y dar a conocer la importancia de esta temática en nuestro país, debido a que constantemente se cometen delitos informáticos y las autoridades competentes no tienen como hacer frente a esta problemática ya que carecen de herramientas informáticas, personal capacitado e instalaciones adecuadas para realizar las pruebas requeridas y si poder asi demostrar cómo se han cometido estos delitos y quiénes son los responsables de éstos(***Anexos N° 2***).

A continuación se presentan los beneficiados de esta investigación:

- La Universidad de El Salvador, podrá conocer, como se encuentra esta especialidad en el pais, el nivel de aplicación por parte de instituciones involucradas en el esclarecimiento de delitos informaticos, la importancia que se da a nivel académico e impartir en un futuro no muy lejano, asignaturas propias a la carrera de Ingeniería Informática y hasta poder contar con una especialización o maestría en esta área.

  Además de brindar herramientas que le permitan medir el avance de la informática forense en el país.

- Para las instituciones que aplican la ley, mostrar que la informática forense cuenta con sólidas bases, que puede ser una herramienta confiable y tranparente en procesos judiciales, permitiendo así dar paso a la utilización de sus métodos de recolección y analisis de la evidencia digital, reconstruir escenas del crímenes, sentar precedentes de delitos que han ocurrido, o servir de evidencia incriminatoria en un juicio.

- A las autoridades policiales hacer de su conocimiento que mediante la aplicación de la tecnologia en el area criminalistica, esta facilitara la obtencion, analisis y preservacion de la evidencia digital encontrada en la escena del crimen.

- A las instituciones de educacion tales como universidades, instituciones que imparten cursos de tecnologías, mostrar la necesidad de implementar nuevas asignaturas, fortalecer áreas curriculares, etc. Para fortalecer los métodos y técnicas tanto de los actuales como futuros profesionales para lograr un mejor desarrollo de tecnologia informatica y aplicar satisfactoriamente la informática forense.

- Al brindar la información de este estudio, ésta puede utilizarse como base estadística para futuras investigaciones

JUSTIFICACIÓN

JUSTIFICACIÓN

A medida que la tecnología avanza en el área de la informática así crece la delincuencia con el uso de ésta, es decir, la ejecución de delitos informáticos va en ascenso con aparicion de las nuevas herramientas informáticas; por tal razón se necesita la aplicación de una especializacion que haga frenrte a los delitos informaticos que se realizan, en el país se efectúan una serie de delitos informáticos entre los cuales se pueden mencionar la pornografía infantil, la piratería, el fraude comercial, la clonación de tarjetas de crédito, robo de información confidencial, virus informáticos y el financiamiento del crimen.

Estudios realizados en Mayo de 2007 por la Alianza del Software para Negocio BSA[1], muestra que la tasa de piratería en El Salvador en el año 2006 fue de un 82%, un punto porcentual más que el año 2005 y se estima que la pérdida por esta asciende a los 18 millones de dólares.

Para Noviembre de 2007 la Procuraduría General de la República, había recibido mil cuatrocientas denuncias de pornografía infantil[2].

Por estos y otros delitos informáticos que no se denuncian debido a que existen vacíos de credibilidad en las instituciones que son las responsables de velar y de hacer que se cumplan los derechos de las personas, ha sido necesario realizar el estudio y analisis sobre la informática forense en el país y así presentar su aplicación para hacer frente a los delitos informáticos y asi obtener pruebas que esclarezcan la culpabilidad o inocencia de un imputado.

Con la elaboración del estudio se busca brindar una metodología con fundamentos acorde a la legalidad de las instituciones para que conozcan los avances de la tecnología informática y puedan realizar cambios dentro de las instituciones para hacer frente a las nuevas formas de proceder de los delincuentes informáticos, además dará mayor credibilidad y permitirá resolver con mayores argumentos casos en los cuales se halle involucrado el uso de un medio electrónico computacional con fines maliciosos.

Los beneficios a lograr con el estudio son:

- Evitar la impunidad en la resolución de los casos que involucren delitos informáticos con procedimientos, técnicas y herramientas informáticas, permitiendo que la evidencia digital sea una prueba admisible en los juicios.
- Fortalecer las vías de comunicación tanto para los profesionales de las ramas de la informática y del derecho, para integrar y complementar los vacíos legales creados por el rápido desarrollo de la tecnología.

[1] Por sus siglas en ingles: Bussines Software Alliance. Ver apartado *Glosario de término* para una mayor comprensión.
[2] Ver apartado *Referencias Bibliográficas II-Sitios Web* literal 26, para su referencia.

- Ayudará al esclarecimiento de los delitos informáticos.
- Conocer cuan importante es el uso de la tecnologia para el esclarecimiento de delitos informaticos.

Aplicar la informática forense, permitirá crear precedentes de hechos cometidos para utilizarlos de referencia en casos similares, además de mostrar la forma de proceder de los delincuentes informáticos y como la aplicación de la tecnologia facilitara el proceder de las intituciones encargardas de velar por la seguridad de los ciudadanos.

ALCANCES Y LIMITACIONES

ALCANCES Y LIMITACIONES

ALCANCES

1. El proyecto de investigación permitirá conocer la situación actual de la informática forense en El Salvador, las instituciones involucradas en su aplicación, el aspecto jurídico en el que se desenvuelve y su aceptación en la resolución de procesos judiciales. Además se presentarán índices que permitan monitorear el avance de la informática forense en el país.
2. No se contempla en la realización de la investigación el desarrollo de herramientas informáticas forenses.

LIMITACIONES

- Falta de denuncias de delitos informáticos que impiden conocer los índices reales de crecimiento de éstos, esta información es de relevancia al momento de verificar los avances que se vayan dando en la informática forense, es decir, se necesita conocer los índices reales de los delitos informáticos para ver su comportamiento y así determinar el grado de crecimiento que debería de tener esta, para el apoyo a las instituciones involucradas en resolución de procesos judiciales

RESULTADOS ESPERADOS

RESULTADOS ESPERADOS

En este apartado se presentan los resultados que se pretenden alcanzar al final del *ESTUDIO Y ANÁLISIS SOBRE LA INFORMÁTICA FORENSE EN EL SALVADOR* las cuales se presentan a continuación:

1. Dar a conocer cual es la situación actual de la informática forense en el país, su conocimiento, y aplicación en la recolección de evidencia digital para ser presentada en un proceso judicial.

2. Creación de indicadores que permitan medir el uso de la informática forense en el país.

3. Propuestas de solución:

   - Presentación de metodologías utilizadas en la informática forense.
     - Presentar ejemplos de guías a seguir utilizadas en informática forense por expertos.
   - Herramientas informáticas: Cuadro explicativo de las herramientas utilizadas en la informática forense; es decir dar a conocer su nombre, costo, descripción, etc. Ademas CD´s que contiene herramientas informaticas utilizadas actualmente para aplicar la informatica forense.
   - Formatos para presentar informes forenses finales.
   - Propuesta de contenido temático para la creación de una materia en base a la informática forense.

     Se presenta esta temática dado que las universidades no contemplan en su plan curricular (**ver *Planes curriculares en CD***) asignaturas relacionadas con la informática forense, además para que se impartan capacitaciones a profesionales involucrados en la resolución de delitos informáticos

CAPITULO 1

INVESTIGACIÓN PRELIMINAR

CAPITULO 1: INVESTIGACIÓN PRELIMINAR

A- ANTECEDENTES

El desarrollo de la tecnología informática ha comenzado a plantear nuevos desafíos y la mayoría de las profesiones se han tenido que adaptar a la era digital, en particular es necesario que la fuerza policial este actualizándose en esta área, dado que el crecimiento de criminalidades en las que se utilizan las tecnologías digitales hacen necesarios nuevos tipos de investigación.

La aplicación de la tecnología informática en la investigación de un ilícito cometido usando una computadora, ha creado una nueva especialización, *la informática forense*, que es el proceso de identificar, preservar, analizar y presentar la evidencia digital de una manera legalmente aceptable.

En 1986, la National Science Foundation (NSF) de EE.UU. inició el desarrollo de NSFNET que se diseñó originalmente para conectar cinco superordenadores. Su interconexión con Internet requería unas líneas de muy alta velocidad. Esto aceleró el desarrollo tecnológico de INTERNET y brindó a los usuarios mejores infraestructuras de telecomunicaciones.

El día 1 de noviembre de 1988 Internet fue "infectada" con un virus de tipo "gusano", creado por Robert Morris, estudiante de la universidad de Cornell, New York, este incidente provocó que el 10% de todos los servidores conectados quedaran inhabilitados. El acontecimiento subrayó la falta de adecuados mecanismos de seguridad en Internet, por lo cual DARPA formó el Computer Emergency Reponse Team (CERT), un equipo de reacción rápida que mantiene datos sobre todas las incidencias en red y sobre las principales amenazas.

Desde el año 1991 la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoría de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Esto ha provocado que se creen instituciones especializadas en el área de la informática forense teniendo como objetivo mediante procesos y metodologías obtener evidencia digital para ser presentada como prueba en un tribunal de justicia.

Países que hacen uso de la informática forense para el esclarecimiento de procesos judiciales.

Bolivia

Bolivia cuenta con el Instituto de Investigaciones Forenses (IDIF)[3], el cual es un órgano dependiente administrativa y financieramente de la Fiscalía General de la República, que está encargado de realizar, con autonomía funcional, todos los estudios científico - técnicos requeridos para la investigación de los delitos o la comprobación de otros hechos por orden judicial. (Ley No. 1970 Nuevo Código de Procedimiento Penal de 25 de marzo de 1999, en su Título II, Capítulo II, Art. 75º.).

Perú

Ley N° 27.309, promulgada el 15 de julio de 2000 y publicada el 17 de julio de 2000, incorporó los delitos informáticos al Código Penal.

Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con sus efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad mediante computadoras 15 de mayo de 1986.

España

Ley Orgánica N°. 10 de 1995, de fecha 23 de Noviembre de 1995.

Dentro de la legislación española, podemos distinguir la aplicación de las siguientes medidas en el ámbito penal.

- Ataques que se producen contra el derecho a la intimidad.
- infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor.
- Falsedades.
- Sabotajes informáticos.
- fraudes informáticos.
- Amenazas.
- Calumnias e injurias, y
- Pornografía infantil.

Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático

[3] Ver Referencias Bibliográficas II-Sitios Web literal 23, para su referencia.

Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987

Esta ley contempla los siguientes delitos:

Destrucción de datos, estafa informática.

De esta forma muchos países han visto la necesidad de implementar reformas dentro de su legislación para apoyar a las entidades respectivas a castigar delitos que antes gozaban de impunidad por una débil estructura de leyes.

Diferencia entre informática forense y seguridad informática

A manera de aclarar cualquier duda o confusión que pueda surgir sobre el tema en estudio y la seguridad informática se presenta a continuación en que consiste la seguridad informática. Cabe recalcar que la informática forense entra en acción después de una violación de seguridad en los sistemas informáticos; por lo tanto es muy importante considerar el nivel de seguridad informática que se pueda tener para la protección de datos en los equipos, sin embargo la seguridad total no existe ya que siempre existen riesgos y debilidades a los que se está expuesto. Además la seguridad informática considera la participación del recurso humano que manipulan los equipos informáticos (estos no necesitan conocimientos especializados en seguridad informática) como elemento importante en su desarrollo o aplicación, caso contrario en la aplicación de la informática forense donde el recurso humano que participa es únicamente personal especializado en informática forense.

Seguridad informática[4]

Definición

Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas y concientizarlas de su importancia en el proceso será algo crítico.

Elementos básicos de la seguridad informática

- **Confidencialidad**

  Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.

- **Integridad**

  Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

- **Disponibilidad**

  Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

[4] Ver Referencia Bibliográfica I-Libros literal 11 y II Sitios Web literales 27.

Seguridad Física y Seguridad Lógica

El estudio de la seguridad informática podríamos plantearlo desde dos enfoques distintos aunque complementarios:

- La seguridad física: puede asociarse a la protección del sistema ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, etc.
- La seguridad lógica: protección de la información en su propio medio, mediante el enmascaramiento de la misma usando técnicas de criptografía.

  La gestión de la seguridad está en medio de las dos, los planes de contingencia, políticas de seguridad, normativas, etc.

Principios de la seguridad informática

Se presentan a continuación los tres principios básicos de la seguridad informática: el del acceso más fácil, el de la caducidad del secreto y el de la eficiencia de las medidas tomadas.

Tras los acontecimientos del 11 de Septiembre de 2001 en Nueva York, los del 11 de Marzo de 2004 en Madrid y los del 7 de Julio de 2005 en Londres, que echaron por tierra todos los planes de contingencia, incluso los más paranoicos, comenzamos a tener muy en cuenta las debilidades de los sistemas y valorar en su justa medida el precio de la seguridad.

Principio del acceso más fácil

En este principio se formula la siguiente pregunta, que ayudará a tomar las consideraciones necesarias para la seguridad en los accesos al sistema.

¿Cuáles son los puntos débiles de un sistema informático?

- El intruso al sistema utilizará el mecanismo que haga más fácil su acceso y posterior ataque.
- Existirá una diversidad de frentes desde los que puede producirse un ataque, tanto internos como externos. Esto dificultará el análisis de riesgo ya que el delincuente aplicará la filosofía del ataque hacia el punto más débil: el equipo o las personas.

Principio de la caducidad del secreto

Se formula la siguiente pregunta, que ayudará a tomar las consideraciones necesarias para la seguridad de los datos.

¿Cuánto tiempo deberá protegerse un dato?

- Los datos confidenciales deben protegerse sólo hasta que ese secreto pierda su valor como tal.
- Se habla, por tanto, de la caducidad del sistema de protección: tiempo en el que debe mantenerse la confidencialidad o secreto del dato.

Principio de la eficiencia de las medidas tomadas.

- Las medidas de control se implementan para que tengan un comportamiento efectivo, eficiente, sean fáciles de usar y apropiadas al medio.

- ✓ Efectivo: que funcionen en el momento oportuno.
- ✓ Eficiente: que optimicen los recursos del sistema.
- ✓ Apropiadas: que pasen desapercibidas para el usuario.

- Y lo más importante: ningún sistema de control resulta efectivo hasta que debemos utilizarlo al surgir la necesidad de aplicarlo. Junto con la concienciación de los usuarios.

Amenazas del sistema

Las amenazas afectan principalmente al hardware, al software y a los datos. Éstas se deben a fenómenos de:

- Interrupción
- Interceptación
- Modificación
- Generación

A continuación se amplia sobre los tipos de amenazas que afectan a los sistemas informáticos:

Amenazas de interrupción

Estas amenazas surgen cuando se daña, pierde o deja de funcionar un punto del sistema. Su detección es inmediata y sus consecuencias son: Destrucción del hardware, borrado de programas, datos y fallos en el sistema operativo.

Amenazas de interceptación

Consiste en el acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos. Su detección es difícil, a veces no deja huellas. Esto provoca que hayan: Copias ilícitas de programas, escucha en línea de datos, etc.

Amenazas de modificación

Acceso no autorizado que cambia el entorno para su beneficio. Su detección es difícil según las circunstancias y permite que existan: Modificación de bases de datos, modificación de elementos del HW.

Amenazas de generación

Creación de nuevos objetos dentro del sistema. Su detección es difícil: delitos de falsificación. Ejemplos de estas amenazas son: Añadir transacciones en red, Añadir registros en base de datos.

Debido a las amenazas antes mencionadas que pueden existir para los equipos informáticos, tanto hardware, software y datos, es que surge la necesidad de aplicar medidas de seguridad que impidan que se efectúen acciones indebidas y así proteger el los activos que se posean.

Sin embargo puede darse el caso que se viole la seguridad, provocando daños como las que se mencionan anteriormente dependiendo del tipo de amenaza que se presente.

Para la compensación de los daños causados ante una situación de estas, buscar los rastros de los individuos responsables y así poder presentar pruebas sobre su delito, se aplica la informática forense que se encarga de la reconstrucción de escenas y análisis de evidencias digitales obtenidas durante la investigación que se este desarrollando, esto por medio del uso de herramientas informáticas especializadas y metodologías establecidas para su aplicación.

B- SITUACIÓN ACTUAL

Surge la inquietud de conocer como, cuando, quienes y donde se aplica la informática forense; ya que en el país se tiene un alto índice de delitos informáticos entre los que están: clonación de tarjetas de crédito, pornografía infantil, robo de información confidencial, piratería de software, robo de base de datos, robo de identidad, financiamiento del crimen es por ello que se hace necesario realizar el estudio de la situación actual de la informática forense como medio de recolección y análisis de evidencia digital que ayude al esclarecimiento de estos delitos.

Con el crecimiento de delitos informáticos que se han dado en El Salvador, se hace más ardua la tarea para las instituciones judiciales y policiales, las cuales trabajan en conjunto con la finalidad de lograr el esclarecimiento de dichos delitos, se hace necesario por parte de estas instituciones la utilización de la tecnología informática para revolver este tipo de delitos, sin embargo, en nuestro país aun no se cuenta con una legislación que ampare el uso de esta tecnología como en otros países donde si está establecido en el código penal leyes sobre la legalidad de la aplicación de la tecnología informática en procesos judiciales.

Instituciones involucradas en la aplicación de la informática forense.

Para evitar que casos de delitos informáticos queden impunes, las instituciones que se encargan de velar por los derechos de las personas y hacer justicia ante situaciones ilegales, cumplen con la actual ley que se tiene para desarrollar sus actividades de manera transparente.

En la resolución de un caso delictivo, La Fiscalía General de la República es la encargada de la parte acusatoria y de la búsqueda de pruebas incriminatorias, La Policía Nacional Civil forma parte en estos procesos judiciales como el ente encargado de guardar la cadena de custodia, La Corte Suprema de Justicia se encarga de verificar el cumplimiento de las leyes y dar el veredicto final en la resolución de un caso por medio del juez.

1. La Fiscalía General de la República

La Fiscalía General es el Órgano del Estado, integrante del Ministerio Público, el cual tiene sus fundamentos en la Constitución de la República, establecidos en el artículo 193. Siendo este articulo de la Constitución el fundamento de la Fiscalía General, ésta es la institución determinada por el estado para actuar con una función requirente "acusar", se le ha dado a ésta una facultad acusatoria donde existe un derecho de perseguir una actuación que constituya un hecho delictivo, donde esta institución buscará la verdad material y real de los hechos, debiendo dirigir la investigación del delito junto con la policía teniendo presente un conjunto de principios que se deben tener en cuenta en todo acto que esta institución realiza.

Dentro de sus funciones están:

- Defender los Intereses del Estado y de la Sociedad.
- Dirigir la investigación del delito con la colaboración de la Policía Nacional Civil, y en particular de los hechos criminales que han de someterse a la jurisdicción penal.

2. La Policía Nacional Civil

Es la encargada ante todo de evitar que la escena de un crimen sea contaminada por personas sin autorización, trabaja en conjunto con la Fiscalía en la investigación del delito, pero no puede tomar decisiones por ella misma, ya que únicamente se dedica a seguir las órdenes indicadas por la Fiscalía. En un caso de homicidio, la policía copia el acta del reconocimiento médico –forense, llevándolo a las oficinas de la institución, siendo este el primer paso para comenzar a buscar posibles sospechosos.

Los detectives policiales investigan a los posibles móviles, descubren a los criminales y tienen autoridad para detener a los sospechosos si las investigaciones indican que hay responsables.

La forma de proceder de esta institución ante delitos informáticos es similar a la de otros delitos, ya que cuando en la escena del crimen está involucrado un dispositivo electrónico computacional como posible móvil, se acordona el lugar impidiendo cualquier tipo de intrusión, esta forma de accionar permite que la obtención de evidencias digitales sea recolectada de forma correcta haciendo uso de la aplicación de la informática forense.

3. Corte Suprema de Justicia.

Esta institución es la que provee los jueces para los tribunales de justicia en donde se vaya a resolver un determinado hecho delictivo. El juez es un ente independiente de las partes procesales pues es la autoridad competente que decidirá la situación jurídica del imputado, se debe basar en el principio de independencia e imparcialidad, pues el dirigirá el proceso, valorará los elementos de prueba y es el que decidirá si el imputado es inocente o culpable.

A continuación se presentan en la ***Tabla N° 1*** delitos informáticos que se han realizado en El Salvador.

DELITOS INFORMÁTICOS	FUENTE
Clonación de tarjetas de crédito 25-Abril-2003	http://www.elsalvador.com/noticias/2003/04/25/nacional/nacio4.html
Pornografía infantil 29-Abril-2003	http://www.elsalvador.com/noticias/2003/05/29/nacional/nacio3.html
Piratería 29-Mayo-2005	http://www.elsalvador.com/vertice/2005/290505/deportada.html
El futuro de los vendedores de piratería 21-Junio-2006	http://www.diariocolatino.com/es/20060621/reportajes/reportajes_20060621_23/
Pornografía 27-Agosto- 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1660998
Clonación de tarjetas 1-Enero al 31 de Diciembre de 2007.	Ver apartado ***Anexos N° 3*** para un mayor detalle.

DELITOS INFORMÁTICOS	FUENTE
1-Enero al 11 de Abril de 2008.	Ver apartado ***Anexos N° 3*** para un mayor detalle.
Piratería 9-Abril-2008	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6410&idArt=2260807
Piratería y pornografía infantil 09-Abril-2008	http://www.laprensagrafica.com/departamentos/1031504.asp
Liberan al "mayor proveedor de CD pirata de la Darío" 22-Abril-2008	http://www.laprensagrafica.com/nacion/1040909.asp

Tabla N° 1 Delitos informáticos cometidos en el país.

Los delitos informáticos antes mencionados es un ejemplo de cómo se encuentra nuestro país, que poco a poco se ve envuelto en delitos que antes no se efectuaban y la necesidad de considerar elementos necesarios para que se pueda combatir y al mismo tiempo evitar la desconfianza de la recolección y análisis de datos que sean validas en juicios.

C- PLANTEAMIENTO DEL PROBLEMA

I. SITUACION PROBLEMÁTICA DE LA INFORMÁTICA FORENSE EN EL SALVADOR

La tecnología ha tenido un desarrollo sorprendente en los últimos años, tanto así que ahora es utilizada para cometer delitos informáticos tales como: clonación de tarjetas, piratería, pornografía infantil entre otros, algunos de estos delitos no están tipificados en la legislación salvadoreña, lo que impide el accionar de las instituciones judiciales.

La Policía Nacional Civil se ve limitada en los procesos de investigación de delitos informáticos, porque no cuenta con suficiente personal capacitado en el uso de herramientas informáticas y metodologías de recolección de evidencia digital.

La Fiscalía General de la República y la Corte Suprema de Justicia presentan debilidades, ya que no tienen leyes en las cuales se puedan amparar para juzgar a individuos detenidos y procesados por cometer delitos informáticos.

Además, las instituciones encargadas de preparar profesionales en informática no han abordado el tema de la informática forense, debido a la falta de personal capacitado, para impartir los conocimientos sobre dicha temática.

La problemática antes mencionada hace surgir la necesidad de aplicar la informática forense, como medio que ayude a esclarecer hechos delictivos informáticos.

II. DIAGRAMA DE CAUSA – EFECTO

Diagrama Causa y Efecto que se ha utilizado para identificar la problemática antes mencionada a la cual se pretende dar solución con la elaboración de este proyecto. Ver ***Figura N°.1***.

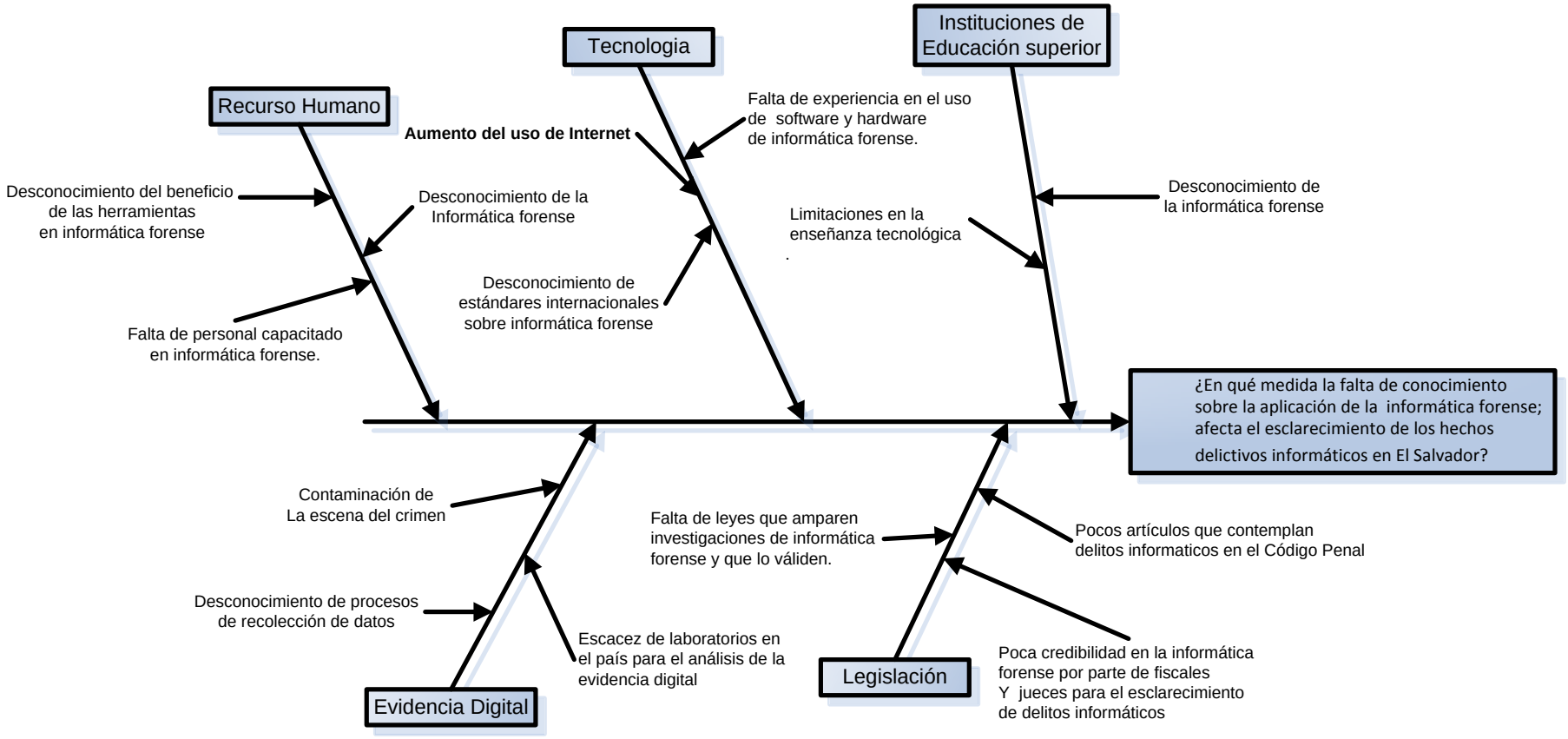


Figura N°.1: Diagrama causa-efecto utilizado para el planteamiento del problema

Elementos de la problemática.

Se presenta a continuación la interpretación de los elementos causales para la determinación de la problemática.

1. ***Recurso humano:*** es el personal encargado de aplicar la informática forense y hacer uso de los resultados obtenidos del análisis forense, para hacer valer la justicia.
2. ***Tecnología:*** comprende la utilización de software, hardware y estándares de informática forense.
3. ***Instituciones de educación superior:*** conjunto de universidades encargadas de preparar profesionales en informática.
4. ***Evidencia digital***[5]***:*** tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.
5. ***Legislación:*** comprende las leyes tanto primaria (constitución de la república) como secundarias (código penal, procesal penal, etc.).

III. FORMULACIÓN DEL PROBLEMA

En la ***Figura N° 2*** se presenta el diagrama donde serepresenta la formulación del problema

Figura N° 2: Diagrama de sistemas utilizado para la representación de la formulación del problema.

IV. ANALISIS DEL PROBLEMA

A continuación se presenta el análisis de las variables involucradas en el problema:

Entrada: Desconocimiento de la existencia de la informática forense en El Salvador.

Variables de entrada:

- Falta de tecnología especializada en la informática forense.
- Recurso humano no calificado
- Falta de conocimiento de la entidades en los procedimientos a seguir para la aplicación de la informática forense.
- Alto índice de delitos Informáticos impunes.

Salida: Elaboración del diagnostico sobre la situación actual y propuestas de solución para la aplicación de la informática forense en El Salvador.

[5] Ver apartado Referencia Bibliográfica II Sitios Web literal 28.

Variables de salida:

- Resolución favorable de delitos informáticos.
- Comprensión de la Tecnología especializada en la informática forense.
- Conocimiento especializado para aplicar la informática forense
- Descripción del rol que juegan las entidades involucradas e integridad que deben poseer para la resolución de delitos informáticos.
- Conocimiento y uso correcto de los procedimientos a seguir por las entidades para su intervención después de un delito informático.

Variables de solución:

- Metodología utilizada en la aplicación de la informática forense.
- Técnicas de recolección de evidencia.
- Conocimiento de Herramientas informáticas forenses.
- Clasificación de delito informático.

V. ENUNCIADO DEL PROBLEMA

¿En qué medida el desconocimiento sobre la aplicación de la informática forense; afecta el esclarecimiento de los hechos delictivos informáticos en El Salvador

D- FORMULACIÓN DE HIPOTESIS

En este apartado se enuncian las hipótesis las cuales ayudaran a resolver el problema que sea identificado.

Se formula la hipótesis general, siendo esta la respuesta tentativa al problema; se presenta una hipótesis nula, que nos servirá para aceptar o rechazar la variable que sea definido como independiente (causa) y como la manipulación afecta la variable dependiente (efecto), además se enuncian hipótesis auxiliares las cuales dando respuesta a cada una de ellas nos permitirá aceptar o rechazar la general que es el centro de la investigación.

I. GENERAL

"La aplicación de la informática forense en los procesos judiciales; favorecerá el esclarecimiento en el 75% de los delitos informáticos"

A continuación se presentan los elementos considerados en la formulación de la hipótesis general.

UNIDADES DE ANÁLISIS	VARIABLES	ELEMENTOS LÓGICOS
Procesos Judiciales	Aplicación Informática forense (VI[6]) (Causa).	Favorecerá, 75%
Delitos informáticos	Esclarecimientos de delitos informáticos (VD[7]) (Efecto)	

II. HIPÓTESIS NULA[8]

La formulación de esta hipótesis indica la información a obtener es contraria a la hipótesis general, con esta hipótesis se pretende negar la variable independiente, es decir, la causa identificada como origen del problema es extraña, por lo tanto debe rechazarse como tal.

Hipótesis Nula:

"La aplicación de la informática forense en los procesos judiciales; no alterará el esclarecimiento de los delitos informáticos".

[6] VI significa: Variable Independiente.
[7] VD significa: Variable Dependiente.
[8] Tomado del libro "Guía para la elaboración de trabajos de investigación, monografías y tesis" Ver *apartado Referencias Bibliográficas, I-Libros* literal 5 para su referencia.

III. AUXILIARES

Se formulan las siguientes hipótesis que facilitarán la aceptación o rechazo de la hipótesis general; una vez aceptadas estas hipótesis.

1. "La falta de herramientas informáticas forenses en las instituciones policiales, determina el 80% de la incidencia de fraudes que se realizan a través de Internet".

2. "La aplicación de una metodología de recolección y análisis de evidencias digitales, causará un rendimiento del 95% en el proceso de obtención de esta".

3. "La falta de personal calificado en informática forense, determina el 85% de la ineficiencia en la resolución de delitos informáticos".

4. "La debilidad de la legislación salvadoreña permite que el 85% de los delitos informáticos no sean esclarecidos en su totalidad".

E- MARCO TEÓRICO

Para una mejor compresión del tema a tratar en el presente trabajo, es necesario conocer la teoría que aclare y respalde los tópicos que serán abordados a lo largo de este documento. Es por esta razón que en este apartado se presenta la teoría y generalidades que son necesarias conocer y entender, para poder llevar a cabo el trabajo de investigación satisfactoriamente. Este apartado consta de 3 partes:

1. **Marco Teórico:** se expone la teoría relacionada con la informática forense y temas afines.
2. **Marco Conceptual:** se define el significado o la interpretación propia, que tendremos de algunos términos que son utilizados a lo largo del documento.
3. **Marco Legal:** se abordara la parte legal que tiene relación con la informática forense y la interpretación de los artículos relacionados con el tema.

I. MARCO TEORICO

El marco teórico consta de los siguientes apartados: delitos informáticos, informática forense, evidencia digital, pruebas periciales y teoría acerca de la metodología empleada para la realización del trabajo de investigación.

A continuación se presenta el desglose de cada uno de ellos.

a. DELITOS INFORMÁTICOS

La informática forense actúa después de que se ha cometido un delito informático, es por ello la importancia y necesidad de conocer a que se le define como delito informático y todos los tópicos que involucra este término.

Es por esta razón que se inicia con el concepto de delitos informáticos y a continuación se presentan las definiciones acerca de este término, posteriormente en el presente ***Capitulo 1*** apartado ***E. Marco Teórico II: Marco Conceptual*** , se definirá cual será la interpretación que se le dará a este término a lo largo del presente documento.

a.1 DEFINICIÓN DE DELITOS INFORMÁTICOS

1. El delito informático implica cualquier actividad ilegal que se pueden enmarcar dentro de las figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad.

2. Toda conducta típica, antijurídica y culpable que se vea facilitada o convertida en más daños o más lucrativa a causa de vulnerabilidades creadas o magnificadas por el uso creciente de los sistemas informáticos. En la delincuencia informática, la computadora puede fungir como objetivo de la acción dañosa, por ejemplo, en el sabotaje informático, o bien como mero instrumento para la realización del hecho, por ejemplo, un fraude informático.

a.2 NATURALEZA DEL DELITO INFORMÁTICO[9]

La naturaleza de los delitos informáticos se refiere específicamente a las actividades dirigidas a las computadoras con el fin hacer mal uso de ellas, a perturbar los sistemas de apoyo para robar, falsificar o destruir la información que almacenan.

Sin embargo, no es raro que la delincuencia informática, para referirse a un espectro más amplio de los actos que no sólo están destinados a las computadoras, muchas veces no se imaginan que puedan ocurrir situaciones como las siguientes:

- El delincuente puede ser un empleado destituido que antes de salir de la empresa instala un código o bomba de tiempo, que más tarde desactiva las computadoras o envía un e-mail amenazando a los jefes de la empresa.
- Un empleado en una firma de abogados roba un juicio, con el fin de venderlo a otra firma de abogados.
- Los empleados de una agencia de hardware/software venden productos sin el consentimiento de la empresa quedando con la ganancia.
- Un estudiante descontento envía un e-mail amenazante, dando lugar a la clausura de su escuela.
- Alguien estafando sitios de subastas.
- Un sitio Web muestra documentos de identificación falsos.
- Numerosas personas venden tarjetas descodificadoras de televisión satelital provocando el tener servicio de cable en las casas sin pagar ningún costo a las empresas que proporcionan este servicio.
- Piratas de software utilizan un sitio en la Web para la distribución de software pirateado.
- Alguien vende software a través de sitios de subastas, alegando que es una copia legal, pero, de hecho, proporciona una copia pirata.
- Un hacker accede a los registros bancarios, roba datos personales, y utiliza estos para obtener el titular de la cuenta.
- El robo de espacio a servidores no protegidos, para intercambio de información o almacenar información considerada ilegal.

La naturaleza del crimen informático va desde la venganza, codicia, corrupción hasta la curiosidad de simple conveniencia pragmática[10], otros criminales se dirigen a la información almacenada en las computadoras, en otros casos, el delito no tiene persona en particular como un objetivo, los autores no hacen más daño del cual podrían hacer, solo el de almacenar archivos innecesarios o ciclos de procesamiento falsos.

La informática forense se utiliza para investigar casos como los crímenes que se perpetran[11], ahora se necesita que la evolución de las técnicas de la informática forense brinden respuestas de los hechos cometidos, la necesidad de enfoques han evolucionado en respuesta para servir de evidencia y condenar acciones que atentan con los derechos de las personas.

[9] Según el libro: Computer And Intrusion Forensics, ver apartado Referencias Bibliográficas *I-Libros* literal 2, para su referencia.
[10] Ver apartado *Glosario de término* para una mayor comprensión.
[11] Ver apartado *Glosario de término* para una mayor comprensión

a.3 TIPOS DE DELITOS INFORMÁTICOS

Los delitos informáticos se definen dentro de tres categorías:

- La computadora puede ser el objetivo de un crimen como robarla, destruirla o utilizarla sin acceso autorizado. (Equipo informático usado como fin).
- La computadora puede ser la herramienta del crimen como en el caso del uso de Internet para enviar pornografía infantil, fraudes informáticos, amenazas y hostigamiento. (Equipo informático usado como medio).
- La computadora puede ser utilizada para almacenar evidencia de un delito como transacciones por lavado de dinero, narcotráfico o registros sensibles apropiados ilícitamente. (Equipo informático usado como método).

b. INFORMÁTICA FORENSE

En esta sección se presenta la teoría relacionada con este tema para una mayor comprensión del mismo.

b.1 DEFINICIÓN DE INFORMÁTICA FORENSE

A continuación se presentan las definiciones de informática forense desde 4 puntos de vistas distintos, los cuales son:

- Desde el punto de vista de Wikipedia: Se suele definir el análisis forense, en su sentido más general, como la "*aplicación de la ciencia a cuestiones de interés legal*". En el contexto de Tecnología de Información T.I[12] y la Seguridad de la Información, se define como "la inspección sistemática y tecnológica de un sistema informático y sus contenidos para la obtención de evidencia de un crimen o cualquier otro caso que se ha investigado".

- Desde el punto de vista de expertos en informática forense: Es una selección de criterios para guiar y asegurar actividades concernientes con el análisis de evidencia digital, él provee de recomendaciones y cubre aspectos legales, policiales y operacionales como requerimientos técnicos para adquisición, análisis y reporte de evidencia, colaboración con otros grupos de investigación, gestión de casos, soporte a la fuerza de la ley, desarrollo de políticas de seguridad para respuesta a incidentes y plan preventivo y de continuidad.[13]

- Desde el punto de vista legal: La informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a ella, las empresas obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través del uso indebido de las tecnologías de la información. Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.[14]

[12] T.I Tecnologías de Información, Para una mayor comprensión ver apartado *Glosario de término*.
[13] Según la asociación Code of practices for *Digital Forensics* - CP4DF
[14] Elena Pérez Gómez, socia de la firma de abogados Sánchez-Crespo Abogados y Consultores

- Desde el punto de vista judicial: La informática forense, es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.[15]

Durante el desarrollo del presente trabajo se utilizará el concepto de informática forense definido por el grupo de investigación en el presente ***Capitulo 1*** apartado ***E: Marco Teórico - II: Marco Conceptual***.

b.2 OBJETIVOS DE LA INFORMÁTICA FORENSE

La informática forense tiene 3 objetivos fundamentales que son:

- La persecución y procesamiento judicial de los delincuentes.
- La compensación de los daños causados por los criminales informáticos.
- La creación y aplicación de medidas para prevenir casos similares.

b.3 ESTUDIOS QUE PERMITE LA INFORMÁTICA FORENSE

Entre los estudios más conocidos que permite la informática forense tenemos:

- Recuperación de evidencias en discos
- Reconstrucción de eventos (Web-Internet)
- Acceso a archivos temporales y de caché
- Recuperación de contraseñas y archivos encriptados
- Detección y recuperación de Virus, Troyanos y Spyware
- Detección de mensajes de esteganografía[16]
- Anonimato
- Recuperación del Registro de Windows
- Investigación de información
- otros.

b.4 USOS DE LA INFORMÁTICA FORENSE

Los usos en los cuales es requerida la informática forense se detallan a continuación:

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

[15] Definición de Federal Bureau of Investigation (FBI)
[16] Ver apartado *Glosario de término* para una mayor comprensión.

- Investigación de Seguros: La evidencia encontrada en las computadoras, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
- Temas corporativos: Puede recolectarse la información en casos que tratan sobre acoso sexual, robo, apropiación de información confidencial o propietaria, de espionaje industrial.
- Mantenimiento de la ley: La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información.
- Seguridad lógica: virus, ataques de denegación de servicio, sustracción de datos, hacking, descubrimiento y revelación de secretos, suplantación de personalidades, sustracción de cuentas de correo electrónico.
- Otros.

b.5 REGLAS GENERALES DE LA INFORMÁTICA FORENSE[17]

Dado que el último producto del proceso forense está sujeto al análisis judicial, es importante que las reglas que lo gobiernan se sigan. Aunque estas reglas son generales para aplicar a cualquier proceso en la informática forense, su cumplimiento es fundamental para asegurar la admisibilidad de cualquier evidencia en un juzgado. La metodología que se emplee será determinada por el especialista forense, el proceso escogido debe aplicarse de forma que no se vulneren las reglas básicas de la informática forense.

Esencialmente, las reglas de la informática forense son 4 y se detallan a continuación:

1. Minimizar el Manejo de los datos originales

   La aplicación del proceso de la informática forense durante el examen de los datos originales se deberá reducir al mínimo posible. Esto puede considerarse como la regla más importante en la informática forense. Cualquier análisis debe dirigirse de manera tal que minimice la probabilidad de alteración cuando sea posible, esto se logra copiando el original y examinando luego los datos duplicados.

   La duplicación de evidencia tiene varias ventajas:

   - Asegurar que el original no será alterado en caso de un uso incorrecto o inapropiado del proceso que se aplique.
   - Permite al examinador aplicar diferentes técnicas en casos dónde el mejor resultado no está claro. Si, durante tales ensayos, los datos se alteran o se destruyen, simplemente se recurre a otra copia.
   - Permite a varios especialistas de informática forense trabajar en los mismos datos, o en partes de los datos, al mismo tiempo. Esto es especialmente importante si las habilidades de los especialistas (por ejemplo, criptoanálisis) se requiere en distintas

[17] Tomado del artículo: A las puertas de una Nueva Especialización: La Informática Forense. Ver apart*ado Referencia Bibliográfica II-Sitios Web* literal 5 para su referencia.

etapas de la tarea. Finalmente, asegura que el original se ha preservado en el mejor estado posible para la presentación en un juzgado.

Aunque hay ventajas al duplicar la evidencia, hay también desventajas.

- La duplicación de evidencia debe realizarse de forma tal y con herramientas, que aseguren que el duplicado es una copia perfecta del original. El fracaso para autenticar el duplicado apropiadamente, producirá un cuestionamiento sobre su integridad, lo que lleva inevitablemente a preguntar por la exactitud y fiabilidad del proceso del examen y los resultados logrados.
- Duplicando el original, se está agregando un paso adicional en el proceso forense. Se requieren más recursos y tiempo extra para facilitar el proceso de duplicación.
- La restauración de datos duplicados para recrear el ambiente original puede ser difícil. En algunos casos para ello serán necesarios dispositivos específicos de hardware o software, más la complejidad y tiempo del proceso forense.

2. Documentar los cambios.

Cuando ocurren cambios durante un examen forense, la naturaleza, magnitud y razón para ellos debe documentarse apropiadamente, puede ser necesario durante cualquier examen alterar el original o el duplicado. Esto se aplica para ambos tanto a nivel físico como lógico. En tales casos es esencial que el examinador entienda la naturaleza del cambio y que es el iniciador de ese cambio. Adicionalmente, el perito debe ser capaz de identificar correctamente la magnitud de cualquier cambio y dar una explicación detallada de por qué era necesario el mismo.

Esto se aplica a cualquier material de evidencia que se obtiene de un proceso forense en el que ha ocurrido un cambio.

Esto no quiere decir que el cambio no ocurrirá sino, que en situaciones dónde es inevitable, el examinador tiene la responsabilidad de identificar correctamente y documentar el cambio, ya que este proceso depende directamente de las habilidades y conocimiento del investigador forense.

Durante el examen forense este punto puede parecer insignificante, pero se vuelve un problema crítico cuando el examinador está presentando sus resultados en un juicio. Aunque la evidencia puede ser legítima, las preguntas acerca de las habilidades del examinador y conocimiento pueden afectar su credibilidad, así como la confiabilidad del proceso empleado. Con una duda razonable, los resultados del proceso forense, en el peor de los casos, se considerarán inadmisibles. Aunque la necesidad de alterar los datos ocurre pocas veces, hay casos dónde al examinador se le exige el cambio para facilitar el proceso del examen forense. Por ejemplo cuando el acceso a los datos se encuentra restringido por alguna forma de control de acceso, el examinador forense se puede ver obligado a cambiar el bit de acceso o una cadena binaria de datos completa (clave de acceso), por ello el perito debe dar testimonio que tales cambios no alteraron significativamente los datos a los que se accedió por medio de esta metodología y que luego son presentados como evidencia.

3. Cumplir con las Reglas de Evidencia

Para la aplicación o el desarrollo de herramientas y técnicas forenses se deben tener en cuenta las reglas pertinentes de evidencia. Uno de los mandatos fundamentales de

informática forense es la necesidad de asegurar que el uso de herramientas y técnicas no disminuye la admisibilidad del producto final. Por consiguiente es importante asegurar que la manera como son aplicadas las herramientas y técnicas, cumpla con las reglas de evidencia. Esencialmente, debe presentarse la información de una manera que sea tan representativa del original como sea posible. Es decir, el método de presentación no debe alterar el significado de la evidencia.

4. No exceda su conocimiento

El especialista en informática forense no debe emprender un examen más allá de su nivel de conocimiento y habilidad. Es esencial que el perito sea consciente del límite de su conocimiento y habilidad. Llegado este punto, tiene varias opciones:

- Detener cualquier examen y buscar la ayuda de personal más experimentado.
- Realizar la investigación necesaria para mejorar su propio conocimiento, para que le permita continuar el examen.

Es indispensable que el examinador forense pueda describir los procesos empleados durante un examen correctamente y explicar la metodología seguida para ese proceso. El fracaso para explicar, competentemente y con precisión, la aplicación de un proceso o procesos puede producir cuestionamientos sobre el conocimiento y credibilidad del examinador. Otro peligro en continuar un examen más allá de las habilidades de uno, es aumentar el riesgo de daño, cambios de los cuales el examinador no es consciente o no entiende y por consiguiente puede ignorar. Esto probablemente será revelado cuando el examinador está dando la evidencia. Esencialmente, los análisis complejos deben ser emprendidos por personal calificado y experimentado que posea un apropiado nivel de entrenamiento.

b.6 RETOS DE LA INFORMÁTICA FORENSE

Los retos a los cuales se enfrenta la informática forense son:

- Las técnicas de la informática forense representan los pasos fundamentales en los planes de actuación ante incidentes, ya que son la única forma de estudiar las causas internas de los mismos, corregir y prevenir su repetición.
- Debido al crecimiento imparable de la digitalización de la información en todos los niveles de la sociedad, y a la necesidad de reconstruir determinados hechos en función de evidencias digitales. Se quiere que en pocos años esta área pase a ser utilizada como parte de los planes de actuación ante incidentes de seguridad, al tiempo que se convierta en un procedimiento indispensable para numerosos procesos judiciales.
- Llegar al proceso de identificación, preservación, análisis y presentación de evidencias digitales por medio de las técnicas necesarias para poder adquirir los resultados esperados.

b.7 DIFERENCIA DE LA INFORMÁTICA FORENSE CON OTRAS ÁREAS DE INFORMÁTICA

La diferencia de la informática forense con cualquier otra área de la tecnología de información, es el requisito de que el resultado final debe derivarse de un proceso que sea legalmente aceptable. Por consiguiente, la aplicación de la tecnología en la investigación de los hechos que poseen estas características específicas debe llevarse a cabo con todos los requisitos que exige la ley. El no hacerlo puede producir que la evidencia digital sea considerada inadmisible o dudosa (contaminada).

b.8 ASOCIACIONES CERTIFICADORAS

La Asociación Internacional de Especialistas en Investigaciones Computacionales IACIS, por sus siglas en ingles[18] y la Red Del Crimen De la Alta Tecnología HTCN[19], son dos asociaciones internacionales que han desarrollado programas de certificación forenses en informática, que permiten de tallar las habilidades requeridas y las capacidades deseables en los investigadores informáticos.

A continuación se presenta ejemplos de las certificaciones expedidas por cada una de las asociaciones antes mencionadas y una breve explicación de éstas:

b.8.1 CREDENCIALES CERTIFICADORAS PARA INVESTIGACIÓN FORENSE EN INFORMÁTICA DE IACIS

La IACIS ofrece la certificación internacional denominada Certificación Externa de Computación Forense CFEC[20] , la cual se encuentra diseñada para personas que pertenecen al área informática y tiene pocos conocimientos del ámbito legal o del policial.

b.8.2 CREDENCIALES CERTIFICADORAS PARA INVESTIGACIÓN FORENSE EN INFORMÁTICA DE HTCN

La HTCN ofrece diversas certificaciones en la línea forense en informática. En particular se menciona la certificación de Investigador Certificado en Delito Informático CCCI[21] nivel básico y avanzado. El propósito de la certificación es desarrollar un alto nivel de profesionalismo y entrenamiento continuo que soporte investigaciones de crímenes de alta tecnología en la industria y las organizaciones.

Esta certificación es avalada y reconocida en diferentes tribunales y cortes del mundo, dada la seriedad y rigurosidad de proceso de certificación.

[18] Por sus siglas en ingles: International Association of Computer Investigative Specialist
[19] Por sus siglas en ingles: High Technology Crime Network
[20] Por sus siglas en ingles: Computer Forensic External Certification
[21] Por sus siglas en ingles: Certified Computer Crime Investigator

c. EVIDENCIA DIGITAL

En este apartado se abordará el tema de la evidencia digital para una comprensión del mismo dentro de la investigación.

c.1 DEFINICIÓN DE EVIDENCIA DIGITAL

El término *evidencia* ha sido en un principio asociado al de física dando como resultado el concepto de evidencia física, lo cual parece ser contrastante con el término evidencia digital, por cuanto, todo aquello relacionado con el término "digital" se ha asimilado al término "virtual", es decir, que tiene existencia en el contexto de una simulación. Es importante aclarar que los datos o evidencia digital, siempre estarán almacenados 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.

c.2 CARACTERÍSTICAS DE LA EVIDENCIA DIGITAL

- La evidencia digital es un tipo de la evidencia física, es menos tangible que otro tipo de evidencias, pero a diferencia de todas las demás evidencias físicas, ésta 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 la evidencia original, lo cual permite realizar diversos tipos de análisis y pruebas sin correr el riesgo de alterar o dañar la evidencia original.
- En contraposición a lo que se piensa, 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.[22]
- La evidencia digital no puede ser destruida fácilmente, tal como piensan los usuarios de computadoras, que creen que con ejecutar un comando de borrado (delete), ya ha desaparecido un documento o archivo objeto del mismo de la máquina. El disco duro de un sistema informático, guarda los datos en sectores creados en el momento del formateo del mismo, lo cual equivale a cuadricular una hoja de papel para insertar números y hacer operaciones matemáticas. Es posible que al guardar un archivo se necesiten varios sectores del disco.
- Los sistemas operativos y hardware o parte física de la computadora, trabajan en conjunto en la ubicación de los archivos y programas para su visualización o ejecución, siendo los responsables específicos del acceso a los archivos, otros archivos denominados Meta Archivos con funciones de índice, contienen la información necesaria para abrir o visualizar rápidamente datos específicos en el disco duro. Lo que hace la ejecución del comando de borrado en la mayoría de los sistemas operativos es una eliminación de datos ubicado en el archivo índice del disco duro sin borrar real y físicamente el archivo en si, por lo que el archivo objeto de la instrucción de borrado queda en el disco duro sin que el usuario este consciente de ello.

[22] Ver apartado *Glosario de término* para una mayor comprensión

c.3 FUENTES DE LA EVIDENCIA DIGITAL[23]

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

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

1. **Sistemas de computación abiertos**, son aquellos que están compuestos de las llamadas computadoras personales y todos sus periféricos como teclados, mouse y monitores, las computadoras portátiles, y los servidores. Actualmente estas computadoras tiene la capacidad de guardar grandes cantidades de información dentro de sus discos duros.
2. **Sistemas de comunicación**, estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet.
3. **Sistemas convergentes de computación**, son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

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

c.4 LIMITACIONES DE EVIDENCIA DIGITAL[24]

Se pueden considerar lo siguiente como limitantes de la evidencia digital:

- El factor humano
- Procedimientos de recolección y análisis de evidencia
- La tecnología

A continuación se detalla la descripción de cada una de estas limitantes.

- El factor humano

  El factor humano como en todos los campos de la ciencia y la tecnología es un factor determinante para la generación de conocimiento y avance. Sin embargo, se requiere una formación básica que oriente las actividades y acciones de los profesionales que se dedican a una parte específica de la ciencia, con el fin de disminuir la incertidumbre de sus resultados y mejorar la efectividad de sus procesos. Es así que las investigaciones forenses en informática no son la excepción. Es un campo de la ciencia que requiere una formación técnica avanzada y detallada en las tecnologías y aplicaciones de software que le permita explorar con profundidad los elementos aportados y poder relacionarlos para fundar hipótesis coherentes y sustentadas en la evidencia digital presentada.

[23] Según el libro: Introducción a la informática Forense, Ver apartado *Referencias Bibliográficas I-Libros* literal 8 para ver su referencia.
[24] Ver apartado *Referencias Bibliográficas IV-Revista Electrónica* literal 1 para ver su referencia.

Es claro, que la formación y la práctica constante de estos profesionales es fundamental para el buen curso de las investigaciones donde se hallen involucrados. Sin embargo, la susceptibilidad de la falla siempre estará presente no sólo por el uso de herramientas tecnológicas involucradas, sino por posibles fallas en los procedimientos aplicados, los cuales son sensibles a la hora de aportar evidencia digital a procesos judiciales.

- Los procedimientos de recolección y análisis de evidencia

  Los procedimientos de recolección y análisis de evidencia digital generalmente se encuentran sustentados en herramientas de software, procedimientos internacionalmente aceptados y experiencia del investigador. Mientras mayor sea la capacidad de las herramientas para identificar, recolectar, asegurar y analizar la evidencia en medios electrónicos, mejores resultados y controles se pueden mantener, dado que la intervención humana en el proceso ha sido mínima. Sin embargo, no podemos perder de vista que el software no es infalible y requiere un proceso de depuración y pruebas que exige una revisión por parte de la comunidad científica, identificación y valoración de sus errores, resultados de uso en casos anteriores, entre otras, que permitan aumentar la confiabilidad y la respetabilidad de los resultados.

- Limitaciones tecnológicas

  Finalmente la tecnología en sí misma, como resultado de una reconstrucción de la realidad humana para mejorar y aumentar la capacidad de acción de los procesos, está fundada en aproximaciones y precisiones previamente establecidas. Por tanto, si es correcto que la tecnología es una realidad cambiante de las necesidades de la humanidad, podemos esperar mejores técnicas y afinamientos que permitan disminuir la variación de probabilidad de error, aumentando las expectativas de control e integridad de medios necesarios para fortalecer los elementos probatorios.

c.5 CRITERIOS DE RECOLECCIÓN Y MANEJO DE EVIDENCIA DIGITAL

La Evidencia Digital puede ser procesada conforme a los criterios de colección y manejo de evidencia que se aplican generalmente en Criminalística, por lo que el proceso se puede resumir en varias fases:

1) Reconocimiento.
2) Captura y preservación.
3) Clasificación e individualización.
4) Reconstrucción.

A continuación se detallan cada una de estas fases:

1) Reconocimiento

El reconocimiento de la evidencia digital incluye la fase de individualización del Hardware o equipos informáticos (cuando se pueda tener acceso físico a ellos), así como la descripción de sistemas operativos y aplicaciones instaladas en los mismos. La ubicación de los datos relevantes al caso es importante en esta fase, los cuales pueden ser de distinta naturaleza, dependiendo del programa que haya sido utilizado para realizar el hecho jurídico informático.

2) La captura y preservación de la evidencia digital

La captura y preservación de la evidencia digital en los casos penales, debe procurarse en su estado original. Para lograr efectivamente la preservación correcta de los datos, los expertos deben realizar copias exactas y fieles, a través del procedimiento conocido como copia bit a bit, el cual garantiza que los datos de un medio de almacenamiento, sean copiados de manera exacta desde su fuente de origen.

Los sistemas operativos instalados en las computadoras utilizan en su mayoría los denominados archivos temporales, denominados también Memoria Virtual, que contienen trazas de las operaciones realizadas en los mismos, así como otro tipo de datos, imágenes y archivos susceptibles de ser recuperados, aún cuando se haya intentado borrarlos, por lo que el perito debe realizar las operaciones de copia con técnicas o herramientas especiales destinadas a tal efecto.

3) Clasificación e individualización

La clasificación de la evidencia digital, es el proceso a través del cual el perito ubica las características generales de archivos y datos, que son útiles a su vez para realizar comparaciones entre archivos similares o bien para individualizar la evidencia, por lo que de esta forma se establecerán los tipos de archivos.

La individualización juega un papel determinante en la experticia informática, la cual se logra a través de la ubicación y análisis de los metadatos, información que se encuentra inmersa de forma oculta dentro de los archivos, siendo los metadatos típicos los relacionados con el título, tema, autor y tamaño de los archivos, incluyéndose también en esta categoría las fechas de creación, modificación e impresión de un documento electrónico. Los metadatos son incorporados a los documentos automáticamente sin que el usuario tenga que realizar ninguna operación destinada a él. Algunos programas toman datos del Hardware o de los equipos donde se encuentran instalados, lo cual en casos determinados puede constituir prueba inequívoca de que un archivo ha sido realizado en una computadora determinada.

4) Reconstrucción

La reconstrucción de los hechos informáticos incluye conceptualmente el establecimiento de la secuencia de producción de actividades en una computadora o en redes. La recuperación de evidencia digital dañada entra también en esta categoría.

Es importante que en la pericia informática registre cada operación durante su práctica a efectos de hacer posible la evaluación de los protocolos de manejo de evidencia o bien a efectos de confirmarse los resultados en ampliaciones y aclaratorias del dictamen.

La reconstrucción relacional de los hechos informáticos es importante a efectos de establecer su relación con otro tipo de evidencia del mismo caso. El perito debe tratar de hacer una especie de línea del tiempo cuando la complejidad de los hechos que está evaluando así lo requiera.

c.6 CICLO DE VIDA PARA LA ADMINISTRACIÓN DE LA EVIDENCIA DIGITAL[25]

El ciclo de vida para la administración de la evidencia digital consta de seis pasos como se muestra en la ***Figura N°.3.***

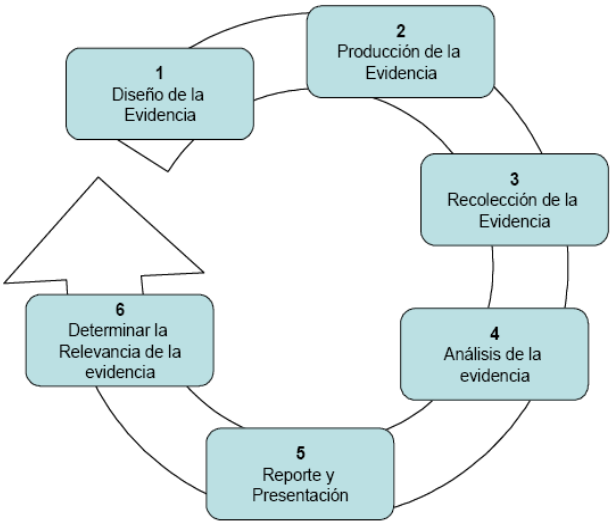


Figura N°.3 Ciclo de vida de la administración de la evidencia digital.

A continuación se detalla en qué consiste cada paso que involucra el ciclo de vida, su concepto y como se pone en práctica:

c.6.1 DISEÑO DE LA EVIDENCIA

Con el fin de fortalecer la admisibilidad y relevancia de la evidencia producida por las tecnologías de información, se detallan a continuación los criterios que se deben considerar para el diseño de la evidencia digital:

a) Asegúrese de que se ha determinado la relevancia de los registros electrónicos, que éstos se han identificado, están disponibles y son utilizables.
b) Los registros electrónicos tienen un autor claramente identificado, cuentan con una fecha y hora de creación o alteración.
c) Los registros electrónicos tienen elementos que permiten validar su autenticidad.
d) Se debe verificar la confiabilidad de la producción o generación de los registros electrónicos por parte del sistema de información.

Algunas prácticas asociadas a lograr lo establecido por esta primera fase son:

1. Clasificar la información de la organización, de tal forma que se pueda establecer cuál es la evidencia relevante y formal que se tiene.
2. La infraestructura tecnológica debe asegurar la sincronización de las computadoras o dispositivos que generen la información, de tal manera que se pueda identificar con claridad la fecha y hora de los registros electrónicos.

[25] Tomado del artículo: Buenas prácticas en la administración de la Evidencia digital, Ver *apartado Referencia Bibliográfica III-Documentos Electrónicos* literal 6 para su referencia.

c.6.2 PRODUCCIÓN DE LA EVIDENCIA

Esta fase requiere el cumplimiento de los siguientes objetivos:

a) Comprobar que el sistema o tecnología de información produzca los registros electrónicos.
b) Identificar el autor de los registros electrónicos almacenados.
c) Identificar la fecha y hora de creación.
d) Confirmar que la aplicación está operando correctamente en el momento de la generación de los registros, bien sea en su creación o modificación.
e) Verificar la completitud de los registros generados.

Las prácticas que se realizan son:

1. Desarrollar y documentar un plan de pruebas formal para validar la correcta generación de los registros de la aplicación.
2. Establecer un servidor de tiempo en el cual se pueda verificar la fecha y hora de creación de los archivos.
3. Contar con pruebas y auditorias frecuentes alrededor de la confiabilidad de los registros y su completitud, frente al diseño previo de los registros electrónicos.
4. Diseñar y mantener un control de integridad de los registros electrónicos, que permita identificar cambios que se hayan presentado en ellos.

c.6.3 RECOLECCIÓN DE LA EVIDENCIA

El objetivo de esta fase es localizar toda la evidencia digital y asegurar que todos los registros electrónicos originales (aquellos disponibles y asegurados en las máquinas o dispositivos) no han sido alterados.

Para ello el estándar establece algunos elementos a considerar como:

a) Establecer buenas prácticas para recolección de evidencia digital.
b) Preparar las evidencias para ser utilizadas en la actualidad y en tiempo futuro.
c) Respetar y validar las regulaciones y normativas alrededor de la recolección de la evidencia digital.
d) Desarrollar criterios para establecer la relevancia o no de la evidencia recolectada.

Las prácticas que se realizan son:

1. Establecer un criterio de recolección de evidencia digital según su volatibilidad; de la más volátil a la menos volátil.
    a. Registros de memoria cache.
    b. Tablas de enrutamiento, estadísticas del funcionamiento del sistema operacional.
    c. Archivos temporales.
    d. Almacenamiento en memorias USB, CD, DVD, etc.
    e. Registro remoto de las actividades de la aplicación y monitoreo del tráfico de los datos.
    f. Configuración física de dispositivos y topología de red.
    g. Manuales y registros disponibles de dispositivos y software bajo estudio.
2. Documentar todas las actividades que el profesional a cargo de la recolección ha efectuado durante el proceso de tal manera que se pueda auditar el proceso en sí mismo.

3. Asegurar el área donde ocurrió el siniestro, con el fin de custodiar el área o escena del delito.
4. Registrar en medio fotográfico o video la escena del posible ilícito, detallando los elementos informáticos allí involucrados.

Levantar un mapa o diagrama de conexiones de los elementos informáticos involucrados, los cuales deberán ser parte del reporte del levantamiento de información en la escena del posible ilícito.

c.6.4 ANÁLISIS DE LA EVIDENCIA

Una vez se ha recolectado la evidencia, tomado las imágenes de los datos requeridos, es tiempo para iniciar el análisis de los registros electrónicos para establecer los hechos de los eventos ocurridos en el contexto de la situación.

Las prácticas que se realizan son:

1. Efectuar copias autenticadas de los registros electrónicos originales sobre medios forenses estériles para adelantar el análisis de los datos disponibles.
2. Capacitar y formar en aspectos técnicos y legales a los profesionales que adelantarán las labores de análisis de datos.
3. Validar y verificar la confiabilidad y limitaciones de las herramientas de hardware y software utilizadas para el análisis de los datos.
4. Establecer el rango de tiempo de análisis y correlacionar los eventos en el context o de los registros electrónicos recolectados y validados previamente.

c.6.5 REPORTE Y PRESENTACIÓN

El profesional a cargo de la investigación es responsable de la precisión y completitud del reporte, sus hallazgos y resultados luego del análisis de la evidencia digital o registros electrónicos.

En este sentido toda la documentación debe ser completa, precisa, comprensiva y auditable.

a) Documentar los procedimientos efectuados por el profesional a cargo.
b) Mantener una bitácora de uso y aplicación de los procedimientos técnicos utilizados.

Las prácticas que se realizan son:

1. Incluir las irregularidades encontradas o cualquier acción que pudiese ser anormal durante el análisis de la evidencia.
2. Preparar una presentación del caso de manera pedagógica, que permita a las partes observar claramente el contexto del caso y las evidencias identificadas.
3. Detallar las conclusiones de los análisis realizados sustentados en los hechos identificados.
4. Evitar los juicios de valor o afirmaciones no verificables.
5. Contar con un formato de presentación de informe de análisis de evidencia digital que detalle entre otros aspectos los siguientes:
    a. Identificación de la agencia o empresa que adelantó el análisis.
    b. Identificador del caso.
    c. Investigador o profesional que ha adelantado el caso.
    d. Identificación de las entidades que han provisto las evidencias.

e. Fechas de recepción y reporte.
f. Lista detallada de elementos recibidos para análisis donde se detallen aspectos como serial, marca y modelo.
g. Breve descripción de los pasos metodológicos seguidos.
h. Resultados de los análisis donde se detallen con claridad los hallazgos
i. Conclusiones.

d. PRUEBAS PERICIALES[26]

La prueba pericial es la que surge del dictamen de los peritos, que son personas llamadas a informar ante el juez, debido a sus conocimientos especiales y siempre que sea necesario tal dictamen científico, técnico o práctico sobre hechos litigiosos[27].

d.1 DEFINICIÓN DE PERITO INFORMÁTICO

A continuación se presenta las definiciones[28] de perito informático:

- Es la persona que tiene conocimientos en informática, cuyos servicios son utilizados por el juez para que lo ilustre en el esclarecimiento de un hecho que requiere los conocimientos especiales, científicos y técnicos relacionados a la informática.
- Es el que posee conocimientos teóricos y prácticos en informática, informa bajo juramento al juez sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia en el campo de la informática.

Durante el desarrollo del presente estudio se utilizará el concepto de perito informático definido por el grupo de trabajo en el ***Capitulo 1*** apartado ***E:Marco Teórico II: Marco Conceptual.*** El cual fue formado tomando en cuenta los conceptos anteriormente expuestos y consolidándolo en uno solo.

d.2 DEFINICIÓN DE PERITAJE[29]

Es el examen y estudio que realiza el perito informático sobre el problema encomendado para luego entregar su informe o dictamen pericial a las autoridades que lo solicitan.

Este será la definición que se manejará y entenderá por peritaje a lo largo del presente estudio.

---

[26] El concepto de prueba pericial, es tomado del trabajo investigativo: *La Prueba Pericial*, realizado por el abogado Lic. Luís Alfredo Alarcón Flores. Ver apartado *Referencia bibliográfica II: Sitios Web* literal 4 para su referencia.

[27] Ver apartado *Glosario de término* para una mayor comprensión.

[28] Estas definiciones son retomadas de los documentos consultados durante la elaboración de la investigación.

[29] El concepto de peritaje, es tomado del trabajo investigativo: *La Prueba Pericial*, realizado por el abogado Lic. Luís Alfredo Alarcón Flores. Ver apartado *Referencia bibliográfica II: Sitios Web* literal 4 para su referencia.

d.3 OBJETO DE LA PRUEBA PERICIAL

El objeto de la pericia es el estudio, examen y aplicación de un hecho, un comportamiento, una circunstancia o fenómeno. Además de la prueba pericial establecer la causa de los hechos y los efectos del mismo, la forma y circunstancia como se cometió el hecho delictivo.

d.4 ELABORACIÓN DEL DICTAMEN PERICIAL

Existen tres fases bien diferenciadas en la elaboración del dictamen pericial: fase de adquisición de las pruebas, fase de investigación y elaboración del informe pericial. Cada una de estas fases requiere un especial cuidado, ya que el más mínimo defecto puede dar lugar a la desestimación del informe del experto.

d.4.1 FASE DE ADQUISICIÓN DE LAS PRUEBAS

La fase de adquisición de las pruebas consiste, tal y como su nombre indica, en la adquisición por parte del perito de todos los elementos que van a intervenir en la investigación. Es importante que el proceso de intervención de las computadoras, se lleve a cabo con todas las garantías para las partes involucradas en el litigio.

d.4.2 FASE DE INVESTIGACIÓN

Durante la fase de investigación, los elementos que deben regir el desarrollo del trabajo del perito son la no alteración de la prueba y el principio de imparcialidad. La mejor manera que tiene un perito para garantizar la no alteración de una prueba es la elaboración de una imagen de todos los dispositivos de almacenamiento, es decir una copia exacta. El perito informático dispone de una ventaja de la que lamentablemente carecen los peritos del resto de disciplinas: la posibilidad de crear un número ilimitado de clones de la prueba principal, eliminando de este modo las posibilidades de contaminación involuntaria de la evidencia y reduciendo al mínimo las posibles fallas en las unidades analizadas.

d.4.3 FASE DE ELABORACIÓN DEL DICTAMEN PERICIAL

En la fase de la elaboración del dictamen pericial, si se cumple con todos estos preceptos anteriormente expuestos, es muy difícil que durante la fase de exposición el testimonio del perito pueda ser rechazado.

Todo dictamen pericial debe contener:

a) La descripción de la persona, objeto o materia de examen o estudio, así como, el estado y forma en que se encontraba.
b) La relación detallada de todas las operaciones practicadas en la pericia y su resultado.
c) Los medios científicos o técnicos de los cuales se auxiliaron para emitir su dictamen.
d) Las conclusiones a las que llegan los peritos.

e. HERRAMIENTAS UTILIZADAS EN INFORMÁTICA FORENSE

En lo referente a las *herramientas para la informática forense*[30], existe una gran variedad y dependen del objetivo para la cual van a ser utilizadas. Existen para la recolección de evidencia, para el monitoreo o control de computadoras, para el marcado de documentos y de hardware (dispositivos físicos para la recolección de evidencia).

En los últimos años se ha aumentado el número de herramientas de informática forense, es posible encontrar desde las más sencillas y económicas cuyas prestaciones habitualmente son muy limitadas, hasta herramientas muy sofisticadas que incluyen tanto software como dispositivos de hardware.

Las siguientes características son una guía a seguir para la selección de una herramienta:

- 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 la evidencia en forma paralela en diferentes medios como discos duros, discos extraíbles, discos "Zip" CD's y otros.
- Capacidad de 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.
- 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.
- Soporte de múltiples sistemas de archivos tales como: 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.
- Recuperación de contraseñas: en muchas ocasiones la información recuperada puede estar protegida con contraseñas por lo que será necesario descifrarlos. Generalmente esta facilidad no viene incluida en estas herramientas, se deben comprar a parte.
- las herramientas debería incluir facilidades de gestión para el manejo mismo de los expedientes y reportes de las investigaciones.

A continuación en la ***tabla N° 2*** se presenta una breve descripción sobre las herramientas de investigación forense más conocidas y utilizadas.

[30] Ver tabla 2 Herramientas de la Información Forense

NOMBRE	DESCRIPCIÓN
F.I.R.E. *	Para realizar análisis, respuesta del incidente, la recuperación de los datos, la exploración de virus y vulnerabilidad del equipo. También proporciona las herramientas necesarias para el análisis forense inmediato.
Encase *	Herramienta para la prevención, detección e investigación de fraudes en entornos virtuales. Dispositivo útil a los peritos forenses en diferentes casos.
ByteBack - Tech Assist, Inc *	Copia de discos duros de cualquier formato, transferencia a otros medios internos o externos, sistema de análisis binario para recuperación no destructiva de particiones y sectores de arranque tipo FAT y NTFS (NT) búsqueda binaria, md5, hash[31] integrado, solución multi-ambiente, acceso directo, diagnóstico de superficie, control de bajo nivel de hardware.
Maresware - Mares and Company Computer Forensics *	consiste en un conjunto de programas para investigación de registros de computador, Incluye herramientas para respuesta a incidentes y ataques, descubrimiento de secretos y evidencia computacional, documentación de los procedimientos, preparación de reportes de hallazgos y de documentos para uso legal
Paraben Forensic Toll - Paraben Computer Forensic Software *	Herramienta de computación forense diseñada para PDAs y PC Pockets.
SafeBack - New Technologies Inc *	Permite hacer copias espejo de archivos de backups o de discos duros completos, para creación de evidencia en sistemas de cómputo basados en Intel, transferencia de información a otros medios y preservación de evidencia.
WinHex *	Software para informática forense y recuperación de archivos, Editor Hexadecimal de Archivos, Discos y RAM.
E E-ROL **	Es una aplicación on-line que permite a los usuarios recuperar los archivos que hayan sido borrados de unidades de disco duro, unidades ZIP y disquetes, en todos los sistemas operativos de la familia Microsoft Windows.
EasyRecovery **	Es para recuperar datos, reparar archivos y correo electrónico y realizar diagnósticos de discos.
Snort **	Sistema de prevención y detección de intrusos en la red, métodos basados anomalía de la inspección.
NMap **	Potente localizador de vulnerabilidades.
Nessus **	Escanear vulnerabilidades.
Ethereal **	Potente sniffer para el rastreo de los paquetes por la red.
Fport **	Identifica puertos abiertos y aplicaciones asociadas a ellos.

[31] Ver *Glosario de término* para una mayor comprensión.

NOMBRE	DESCRIPCIÓN
Putty **	Cliente que utiliza el protocolo de seguridad SSH.
AirSnort **	Herramienta Wireless para recuperar claves cifradas.
Aircrack **	sniffer y WEP craqueador de Wireless.
NetStumble **	Localizador de los puntos de acceso Wireless.
The Autopsy **	Browser para la informática forense.

** Herramientas que ofrecen garantía y la transparencia permitiendo su confiabilidad durante un proceso judicial.*

*** 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.*

Los productos mencionados en este cuadro es una muestra representativa de las distintas herramientas que se pueden encontrar en el mercado para apoyar a un informático forense.

Tabla N° 2: Herramientas de software como apoyo a la Información Forense

f. MARCO TEÓRICO DE LA METODOLOGÍA OCUPADA EN EL ESTUDIO

A continuación se hace una descripción de los conceptos utilizados para la elección y realización de la metodología que se llevará a cabo en la investigación.

f.1 INVESTIGACIÓN

En este apartado se dan a conocer las diferentes temáticas que se abordan a la hora de llevar a cabo la investigación y todo lo que se debe conocer para determinar que tipo de investigación se desea realizar.

f.1.1 DEFINICIÓN[32]

Conjunto de estudios o experimentos con el fin de realizar descubrimientos científicos o resolver un problema práctico determinado.

Se basa sobre el análisis crítico de proposiciones hipotéticas para el propósito de establecer relaciones causa-efecto, que deben ser probadas frente a la realidad objetiva.

Este propósito puede ser ya la formulación-teoría o la aplicación-teoría, conduciendo a la predicción y últimamente, al control de hechos que son consecuencia de acciones o de causas específicas.

f.1.2 CARACTERÍSTICAS

Una investigación se caracteriza por ser un proceso que:

- Proporciona la adquisición de conocimientos de fuentes primarias acerca de un aspecto de la realidad con el fin de actuar sobre ella y permitir enriquecer el conocimiento de una ciencia o una disciplina.
- Es una forma de plantear problemas y buscar soluciones mediante una indagación o búsqueda que tiene un interés teórico o una preocupación práctica.
- Sistemático: a partir de la formulación de una hipótesis u objetivo de trabajo, se recogen datos según un plan preestablecido que, una vez analizados e interpretados, modificarán o añadirán nuevos conocimientos a los ya existentes, iniciándose entonces un nuevo ciclo de investigación. La sistemática empleada en una investigación es la del método científico.
- Organizado: todos los miembros de un equipo de investigación deben conocer lo que deben hacer durante todo el estudio, aplicando las mismas definiciones y criterios a todos los participantes y actuando de forma idéntica ante cualquier duda. Para conseguirlo, es imprescindible escribir un protocolo de investigación donde se especifiquen todos los detalles relacionados con el estudio.
- Objetivo: las conclusiones obtenidas del estudio no se basan en impresiones subjetivas, sino en hechos que se han observado y medido, y que en su interpretación se evita cualquier prejuicio que los responsables del estudio pudieran tener.

[32] Ver apartado *Referencia Bibliográfica I:Libros* literal 9: Técnicas de Investigación Social.

- La investigación se registra y expresa en un informe, documento o estudio.

f.1.3 ACTIVIDADES

Las actividades de una investigación son:

1. Medir fenómenos.
2. Comparar los resultados obtenidos.
3. Interpretar los resultados en función de los conocimientos actuales, teniendo en cuenta las variables que pueden haber influido en el resultado.

f.1.4 LA INVESTIGACIÓN COMO UN PROCESO Y SUS ETAPAS

Según Ezequiel Ander– Egg[33], en su libro Técnicas de Investigación Social, la investigación es un proceso porque se crea un procedimiento para descubrir verdades parciales, y se compone de 9 etapas:

1. Formulación y definición del problema
2. Estructuración de un marco teórico
3. Formulación de hipótesis
4. Recopilación de datos
5. Sistematización y elaboración de datos
6. Prueba de hipótesis
7. Formulación de deducciones y proposiciones generales.
8. Análisis de los resultados
9. Propuestas derivadas del estudio

f.1.5 EL MÉTODO

El método se refiere a los procedimientos que se pueden seguir con el propósito de llegar a demostrar la hipótesis, cumplir con los objetivos o dar una respuesta concreta al problema que se identificó. El método que se espera seguir en la investigación, debe hacerse siempre referido al problema planteado.

f.1.6 LA TÉCNICA

Es el conjunto de instrumentos y medios a través del cual se efectúa el método y solo se aplica a una ciencia.

[33] Consultor de las Naciones Unidas en planificación nacional y local, de la UNICEF en política social, de la UNESCO para América Latina en el campo de la política cultural.

f.1.7 LA METODOLOGÍA

La metodología es el instrumento que enlaza el sujeto con el objeto de la investigación, Sin la metodología es casi imposible llegar a la lógica que conduce al conocimiento científico.

El estudio del método, también se le denomina metodología, y abarca los diversos procedimientos concretos que se emplean en las investigaciones y la discusión acerca de sus características, cualidades y debilidades. Se habla así de "metodología de la investigación" para hacer referencia a los pasos y procedimientos que se han seguido en una investigación determinada, para designar los modelos concretos de trabajo que se aplican en una determinada disciplina o especialidad.

f.1.8 MÉTODO DE INVESTIGACIÓN

Es el procedimiento riguroso, formulado de una manera lógica, que el investigador debe seguir en la adquisición del conocimiento.

Toda investigación parte de un conjunto de ideas y proposiciones que se basan sobre la realidad y sus descripciones y explicaciones; el científico, por más que esté persuadido de la verdad de estas proposiciones, no las podrá sostener hasta que, de algún modo, puedan ser verificadas en la práctica. Una proposición es verificable cuando es posible encontrar un conjunto de hechos, previamente delimitados, que sean capaces de determinar si es o no verdadera.

f.2 FUENTES DE INFORMACIÓN

Fuentes de Información se le denomina al término que se refiere a los orígenes de los cuales se puede extraer conocimiento necesario proporcionado por Personas, documentos o actividades de donde proceden los datos que sirven como base para la realización de cualquier tipo de investigación, estudio o análisis.

Las fuentes de información se pueden clasificar en base al *grado de información* proporcionado por éstas en fuentes: *primarias y secundarias.*

f.2.1 FUENTES PRIMARIAS

Las fuentes primarias son aquellas que proporcionan información nueva, original y final en sí misma. No remiten a ninguna otra fuente ni la complementan. La información que se ofrece empieza y acaba en el mismo documento.

Normalmente, se presentan en forma de monografías, publicaciones periódicas, personas expertas en las temáticas tratadas y en el colectivo denominado literatura gris (tesis, actas de congresos, documentos de trabajo, etc.).

f.2.2 FUENTES SECUNDARIAS

Las fuentes secundarias son textos basados en fuentes primarias que tienen por finalidad indicar qué documentos contienen o puede proporcionar información final. No contienen información acabada, sino que siempre remiten documentos primarios. Implican

generalización, análisis, síntesis, interpretación o evaluación. Una fuente secundaria es normalmente un comentario o análisis de una fuente primaria.

Se identifican como fuentes secundarias las obras de referencia o de consulta como las bibliografías, los catálogos y los buscadores.

f.3 DIAGRAMA CAUSA Y EFECTO.

Un diagrama de causa y efecto es la representación de varios elementos (causas) de un sistema que pueden contribuir a un problema (efecto). Es una herramienta efectiva para estudiar procesos, situaciones y para desarrollar un plan de recolección de datos.

f.3.1 CARACTERÍSTICAS PRINCIPALES

- Es una representación visual de todos los factores que pueden contribuir al efecto observado.
- La interrelación entre los posibles factores causales son claramente mostrados. Un factor causal puede aparecer en varios sitios del diagrama.
- Las interrelaciones son generalmente hipotéticas y cualitativas.

f.3.2 CUANDO SE UTILIZA

El Diagrama de causa y efecto es utilizado para identificar las posibles causas de un problema específico. La naturaleza gráfica del diagrama permite que los grupos organicen grandes cantidades de información sobre el problema y determinar exactamente las posibles causas. Finalmente, aumenta la probabilidad de identificar las causas principales.

El diagrama de Causa y Efecto se debe utilizar cuando se pueda contestar "si" a una o a las dos preguntas siguientes:

1 ¿Es necesario identificar las causas principales de un problema?

2 ¿Existen ideas y/u opiniones sobre las causas de un problema?

f.3.3 CÓMO SE UTILIZA

1. Identificar el problema. El problema (el efecto generalmente está en la forma de una característica de calidad) es algo que queremos mejorar o controlar.
2. Registrar la frase que resume el problema. Escribir el problema identificado en la parte extrema derecha del papel y dejar espacio para el resto del Diagrama hacia la izquierda. Dibujar una caja alrededor de la frase que identifica el problema (algo que se denomina algunas veces como la cabeza del pescado).
3. Dibujar y marcar las espinas principales. Las espinas principales representan el input principal/ categorías de recursos o factores causales. No existen reglas sobre qué categorías o causas se deben utilizar, pero las más comunes utilizadas por los equipos son las materiales, métodos, máquinas, personas, y/o el medio. Dibujar una caja alrededor de cada título. El título de un grupo para su Diagrama de Causa y Efecto puede ser diferente a los títulos tradicionales; esta flexibilidad es apropiada y se evita considerarla.

4. Realizar una lluvia de ideas de las causas del problema. Este es el paso más importante en la construcción de un Diagrama de Causa y Efecto. Las ideas generadas en este paso guiarán la selección de las causas de raíz. Es importante que solamente las causas, y no soluciones del problema sean identificadas. Para asegurar que su equipo está a nivel apropiado de profundidad, se deberá hacer continuamente la pregunta Por Qué para cada una de las causas iníciales mencionadas.
5. Identificar los candidatos para la "causa más probable". Las causas seleccionadas por el equipo son opiniones y deben ser verificadas con más datos. Todas las causas en el Diagrama no necesariamente están relacionadas de cerca con el problema; el equipo deberá reducir su análisis a las causas más probables. Encerrar en un círculo la causa (s) más probable seleccionada por el equipo o marcarla con un asterisco.

Cuando las ideas ya no puedan ser identificadas, se deberá analizar más a fondo el Diagrama para identificar métodos adicionales para la recolección de datos.

f.4 HIPÓTESIS

f.4.1 DEFINICIÓN

- Dentro de la investigación científica, son proposiciones tentativas acerca de las relaciones entre dos o más variables y se apoyan en conocimientos organizados y sistematizados.

Las primeras versiones de las hipótesis surgen desde el momento de enunciar el problema. Esto se debe a que al analizar los aspectos y relaciones del fenómeno formulamos algunos supuestos preliminares, mismos que se superan a medida que se completa y profundiza el planteamiento del problema.

f.4.2 ELEMENTOS DE LAS HIPÓTESIS[34]

Las hipótesis tienen tres elementos estructurales.

1. **Las unidades de análisis**, pueden ser los individuos, grupos, viviendas, instituciones, etc.
2. **Las variables**, es decir, las características o propiedades cualitativas o cuantitativas que presentan las unidades de análisis.
3. **Los elementos lógicos** que relacionan las unidades de análisis con las variables y a estas entre si.

En todo trabajo de investigación y para ser lógicos con la realidad, se debe formular hipótesis estadísticas siguientes:

- ***Hipótesis nula:*** Es aquella por la cual se indica que la información a obtener es contraria a la hipótesis general.

[34] Tomado del libro "Guía para la elaboración de trabajos de investigación, monografías y tesis" Ver apartado *Referencias Bibliográficas, I-Libros* literal 5 para su referencia.

- ***Hipótesis alterna:*** Predice generalmente la relación entre variables y se formula afirmativamente.

f.5 MUESTREO

Es el proceso por el cual se seleccionan de manera sistemática elementos representativos de una población.

f.5.1 OBJETIVOS EN EL MUESTREO DE LOS DATOS

1. Costo de la recopilación de datos

   Sería demasiado costoso examinar cada nota escrita o entrevistar a cada uno de los integrantes de una organización, ya que se incurre en el desperdicio del valioso tiempo de los empleados y la duplicidad de cuestionarios, todo ello, redundaría en gastos innecesarios.

2. Agilizar la recopilación de datos.

   El muestreo agiliza el proceso, por medio de la recopilación de datos seleccionados y no de todos los datos de la población.

3. Mejorar la eficacia de la recopilación de datos.

   Se mejora la calidad de la recopilación de los datos al brindar una información más precisa, esto se logra al entrevistar a solo algunos cuantos empleados, pero haciéndoles preguntas más precisas.

4. Reducción del sesgo en los datos.

   El muestreo en si reduce la parcialidad de los datos recopilados.

f.5.2 DISEÑO DEL MUESTREO

Considerando una población finita para obtener una distribución real de valores, es necesario, en general una muestra, una parte de la población, e inferir de su análisis cuyos resultados pertenezcan a la población total, por lo tanto esta muestra tiene que ser representativa.

Para tener la seguridad de que la muestra en estudio es representativa de la población que se ha obtenido y crear una estructura en la que podamos aplicar utilizaremos las muestras aleatorias que es en la que tomando un conjunto de observaciones x1, x2, x3, …… xn constituye una muestra aleatoria de tamaño n, para una población de tamaño N, si se escoge de tal forma que cada subconjunto de n elementos entre los N de la población tiene una misma probabilidad de ser escogidos.

Pasos a seguir para lograr un buen diseño del muestreo.

1. Determinar con precisión los datos que se van a recopilar o a describir.
2. Delimitar la población sujeta a selección de muestras.
3. Elegir el tipo de muestra.
4. Decidir el tamaño de la muestra.

Estos pasos se describen en detalle a continuación:

1. Determinar con precisión los datos que se van a recopilar o a describir

Se debe contar con un plan realista sobre lo que se hará con los datos, aun antes de llevar a cabo la recopilación, las responsabilidades del analista de sistemas son identificar las variables, atributos y los datos asociados a los artículos que serán recopilados en el muestreo.

2. Delimitar la población que se va a estudiar

Cuando se investigan datos concretos el analista de sistemas necesita decidir, entre otras cosas, si los últimos dos meses serán suficientes o si requerirá de un año completo para el análisis de la información. De igual forma cuando decida a quien entrevistar, el analista de sistemas tiene que definir si la población incluye un solo nivel de la organización, o si considera todos los niveles de esta.

3. Elección del tipo de muestra

El tipo de muestra seleccionada para la investigación es: *Muestras aleatorias complejas:* con frecuencia, puede satisfacer los objetivos del muestreo al elegir un muestreo aleatorio complejo. El enfoque más adecuado para la selección de la muestra es: muestreo estratificado.

La estratificación es el proceso mediante el cual se identifican subpoblaciones (estratos), para luego, mediante el muestreo, seleccionar a sujetos de estas subpoblaciones. La estratificación será esencial si el analista de sistemas requiere una recopilación de datos eficiente, también sirve para recopilar información de diversos subgrupos.

4. Decisión sobre el tamaño de la muestra

Es necesario recordar que en el muestreo es más importante un número absoluto que el porcentaje de la población. El tamaño de la muestra depende de varios elementos, pero el analista de sistemas lo establece con base en su conocimiento de la población en si y en otros aspectos importantes, puede elegir un intervalo estimado aceptable(esto es, el grado de precisión deseado) y el error estándar(al elegir el nivel de confianza)

4.1 Decisión sobre el tamaño de la muestra para datos de atributos

Para determinar el tamaño de la muestra se utiliza la ecuación de muestreo aleatorio simple para población finita:

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

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: universo

e: Error muestra máximo permitido.

Para un nivel de confianza del 97%, Z = 2.17 (puede localizarse en la ***tabla N° 3***.), ya que se desea que los resultados sean confiables por lo menos un 97%. En la población porque uno más alto elevaría los costos de la investigación.

Para la probabilidad de éxito y de rechazo, tiene igual probabilidad de ser aceptado o rechazado p = 0.5, q=0.5 por que q = 1-0.5 = 0.5. Considerando que no se han realizado estudios previos y que el tema en estudio es de importancia para nuestro país.

Se espera que los resultados se desvíen hasta un máximo de 3% de los datos originales o reales, por lo tanto e = 3% lo que implica que se tiene un 97% de confianza en los resultados de las encuestas.

Nivel de confianza (%)	Coeficiente de confiabilidad (valor z)
99	2.58
98	2.33
97	2.17
96	2.05
95	1.96
90	1.65
80	1.28
50	0.67

Tabla N° 3: Determinación del coeficiente de confiabilidad**,** estos datos son obtenidos de la tabla "Áreas bajo la curva normal tipificada del 0 a Z[35].

f.5.3 TIPOS DE INFORMACIÓN QUE SE OBTIENEN DURANTE LA INVESTIGACIÓN

Los tipos de datos que se obtienen durante la investigación son:

- Hechos y datos
- Información financiera
- Contexto de la organización
- Tipos de documentos y problemática.

f.5.4 TIPOS DE DATOS CONCRETOS

Conforme el analista de sistemas se va adentrando en la organización y en sus requerimientos de información, se torna importante examinar los diferentes tipos de datos que aportan

[35] Estos valores fueron tomados de la tabla "Áreas bajo la curva normal tipificada del 0 a Z". Ver apartado *Anexos Anexo # 4* para una mayor comprensión.

información, que de otra manera no podría obtenerse. Los datos concretos revelan la trayectoria de la organización y hacia donde se dirige según sus miembros. Con el fin de conformar una imagen precisa, el analista necesita examinar ambos tipos de datos concretos, los cualitativos y los cuantitativos.

f.5.5 ANÁLISIS DE LOS DOCUMENTOS CUANTITATIVOS

Dentro de estos documentos están los informes corporativos, los informes utilizados para la toma de decisiones, los informes de desempeño y formas diversas.

f.5.6 ELEMENTOS A CONSIDERAR

- **Parámetro:** Son las medidas o datos que se obtienen sobre la distribución de probabilidades de la población, tales como la media, la varianza, la proporción, etc.
- **Estadístico:** Los datos o medidas que se obtienen sobre una muestra y por lo tanto una estimación de los parámetros.
- **Error Muestral:** de estimación o standard. Es la diferencia entre un estadístico y su parámetro correspondiente. Es una medida de la variabilidad de las estimaciones de muestras repetidas en torno al valor de la población, nos da una noción clara de hasta dónde y con qué probabilidad una estimación basada en una muestra se aleja del valor que se hubiera obtenido por medio de un censo completo. Siempre se comete un error, pero la naturaleza de la investigación nos indicará hasta qué medida podemos cometerlo (los resultados se someten a error muestral e intervalos de confianza que varían muestra a muestra). Varía según se calcule al principio o al final. Un estadístico será más preciso en cuanto y tanto su error es más pequeño. Podríamos decir que es la desviación de la distribución muestral de un estadístico y su fiabilidad.
- **Nivel de Confianza**: Probabilidad de que la estimación efectuada se ajuste a la realidad. Cualquier información que queremos recoger está distribuida según una ley de probabilidad (Gauss o Student), así llamamos nivel de confianza a la probabilidad de que el intervalo construido en torno a un estadístico capte el verdadero valor del parámetro.
- **Varianza Poblacional:** Cuando una población es más homogénea la varianza es menor y el número de entrevistas necesarias para construir un modelo reducido del universo, o de la población, será más pequeño. Generalmente es un valor desconocido y hay que estimarlo a partir de datos de estudios previos.

f.6 INSTRUMENTOS PARA LA RECOLECCIÓN DE DATOS

Un instrumento de medición adecuado es aquel que registra datos observables que representan verdaderamente a los conceptos o variables que el investigador tiene en mente.

En investigaciones de campo, tanto cuantitativas como cualitativas, el investigador requiere utilizar instrumentos apropiados para que la información que obtenga sea válida.

Por tal motivo necesita, entonces, contar con instrumentos que, en primer lugar, sean confiables, es decir que al replicarlos en condiciones similares arrojen aproximadamente los mismos resultados. En

segundo lugar, deben ser válidos, esto es, que efectivamente midan lo que el investigador pretende medir.

Adicionalmente un instrumento de medición debe cumplir las propiedades de conceptualización y de representatividad. La conceptualización involucra una serie de procesos, por medio de los cuales las ideas y los conceptos se clasifican y se diferencian, de forma tal que se produzcan definiciones que permitan lograr acuerdos acerca de las teorías que se tratan de expresar. Al menos se trata de lograr que otros entiendan, aunque no compartan lo que tratamos de decir. Por lo tanto la conceptualización se refiere al proceso por medio del cual nos movemos de la idea a la estructura de las operaciones en la investigación, mientras que la medición se refiere al proceso que nos lleva de la operación física al lenguaje matemático.

El concepto de representatividad, o generalidad, tiene que ver con el grado en que los resultados, a partir de la muestra, pueden ser atribuidos a la población en general. La representatividad es importante cuando se quiere estimar parámetros o proyectar la población, pero no tanto cuando se quiere, simplemente, analizar relaciones.

f.6.1 CONFIABILIDAD

La confiabilidad de un instrumento de medición hace referencia al grado en que la aplicación repetida del instrumento, a un mismo objeto o sujeto, produzca iguales resultados. Cuanto más confiable sea un instrumento, más similares serán los resultados obtenidos en varias aplicaciones de éste.

f.6.2 ESTIMACIÓN DE LA CONFIABLIDAD

Existen varios métodos para estimar la confiabilidad de una prueba, los cuales difieren en la forma como consideran las fuentes de error. Los más usuales son: Medidas de Estabilidad, Medidas de Equivalencia y Medidas de Consistencia Interna.

- **Medidas de estabilidad**. También conocidas con el nombre de test-retest de confiabilidad. Esta medida se obtiene aplicando una prueba a un grupo de individuos en dos momentos diferentes y correlacionando las dos series de puntos alcanzadas. Cuando se utiliza la medida de estabilidad, ésta debe ir acompañada de la especificación del tiempo transcurrido entre las dos situaciones de prueba, así como de una descripción de las experiencias pertinentes que intervinieron.
- **Medidas de equivalencia**. Para obtener una medida de equivalencia, se aplican dos formas (con contenido, medias y varianzas iguales) de una prueba en el mismo día al mismo grupo de individuos y se correlacionan los resultados obtenidos. Con este procedimiento se evita el efecto intertemporal en los resultados, así como el de aprendizaje por parte de los participantes. En algunos casos se puede obtener un coeficiente de equivalencia y de estabilidad aplicando primero una forma de la prueba y posteriormente la otra.
- **Medidas de consistencia interna**. La principal ventaja de las medidas de consistencia interna es que solamente requieren de un conjunto de datos. Las tres medidas más comunes de consistencia interna son: separación en dos mitades, las estimaciones de Kuder-Richardson y la técnica de Hoyt. Las dos últimas permiten construir índices de homogeneidad de los ítems presentados en la prueba.

f.6.3 FACTORES QUE PUEDEN INFLUIR EN LA CONFIABILIDAD

Los principales factores que influyen en la evaluación de la confiabilidad de una prueba son: Longitud de la prueba. La confiabilidad de una prueba aumenta en la medida en que se incluyan ítems equivalentes; sin embargo, no debe caerse en el error de adicionar ítems innecesariamente.

1. Velocidad. Debe darse el tiempo suficiente para contestarse la prueba. De esta manera se obtienen resultados más confiables.
2. Homogeneidad del grupo. Cuanto más homogéneo sea el grupo, mayor será la confiabilidad de la prueba.
3. Dificultad de los ítems. Existen pruebas en las cuales hay gran cantidad de ítems fáciles que nadie alcanza a responder en su totalidad en el tiempo establecido; en otras, se presentan pocos ítems de gran dificultad que tampoco pueden ser contestados completamente. Ambas situaciones afectan la con-fiabilidad de la prueba.
4. Objetividad. En ítems de respuesta abierta, en ensayos y en otras pruebas de este tipo, la objetividad que posea el juez para la asignación de la calificación en los ítems afecta significativamente la confiabilidad de la prueba realizada.

f.7 MATRIZ DE CONGRUENCIA

En el ámbito académico es común trabajar con proyectos de investigación que incluyen el diseño de la estrategia metodológica para alcanzar el conocimiento que solucione el problema que originó el estudio. El proyecto abarca desde la estructura teórica del proceso de investigación, hasta el diseño de la estructura real de las etapas que se van a seguir en el estudio. En este entorno es donde se inserta la aparición de la matriz de congruencia.

La matriz de congruencia es una herramienta que brinda la oportunidad de abreviar el tiempo dedicado a la investigación, su utilidad permite organizar las etapas del proceso de la investigación de manera que desde el principio exista una congruencia entre cada una de las partes involucradas en dicho procedimiento.

Su presentación en forma de matriz permite apreciar a simple vista el resumen de la investigación y comprobar si existe una secuencia lógica, lo que elimina de golpe las ambigüedades que pudieran existir durante los análisis correspondientes para avanzar en el estudio.

II. MARCO CONCEPTUAL

a. DEFINICIÓN DE DELITO INFORMÁTICO

El delito informático implica cualquier actividad ilegal que se pueden enmarcar dentro de las figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad.

b. DEFINICIÓN DE INFORMÁTICA FORENSE

La informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. Mediante la selección de criterios que se usan para guiar y asegurar actividades concernientes con el análisis de evidencia digital, él cual provee recomendaciones y cubre aspectos legales, policiales y operacionales como requerimientos técnicos para adquisición, análisis y reporte de evidencia, colaboración con otros grupos de investigación, gestión de casos, soporte a la fuerza de la ley, desarrollo de políticas de seguridad para respuesta a incidentes y plan preventivo y de continuidad.

c. DEFINICIÓN DE RESOLUCIÓN FAVORABLE

Se entenderá por resolución favorable cuando la evidencia digital ha sido aceptada en un juicio como una prueba tanto para acusar como para defender.

d. DEFINICIÓN DE PERITO INFORMÁTICO

Es la persona que tiene conocimientos en informática, cuyos servicios son utilizados por el juez para que lo ilustre en el esclarecimiento de un hecho que requiere los conocimientos especiales, científicos y técnicos relacionados a la informática y hace un análisis exhaustivo de los equipos informáticos, y sobre todo de las unidades de almacenamiento de datos en busca de todos aquellos elementos que puedan constituir prueba o indicio en el caso en cuestión de cómo se cometió un delito informático.

III. MARCO LEGAL

ARTÍCULOS DEL CÓDIGO PROCESAL PENAL DE EL SALVADOR RELACIONADOS CON PERITOS

Garantías de prueba pericial según el "Código Procesal Penal de El Salvador, Sección del Capítulo VI Peritos"

A continuación se presentan los artículos relacionados con peritos y su participación dentro de los procesos legales en El Salvador, además se expone la interpretación de cada uno de estos[36].

- **Calidad Habilitante**

  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.

  Interpretación: es el permiso que se les da a ciertas personas que tienen una habilidad o profesión en ciertas áreas, ciencia o arte, posee especiales conocimientos teóricos o prácticos para que nos de certeza de un acto, debe de presentar la preparación como un titulo. Puede ser salvadoreño o extranjero.

- **Nombramiento y Notificación**

  Art. 200.- El juez o tribunal designará un perito, salvo que estime necesario nombrar otros. La realización de la pericia será notificada a las partes con la indicación de los puntos de pericia y del nombre del perito.

- **Facultad de Proponer**

  Art. 201.- En el término de tres días a partir de la notificación, las partes podrán proponer a su costa otro perito, sin perjuicio de la participación de los consultores técnicos.

  También podrán proponer puntos de pericia distintos u objetar los propuestos por el juez o tribunal. Este resolverá de inmediato, sin recurso alguno.

  Interpretación de los artículos 200 y 201: el juez puede de oficio proponer un perito para la realización de dicho peritaje pero no se excluye a las partes proponer también ellos, el perito que estimen conveniente siempre que se cumpla el término de tres días después de la notificación. En ambos casos se debe indicar los puntos de la pericia y el nombre del perito.

- **Dirección del Peritaje**

  Art. 202.- El juez o tribunal formulará las cuestiones objeto del peritaje, fijará el plazo en que ha de realizarse el peritaje y pondrá a disposición de los peritos las actuaciones y elementos necesarios para cumplir el acto.

  Interpretación: el juez es el que llevará el control del peritaje dará la dirección donde especificará el objeto del peritaje, el tiempo en que se realizará y pondrá a disposición de este lo necesario para llevar a cabo el acto.

[36] La interpretación fue realizada por la Licenciada en Ciencias Jurídicas Johanna Álvarez. Ver apartado *Referencias Bibliográficas, VI-Referencia de fuentes personales*, para su referencia.

- **Conservación de Objetos**

Art. 203.- Tanto el juez o tribunal como los peritos procurarán que los objetos a examinar sean en lo posible conservados, de modo que el peritaje pueda repetirse. Si es necesario destruir o alterar los objetos o sustancias a analizarse o existe discrepancia sobre el modo de realizar las operaciones, los peritos informarán al juez antes de proceder.

Interpretación: las partes que intervinieren en el proceso procuraran conservar el objeto que será analizado y cualquier duda al respecto deben informar al juez.

- **Ejecución**

Art. 204.- Siempre que sea posible y conveniente, los peritos practicarán conjuntamente el examen y deliberarán en sesión conjunta a la que podrán asistir los consultores técnicos, las partes y quien designe el juez o tribunal.

Interpretación: dice las personas que pueden concurrir al examen para que puedan interactuar respecto a dicho objeto de pericia.

- **Dictamen**

Art. 206.- El dictamen pericial se expedirá por escrito o se hará constar en acta, y contendrá en cuanto sea posible:

1) La descripción de la persona, objeto, sustancia o hecho examinado, tal como han sido observados.
2) Una relación detallada de las operaciones, de su resultado y la fecha en que se practicaron.
3) Las observaciones de los consultores técnicos.
4) Las conclusiones que formulen los peritos.

Interpretación: da un parámetro de lo que contiene el acta levantada por un perito y son requisitos necesarios para la validación de la misma.

- **Cotejo de Documentos**

Art. 207.- Cuando se trate de examinar o cotejar escritos, el juez o tribunal ordenará la presentación de escritura de comparación, pudiendo usarse documentos públicos, auténticos o privados, si no existen dudas sobre su autenticidad. Para la obtención de ellos podrá disponer el juez o el tribunal el secuestro, salvo que se trate de documentos excluidos. También dispondrá que alguna persona escriba de su puño y letra un cuerpo de escritura, siempre con su consentimiento.

Interpretación: este artículo se trata de cotejo de documentos donde este perito especializado deberá ver la autenticidad de documentos públicos, son los dictados por un juez; Auténticos son los elaborados por notarios; privados son los realizados por personas sin presencia de alguna autoridad.

- **Reserva**

  Art. 208.- El perito guardará reserva de todo cuanto conozca con motivo de su actuación.

  El juez o tribunal sustituirá a los peritos en caso de mal desempeño de sus funciones.

  Interpretación: la reserva es la confidencialidad del caso pues es la profesión la que obliga a la no divulgación.

- **Honorarios**

  Art. 209.- Los peritos nombrados de oficio tendrán derecho a cobrar los honorarios que fije el juez o tribunal, de acuerdo a la ley, salvo cuando reciban un sueldo como peritos permanentes.

  Interpretación: Honorarios es lo que se le tendrá que pagar por la investigación realizada y el acta que se levanto.

CAPITULO 2

DISEÑO DE LA INVESTIGACIÓN

CAPITULO 2: DISEÑO DE LA INVESTIGACIÓN

A- METODOLOGÍA

En este apartado se establece como se llevara a cabo la metodología del estudio. Para el desarrollo del proyecto se hizo uso del proceso de investigación que se presenta en la ***figura N° 4***.

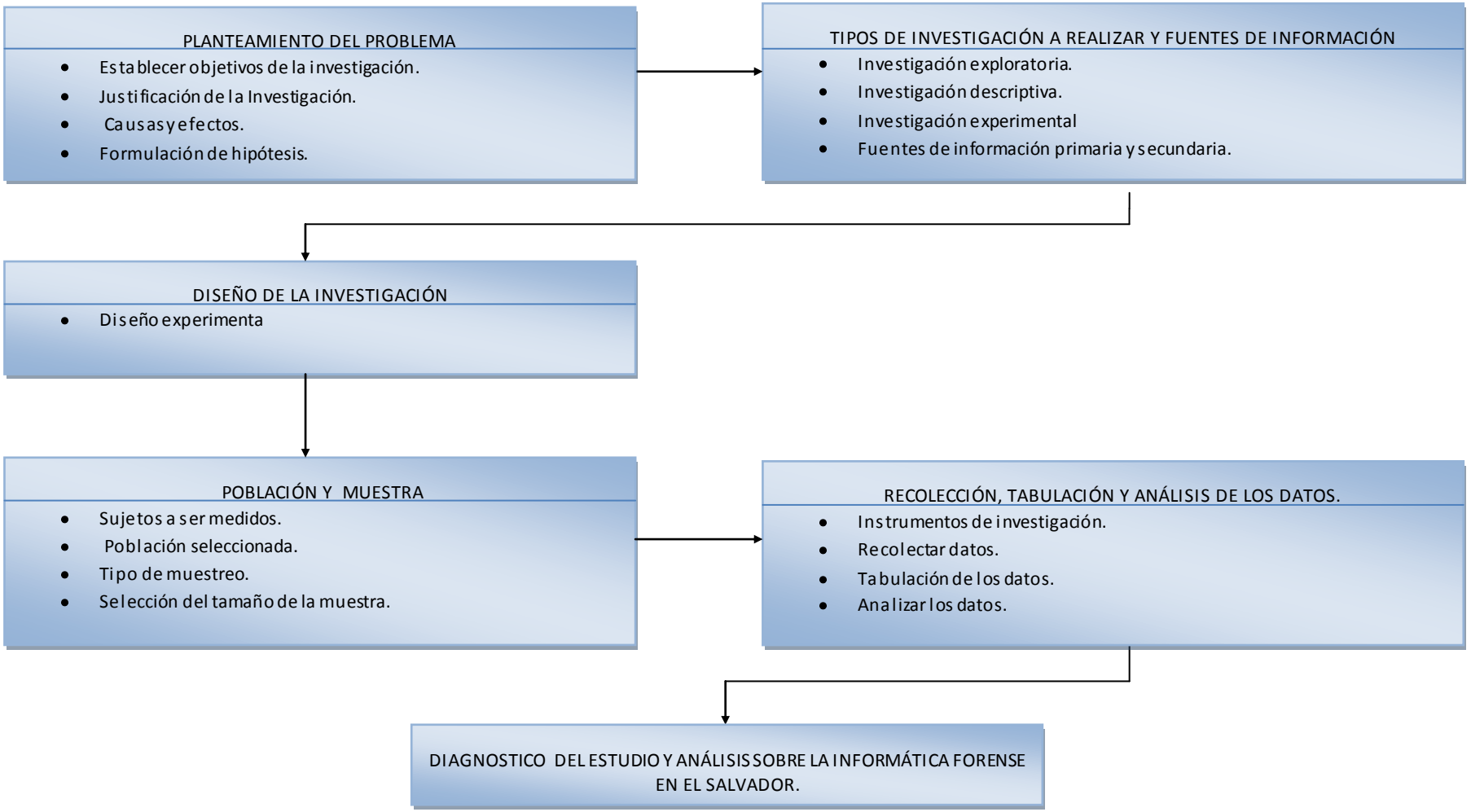


Figura N°. 4 Diagrama de la metodología utilizada para la realización del estudio

I. PLANTEAMIENTO DEL PROBLEMA

a. ESTABLECER OBJETIVOS DEL ESTUDIO

Como paso inicial se establecieron los objetivos que se pretenden alcanzar con la realización de este estudio, para ello se ocupó el método de la lluvia de ideas para determinar, de manera conjunta, el objetivo general y los objetivos específicos que nos conllevarán a cumplir de manera integral el general.

b. JUSTIFICACIÓN DEL ESTUDIO

Para la elaboración de la justificación de nuestro estudio se plantearon las interrogantes de porque es necesario e importante realizar dicho estudio, para ello se empleo el método de la lluvia de ideas y se apoyó en la recabación de información que permitirá ampliar el tema y los conocimientos acerca de este a nivel internacional como nacional. Los medios utilizados para la recabación de la información fueron: sitios, páginas y documentos electrónicos, libros y periódicos de circulación nacional.

c. DIAGRAMA CAUSA-EFECTO

Utilizamos el diagrama causa y efecto, porque nos permite plantear las posibles causas que provocan la problema en estudio. De esta manera definimos los elementos principales y su interrelación con el problema.

d. FORMULACIÓN DE HIPÓTESIS

Se utilizarán Hipótesis descriptivas puesto que estas son el tipo de hipótesis que se usan en el tipo de investigación que es descriptiva y son afirmaciones más generales que pueden involucrar una variable, dos o más variables.

II. TIPOS DE INVESTIGACIÓN A REALIZAR Y FUENTES DE INFORMACIÓN.

a. INVESTIGACIÓN EXPLORATORIA.

La causa por la cual nuestra investigación es exploratoria se debe a que se efectuará sobre un tema poco estudiado como lo es la informática forense en el país, por lo que sus resultados constituyen una visión aproximada de dicho objeto, este tipo de investigación se orienta a

a) La formulación precisa del problema planteado en la investigación, y

b) Conducente al planteamiento de una hipótesis.

b. INVESTIGACIÓN DESCRIPTIVA.

Según la naturaleza de los objetivos en cuanto al nivel de conocimiento que se desea alcanzar, la investigación es descriptiva porque se interpretará y presentará la realidad de cómo está actualmente la informática forense en el país.

c. INVESTIGACIÓN EXPERIMENTAL.

Además la investigación será experimental en la realización del estudio debido a que está integrada por un conjunto de actividades metódicas y técnicas que se realizan de manera conjunta para recabar la información y datos necesarios sobre el tema de la informática forense en El Salvador y el problema a resolver. Mediante la manipulación de una variable experimental no comprobada, el experimento será llevado a cabo en la vida real y se pretende controlar el aumento o disminución de la variable y su efecto en las conductas observadas, para describir de qué modo o por qué causas se produce una situación o acontecimiento particular.

d. FUENTES DE INFORMACIÓN PRIMARIA Y SECUNDARIA.

d.1 PRIMARIAS

Las fuentes de información primarias que se han determinado para la realización de este proyecto son:

Fiscalía General de la República, Policía Nacional Civil y Corte Suprema de Justicia, ya que estas tres instituciones son las que están directamente involucradas en:

- Recolección de evidencia cuando se ha cometido un delito.
- Esclarecimiento de cómo fueron los hechos y
- Resolución de juicios en casos de delitos informaticos.

d.2 SECUNDARIAS

Las fuentes de información que se establecieron como secundarias será la información que se obtendrá de documentos consultados por internet, libros, revistas, periódicos pero sobre todo será la brindada por aquellas Instituciones de educación superior que imparten la carrera o técnicos relacionados con Informática, ya que éstas son las indicadas para impartir conocimiento sobre nuevas tendencias, temáticas y tecnologías utilizadas en otros países e involucradas en el campo de acción de la informática.

III. DISEÑO DE INVESTIGACIÓN.

a. DISEÑO EXPERIMENTAL.

El diseño de la investigación será el experimental debido a que ocupa técnicas estadísticas para planear experimentos y analizar sus resultados de una manera ordenada y eficiente. Se aplica a una situación desconocida para llegar a una hipótesis y después a un resultado. Además se dice que cuando se carece de información suficiente para resolver un problema, el método de ensayo y error o experimentación es la alternativa para encontrar una solución.

IV. POBLACIÓN Y MUESTRA

a. SUJETOS A SER MEDIDOS.

Los elementos a medir para el estudio y análisis sobre la informática forense son:

- La computadora y la red en la cual éste está conectada.
- Los delitos informáticos.
- La evidencia digital.
- Metodologías aplicadas.
- Entidades policiales y judiciales.

b. POBLACIÓN SELECCIONADA.

El estudio contara con 4 universos los cuales son: la Fiscalía General de la República, Policía Nacional Civil, Corte Suprema de Justicia y las Universidades que imparten carreras en informática. De estos universos se determinara la población a la cual se enfocara directamente el estudio, para poder determinar luego la muestra necesaria que de cómo resultado el reflejo y la representación real-equitativa de todas las entidades involucradas en el tema dentro del estudio.

c. TIPO DE MUESTREO

El tipo de muestreo que se eligió es el muestreo estratificado debido a que nuestro universo no es homogéneo, sino que está formado por estratos diferentes que constituyen categorías importantes para la investigación, como lo son: la Fiscalía General de la República, la Corte Suprema de Justicia, Policía Nacional Civil y las Universidades tanto privadas como publica.

La elección de la muestra no debe hacerse globalmente para todos los estratos a la vez, ya que nos expondríamos a que unos estratos estuvieran más representados que lo que proporcionalmente les corresponde. Una vez definidos los estratos, dentro de cada uno de ellos se llevará a cabo un muestreo aleatorio simple o sistemático para elegir la sub-muestra correspondiente a cado uno de éstos y al mismo: la determinación del número de elementos que ha de tener cada una de estas sub-muestras denomina *afijación de la muestra*.

d. SELECCIÓN DEL TAMAÑO DE LA MUESTRA

Se tendrá una muestra de las cuatro poblaciones involucradas en el estudio, para que los datos obtenidos sean representativos y obtener una estimación apropiada de los objetos. Esto se llevara a cabo mediante la determinación con el nivel de confianza 97%, un error muestral de 3%.

V. RECOLECCIÓN, TABULACIÓN Y ANÁLISIS DE LOS DATOS

a. INSTRUMENTOS DE INVESTIGACIÓN

Los instrumentos que se diseñarán para la recolección de la información son la entrevista, encuesta y cuestionario. Para ellos se harán preguntas abiertas y cerradas.

b. RECOLECTAR DATOS

La recolección de datos se llevará acabo utilizando los instrumentos diseñados, los cuales serán distribuidos entre la muestra poblacional y las fuentes de información que se establecieron para la realización de este estudio.

c. TABULACIÓN DE LOS DATOS

Para la tabulación se emplearán los métodos de procesamiento datos tales como: Tabulación y proyección y el software SPSS.

d. ANALIZAR LOS DATOS

Para la elaboración del análisis de los datos, se llevará a cabo apoyándose en los resultados arrojados en la tabulación de los datos y el criterio del grupo para dar una explicación correcta y adecuada de los datos presentados. Se prepararán totales, porcentajes, promedios, índices e indicadores que den información básica sobre la realidad de la informática forense en El Salvador.

VI. DIAGNÓSTICO DEL ESTUDIO Y ANÁLISIS SOBRE LA INFORMÁTICA FORENSE EN EL SALVADOR

Para la elaboración del diagnóstico se apoyará en el análisis de los datos y la comprobación de las hipótesis planteadas dando como resultado la descripción de cómo se encuentra la situación actual de la informática forense en El Salvador y posteriormente se harán las conclusiones del estudio y las recomendaciones para las entidades involucradas, a las cuales se plantean los beneficios que obtendrían de una aplicación de la informática forense en El Salvador y cuales serian las funciones que cada una de ellas tendría que ocupar para trabajar de manera conjunta en el esclarecimiento de procesos judiciales

B- MATRIZ DE CONGRUENCIA

A continuación se presenta en la ***tabla N°4*** la matriz de congruencia para el presente proyecto de graduacion que lleva por titulo:

ESTUDIO Y ANALISIS SOBRE LA INFORMATICA FORENSE EN EL SALVADOR.

PROBLEMAS	OBJETIVOS DEL ESTUDIO	HIPÓTESIS DE LA INVESTIGACIÓN	MÉTODOS, TÉCNICAS, PROCEDIMIENTOS E INSTRUMENTOS	BOSQUEJO DEL PROYECTO CAPITULACIÓN TENTATIVA.
Falta de tecnología, recurso humano calificado, técnicas y herramientas informáticas en la informática forense para resolver procesos judiciales. Desconocimiento de la informática forense. Código penal sin reformas, en la contemplación de delitos informáticos. Falta de leyes que amparen la aplicación de la informática forense.	General Realizar el estudio y análisis sobre la informática forense en El Salvador para conocer la situación actual y determinar su incidencia en los procesos judiciales. Específicos: Definir la población y muestra. Elaborar los instrumentos para la recolección de datos. Plantear las hipótesis. Recopilar y tabular los datos.	General: "La aplicación de la informática forense en los procesos judiciales; favorecerá el esclarecimiento en el 75% de los delitos informáticos" Hipótesis nula "La aplicación de la informática forense en los procesos judiciales; no alterará el esclarecimiento de los delitos informáticos" Auxiliares: "La falta de herramientas informáticas forenses en las instituciones policiales, determina el 80% de la incidencia de fraudes que se realizan a través de	Tipo de investigación. Exploratoria Descriptiva Experimental Métodos de investigación. Análisis. Síntesis. Técnicas para la recolección de datos Entrevista. Encuesta. Instrumento de recolección de datos Cuestionario. Técnicas estadísticas	CAPÍTULO I: GENERALIDADES DEL PROYECTO A. INTRODUCCION B. OBJETIVOS I. General II. Específico C. IMPORTANCIA D. JUSTIFICACIÓN E. ALCANCES Y LIMITACIONES CAPÍTULO II: ESTUDIO PRELIMINAR A. ANTECEDENTES B. SITUACIÓN ACTUAL C. PLANTEAMIENTO DEL PROBLEMA I. Problemática de la informática forense en El Salvador II. Diagrama de causa – efecto III. Formulación del problema IV. Análisis del problema

PROBLEMAS	OBJETIVOS DEL ESTUDIO	HIPÓTESIS DE LA INVESTIGACIÓN	MÉTODOS, TÉCNICAS, PROCEDIMIENTOS E INSTRUMENTOS	BOSQUEJO DEL PROYECTO CAPITULACIÓN TENTATIVA.
	Elaborar gráficos estadísticos. Mostrar artículos contemplados dentro de la legislación salvadoreña. Explicar los procedimientos actuales para la recolección de la evidencia digital. Investigar las herramientas informáticas que son utilizadas. Mostrar cómo influye la presentación de evidencia digital, en el veredicto final de un juicio. Elaborar indicadores que permitan monitorear el avance de la informática forense.	Internet" "La aplicación de una metodología de recolección y análisis de evidencias digitales, causará un rendimiento del 95% en el proceso de obtención de esta" "La falta de personal calificado en informática forense, determina el 85% de la ineficiencia en la resolución de delitos informáticos" "La debilidad de la legislación salvadoreña permite que el 85% de los delitos informáticos no sean esclarecidos en su totalidad"	Paquete de Estadística para las Ciencias Sociales (SPSS)[37] Procedimientos Chi cuadrado. Prueba de hipótesis.	V. Enunciado del problema D. FORMULACIÓN DE HIPÓTESIS I. Hipótesis General II. Hipótesis Nula III. Hipótesis Auxiliares E. MARCO TEÓRICO I. Marco Teórico II. Marco Conceptual III. Marco Legal CAPÍTULO III: METODOLOGÍA GENERAL ESTABLECIDA PARA LA REALIZACIÓN DEL PROYECTO A. METODOLOGÍA I. Metodología para Planteamiento del problema e. Establecer objetivos de la investigación. f. Justificación de la Investigación. II. Metodología para Definición del tipo de investigación a realizar y fuentes de información a. Investigación exploratoria.

[37] Por sus siglas en Ingles: Statistical Package for the Social Sciences.

PROBLEMAS	OBJETIVOS DEL ESTUDIO	HIPÓTESIS DE LA INVESTIGACIÓN	MÉTODOS, TÉCNICAS, PROCEDIMIENTOS E INSTRUMENTOS	BOSQUEJO DEL PROYECTO CAPITULACIÓN TENTATIVA.
				b. Investigación descriptiva. c. Investigación experimental d. Fuentes de información primaria y secundaria. III. Metodología para Seleccionar el diseño de investigación a. Diseño experimental IV. Metodología para Formulación de hipótesis. V. Metodología para Seleccionar población y muestra e. Definir los sujetos a ser medidos. f. Definir la población g. Selección el tipo de muestreo. h. Selección del tamaño de la muestra. VI. Metodología para Recolección, tabulación y análisis de los datos. e. Elaborar instrumentos de investigación. f. Recolectar datos. g. Tabulación de los datos. h. Analizar los datos. VII. Metodología para elaboración del Diagnóstico del estudio y análisis sobre la informática forense

PROBLEMAS	OBJETIVOS DEL ESTUDIO	HIPÓTESIS DE LA INVESTIGACIÓN	MÉTODOS, TÉCNICAS, PROCEDIMIENTOS E INSTRUMENTOS	BOSQUEJO DEL PROYECTO CAPITULACIÓN TENTATIVA.
				en el salvador. B. MATRIZ DE CONGRUENCIA C. CRONOGRAMA DE ACTIVIDADES Y EVALUACIONES D. PLANIFICACIÓN DE RECURSOS I. Recurso Humano II. Equipos y Otros costos III. Imprevistos IV. Presupuesto CAPÍTULO IV: RECOLECCIÓN Y TABULACIÓN DE DATOS A. SELECCIÓN POBLACIÓN Y MUESTRA I. Definir los sujetos a ser medidos II. Definir la población III. Selección el tipo de muestreo IV. Selección del tamaño de la muestra V. Defunción del error muestral B. INSTRUMENTOS DE RECOLECCIÓN DE DATOS (IRD). I. Definición de recolección de datos

PROBLEMAS	OBJETIVOS DEL ESTUDIO	HIPÓTESIS DE LA INVESTIGACIÓN	MÉTODOS, TÉCNICAS, PROCEDIMIENTOS E INSTRUMENTOS	BOSQUEJO DEL PROYECTO CAPITULACIÓN TENTATIVA.
				II. Definición de IRD III. Características de los IRD IV. Validez de los IRD V. Elaboración de Cuestionarios VI. Elaboración de Entrevistas C. RECOLECCIÓN DE LOS DATOS I. Recolección de datos primarios II. Recolección de datos secundarios D. PROCESAMIENTO DE LOS DATOS I. Tabulación de los datos II. Utilización de Métodos estadísticos CAPÍTULO V: ANÁLISIS Y DIAGNÓSTICO SOBRE LA INFORMATICA FORENSE EN EL SALVADOR A. ANÁLISIS E INTERPRETACIÓN DE DATOS I. Realización de Análisis cuantitativo y cualitativo II. Elaboración de Índices, Indicadores y cuadros estadísticos III. Comprobación de Hipótesis

PROBLEMAS	OBJETIVOS DEL ESTUDIO	HIPÓTESIS DE LA INVESTIGACIÓN	MÉTODOS, TÉCNICAS, PROCEDIMIENTOS E INSTRUMENTOS	BOSQUEJO DEL PROYECTO CAPITULACIÓN TENTATIVA.
				B. PROPUESTAS DERIVADAS DEL ESTUDIO I. Elaboración del Diagnostico sobre la situación actual sobre la informática forense en El Salvador II. Conclusiones sobre el Estudio realizado III. Recomendaciones sobre el Estudio realizado CAPÍTULO VI: DEMOSTRACION SOBRE LA UTILIZACION DE LA INFORMÁTICA FORENSE A. PREPARACIÓN DE LA DEMOSTRACIÓN DE LA INFORMÁTICA FORENSE I. Preparación de técnicas utilizadas en informática forense II. Elaboración de la estructura de un peritaje informático

Tabla N°4: Matriz de Congruencia utilizada para la realización del presente estudio

C- CRONOGRAMA DE ACTIVIDADES Y EVALUACIÓN

En este apartado se presenta el cronograma de actividades y evaluaciones elaborado para el desarrollo del ESTUDIO Y ANÁLISIS SOBRE LA INFORMÁTICA FORENSE EN EL SALVADOR.

Para un mejor entendimiento de las actividades a realizar se ha divido en cronograma en 4 partes:

1. ***Cronograma consolidado:*** en el cual se presentan las 3 etapas que formarán parte en la realización del proyecto las cuales son: *Anteproyecto, Etapa 1: Recolección, tabulación y análisis de los datos y Etapa 2: Diagnostico sobre el estudio de la informática forense en El Salvador*, además de las actividades a realizar en cada una de éstas.

2. ***Cronograma del Anteproyecto:*** en el cual se presentan de manera detallada las actividades y tareas a realizar en esta etapa.

3. ***Cronograma de Etapa 1:*** se presentan de forma detallada las actividades y tareas con las cuales consta esta etapa.

4. ***Cronograma de Etapa2:*** al igual que las etapas anteriores, se presenta de manera detallada las actividades y tareas relacionadas a esta etapa.

A continuación se presenta el cronograma detallado de cada una de estas etapas:

CRONOGRAMA CONSOLIDADO

Para poder ver este cronograma es necesario tenga instalado Microsoft Office Project 2007.

consolidado.mpp

CRONOGRAMA ANTEPROYECTO

Para poder ver este cronograma es necesario tenga instalado Microsoft Office Project 2007.

ANTEPROYECTO.mpp

CRONOGRAMA ETAPA 1: RECOLECCIÓN, TABULACIÓN Y ANÁLISIS DE LOS DATOS

Para poder ver este cronograma es necesario tenga instalado Microsoft Office Project 2007.

ETAPA I_RECOLECCIÓN_TABULACIÓN_Y_ANÁLISIS_DE_DATOS.mpp

CRONOGRAMA ETAPA 2: DIAGNÓSTICO SOBRE EL ESTUDIO DE LA INFORMÁTICA FORENSE EN EL SALVADOR

Para poder ver este cronograma es necesario tenga instalado Microsoft Office Project 2007.

ETAPA II DIAGNÓSTICO DEL ESTUDIO Y ANÁLIS DE DATOS.mpp

D- PLANIFICACIÓN DE LOS RECURSOS

CÁLCULO DE LOS COSTOS DE DESARROLLO

En este apartado se detalla el desglose de los recursos que se consideraron necesarios para la realización del proyecto, la asignación de sus respectivos costos y la elaboración del presupuesto en base a los recursos, costos, duración y actividades establecidas, estas últimas dos se obtuvieron del Cronograma de Actividades y Evaluaciones anteriormente definido.

Los costos se han basado en estimaciones establecidas por el grupo de trabajo.

I. RECURSO HUMANO

El recurso humano que se establecido para la elaboración del proyecto está conformado por los cuatro miembros del grupo de graduación. Se estimó que el salario de cada miembro será calculado en base a las horas trabajadas diariamente, para ello se tomó como salario base el de un recién egresado, el cual asciende a $600.00[38].

El mes tendrá 20 días laborables, es decir, la semana laboral se ha considerado de lunes a viernes, 8 horas diarias.

El periodo de duración para la realización del proyecto será de 8 meses contando a partir del mes de Febrero hasta Septiembre.

Para determinar el salario diario de cada uno de los miembros del grupo, se dividió $600 entre los 20 días laborales en el mes y el cual asciende a $30.00 diarios.

$$\text{Salario individual diario} = \frac{600}{20} = 30$$

Es así como se determino que el ***salario individual diario*** por el recurso humano es de ***$30.00 por persona.***

A continuación se presenta en la ***tabla N° 5*** el desglose de los costos por Recurso Humano y el total de costos en concepto de salario por día de cada miembro del grupo.

[38] Salario que gana una persona recién egresada de Ingeniera de Sistemas Informáticos Dato tomado del Libro: Gerencia Informática, Ver apartado *Referencia Bibliográfica I-Libros* literal 10 para su referencia.

RECURSO HUMANO		
RECURSO HUMANO	**SALARIO POR DÍA**	
Ingeniero 1	$	30.00
Ingeniero 2	$	30.00
Ingeniero 3	$	30.00
Ingeniero 4	$	30.00
TOTAL SALARIO DIARIO:	**$**	**120.00**
TOTAL SALARIO MENSUAL	**$**	**2,400.00**
TOTAL SALARIO 8 MESES	**$**	**19,200.00**

Tabla N° 5: Costos en Recurso Humano

II. RECURSOS CONSUMIBLES

Para calcular el costo de estos recursos se ha considerado lo siguiente:

a. COSTO DE IMPRESIÓN

El costo unitario de las páginas impresas, se obtuvo de esta manera:

IMPRESOR 1[39]

Costo de cartucho de tinta

- Cartucho negro = $ 2.00 e imprime aproximadamente 150 páginas.
- Cartucho a color = $ 2.50 (Utilizado de manera conjunta con el cartucho negro).

Costo de impresión

El costo de imprimir es obtenido por $2 / 150 hojas = 0.013 gasto de tinta al imprimir una hoja.

El costo por hoja es determinado de la siguiente manera: la resma vale $4.60[40] la dividimos entre 500 hojas y es igual a 0.0092 que es el costo de una hoja de papel.

Total = 0.013 + 0.0092 = 0.022 ctvs.

Haciendo un total de **$0.022 ctvs**. Es el costo de imprimir una hoja de papel.

[39] Canon Pixma IP1000
[40] Dato tomado de OfficeDepot Sucursal Flor Blanca

IMPRESOR 2[41]

Costo de cartucho de tinta

Cartucho negro = $ 8 e imprime aproximadamente 400 páginas.

Cartucho a color = $ 20 (Utilizado de manera conjunta con el cartucho negro).

Costo de impresión

El costo de imprimir es obtenido por $8 / 400 hojas = 0.02 gasto de tinta al imprimir una hoja.

El costo por hoja es determinado de la siguiente manera: la resma vale $4.60[42] la dividimos entre 500 hojas y es igual a 0.0092 que es el costo de una hoja de papel.

Total = 0.02 + 0.0092 = 0.0292 ctvs.

Haciendo un total de ***$0.0292 ctvs***. Es el costo de imprimir una hoja de papel.

b. COSTO DE ANILLADO Y EMPASTADO

Los anillados se utilizarán para los documentos que se entregan al final de cada etapa y el empastado será para los documentos finales del proyecto. A continuación se presenta el resumen de estos costos en la ***tabla N° 6***.

Etapa	Empastados	Costo Empastado Unitario $	Anillado	Costo Anillado Unitario $	Costo Total $
Anteproyecto			3	2.50	7.50
Etapa I			3	2.50	7.50
Etapa II			3	2.50	7.50
Proyecto Completo	6	$9.50[43]			57.00
TOTAL INCURRIDO DURANTE 8 MESES					**$ 79.50**

Tabla N° 6: Costo de anillado y empastado.

[41] Canon Pixma IP1800

[42] Dato tomado de OfficeDepot Sucursal Flor Blanca

[43] Precio de empastado en la imprenta de la Facultad de Ingeniería y Arquitectura de la Universidad de El Salvador.

c. COSTO POR PAPELERÍA

Para el cálculo de este costo se hace un estimado del número de páginas a utilizar por cada etapa del proyecto. Por lo que se detalla a continuación en la ***tabla N° 7***::

PROMEDIO[44] DE PAGINAS A UTILIZAR			
	Páginas	**Tomos**	**Total**
Anteproyecto	150	3	450
Etapa I	400	3	1,200
Etapa II	200	3	600
Proyecto Completo[45]	750	6	4,500
TOTAL INCURRIDO DURANTE 8 MESES			**6,750**

Tabla N° 7: Costos por papelería.

1 resma de papel contiene 500 hojas. El cálculo de resmas a utilizar lo hacemos por medio de la regla de tres simple de la siguiente manera:

1 resma _____ 500 hojas

X _____ 6750 hojas

Por lo que se tiene: 13.5 redondeando 14 resmas aproximadamente con un costo total de $4.60 cada una. Haciendo un total de: **$64.40**

[44] Estos datos son estimados y se consideran los tres tomos a entregar en cada defensa.

[45] Esta etapa comprende el Anteproyecto, Etapa I, Etapa II, los seis tomos son los establecidos a entregar por la escuela de Ingeniería de Sistemas Informáticos.

d. CONSOLIDADO DE LOS RECURSOS CONSUMIBLES

A continuación se detallan los **Costos Consumibles** en la ***tabla N° 8*:**

RECURSOS CONSUMIBLES	CANTIDAD	PRECIO UNITARIO $	TOTAL $
Fotocopias de documentos	600	0.03	18.00
Impresiones de páginas			
• Impresora 1 [46]	2250	0.022	49.50
• Impresora 2[47]	4500	0.0292	131.40
Resma de papel bond Tamaño Carta, base #20[48]	14	4.60	64.40
Torre de discos 25 unidades [49]	1	6.25	6.25
Cartuchos de tinta para Canon Pixma IP1000			
• Cartucho negro.	15	2.00	30.00
• Cartucho a colores.	2	2.50	5.00
Cartuchos de tinta para Canon Pixma IP1800			
• Cartucho negro.	12	8.00	96.00
• Cartucho a colores.	2	20.00	40.00
Empastado	6	9.50	57.00
Anillados	9	2.50	22.50
Memoria de 1 Gb USB	1	10.00	10.00
Gastos Varios (Lapiceros, Portaminas, Borradores, Fólderes, Fastener, Sobres Manila)			15.00
TOTAL INCURRIDO DURANTE 8 MESES			**$ 545.05**

Tabla N° 8: Costos por Recurso Consumibles

El **costo de recursos consumibles total** estimado para la realización del proyecto de graduación es de **$545.05.**

[46] Esta impresora esta destinada a imprimir el Anteproyecto, Etapa I y Etapa II
[47] Esta impresora esta destinada a imprimir el trabajo de graduación completo.
[48] Precios de Resma de papel y Gastos Varios , Fuente: OfficeDepot Sucursal Flor Blanca
[49] Precios de torre de discos, Cartucho de tinta y CD's, Fuente: OfficeDepot Sucursal Flor Blanca

III. RECURSO TECNOLÓGICO

En este apartado se consideran los recursos como equipo informático y los costos consumibles necesarios para el desarrollo del proyecto.

Para el desarrollo de este proyecto se hará uso de los equipos que se presentan detallados en la ***tabla N°9***[50]:

EQUIPO	CANTIDAD	PRECIO UNITARIO($)	COSTO $
Computadora de Escritorio	2	200.00	400.00
Laptop	1	700.00	700.00
Impresor Canon Pixma IP 1000	1	48.00	48.00
Impresor Canon Pixma IP 1800	1	39.00	39.00
UPS / REGULADOR	2	48.00	96.00
TOTAL INCURRIDO DURANTE 8 MESES			**$1,283.00**

Tabla N° 9: Costos por Recurso Tecnológico.

A continuación en la ***tabla N° 10 y 11*** se describe las características de los equipos anteriormente mencionados.

DESCRIPCIÓN DE COMPUTADORAS	
Procesador:	Celeron 1.6 / 800
Memoria Caché:	512 KB
Memora RAM:	512 MB DDR2
CD-ROM	52X
Disco Duro:	80 GB
Disco Flexible:	3.5", 1.44 MB
Dispositivos Periféricos	Ratón óptico, teclado

Tabla N° 10: Descripción de computadoras de escritorio.

[50] Fuente: TECNO SERVICE sucursal Flor Blanca

DESCRIPCIÓN COMPUTADORA PORTÁTIL	
Procesador:	Celeron 2.00GHz
Memoria Caché:	512 KB
Memora RAM:	512 MB
Video:	8 MB
DVD-ROM	16X
Disco Duro:	80GB

Tabla N° 11: Descripción de Computadora portátil

Calculo de la Depreciación del Equipo

Para establecer el monto de la depreciación del equipo se utiliza el Método de Línea Recta, el cual consiste en:

El valor de adquisición lo dividimos entre los años de vida del equipo, multiplicamos este resultado por el porcentaje, obteniendo el monto de depreciación anual. El porcentaje es retomado según lo establece la Ley de Impuesto sobre la Renta[51], el cual es del 50% para los bienes muebles, basándonos en esta ley calculamos la depreciación para el equipo.

A continuación se muestra la formula[52] para la depreciación.

$$Depreciación = \frac{\text{Valor de adquisicion}}{\text{Años de vida}} \times Porcentaje\ del\ precio\ del\ equipo$$

La depreciación del equipo informático utilizado para el desarrollo, se especifica a continuación en la ***tabla N° 12***:

[51] Ley de Impuesto sobre la Renta, Art. 30, Inciso 3. Ver apartado *Referencia Bibliográfica III: Documentos Electrónicos* literal 7 para su referencia.

[52] Esta formula fue tomada de Ley de Impuesto sobre la Renta, Art. 30, Inciso 3. Ver apartado *Referencia Bibliográfica III: Documentos Electrónicos* literal 7 para su referencia.

EQUIPO	AÑOS DE VIDA	PORCENTAJE DEL PRECIO DEL EQUIPO	VALOR DE ADQUISICIÓN $	MONTO DE LA DEPRECIACIÓN $
Computadora[53] 1	5	50%	200.00	20.00
Computadora 2	5	50%	200.00	20.00
Computadora Portátil	3	50%	700.00	116.67
Impresor 1	2	50%	48.00	12.00
Impresor 2	2	50%	39.00	9.75
UPS 1	2	50%	48.00	12.00
UPS 2	2	50%	48.00	12.00
Depreciación anual			**1,283.00**	**$ 202.42**
Depreciación mensual				**$ 16.87**
Depreciación por 8 meses				**$ 134.95**

Tabla N° 12: Costos por Depreciación del Equipo informático

La Depreciación de los equipos anual equivale a = $ 202.42. Para calcula este valor se utilizó el porcentaje máximo de depreciación anual permitido, el cual es del 50%[54].

Por lo que se tiene:

Depreciación anual = $202.42

Depreciación mensual = $ 202.42 /12 meses = $16.87

Y el monto de la **depreciación para todo el tiempo** (8 meses) que durara el proyecto es de: $ 16.87 * 8 meses = **$134.95.**

En la ***tabla N° 13*** se presentan los ***Costos de las Licencias de Software a utilizar en el desarrollo del proyecto:***

[53] La vida útil determinada para computadoras personales se estima que es de cinco años y para una laptop es de tres años. Según el articulo **"**información general de desperdicios electrónicos o "e-waste"" tomado de internet. Ver apartado *Referencia Bibliográfica II: Sitios Webs* literal 24 para su referencia.

[54] Porcentaje para la depreciación según el artículo 30 inciso 3 de la Ley de Impuesto sobre la Renta.

LICENCIAS DE HERRAMIENTAS DE DESARROLLO	COSTO $
OpenOffice	Gratis
Fedora Core 7	Gratis
TOTAL INCURRIDO DURANTE 8 MESES	**$ 0.00**

Tabla N° 13: Costos de Licencias de software para el desarrollo del proyecto

IV. RECURSOS DE OPERACIÓN

a. COSTO MENSUAL DE ENERGÍA ELÉCTRICA

Los cálculos para el costo mensual de Energía Eléctrica se tomaron en cuenta, cuantos Watts/hora, recordando que Watts son las unidades en que se mide la potencia, consume cada equipo a utilizar. Para ello se describe en base a las especificaciones técnicas y se obtiene con la siguiente fórmula[55]:

$$\boldsymbol{Watts}_{\boldsymbol{Hora}} = Voltaje \times Amperios$$

En la cual se establece el consumo en Watts de un equipo electrónico por cada hora de utilización.

$$\boldsymbol{Total\ de\ Watts/Dia} = \frac{Watts}{hora} \times Horas\ de\ utilizacion\ diarias \times Cantidad\ de\ equipos$$

Además se presentan las demás formulas para convertir los Watts hora a Kwh., para esto se divide el total en Watts entre 1000 para convertirlos en Kwh.,

$$\boldsymbol{Total\ de\ KWh\ por\ equipo} = Total\ en \frac{Watts}{1000}$$

$$\boldsymbol{Total\ Kwh\ Estimado\ Mensual} = Total\ KWh\ por\ equipo \times Total\ de\ Dias\ al\ mes$$

En donde:

El voltaje utilizado por el país es de 120V

Amperio es el especificado por cada equipo que se presenta en la ***tabla N° 14*** a continuación:

[55] Esta formula fue tomada del articulo "¿Cuánta energía cuesta tener un equipo de computo encendido?" tomado de internet. Ver apartado *Referencia Bibliográfica II: Sitioss Webs* literal 25 para su referencia.

EQUIPO	AMPERIOS[56]	WATTS /HORA	HORAS DE UTILIZACIÓN DIARIAS	CANTIDAD DE EQUIPO	TOTAL WATTS/DIA
Equipo informático[57]		425[59]	5	2	4,250
Portátil	2.3	276	5	1	1,380
UPS	0.6	72	5	2	720
Impresor 1	0.36	43.2	1	1	43.2
Impresor 2	0.7	84	1	1	84
Total en Watts por Equipo					6,477.2
Total en Kwh. por Equipo					6.4772
Total días laborales en el mes					20
TOTAL KWH. ESTIMADO MENSUAL					**129.54**
VALOR APROXIMADO ≈					**130**

Tabla N° 14: Consumo de KWH estimado mensualmente.

En la siguiente ***tabla N° 15*** se presenta el costo mensual por el consumo de Energía Eléctrica y para esto se hace la sumatoria de los cargos de distribución, tasa municipal por poste, comercialización y energía, los cuales se detallan a continuación:

COSTO DE ENERGÍA ELÉCTRICA[58]	COSTO $
Cargo de Distribución	
• Kwh. consumido X 0.029932058[60]	3.89
Cargo por tasa municipal por poste	0.17
Cargo de Comercialización	0.85
Cargo por Energía	
• Kwh. consumido X 0.115301458[60]	14.99
Costo Mensual	**$19.90**
Costo Diario	**$0.995**
TOTAL INCURRIDO DURANTE 8 MESES	**$159.20**

Tabla N° 15: Costos por Energía Eléctrica.

[56] Estos datos fueron tomados de las especificaciones de los fabricantes que viene en la parte trasera de los equipos.

[57] Se entenderá por equipo informático: CPU =350 W y monitor 15"= 75 W. Esto datos en Watts es tomado del articulo "¿Cuánta energía cuesta tener un equipo de computo encendido?" tomado de internet. Ver apartado *Referencia Bibliográfica II: SitiosWebs* literal 25 para su referencia.

[58] Las tarifas y costos fijos de energía eléctrica son los establecidos por el proveedor del servicio de alumbrado eléctrico CAESS.

b. COSTOS DEL SERVICIO TELEFÓNICO

Partiendo de la ***tabla N° 16*** se realizan los cálculos pertinentes para el servicio telefónico a utilizar en el desarrollo del proyecto:

Tarifas Para Telefonía Fija[59]

Se estima un promedio mensual de 100 minutos de llamadas locales, con restricción de llamadas a celulares.

Costo de llamada Local es de $0.02.

	MINUTOS	CARGO $	CARGO $
Llamadas locales	100	0.02	2.00
Servicio restringido para teléfonos Celulares			0.65
Cuota Fija			9.42
Total			**$ 12.07**
Menos Impulsos Gratis			$ (1.94)
Total a Pagar mensual			**$ 10.13**
Total a Pagar diario			**$ 0.51**
TOTAL INCURRIDO DURANTE 8 MESES			**$ 81.04**

Tabla N° 16: Costos por Servicio Telefónico

c. SERVICIO DE INTERNET

El costo mensual que se paga en concepto de servicio de internet[60] es de $28.25.

El costo diario por la utilización de este servicio es de $1.41 y se calculó de la siguiente forma:

$$Costo\ diario\ por\ internet\ = \frac{28.25}{20} = 1.41$$

El costo mensual por el servicio que es de $28.25 es dividido entre los días laborales que tiene el mes que para nuestro caso son de 20 días laborales, dando como resultado que el ***costo diario por internet*** es de: ***$1.41***

El costo total incurrido durante 8 meses en concepto de **Servicio de internet** es: **$226.00.**

[59] Fuente: www.siget.gob.sv

[60] Dato tomado de la cuota que se paga mensualmente por el servicio de internet que presta la compañía AMNET S.A. de C.V. para una velocidad de 512 kbps la cual es de $25 + IVA.

d. VIÁTICOS

Los viáticos[61] se han calculado estimando los gastos que se tiene diarios en concepto de transporte y alimentación por cada miembro diariamente.

Se a considerado que el gasto por transporte será de $2.00 diarios y el gasto por alimentación, tomando 1 tiempo de comida, será de $2.00 por cada recurso humano. Para calcular el costo mensual se toma en cuenta 20 días laborales en el mes. Estos costos se presentan en la ***tabla N°17.***

VIATICO	RECURSO HUMANO	COSTO DIARIO $	COSTO MENSUAL $
Transporte			
• Ingeniero 1	1	2.00	40.00
• Ingeniero 2	1	2.00	40.00
• Ingeniero 3	1	2.00	40.00
• Ingeniero 4	1	2.00	40.00
Alimentación			
• Ingeniero 1	1	2.00	40.00
• Ingeniero 2	1	2.00	40.00
• Ingeniero 3	1	2.00	40.00
• Ingeniero 4	1	2.00	40.00
TOTAL MENSUAL			**$ 320.00**
TOTAL DIARIO			**$ 16.00**
TOTAL INCURRIDO DURANTE 8 MESES			**$2,560.00**

Tabla N° 17: Costos por Viáticos.

[61] Estos costos han sido establecidos tomando como base el costo actual en el que cada uno de los miembros del grupo incurre.

e. CONSOLIDACIÓN DE LOS RECURSOS DE OPERACIÓN

Tomando en cuenta el costo diario y mensual de cada recurso, el ***costo total de operación*** para el proyecto se muestra a continuación en la ***tabla N° 18***:

SERVICIOS BÁSICOS	CANTIDAD	COSTO UNITARIO $	COSTO DIARIO $	COSTO MENSUAL $	MESES	COSTO TOTAL DEL PROYECTO $
Agua Potable[62]	8[63]	1.90	0.76	15.20	8	121.60
Energía Eléctrica	-	-	0.99	19.90	8	159.20
Teléfono	1	10.13	0.51	10.13	8	81.04
Navegación en Internet	1	28.25	1.41	28.25	8	226.00
Viáticos	-	-	16.00	320.00	8	2,560.00
Alquiler de local[64]	1	57.00	2.85	57.00	8	456.00
TOTAL			**22.52**	**450.48**		**3,603.84**

Tabla N° 18: Costos consolidados de Recursos de operación

El **costo total por recursos de operaciones total** estimado para la realización del proyecto de graduación es de **$3,603.84.**

[62] El costo de cada recipiente de 5 galones de agua cristal es de $1.90.
[63] Consumo promedio de agua mensual en una casa con 4 personas.
[64] El alquiler del local es de $57.00 mensuales y este dato fue tomado de lo actualmente se paga por pupilaje en San Salvador.

V. CONSOLIDACIÓN DE LOS RECURSOS A UTILIZAR EN LA REALIZACIÓN DEL PROYECTO.

A continuación en la ***tabla N° 19*** se presenta el costo total de desarrollo para la realización del proyecto de graduación durante los 8 meses**.**

RECURSO		COSTO TOTAL $
curso humano		19,200.00
cursos consumibles		545.05
cursos tecnológicos		1,148.05
• Equipo Informático	$1,283.00	
• Depreciación del Equipo informático	$ (134.95)	
• Herramientas de desarrollo	$ 0.00	
cursos de operación		3, 603.84
tal costo de desarrollo del proyecto		**24, 496.94**
previstos[65] (10%)[66]		**2,449.69**
sto total del presupuesto destinado para el proyecto de graduación		**26,946.63**

Tabla N° 19: Costos de Desarrollo total del proyecto durante los 8 meses de su realización.

El **costo total** para la realización del presente trabajo de graduación es de: **$ 26,946.63.**

[65] Dentro de los imprevistos están considerados además el gasto por transporte y papelería extra que se puede dar dentro de la etapa de recolección de datos.

[66] Tomado del libro Gerencia Informática Ver apartado *Referencia Bibliográfica I- Libros* literal 10 para su referencia.

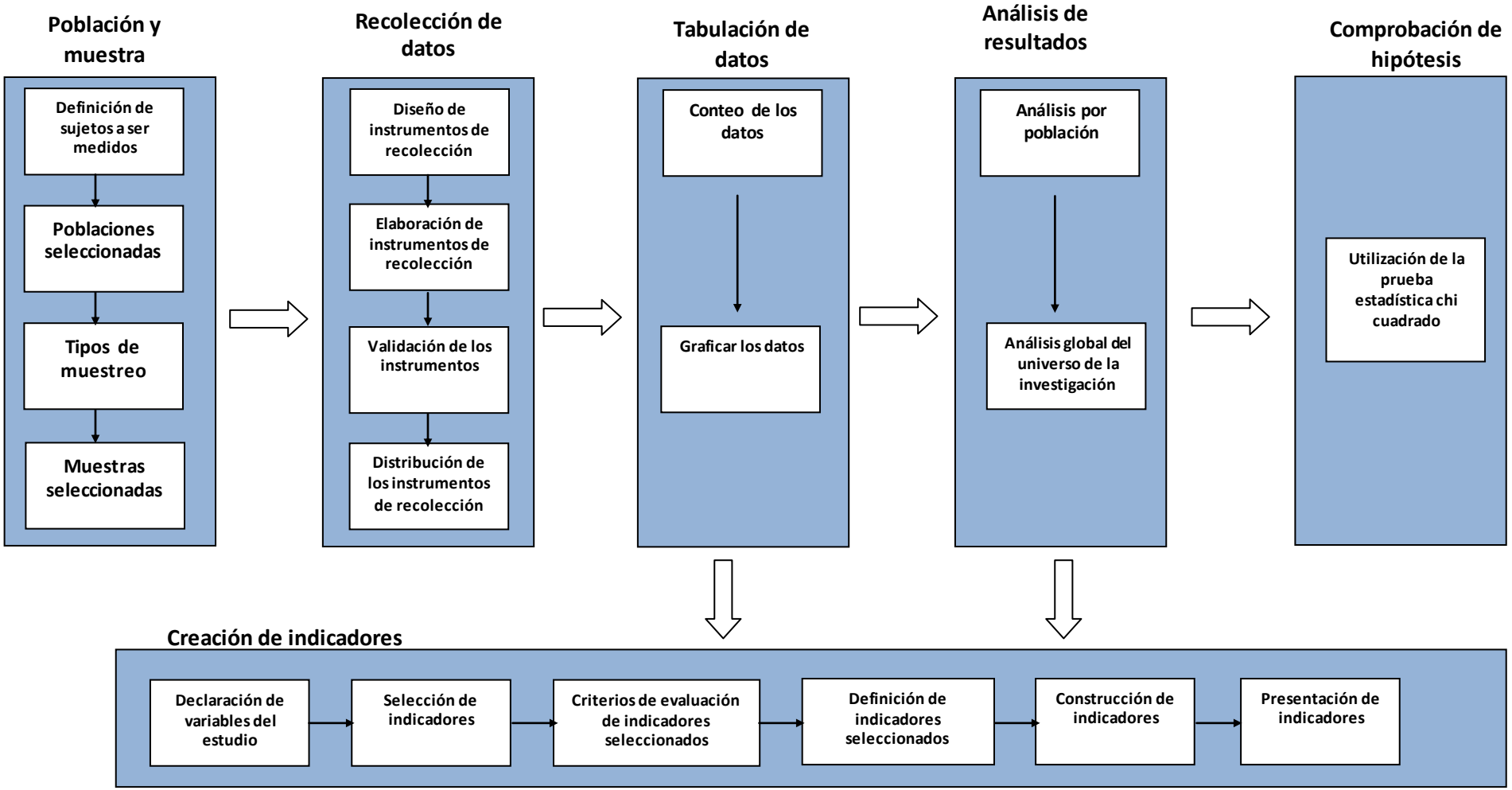
CAPITULO 3

RECOLECCIÓN, TABULACIÓN Y ANÁLISIS DE DATOS

CAPITULO 3: RECOLECCIÓN, TABULACIÓN Y ANÁLISIS DE DATOS

A- DISEÑO DE LA INVESTIGACIÓN

El diseño de la investigación que se utilizo muestra una serie de pasos que permitieron organizar la información para poder estructurarla y analizarla de la manera más eficiente. A continuación se presenta el modelo utilizado en esta investigación:



B- POBLACIONES YMUESTRA

I. JUECES

a- POBLACION

El sector que se estableció como población, desde el punto de vista judicial, para la realización de nuestra investigación fue el Centro Judicial Isidro Menéndez, debido a que es en este lugar donde se tiene la mayor concentración de tribunales del área metropolitana de San Salvador[67], y en especifico los juzgados de instrucción, ya que es en este tribunal donde se realizan los juicios, una vez se haya determinado que el imputado es sospechoso de haber cometido el delito que se le atribuye.

Además es en esta fase de instrucción donde se presentan todas las pruebas de un determinado delito por parte de la fiscalía y defensoría, se realizan los alegatos por ambas partes y se dictamina la inocencia o culpabilidad del imputado.

Al mismo tiempo, es aquí donde el juez, fiscal y defensor, aplican el derecho al caso concreto. Esto quiere decir, que tanto el juez como el fiscal y el defensor, tiene que estar seguros que los cargos que se le imputan a una persona, son realmente delitos tipificados dentro del código penal, ya que de lo contrario la persona ofendida podría demandarlos por difamación. Es por esta razón que los casos que se presentan en este juzgado son indiscutiblemente, delitos tipificados en el código penal, el cual especifica cuáles son las conductas o hechos que se catalogan como delitos dentro de nuestra sociedad salvadoreña, y se le da el seguimiento establecido en la ley para este tipo de proceso judicial.

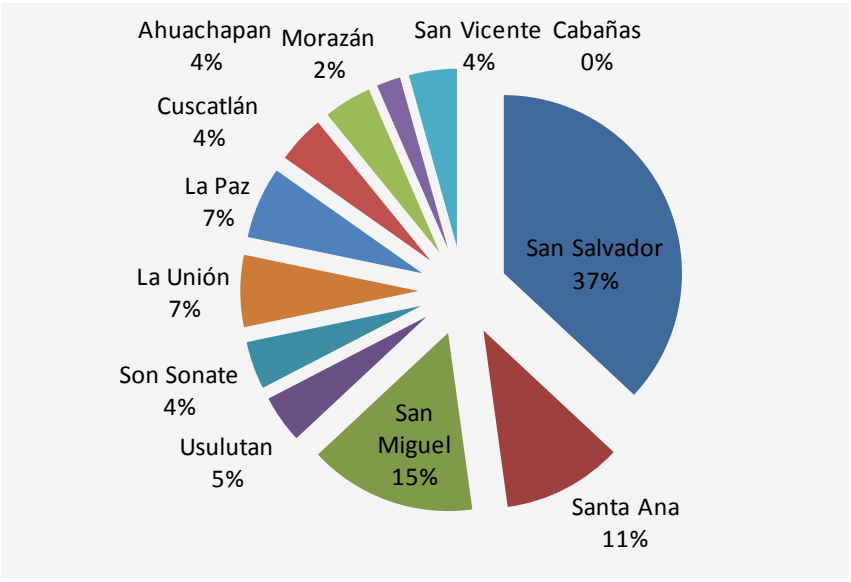
Es por estas razones que fue elegido el Centro Judicial Isidro Menéndez ya que es aquí donde la policía en conjunto con la fiscalía, presentan las evidencias necesarias para esclarecer como sucedió un delito en especifico, y en particular para los delitos informáticos, es en este lugar donde se presentan las evidencias digitales, las cuales se analizan a través de informática forense, para comprobar cómo se realizaron los hechos y se evalúa la confiabilidad y credibilidad de la evidencia ante el juez.

b- MUESTRA POBLACIONAL

De los 17 juzgados de instrucción que se encuentran en San Salvador, 10 de estos se encuentran dentro del Centro Judicial Isidro Menéndez y los 7 restantes se encuentran en el municipio de Soyapango. Cada juzgado cuenta con un juez titular. ***Anexos N° 4***para mayor detalle. En el ***gráfico N° 1*** se muestra la distribución en porcentajes de juzgados de instrucción en El Salvador.

Una vez establecida que la población de jueces a encuestar sería del Centro Judicial Isidro Menéndez, se determino que se llevaría a cabo un censo y no un muestreo, debido a que la población de jueces de instrucción es pequeña y permite esto.

[67] Fuente: Ver apartado Referencias Bibliográficas- II: Sitios Web: numeral 40. Juzgados de Primera Instancia: Instrucción.



Distribución de Juzgados de instrucción en El Salvador	
San Salvador	17
Santa Ana	5
San Miguel	7
Usulután	2
Sonsonate	2
La Unión	3
La Paz	3
Cuscatlán	2
Ahuachapán	2
Morazán	1
San Vicente	2
Cabañas	0

Gráfico N° 1: Porcentaje De distribución de juzgados de instrucción en El Salvador[68]

El censo se realizo a los 10 jueces con el que cuenta el Centro Judicial en total.

Total de jueces encuestados: 10 jueces

II. ABOGADOS

a- POBLACION

Para conocer el tamaño de la población y la determinación del tamaño de la muestra de los abogados, se tomo en cuenta los que laboran en la Procuraduría General de la República, ya que es quién vela por la defensa de la familia, de las personas e intereses de los menores e incapaces. Bajo este precepto la Procuraduría General de la República, ejerce el servicio legal en cumplimiento de una obligación del Estado, tal como los servicios de salud y educación.

La distribución de los defensores se muestra en la ***tabla N° 20***, en la cual se muestra la cantidad defensores por departamento, en nuestro caso en el área de San Salvador se encuentra concentrado el mayor número de abogados, que son 127. El cual representa el 39 % de la totalidad de ellos en El Salvador según el ***gráfico N° 2***.

Dando como resultado:

$$N = 127 \quad número\ de\ abogados\ que\ conforman\ la\ poblacion\ total.$$

[68] Datos obtenidos por la Corte Suprema de Justicia, Fuente: Ver apartado Referencias Bibliográficas - II: Sitios Web: numeral 40. **Fuente del gráfico: elaboración propia**.

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 N° 20: Distribución de defensores asignados a cada departamento[69]

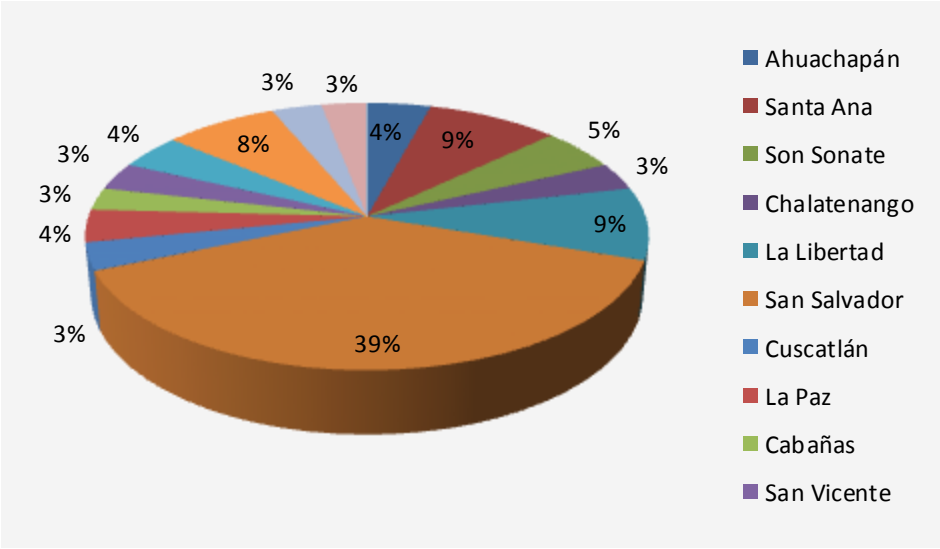


Gráfico N° 2: Porcentaje de defensores asignados por departamentos[70]

[69] Fuente: Procuraduría General de la República.
[70] Fuente: Procuraduría General de la República

b- MUESTRA POBLACIONAL

Media vez se conoció que la población a encuestar de abogados era de 127, se procedió a establecer la muestra que permitiera recabar los datos necesarios para el estudio en desarrollo, por lo que se utilizo el diseño de Muestreo Aleatorio Simple, el cual permitió el cálculo de **n**(muestra), a través de la siguiente formula.

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

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 desea que los resultados del estudio sean confiables por lo menos en un 95%, por lo que se tomara en cuenta un nivel de confianza del 95%, dando así un valor de **Z = 1.96** ***Anexos N° 5***. Debido a que por lo general se acostumbra a utilizar un nivel de confianza igual a 95% (que corresponde en la curva de Gauss a 2 sigmas)[71].

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 conozcan del tema o no lo conozcan. Considerando que no se han realizado estudios previos y que el tema en estudio es de importancia para nuestro país.

Se espera que los resultados se desvíen hasta un máximo de 5% de los datos originales o reales, por lo tanto **e = 5%** ***Anexos N° 6,*** lo que implica que se tiene un 95% de nivel de confianza en los resultados de las encuestas.

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:

$$n = \frac{1.96^2 * 0.5 * 0.5 * 127}{127 - 1 \ * 0.05^2 \ + \ 1.96^2 * 0.5 * 0.5}$$

$$n = 95.63 \ \cong \ 96 \ tamaño \ de \ la \ muestra$$

Es decir que el número de abogados en total que se encuesto fue de **96** según lo indica el tamaño de la muestra.

[71] Ver apartado Referencias Bibliográficas- II: Sitios Web: numeral 31.

III. PERITOS

Para la realización de las encuestas se conto con la ayuda de dos clases de peritos informáticos: nacionales e internacionales.

a- PERITOS NACIONALES

Uno de los peritos nacionales encuestados, se contacto a través de ACFES la cual es la única asociación de ciencias forenses en EL Salvador donde están agrupados los diferentes tipos de peritos forenses independiente de la especialidad en la que trabajen, como por ejemplo existen peritos forenses en química, balística, informática, etc. En esta asociación se encontró registrado un perito informático y además éste labora en la policía nacional civil.

El otro profesional que colaboro con las encuestas es un ingeniero en sistemas que ha servido como perito informático en juicios cuando éste ha sido requerido por los jueces debido a la cercanía que estos tiene con su persona, ya que él labora dentro del órgano judicial.

Y el tercer perito que participo en esta encuesta, es un elemento que trabaja en la INTERPOL.

Se desconoce la población de peritos informáticos que existen en el país debido a que esta información no se pudo obtener para esta investigación ya que no se encuentra disponible para el público en general además que se desconoce si se tiene un banco de datos con esta información y la institución encargada de llevar este registro.

A manera de comentarios se nos dijo por parte de los jueces, que cuando ellos solicitan los servicios de un perito informático, acuden a ingenieros informáticos conocidos por ellos o es a éstos mismos que les preguntan por otros ingenieros que puedan servir como peritos en un juicio.

Numero de Peritos Informáticos Nacionales Encuestados: **3**

b- PERITOS INTERNACIONALES

La ayuda de los peritos internaciones fue gestionada a través de correos electrónicos; se buscaron portales en internet donde se mostrase los servicios y el trabajo que ofrecían como peritos en informática forense.

De esta forma se consiguió el aporte y la ayuda invaluable de peritos de distintas nacionalidades como lo son Argentina, España y Estados Unidos.

Numero de Peritos Informáticos Internacionales Encuestados: **8**

IV. UNIVERSIDADES

a- POBLACION

Las Universidades privadas y pública que se encuentran ubicadas en el área metropolitana de San Salvador, son otras poblaciones que han sido seleccionadas para el desarrollo del estudio, se considera como tal, por la razón de ser las instituciones responsables de preparar profesionales en el área de la informática.

Cabe mencionar que se tomaron en cuenta 12 universidades privadas ubicadas en el área metropolitana de San Salvador, las cuales imparten la carrera ya sea de Licenciatura o Ingeniería en Computación. Además de contar con la Universidad de El Salvador como la única institución publica en el país.

Esta población permitirá la recolección de información correspondiente al nivel de conocimiento sobre informática forense que poseen los docentes de las carreras a fines a la informática.

Además el rápido avance de las tecnologías de información y comunicaciones obliga a que las instituciones educativas vayan preparándose acorde a lo nuevo que surge en el mercado en cuanto a tecnología informática.

b- MUESTRA POBLACIONAL

La determinación de la muestra de esta población se realizo en base a la cantidad de docentes que tengan las instituciones educativas y de las cuales posean carreras a fines a la informática, sin embargo no se trataran por igual la Universidad pública como 12 de las Universidades privadas que se encuentran en el área metropolitana de San Salvador que imparte la carrera de Licenciatura o Ingeniería en Computación.

La forma de determinación de la muestra para ambas se define a continuación.

Universidad Pública

Por ser la única institución pública de educación superior en el país, se realizo un censo a los 24 docentes que imparten materias en la carrera de Ingeniería de Sistemas Informáticos de la Universidad de El Salvador, por medio de un cuestionario, el cual ayudara a la recolección de información referente al nivel de conocimiento que posean los docentes relacionado a la informática forense.

Universidades Privadas

Para la determinación de la muestra de las universidades privadas del país, se tomaron en cuenta los docentes de 12 de estas instituciones, esto por ser las que tienen en su pensum carreras de ingeniería o licenciatura en sistemas y son las que se encuentran ubicadas en el área metropolitana de San Salvador. Para esta parte de la población fue necesario conocer cuál sería la muestra que permitiera recabar los datos necesarios para el estudio en desarrollo, por lo que se utilizo el diseño de Muestreo Aleatorio Simple, el cual permitió el cálculo de **n**(muestra), a través de la siguiente formula.

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

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 N° 21*** se muestra las universidades que se encuentran en el área metropolitana de San Salvador, en las cuales hay escuelas que imparten carreras a fines a la informática; se les pasara a los docentes de estas escuelas una encuesta para determinar el grado de conocimiento que tienen sobre informática forense.

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.

Tabla N°21: Universidades del área metropolitana de San Salvador.

La ***tabla N° 22*** muestra la cantidad de docentes a tiempo completo de las escuelas de las universidades que imparten Ingeniería o Licenciatura en informática.

No.	ACRÓNIMO	DOCENTES
1	UCA	6
2	UFG	6
3	UTEC	6
4	UPES	4
5	UAE	4
6	UEES	4
7	ULS	4
8	UDB	7
9	UCAD	6
10	UNAB	5
11	USAM	5
12	UMA	3
	Total:	**60**

Tabla N°22: Docentes a tiempo completo en la escuela de cada universidad.

- Dando como resultado:

$$N = 63 \quad número\ de\ docentes\ que\ conforman\ la\ poblacion\ total$$

Se desea que los resultados del estudio sean confiables en el 97% y un **e = 3%,** por lo que se tomara en cuenta un nivel de confianza del 97%, dando así un valor de **Z = 2.17** ***Anexo N° 5***.

Se utilizo el 97% de confiablidad para esta población debido a que:

- A diferencia de las otras poblaciones que están involucradas en este estudio: Jueces, Fiscales, Abogados, Policías y Peritos; la población de universidades es más accesible y puede ser encuestados en el tiempo estimado para la realización del presente estudio.
- Es más factible en comparación de tiempo porque el desarrollo de las actividades de los docentes se realizan al interior de las universidades encuestadas, debido a que se tomo en cuenta solo a los docentes de tiempo completo y ellos presentan mayor disponibilidad de brindar su apoyo para la realización del presente estudio.
- Aunque esta población no está directamente relacionada con el esclarecimiento de delitos informáticos, se ha considerado porque son las instituciones encargadas de brindar el conocimiento para el desarrollo de los futuros profesionales en el área informática.

Para la probabilidad de éxito y de rechazo, tiene igual probabilidad de ser aceptado o rechazado **p = 0.5, q=0.5** por que q = 1-0.5 = 0.5. Considerando que no se han realizado estudios previos y que el tema en estudio es de importancia para nuestro país.

Tamaño de la muestra

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:

$$n = \frac{2.17^2 * 0.5 * 0.5 * 63}{63 - 1 \ * 0.03^2 \ + \ 2.17^2 * 0.5 * 0.5}$$

$$n = 57.41 \cong 57 \ tamaño \ de \ la \ muestra$$

Es decir que el número de docentes en total a encuestar será de 57.

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

$$n = \frac{57}{12} = 4.75 \cong 5$$

Es decir que se encuestaran a 5 catedráticos en cada escuela informática de universidad.

Tamaño de la muestra a encuestar en total= 57 docentes.

Tamaño de la muestra a encuestar en cada universidad=5

Como se mencionó anteriormente algunas de estas universidades solo tienen 4 docentes contratados a tiempo completo, por lo que se encuestaron a más de 5 docentes de otras universidades, siempre dentro de las 12 universidades que se consideraron para la recolección de datos. De esta forma se busco una compensación entre ellas.

V. POLICÍA NACIONAL CIVIL

En el caso especifico de esta poblacion, no se pudo tener acceso a conocer el numero de elementos que laboran directamente en los casos por delitos informáticos, ya que se nos denego el acceso a ella y no se conto con el apoyo de esta institucion, **ver Anexo N° 7.**

Grupos elites de la policía nacional civil.

- Subdirección investigaciones
- División Investigación y Homicidios (DIHO)
- División Elite contra el Crimen Organizado (DECO)
- División Investigación Criminal (DIC)
- División Protección al Transporte (DPT)
- División Finanzas
- División de Fronteras

- División Interpol
- División Policía Técnica Científica (DPTC)
- División Puertos y Aeropuertos

Para la realización de esta investigación se han considerado 3 de los grupos elites de la Policía Nacional Civil, por ser los grupos que tienen en sus tareas llevar una investigación de los delitos que tratan con el uso de la tecnología y que se realizan en nuestro país, estos grupos se describen a continuación:

a. DIVISIÓN INVESTIGACIÓN CRIMINAL (DIC)

Esta división se encarga de investigar los hechos delictivos de trascendencia a nivel nacional, específicamente los relacionados a estafas, robo agravado, delitos sexuales y delitos de cuello blanco[72]; así como también concentrar la información delincuencial a nivel nacional para la elaboración de análisis estratégicos.

Principales funciones.

- Identificar, investigar y capturar estructuras delincuenciales especialmente los que se dediquen a robos, estafas, delitos sexuales y de cuello blanco.
- Concentrar la información de los departamentos de investigación criminal a nivel nacional y elaborar análisis operativos y estratégicos.
- Retomar algunos casos a nivel nacional y que sea necesario retornarlos de acuerdo a los criterios de intervención establecidos.
- Elaborar periódicamente informe a la subdirección de investigaciones relacionados a la incidencia delincuencial a nivel nacional.

Procedimiento de la División Investigación Criminal[73] en una investigación de casos de delitos que involucren incautar evidencia de carácter tecnológico.

Este procedimiento cuenta con tres pasos a seguir, los cuales se describen a continuación:

Paso 1: **<u>Secuestrar la evidencia:</u>**

En este paso los especialistas se encargan de hacer una inspección ocular policial, es decir, toman fotografías de todo los elementos encontrados en la escena del delito, se procede a embalar[74] la evidencia y desde este momento inicia la cadena de custodia[75] de la evidencia, además aquí es cuando se hace una acta que hace

[72] Para una mayor comprensión Ver apartado Glosario de Términos.

[73] Fuente: subinspector de la División Investigación Criminal

[74] Para una mayor comprensión Ver apartado Glosario de Términos.

[75] Para una mayor comprensión Ver apartado Glosario de Términos.

constar todo lo encontrado en dicha escena, esta describe todo lo que ahí se encuentra, quienes hacen la inspección ocular, la hora en la cual se hace la acta, entre otros datos.

Paso 2: **Fijación de la evidencia.**

En este paso la División manda la evidencia al Laboratorio que se encuentra en la División Técnica Científica Policial para que le realicen las respectivas pruebas, además, en la División Investigación Criminal se hace un registro de todo lo que se manda al laboratorio para hacer constar el trabajo que se desarrollo y de qué manera se hizo.

Paso 3: **Presentación de la evidencia al Juez.**

Finalmente sale la evidencia del laboratorio analizada, cuando el tratamiento de esta es muy complejo y el Laboratorio no posee los recursos necesarios para su análisis es presentada al juez y al fiscal, en caso de que sea necesario validar la información proporcionada, ellos contratan a peritos Informáticos para que compruebe la validez de la evidencia para que en un juicio sea presentada como prueba admisible.

Esta división presenta deficiencia de personal y recurso tecnológico para poder realizar investigaciones sobre delitos informáticos ya que cuando se han enfrentado a este tipo de casos, remiten la evidencia o piden a otras divisiones policiales su apoyo, ***Anexo N° 8***, para ayudar a recolectar la evidencia necesaria la cual es presentada como prueba ante un tribunal.

b. DIVISIÓN INTERPOL

La misión que tiene esta división es la de transmitir e intercambiar con la organización internacional de policía criminal de otros países o instituciones salvadoreñas competentes información relacionada a crímenes, sobre autores y cómplices, proceder a la captura o búsqueda de los mismos y poner a disposición de la autoridad judicial si fuera requerido; enviar a nivel internacional las ordenes de captura cuando en ellas se disponga. Facilitar en todo momento la ejecución de cartas rogatorias, investigaciones y cualquier seguimiento informático que se solicite a esta división.

Principales funciones.

- Gestionar sistemas de procesamiento de información, así como desarrollar e instalar la tecnología indispensable para el buen funcionamiento de la organización en materia de información y telecomunicaciones.
- Coordinar acciones que contribuyan a la lucha contra la delincuencia del derecho común, en la esfera internacional, intercambio de información e iniciación de investigaciones internacionales.
- Coordinar la sistematización centralizada y compartida la información y documentación sobre la actividad delictiva nacional, de interés internacional y transmitirla a las oficinas centrales nacionales y a la secretaría general de Interpol.
- Coordinar y sostener la oficina regional en todas las áreas especiales de Interpol, transmisión de peticiones, identificaciones e iniciación de investigaciones y detenciones.

- Supervisar y velar por la ejecución nacional de las resoluciones tomadas por la asamblea general de Interpol, de acuerdo al marco legal vigente.

La División Interpol de la Policía Nacional Civil trabaja en conjunto con la Fiscalía, la cual les solicita los requerimientos de la investigación que se realiza, en el trato de delitos informáticos se tiene un apoyo con instituciones(INTERPOL) internacionales en cuanto a capacitaciones sobre informática forense a los agentes de esta División encargados de las investigaciones de estos delitos, sin embargo estas capacitaciones no benefician totalmente esta temática en el país, ya que se presentan muchas limitantes que impiden las labores que se llevan a cabo en esta división, el personal poco capacitado y el no contar con tecnología informática especial para recolección y análisis de evidencia digital impide que muchos casos de delitos informáticos no se esclarezcan.

En El Salvador esta, es una de las divisiones que hace un mayor esfuerzo para enfrentar la ola de delitos informáticos, ***Anexo N° 9***, que se dan actualmente en el país.

c. DIVISIÓN POLICÍA TÉCNICA CIENTÍFICA

La misión de la División Técnico Científica de la Policía Nacional Civil es brindar las herramientas técnicas y/o científicas a la Policía Nacional Civil, Fiscalía General de la República, órganos de justicia y otros para el esclarecimiento de hechos delictivos, mediante la realización de análisis a evidencias ya sea recolectadas en la escena del crimen o remitidas por otras instituciones.

Principales funciones.

- Aplicar pruebas de serología forense[76] a los fluidos corporales, en colaboración de la Policía Nacional Civil, Procuraduría General de la República, Fiscalía General de la República, órgano judicial y otras del sector justicia.
- Realizar análisis físico químico sobre micro evidencias o residuos recogidos en la escena de los hechos, que aporten a la clarificación de las situaciones en investigación.
- Mantener estrecha comunicación con los juzgados, Fiscalía General de la República, Procuraduría General de la República y órgano judicial, a fin de proporcionarles cualquier ayuda que requieran para el esclarecimiento de hechos.
- Aplicar técnicas especializadas de balística[77] en la investigación de hechos criminales donde se identifique participación de armas de fuego.
- Analizar sustancias controladas para determinar su grado de pureza, así como realizar la cromatografía de gases.

[76] Para una mayor comprensión Ver apartado Glosario de Términos
[77] Para una mayor comprensión Ver apartado Glosario de Términos.

La División Técnico científica de la Policía Nacional Civil, se encarga del análisis de todo tipo de evidencias que otras divisiones policiales secuestran por el hecho de que todas las evidencias son llevadas a este lugar solicitándose un análisis que permita conocer las causas de su procedencia o utilización. Para el análisis de evidencias digitales se requiere de herramientas informáticas especiales y de recurso humano capacitado en el uso de estas y en la forma de proceder en el análisis. Esta División Policial presenta limitantes en el trato de evidencia digital[78] ya que posee poco conocimiento y aplicación de tecnología informática especializada; además entre sus funciones no contemplan aun hacer frente a los delitos informáticos que afronta el país

VI: FISCALÍA GENERAL DE LA REPÚBLICA

Otra de nuestras poblaciones es esta institución, que es la encargada de recibir denuncias de todo tipo de delitos, por lo tanto proporciona información importante para el desarrollo de nuestra investigación. Esta compuesta por las siguientes unidades especializadas para las investigaciones de los delitos.

Unidades fiscales especializadas

- Delitos de corrupción.
- Delitos de investigación financiera.
- Delitos de crimen organizado.
- Delitos de narcotráfico.
- Delitos de extorsión.
- Delitos de tráfico ilegal de personas.

[78] Fuente: Ver apartado Referencias Bibliográficas- II: Sitios Web: numerales 41 y 42.

C- CONFIABILIDAD DE LAS ENCUESTAS[79]

Para determinar la confiabilidad de las preguntas elaboradas en las encuestas para cada una de las poblaciones, se realizo previamente una "pre-encuestas" a un grupo de 20 personas con el fin de hacer observaciones tales como:

- Redacción de pregunta.
- Ambigüedad en preguntas
- Objetivos de la encuesta.
- Diseño de la encuesta.

Con los resultados obtenidos de la ***tabla N° 23*** se determino lo siguiente:

	ENCUESTA UNIVERSIDADES	ENCUESTA FISCALÍA	ENCUESTA JUECES	ENCUESTA PERITOS INFORMÁTICOS.
Objetivos de la encuesta.	7	0	0	0
Ambigüedad en preguntas.	3	0	2	1
Redacción de pregunta.	3	1	2	3
Diseño de la encuesta.	2	0	0	0

Tabla N° 23: Resultados de la pre encuesta.

Los números representan las correcciones realizadas por las personas a quienes se le ha pasado la "pre-encuesta", de esta forma se depuraron los errores y las observaciones tomadas por el grupo.

Los criterios mediante los cuales se evaluaron las preguntas de las encuestas fueron los siguientes:

Validez

La validez de una encuesta se refiere a lo *que* mide y a *cómo* lo mide. Es el grado en que un instrumento de medida mide aquello que realmente pretende medir o sirve para el propósito para el cual ha sido construido. 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.

Confiabilidad

Una pregunta es confiable si significa lo mismo para todos los que la van a responder. Se puede confiar en la redacción de una pregunta cuando produce constantemente los mismos resultados al aplicarla a sujetos similares. La confiabilidad implica consistencia el investigador debe asegurarse que

[79] Ver apartado Referencias Bibliográficas- I:Libros: numeral 15.

el tipo de persona a quien se le van a hacer las preguntas tenga la información necesaria para poder responder. El asegurar la respuesta de los que se les aplique el cuestionario redundará en resultados confiables.

El objetivo de aplicar estos criterios a las encuestas que se diseñaron fue para evitar que existieran errores en su redacción y así poder obtener la información deseada, es decir que esta evaluación de criterios nos ayudo a detectar errores que hubiesen afectado los resultados. Por tal razón se hicieron las correcciones pertinentes y así se logro el diseño del instrumento de recolección de datos que se les proporciono a las poblaciones.

Por tanto una vez aplicado estos criterios se presentan los modelos de encuestas utilizados en esta investigación, los cuales se pueden observar en el ***Anexo N° 10***.

FUENTES DE INFORMACION SECUNDARIAS

Las fuentes de información secundarias que se utilizaron para la realización de esta investigación fueron:

1. Periódicos nacionales
2. Defensoría del consumidor
3. Tesis

Revistas especializadas en la presentación de indicadores a nivel de El Salvador

D- TABULACIÓN Y ANÁLISIS

I. TABULACIÓN Y ANÁLISIS DE JUECES

A continuación se presentan las preguntas realizadas en la encuesta a los jueces junto con su objetivo, resultado y su análisis respectivo. Fueron 9 preguntas realizadas a 10 jueces del área metropolitana de San Salvador.

Pregunta: 1- ¿Ha escuchado el término de informática forense?

Objetivo: Conocer si los jueces han escuchado el término Informática Forense, cuando han participado en casos relacionados con delitos informáticos, como una herramienta utilizada para el esclarecimiento de éstos.

Criterios	**Gráfico**
Si 10 No 0 **total de encuestados:** 10	

Análisis: Todos los jueces encuestados dijeron que han escuchado sobre informática forense y revela que este tema ya está siendo abordar en el país. Esto es positivo porque indica que se está presentando la necesidad de poder contar con herramientas precisas que expliquen cómo fueron cometidos los delitos informáticos en el país. Estos delitos tienen un modo distinto de proceder y utilizan herramientas diferentes a las comúnmente conocidas. De continuar esta tendencia, los jueces podrán darse cuenta de las facilidades y beneficios que proporciona el uso de la informática forense para emplearla como una herramienta que ayude al esclarecimiento de este tipo de delitos. El uso de la informática forense da como resultado que menos casos queden en la impunidad por falta de pruebas y que puedan explicar todos los pormenores de quien, cuando y como fueron cometidos los delitos.

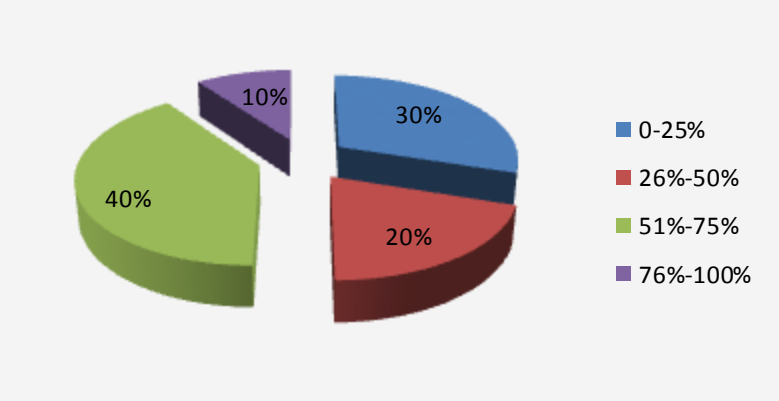
Pregunta: Representación de su conocimiento sobre informática forense

Objetivo: Determinar el grado de conocimiento que se tiene sobre la informática forense

Criterios	
0-25%	3
26%-50%	2
51%-75%	4
76%-100%	1

total de encuestados: 10

Gráfico



Análisis: El 50% de los jueces dijeron que su grado de conocimiento se encuentra entre el 51% y el 100%, en contraparte con el otro 50% que contesto que su máximo de conocimiento sobre la informática forense es de un 50%. Esto indica que el grado de conocimiento que tienen los jueces está dividido.

La mitad de los jueces encuestados poseen un nivel de conocimiento mayor en el tema, lo cual es positivo, debido a que esto les permite dictaminar quienes fueron los responsables de haber cometido un ilícito de este tipo y hacer justicia. Ya que por sus conocimientos en el tema, cuentan con un mayor criterio para poder tomar y justificar su decisión en base a las pruebas presentadas, dando como resultado el poder esclarecer los hechos de manera justa y correcta.

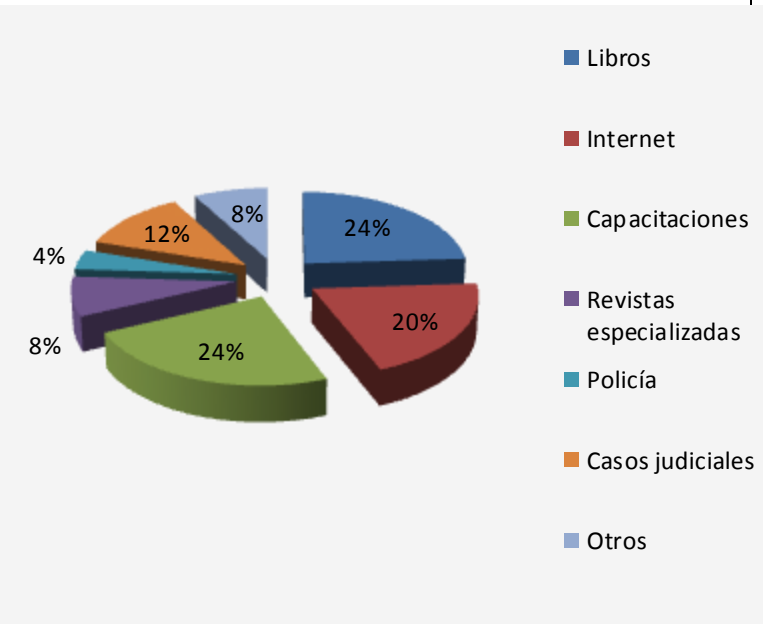
Pero esto no es suficiente ya que no son todos los jueces los que tienen conocimientos amplios acerca del uso y la credibilidad que proporciona la informática forense como herramienta para el esclarecimiento de delitos informáticos, lo cual implica que ellos pueden dudar de la validez las pruebas presentadas, impidiendo así el poder llegar a la verdad de cómo sucedieron los hechos y permitir determinar, en base al análisis de las pruebas presentadas junto con los alegatos, quien es el verdadero culpable de haber cometido los ilícitos.

Pregunta: 2- ¿Por qué medio ha escuchado de informática forense?

Objetivo: Determinar las fuentes de información por las cuales conocieron el tema y así conocer si las razones son autodidactas, capacitaciones en sus lugares de trabajo, si son fuentes nacionales o internaciones para poder ver si en el país se aborda este tema.

Criterios	
Libros	6
Internet	5
Capacitaciones	6
Revistas especializadas	2
Policía	1
Casos judiciales	3
Otros	2
total de encuestados:	10

Gráfico



Análisis: Los resultados de esta pregunta son positivos ya que muestran que el 24 % del conocimiento que tienen aquellos jueces que han enfrentado algún proceso judicial referente a delitos informáticos, ha sido adquirido a través de capacitaciones, lo que muestra el interés, por parte de la institución en la cual laboran o por iniciativa personal, por conocer este tema que les permitan esclarecer los delitos informáticos e implica que están reconociendo el crecimiento y la necesidad de enfrentar este tipo de delitos en el país. Ya que al ver la necesidad de las capacitaciones, indican que si se están preocupando por saber cómo esclarecer este tipo de delitos para evitar la impunidad en este tipo de casos.

Otra fuente de información predominante, con un 24% también, fue el conocimiento a través de los libros, esto quiere decir que los jueces se están autocapacitando y buscando literatura para conocer un poco más sobre este tema y así poder tener un criterio correcto para concluir un juicio y dictaminar quienes son los verdaderos responsables de los delitos. Permitiendo así que menos casos queden impunes por la falta de pruebas.

Como segunda fuente de información, con un 20%, se tiene que el conocimiento fue adquirido por medio de internet, lo cual es positivo, ya que indica que más jueces se están interesando en el tema y están buscando información no solo sobre su teoría y en nuestro entorno; sino también conocer la opinión de otros países con respecto a este tema, ver como se percibe o entiende a la informática forense a nivel internacional. Ayudando así a que ellos admitan el uso de la informática forense en los juicios y reconozcan su utilización en la explicación de cómo fueron cometidos los delitos.

En tercer lugar con un 12%, se tiene que los jueces respondieron que fue a través de casos judiciales, esto implica que se está conociendo el tema a través de casos reales en los cuales ha sido utilizada la informática forense, lo cual indica que ya esta siendo utilizada durante los juicios por este tipo de delitos y de seguir con esta tendencia se podrán esclarecer con mayor facilidad y precisión como se realizan este tipo de delitos ayudando a su pronta resolución, haciendo justicia al dictaminar quienes

son los responsables del hecho y disminuyendo la impunidad en este tipo de delitos en el país.
El 8%, está dividida entre revistas especializadas y través de otros medios como por ejemplo el hablar con personas que están inmersas en la informática forense. Lo cual indica una desventaja, ya que no existe mucha literatura acerca de este tema en el país, impidiendo el poder conocer como ésta puede ser una herramienta valida y útil en la investigación de este tipo de delito, porque éstos afectan a toda la sociedad en general debido al auge que está teniendo en el país por la era digital en la cual estamos inmersos y los cambios que ésta genera en las nuevas formas de comercialización y transacciones en general.
Como quinta fuente de conocimiento tenemos a la policía con un 4%, esto es beneficioso porque es la policía los que la utilizan y saben su funcionamiento brindándoles a los jueces conocimientos, con bases reales y solidas, de que es la informática forense, para que ellos puedan determinar si el imputado es responsable o no de haber cometido el delito dentro de un juicio, dando como consecuencia el esclarecimiento y evitando la impunidad de éstos. Ya que si no conocen la seriedad y las facilidades que ofrece el análisis presentado de la evidencia digital procesada por la informática forense o como interpretar la evidencia que la policía les proporciona, no podrán hacer justicia dejando libres a los culpables y acusando a inocentes, fomentando aun más la impunidad. Pero esto no es representativo ya que es el porcentaje menor el que dice conocer del tema a través de la policía, lo cual refleja que entre los jueces y policía aun no están compartiendo conocimientos que les permitan a ambas partes realizar mejor su trabajo, el cual es aclarar como se realiza este tipo de delitos en el país y quienes son los responsables. Y como conclusión se tiene que las fuentes de información por las cuales están recibiendo los conocimientos los jueces son confiables ya que tanto las capacitación como los libros son elaborados por personas expertas en el tema que proporcionan bases solidas para justificar y demostrar el beneficio que se tiene al utilizar la informática forense en el análisis de la evidencia digital.

Pregunta: 3- ¿Ha escuchado hablar sobre evidencia digital o prueba científica?

Objetivo: Conocer si los jueces han escuchado el término evidencia digital o prueba científica, cuando han participado en casos relacionados con delitos informáticos y éstas han servido como prueba de estos crímenes.

Criterios	**Gráfico**
Si 10 No 0 **total de encuestados:** 10	

Análisis: Todos de los jueces han escuchado hablar de evidencia digital o prueba científica, esto es un elemento positivo ya que el hablar de este tipo de evidencia, no se genera incertidumbre. Además trae como consecuencia que los jueces posean conocimiento sobre el objetivo y la función que este tipo de evidencia tiene, ya que cuando se cometen delitos informáticos, implica que hay de por medio el uso de medios electrónicos y los registros que se almacenan en estos dispositivos son las pruebas en el momento de comprobar cómo, quién y cuándo fue realizado un ilícito. Este conocimiento les brinda a ellos la posibilidad de poder aceptar la presentación de evidencias digitales como prueba en los juicios porque saben la información que ésta contiene y como puede ayudar aclarar un caso de este tipo evitando así que este tipo de delitos quede sin resolver por falta de pruebas.

Pregunta: 4- Según su experiencia y conocimiento. ¿Considera la evidencia digital o prueba científica confiable y válida para el esclarecimiento y resolución de casos por delitos informáticos?

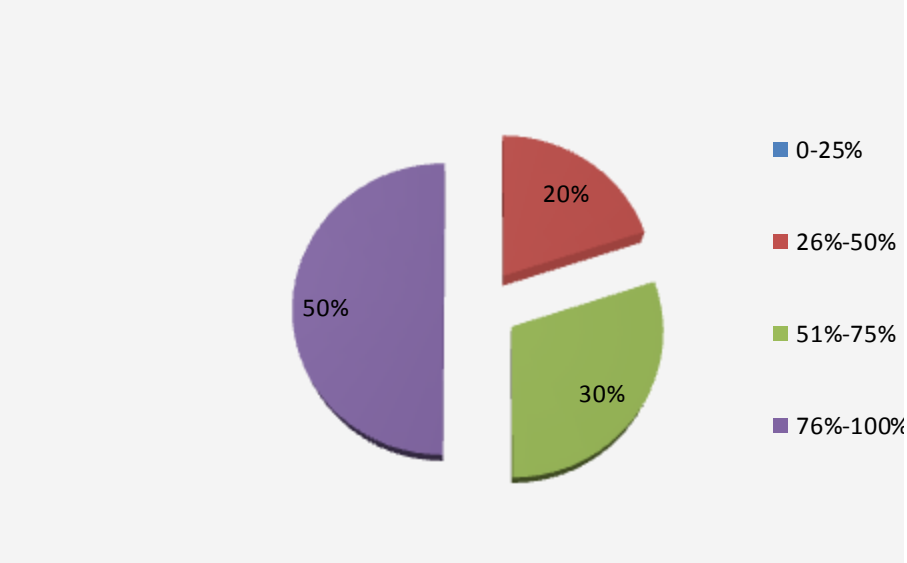
Objetivo: Conocer si para los jueces es confiable y valida la evidencia digital como una herramienta utilizada para el esclarecimiento de los delitos informáticos.

Criterios	**Gráfico**
Si 10 No 0 **total de encuestados:** 10	

Análisis: Todos los jueces afirmaron que la evidencia digital es confiable, esto es beneficioso en un proceso judicial ya que permite el esclarecimiento de este tipo de delitos informáticos. Además es favorable porque son los responsables de juzgar entre otras cosas, las evidencias que se admiten y las que no, aceptarían la presentación de esta evidencia como parte de las pruebas que explican cómo sucedieron los ilícitos, porque sabrían la validez y la confiabilidad que ésta representa, ayudando así en la demostración de cómo sucedieron los hechos y brindándoles a los jueces más criterios para promulgar el veredicto, sentenciando a quienes realmente son los responsables de éstos con mayor precisión y confiabilidad, fomentando así un mayor uso de esta evidencia en estos tipos de casos, otorgándole credibilidad a este tipo de evidencia y evitando que más delitos queden sin resolver por falta de las pruebas necesarias para llegar al esclarecimiento de los hechos y permitiendo llegar a la fase de sentencia evitando la impunidad.

Pregunta: Si su respuesta es si, marque la casilla que mejor represente su consideración sobre la confiabilidad y validez en la evidencia digital.

Objetivo: Establecer el grado de confianza y credibilidad con la que cuenta la evidencia digital desde el punto de vista de los jueces en un juicio y así poder medir el grado de aceptación de ésta

Criterios		Gráfico
0-25%	0	
26%-50%	2	
51%-75%	3	
76%-100%	5	
total de encuestados:	10	

Análisis: La mitad de los jueces encuestados manifestó que el nivel de confianza que tienen sobre la evidencia digital está entre un 26% a un 75%, esto indica que si bien se considera valida a ésta y se confía en ella en un 75%, no es suficiente, ya que en este rango existen jueces que consideran que solo se puede confiar en ella en un 50% o menos. Reflejando que el nivel de confianza no es suficiente para que ellos puedan tomar una decisión, llegar a un veredicto final y determinar quiénes son los responsables de haber cometido un delito basándose en esta evidencia, evitando el pronto esclarecimiento de éstos y generando mayor impunidad por este tipo de casos.

La otra mitad dijo que confían en la evidencia digital entre un 76% a un 100%, esto refleja que si se considera a la evidencia digital una prueba válida que puede explicar cómo se cometió un delito de este tipo ayudando en gran manera a reducir el tiempo empleado en la resolución de un juicio y permitiendo tener las bases necesarias a la hora de emitir una sentencia justa para la persona involucrada. Dando como resultado que más casos se resuelven satisfactoriamente, ya que mientas más casos de este tipo se resuelven, menor serán los índices de impunidad que existan en el país con respecto a estos delitos.

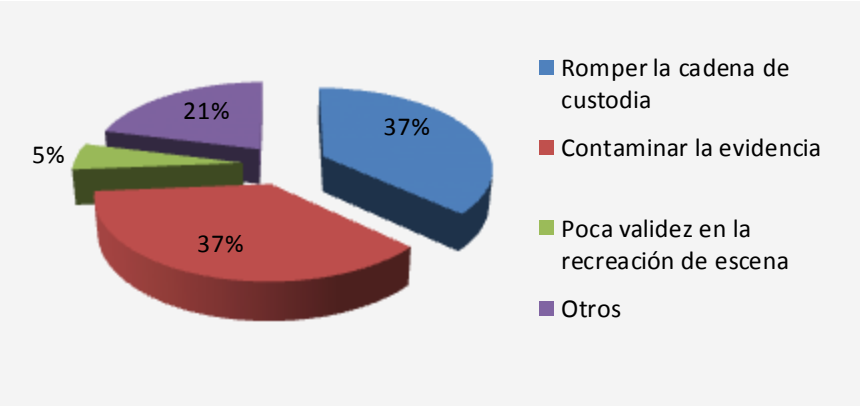
Como se puede apreciar, el nivel de confianza en la evidencia digital esta dividido, un 50% dice que su nivel de confianza puede llegar hasta un 100%, pero el otro 50% dice que lo más que confían en ella es en un 75%, esto tiene como consecuencia que siempre existirían casos que queden sin resolver porque no siempre se confiaría en este tipo de evidencia para aclarar los hechos, perjudicando a que los casos se resuelvan correctamente y provocando que estos delitos sigan ocurriendo en el país sin poder detenerlos.

Pregunta: 5- ¿Qué factores considera que hacen inválida la confiabilidad y la validez de la evidencia digital en un juicio?

Objetivo: Averiguar cuáles son los errores que se cometen a la hora de la recolección de la evidencia digital que la hacen inválida, poder indicar cuáles son las debilidades y proponer mejoras en la recolección de ésta a la entidad responsable de esta labor.

Criterios	
Romper la cadena de custodia	7
Contaminar la evidencia	7
Poca validez en la recreación de escena	1
Otros	4
total de encuestados:	10

Gráfico



Análisis: El resultado de esta pregunta muestra que existen dos elementos influyentes que provocan la invalidez de la evidencia digital presentada durante un juicio, el romper la cadena de custodia con el 37% y la contaminación de la evidencia con 37% también. Esto indica que la confiabilidad por parte de los jueces se ve disminuida por los errores que se comenten a la hora de hacer el levantamiento de la escena del crimen y la recolección de la evidencia, generando dudas sobre su validez y hasta que sea eliminada como prueba en el juicio. Como consecuencia se tiene que al no tener confianza en la evidencia presentada, no serán aceptadas, por parte del juez, las explicaciones que se le proporcionen de cómo fueron cometidos los hechos y los posibles responsables de éstos, el caso no podrá esclarecerse ya que los jueces desestimarían la evidencia digital como un elemento que ayude a presentar la verdad y dar un veredicto justo al respecto, ocasionando impunidad y dejando sin castigo a los verdaderos culpables de haber cometido el ilícito.

Existen otros elementos que interfieren con la confiabilidad, viéndose reflejado con el 21% los cuales son:

- Peritos o expertos informáticos no idóneos para desarrollar una tarea determinada.
- Falta de experiencia en un determinado delito informático.
- Facilidad de alteración de la evidencia.

Esto impide que los casos se resuelvan en el menor tiempo posible generando aglomeración de este tipo de juicios en los juzgados y permitiendo mientras tanto que más delincuentes sigan cometiendo esa clase de fechorías afectando a toda la sociedad salvadoreña en general. Ya que a criterio de los jueces, estos elementos no proporcionan los criterios necesarios que les permitan tener una visión clara de los hechos y por lo tanto no se podría hacer justicia para las personas involucradas y permitiendo enjuiciar a inocentes, dejando libres a los verdaderos delincuentes.

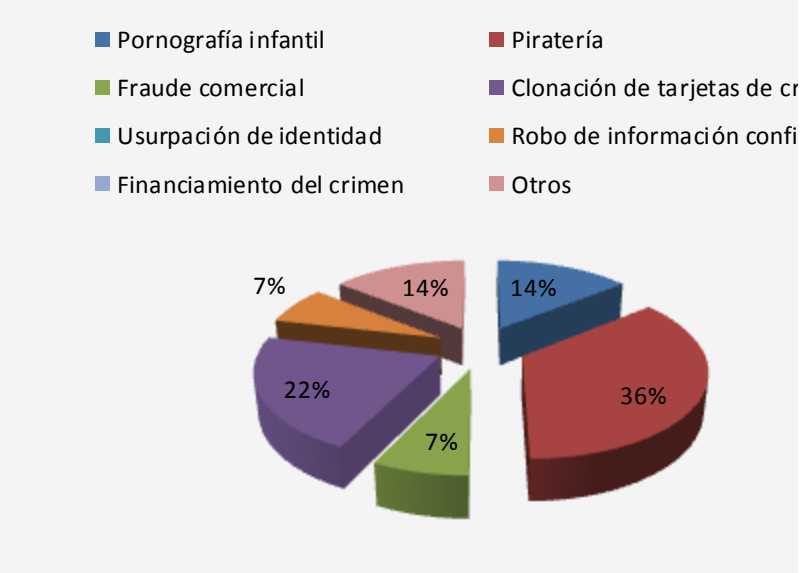
La recreación de la escena está considerada con el 5%, y aunque este no es un factor predominante si es considerado como factor que invalida la evidencia pero en menor grado, ya que si no se hace una correcta recreación de la escena del crimen, las demostraciones presentadas al juez de cómo sucedieron los eventos, no serán lo suficientemente convincentes para justificar como se realizo el delito y persuadir al juez que la explicación brindada es la correcta en base a la evidencia presentada, provocando que todo el trabajo realizado sea descartado impidiendo el esclarecimiento de los hechos y el castigo para los responsables que los realizaron. Ya que si el juez no encuentra razones suficientes para enjuiciar a un imputado, queda en libertad y sin la posibilidad de poder conocer si realmente es inocente o es culpables de los cargos, ayudando al fomento de la impunidad por este tipo de delitos en el país.

Pregunta: 6- Según su experiencia y conocimiento. ¿Qué tipo de delitos informáticos ocurren con mayor frecuencia en el país?

Objetivo: Saber cuáles delitos informáticos son los que se cometen en el país para poder determinar que herramientas de informática forense serian las recomendadas para esclarecerlos.

Criterios	
Pornografía infantil	4
Piratería	10
Fraude comercial	2
Clonación de tarjetas de crédito	6
Usurpación de identidad	0
Robo de información confidencial	2
Financiamiento del crimen	0
Otros	4
total de encuestados:	10

Gráfico



Análisis: La piratería es el delito que ocurre con mayor frecuencia en el país según la opinión de los jueces encuestados con un 36%, todos los jueces encuestados la mencionaron y esto es comprobado diariamente en la sociedad salvadoreña.

En segundo lugar se encuentra la clonación de tarjetas de crédito con un 22% este dato se puede observar con los datos obtenidos con la Defensoría del consumidor, ***Anexo N° 3,*** donde se muestra la cantidad de personas estafadas y con reporte de clonación de tarjeta de crédito.

La encuesta revela que la pornografía infantil tiene un 14% según los jueces, esto es alarmante porque indica que este tipo de delitos es uno de los más comunes en el país, y se están quebrantando las leyes que existen para la protección de los menores debido a que este tipo de delito si está tipificado en las leyes salvadoreñas, dando como resultado que exista una mayor violación a los derechos que tiene los niños, su dignidad y su infancia.

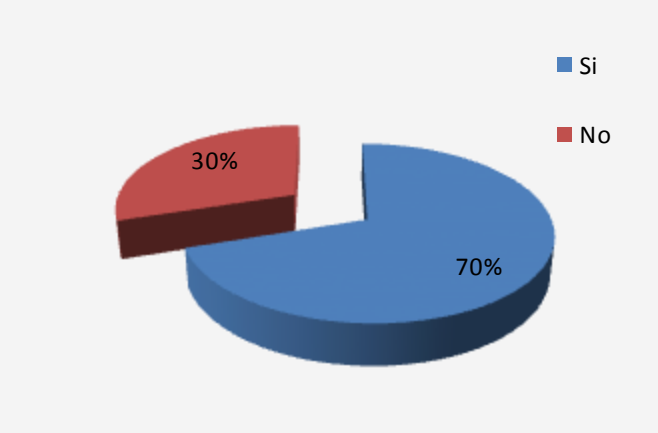
El otro 14% respondió que existen otros tipos de delitos que suceden con mayor frecuencia en el país como lo son: Información sustraída sin permiso, Estafa electrónica y Hurto electrónico.

El robo de información confidencial y el fraude comercial poseen el 7% encontrándose como uno de los más bajos según la encuesta.

Todo esto refleja que en el país, sin tomar en cuenta el porcentaje que representa cada delito, existen una gran cantidad de delitos informáticos que se comenten diariamente y que si no se trabaja en su erradicación, esto podría salirse de control, provocando que la sociedad se vea afectada en todos los sentidos y evitando que el país pueda defenderse ante este tipo de ataque que la era digital trae consigo, porque mientras más pasa el tiempo los delincuentes buscan y encuentran nuevas formas de realizar estos delitos, nuevas técnicas o herramientas para cometerlos y sin dejar el menor rastro posible.

Pregunta: 7- ¿Considera que existen vacíos en las leyes salvadoreñas que impiden el esclarecimiento de un caso por delitos informáticos?

Objetivo: Conocer desde el punto de vista de jueces, si existen vacios en las leyes que pueden provocar que juicios donde se involucran delitos informáticos lleguen a quedar impunes y conocer si existen leyes que amparen el uso de la informática forense.

Criterios	**Gráfico**
Si 7 No 3 **total de encuestados:** 10	

Análisis: El 70% de los jueces encuestados consideran que existen vacios en las leyes actuales de nuestro país, esto refleja que aun los mismos legisladores reconocen que las leyes no se han adecuado a las nuevas formas de proceder y tecnologías por medio de las cuales se pueden cometer delitos informáticos hoy en día.

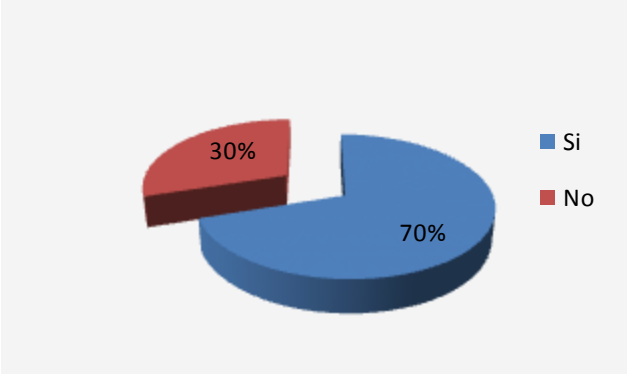
Al no existir leyes en particular que castiguen a los delitos informáticos, esto acarrea como consecuencia que puedan quedar impunes ya que si no están tipificados dentro de las leyes como figura de un delito como tal, los jueces no podrán aplicar la ley, ya que no se podría enjuiciar a estos delincuentes por no estar contempladas estas conductas como delitos y permitir ser penalizados ante la justicia, fomentando así la impunidad y permitiendo actuar al delincuente sin restricciones cometiendo el delito ya que no existiría manera de comprobar que su actuar es de un delincuente.

El 30% restante de los encuestados, opinan que las leyes actuales son suficiente para poder castigar todo tipo de delitos incluyendo a los que involucra delitos informáticos. Esto indica que hay jueces que tiene poco interés en el tema, aun no advierten la diferencia ni las consecuencias que generan los tipos de delitos comunes y los informáticos, implicando a que estos últimos sean tratados como los demás y permitiendo la impunidad ya que el modo de proceder de los delincuentes y las evidencias son diferentes al resto de delitos que existen en nuestro país. Si no se cuenta con un marco legal que los regule no se podrá hacer nada para evitarlos.

Este resultado muestra la necesidad que existe de fortalecer la legislación de nuestro país, para poder brindarles a los jueces el respaldo legal y las herramientas necesarias para poder enjuiciar a estos delincuentes, el poder hacer justicia ante este tipo de amenazas y poder actuar frente a la nueva forma de operar de los delincuentes.

Pregunta: 8- ¿Cree necesario realizar reformas al código penal para que contemple artículos relacionados con delitos informáticos?

Objetivo: Determinar que tan importante y necesario consideran los jueces el fortalecer las leyes para proteger a la sociedad salvadoreña contra delitos informáticos, para conocer en un futuro si existiría un marco legal que reconozca a esta clase de delitos en el código penal y así poder contemplar a la informática forense como una herramienta de apoyo valida en el esclarecimiento de éstos.

Criterios	**Gráfico**
Si 7 No 3 **total de encuestados:** 10	

Análisis: La mayoría de los jueces encuestados, el 70% del total, opina que es necesario hacer reformas al código penal para fortalecer las leyes e incluir a los delitos informáticos, tipificándolos como tales dentro de éste lo más pronto posible, de esta forma permitirá que los Agentes de la ley, Fiscales y jueces cuenten con un respaldo legal que los ampare para realizar sus funciones, haciendo más difícil que un crimen quede sin castigo. La creación de reformas a las leyes permitirían tener un marco legal que se acople a la realidad de nuestro país y poder así proceder contra este tipo de delincuentes evitando que continúe el aumento de personas que se ven afectadas por este tipo de delitos, utilizando a la informática forense para descubrir cuáles son los grupos o personas responsables de cometer este tipo de crímenes.

El 30% de los jueces encuestados, manifestaron que no creen necesario realizar reformas al código penal con respecto a los delitos informáticos, pues opinan que la ley contempla la libertad probatoria y por lo tanto al tener los medios necesarios para analizar la evidencia y la realización de una buena investigación, estos hechos se pueden esclarecer. Estas respuestas perjudican el desempeño a futuro de los fiscales así como de la policía sin una ley que respalde sus acciones.

Pregunta: 9- ¿Conoce si se están realizando reformas en el código penal para enfrentar casos por delitos informáticos?

Objetivo: Saber si actualmente se ha considerado, por parte de las autoridades respectivas, el tipificar a los delitos informáticos dentro del código penal como un nuevo tipo de delito en el país.

Criterios	**Gráfico**
Si 0 No 10 **total de encuestados:** 10	

Análisis: Esta encuesta revela que el 100% de los jueces encuestados tiene desconocimiento en la elaboración de leyes, ratificación de leyes, proyectos de ley o si se están realizando modificaciones al código penal, este es un elemento preocupante porque al no ser tipificados estos delitos, existe la posibilidad que los que realizan delitos informáticos logren salir de los cargos levantados por tecnicismo de las leyes.

Para ver las tabulaciones de las poblaciones ver CD apartado TABULACION DE DATOS.

E- ANÁLISIS GENERAL PARA CADA POBLACIÓN

I. ANÁLISIS GENERAL PARA LA POBLACIÓN DE JUECES

Tomando como base los resultados obtenidos por la encuesta distribuida entre 10 jueces, todos manifestaron conocer el termino Informática forense, lo cual indica que en nuestro país ya se empieza abordar este tema a nivel del Órgano Judicial.

El mayor grado de conocimiento que manifestaron tener los jueces en el tema es de un 51 a un 75%, lo cual indica que por sus conocimientos en el tema, cuentan con un mayor criterio para poder tomar y justificar su decisión de admitir o no la evidencia digital, como parte de las pruebas incriminatorias de un delito y el análisis que la informática forense realiza sobre la evidencia digital recolectada. Debido a que conocen cual es el objetivo de la informática forense y su funcionamiento.

Si bien este grado de conocimiento proporciona elementos que ayudan al juez a realizar mejor su función de administrar la justicia y decidir el destino de un acusado en base a las pruebas presentadas, esto no es suficiente, ya que menos de la mitad manifestaron que poseen este conocimiento, solo el 40% del total, lo cual indica que la mayoría de jueces aun no tienen entendimientos amplios acerca del uso y la credibilidad que proporciona la informática forense, esto puede hacer dudar de la validez del análisis presentado, desechándolo e impidiendo el poder explicar, desde el punto de vista informático, como fueron realizados los delitos. Si bien es cierto que poseen un alto grado de conocimiento, este no es suficiente porque son una minoría los que dice tener este grado de conocimiento.

Las dos principales fuentes de información por las cuales los jueces han conocido sobre el tema es a través de libros y capacitaciones, lo cual es positivo porque éstas son fuentes de información formales que permiten brindarles conocimientos con bases solidas y confiables sobre la informática forense, debido a que son expertos en el tema los encargados de elaborar este tipo de contenido, permitiéndoles a los jueces darse cuenta de las facilidades y beneficios que proporciona el uso de la informática forense al emplearla como una herramienta que ayude al esclarecimiento de este tipo de delitos. Además indica que se está reconociendo el crecimiento de los delitos informáticos en el país, el interés por parte de la institución en la cual laboran o por iniciativa personal por conocer acerca del tema y la necesidad que existe de enfrentarlos con las herramientas informáticas necesarias para su comprobación.

Al hablar de informática forense está inmerso el termino evidencia digital, ya que se utiliza a la informática forense como una herramienta para su análisis, y esto se comprueba porque en las respuesta de las encuestas pasadas a los jueces, todos dijeron conocer este término. Esto es un elemento positivo ya que el hablar de este tipo de evidencia, no se genera incertidumbre. Además trae como consecuencia que los jueces posean conocimiento sobre la función que este tipo de evidencia tiene en particular, ya que cuando se cometen delitos informáticos, implica que hay de por medio el uso de medios electrónicos y los registros que se almacenan en estos dispositivos son las pruebas en el momento de comprobar cómo, quién y cuándo fue realizado un ilícito. Este conocimiento les brinda la posibilidad de poder aceptar la presentación de evidencias digitales como prueba en los juicios porque comprenden la información que ésta contiene y como puede ayudar aclarar un caso de este tipo.

Además todos manifestaron que la evidencia digital si es confiable para ser presentada en un juicio, lo cual es beneficioso porque son ellos los responsables de juzgar, entre otras cosas, las evidencias que se admiten y las que no, fomentando así un mayor uso de esta evidencia en estos tipos de casos, otorgándole mayor credibilidad y evitando que más delitos queden sin resolver por falta de las pruebas necesarias que los comprueben.

Pero el nivel de confianza que manifestaron tener en la evidencia digital no es suficiente. Esto indica que si bien el término es conocido, se considera válida a ésta y se confía en ella, ésta no es suficientemente confiable para ellos, ya que solo la mitad manifestó que confían en ella un máximo de 75%. Esto tiene como consecuencia la existencia de casos que queden sin resolver porque no se confía en este tipo de evidencia para aclarar los hechos, perjudicando a que los casos se resuelvan correctamente y provocando que estos delitos sigan ocurriendo en el país sin poder detenerlos.

La razón por las cuales ellos desestiman la credibilidad de la evidencia digital es porque la consideran una evidencia muy fácil de manipular y en la cual es muy difícil determinar, a su criterio, si ésta ha sido contaminada o no previamente. Debido a que para los jueces las dos principales causas por las cuales una evidencia puede quedar invalida son el romper la cadena de custodia y la contaminación de la evidencia digital, ya que al romper la cadena de custodia automáticamente se asume que la evidencia fue contaminada quedando invalida para ser utilizada como prueba del delito en un juicio.

Por su experiencia, todos los jueces encuestados dijeron que el delito que ocurre con mayor frecuencia en el país es la piratería y esto es comprobado diariamente en la sociedad salvadoreña. Lo cual refleja que en el país, independientemente del tipo de delito informático que se estudie, existen una gran cantidad de ellos que se comenten diariamente y que si no se trabaja en su erradicación, esto podría salirse de control, provocando que la sociedad se vea afectada en todos los sentidos y evitando que el país pueda defenderse ante este tipo de ataque que la era digital trae consigo, porque mientas más pasa el tiempo los delincuentes buscan y encuentran nuevas formas de realizar estos delitos, nuevas técnicas o herramientas para cometerlos y sin dejar el menor rastro posible.

Además sin leyes que castiguen a estos delitos, la realización de ellos en el país irá en aumento, y esto está respaldado con las respuesta obtenidas por parte de los jueces en el cual, la mayoría admitieron que si existen vacios en nuestras leyes para poder hacerle enfrente a este tipo de delito en el país y también admitieron que es necesario hacer reformas al código penal para incluir a los delitos informáticos, tipificándolos como tales dentro de éste lo más pronto posible ya que si no están tipificadas estas conductas dentro del código penal como delitos, lo jueces no podrán aplicar la ley.

Al mismo tiempo estas reformas permitirán que los Agentes policiales, Fiscales y Jueces cuenten con un respaldo legal que los ampare a la hora de realizar sus funciones, haciendo más difícil que un crimen quede sin castigo.

Esto refleja que aun los mismos legisladores reconocen que las leyes no se han adecuado a las nuevas formas de proceder y tecnologías por medio de las cuales se pueden cometer delitos informáticos hoy en día.

La creación de reformas a las leyes permitirían tener un marco legal que se acople a la realidad de nuestro país y poder así proceder contra este tipo de delincuentes evitando que estos casos queden impunes y que continúe el aumento de personas que se ven afectadas por este tipo de delitos, utilizando a la informática forense para evitar que éstos queden sin resolverse por falta de pruebas de índole digital.

Desafortunadamente todos los jueces dijeron que no conocen si se están llevando a cabo este tipo de reformas a las leyes de nuestro país. Este es un elemento preocupante porque al no ser tipificados estos delitos ni crear leyes especificas para ellos, existe la posibilidad que los delincuentes informáticos logren salir libre de los cargos por tecnicismo y vacios de las leyes. Además refleja el poco interés que tiene el órgano legislativo por promulgar leyes contra este tipo de delitos y tratar de disminuir el índice de ocurrencia y la impunidad de estos en el país.

II. ANÁLISIS GENERAL PARA LA POBLACIÓN DE ABOGADOS

Los resultados obtenidos por la encuesta distribuida entre 96 abogados, reflejaron que ellos si conocen el termino de informática forense, aunque no todos aun, ya que solo el 60% de ellos manifestó haber escuchado antes sobre este término. Pero aunque la mayoría conoce, esto no es suficiente, ya que aun existen abogados que no saben sobre su existencia, su función y el objetivo de ésta. Si bien han escuchado del tema, el grado de conocimiento que dicen tener por parte de la mayoría de los abogados es limitado, porque seleccionaron que su conocimiento se encuentra entre el 0% al 25%. Lo cual indica un problema porque no solo basta con tener conocimientos básicos del tema sino una comprensión amplia y con exactitud de cómo funciona para poder utilizar el informe generado por la informática forense correctamente. Además esta falta de conocimiento hace que el resto de abogados, desconfíen y no admitan la utilización de esta herramienta, desconocida para ellos, en un juicio, a la hora de presentar el informe proporcionado por la informática forense como evidencia. Aunque esto les beneficia a los abogados en su misión de defender a un imputado, si éste es culpable de los delitos, impediría el esclarecimiento de ellos y dará paso a la impunidad de este tipo de casos.

La mayor fuente de información que utilizan los abogados para adquirir sus conocimientos es a través de Internet, si bien este medio presenta aspectos positivos también los tiene negativos. Dentro de los positivos se encuentran:

- La iniciativa por conocer el tema de manera autodidacta, lo cual refleja el interés que está surgiendo en los abogados por conocer sobre informática forense.
- Además les permite no solo saber la teoría acerca de este tema sino también interaccionar con personas de otros países y poder conocer como ellos la utilizan y aplican en su sistema judicial para esclarecer los delitos informáticos.
- También les permite tener un marco de referencia de cómo podría ser la incorporación de ésta en nuestro país y su funcionamiento, permitiéndoles conocer cuáles son los inconvenientes y errores que otros países han experimentado y tratar de evitarlos en nuestro sistema judicial fomentando el esclarecimiento de este tipo de delitos.

Pero dentro de los aspectos negativos que presenta esta fuente de información se encuentra:

Que este medio de información no es el idóneo ni formal para transmitir este tipo de conocimiento, ya que no existe nadie que regule que información es presentada en internet y cual no, además de que no se puede garantizar que los autores de esos artículos escritos, son los idóneos para hablar sobre el tema por ser expertos en la materia.

El hablar sobre informática forense supone ya el conocimiento sobre el término evidencia digital, debido a que el análisis realizado por la informática forense se basa en la evidencia digital, y esto se

comprueba porque en la respuesta de las encuestas pasadas a los abogados, la mayoría admitió conocer este término.

La mayoría de los abogados que conocen sobre evidencia digital manifestaron que ésta es confiable para ser utilizada en el esclarecimiento de delitos informáticos, porque entienden la clase de información que ésta contiene, indicando la aceptación por parte de ellos de la presentación y uso de esta evidencia como parte de las pruebas que explican cómo sucedieron los ilícitos, ayudando a esclarecer los hechos y señalando quienes son los responsables de haberlo cometido con mayor precisión y confiabilidad, fomentando así un mayor uso de la evidencia digital en estos casos, otorgándole credibilidad a este tipo de evidencia y evitando que más delitos queden sin resolver por falta de pruebas.

Si bien la mayoría de los abogados acepto conocer sobre evidencia digital y aseguro que si es confiable para ser utilizada en un juicio, el nivel de confianza que ellos revelan que tienen sobre la evidencia digital se encuentra divido. Un 51% dice que su nivel de confianza puede llegar hasta un 100%, pero el otro 49% dice que lo más que confían en ella es en un 50%, esto trae como consecuencia un gran problema, porque entonces siempre existirán casos que queden sin resolver debido a que el nivel de confianza reflejado demuestra que no es lo suficiente para que los abogados opten por su uso a la hora de explicar cómo sucedieron los hechos y establecer quiénes son los responsables del delito, basándose en dicha evidencia. Perjudicando a que los casos se resuelvan correctamente y provocando que estos delitos sigan ocurriendo en el país sin poder detenerlos.

Las razones por los cuales los abogados dijeron no confiar en la evidencia digital es porque la consideran una prueba fácil de manipular y en la cual no se puede detectar a simple vista si ha sido contaminada o no por alguna persona. Esto se debe a que para los abogados los dos elementos influyentes que provocan la invalidez de la evidencia digital son el romper la cadena de custodia y la contaminación de la evidencia. Esto indica que por los errores que se comenten a la hora de la recolección de la evidencia la confianza se vea disminuida provocando incertidumbre sobre su validez por parte del abogado para decidir su utilización y también por las demás partes involucradas en el juicio. Impidiendo que los casos se esclarezcan en el menor tiempo posible, causando aglomeración de éstos en los juzgados y mientras tanto se les brinda a otros delincuentes la oportunidad de seguir infringiendo la ley y afectando a la sociedad salvadoreña en general.

El delito informático que ocurre con mayor frecuencia en el país desde el punto de vista de los abogados es La piratería y esto es una realidad que se ve constantemente en cualquier punto de país con la venta de toda clase de información copiada de los programas originales. Actualmente en El Salvador se registra una gran proliferación de este tipo de delitos informáticos, los cuales diariamente ocurren en nuestro país. Y si no se empieza a trabaja en su disminución y su posterior erradicación estos delitos seguirán afectando a toda la población en general sin que exista forma de cómo hacerle frente para evitarlos, y se tiene que tomar las medidas necesarios lo más pronto posible porque mientas el tiempo avanza así van avanzando los conocimientos que los delincuentes van adquiriendo para cometer nuevas clases de delitos o nuevos medios para realizarlos, buscando nuevas tecnologías, formas y herramientas que les permitan la realización de este tipo de delitos sin dejar el menor rastro posible para evitar ser detectados.

La propagación de este tipo de delitos en el país se debe a las debilidades que actualmente nuestras leyes adolecen. Lo cual es corroborado por los abogados que participaron en el estudio, ya que la mayoría respondió que si existen vacios en las leyes actuales de nuestro país con respecto a los delitos informáticos, lo cual impide sancionar al delincuente, porque no existen leyes específicas que aborden y tipifiquen estas conductas ilícitas como delitos. Este resultado muestra que los abogados si reconocen la necesidad que existe de fortalecer la legislación de nuestro país, para poder actuar ante

la nueva forma de operar de los delincuentes y así evitar que este tipo de delitos sigan ocurriendo en el país. Además reconocieron que se necesita hacer reformas al código penal para que contemple la tipificación de los delitos informáticos como tales dentro de éste lo más pronto posible ya que la tecnología va a pasos agigantados y no así las leyes salvadoreñas que no cambian y no se acoplan tan rápido, ni con tanta facilidad a los nuevo cambios y tampoco están preparadas para hacerle frente a la nueva forma de operar de los delincuentes informáticos.

Ya que al no haber una legislación específica que diga que conductas se consideran delitos y cuáles no, es posible que no se pueda enjuiciar a un delincuente solo por tecnicismo de la ley que los ampare por no considerar a esta conducta como delito solo por no estar contemplada en el código penal actual, dando como resultado que los delincuentes queden en libertad por no comprobárseles que han cometido algún delito.

Lastimosamente solo una minoría manifestó conocer que se están realizando reformas al código penal, la mayor parte de los abogados dice desconocer si se están elaborando. Este es un elemento preocupante porque al no estar tipificados estos delitos dentro del código penal, existe la posibilidad que los delincuentes informáticos logren salir libres por tecnicismo de las leyes, generando un problema, ya que la ley no puede enjuiciar dos veces a una persona por el mismo delito, es decir, que cuando alguien quebranta la ley de alguna forma y sale absuelto de los cargos, no puede atribuírsele el mismo delito otra vez. Además esto refleja el poco interés que tiene las autoridades judiciales por crear mecanismos y leyes que permitan el esclarecimiento de este tipo de delitos en el país, ya que sin las leyes necesarias que dictaminen como se debe proceder para enjuiciar a los delincuentes informáticos, estos quedarían libres, permitiendo así el poder continuar con sus actos ilícitos y generando mayor impunidad por este tipo de delito en el país.

III. ANÁLISIS GENERAL PARA LA POBLACIÓN DE PERITOS INFORMÁTICOS NACIONALES

Se obtuvieron tres respuestas de peritos nacionales el cuál involucra el conocimiento de un elemento de la Asociación de Ciencias Forenses de El Salvador ACFES, un elemento de la INTERPOL y un profesional que realiza peritajes en la Corte Suprema de Justica.

Los involucrados en la encuesta conocen el término de informática forense, pero solo uno de ellos muestra que su conocimiento esta en el rango de 76% al 100%, si bien es cierto que esto es favorable para las investigaciones donde se involucra evidencia digital, debido que es una ciencia nueva en El Salvador y le permite al experto informático hacer uso de estándares de tratamiento de evidencia digital, uso de herramientas que se acoplen a las necesidades del momento para apoyar el desarrollo de casos en los cuales se requieran. Esto no es suficiente ya que aun son muy pocos los peritos informáticos que existen en el país y que poseen conocimientos con bases solidas en el tema, evitando que se pueda realizar, con la evidencia digital que el fiscal manda, el análisis correcto respectivo a cada evidencia u ocupar herramientas más idóneas en base a su experiencia para la realización de dicho análisis. Y así poder entregarle al Fiscal el análisis requerido para poder presentarlo como prueba en un juicio.

El desarrollo profesional que han tenido los peritos informáticos ha sido a través de capacitaciones fuera del país lo cual es un aspecto negativo. El no tener una institución salvadoreña que pueda realizar capacitaciones y brindar certificados a los peritos sobre informática forense trae como consecuencias: poca credibilidad de los análisis forenses realizados a la evidencia digital, deficiencias en mecanismos de tratamiento de la evidencia, desconocimiento de nuevas herramientas y los beneficios de su aplicación, además de un desconocimiento de las tendencias de los criminales informáticos. Entre los países que brinda este tipo de capacitaciones según los encuestados se

encuentra Estados Unidos como uno de los países que además de ofrecer capacitaciones brinda certificaciones de expertos informáticos por medio de instituciones especializadas en el tema y acreditadas para extender dichas certificaciones.

La investigación demuestra que la aplicación de la informática forense en el Salvador no es del 100% según los encuestados está entre 51 al 75%. Este dato refleja la necesidad de fortalecer la legislación con temas relacionados a crímenes informáticos para permitir una mejor aplicación y desarrollo de la informática forense en el país. De igual forma según las respuestas obtenidas por los peritos informáticos no es muy aceptada por parte del órgano judicial, es decir, los jueces no confían en un 100% el usar informática forense para la resolución de un caso. Según revelan los peritos informáticos la confianza que le dan los Jueces u Órgano Judicial es de un 51 al 75% este dato nos permite conocer que es un tema aceptado y conocido que está creciendo moderadamente y que es utilizado para disminuir la delincuencia cibernética, pero aun así no está siendo totalmente aceptada.

La percepción que tienen los peritos informáticos de la aceptación de la Fiscalía General de la República en cuanto a pruebas digitales o evidencia digital es positiva, ya que uno de ellos afirma que hay un 100% de aceptación por este Órgano del Estado, esto demuestra que esta institución se beneficia de todas las investigaciones y análisis hechos para poder levantar acusaciones contra personas que se les atribuye un hecho de crimen informático y basar sus alegatos en dichos resultados. Existe la necesidad que la evidencia presentada por el investigador forense o del experto informático debe ser lo más tranparente posible para evitar dudas que permitan la libertad del delincuente.

A través de esta encuesta nos damos cuenta que un perito informático debe tener conocimientos en todas las áreas de computación desde el manejo de bases de datos, redes, criptografías entre otras disciplinas que le permiten tener más perspicacia y sentido común para realizar los análisis agotando todas las posibilidades que existen para la realización de su informe pericial. Existen otros elementos que permitirían fortalecer o reforzar la informática forense; los más sobresalientes en esta investigación a través de los expertos informáticos nacionales son: el fortalecimiento de la legislación con leyes que apoyen el trabajo del perito informático además de respaldar sus acciones, la capacitación del Órgano Judicial para el conocimiento de nuevos delitos de índole informática así como los requerimientos que deben de pedirle al experto informático en base a lo que quieren demostrar y por último fomentar temas, capacitaciones, seminarios que permitan difundir estos conocimientos a los actuales profesionales y los futuros.

La existencia de estándares para la recolección y tratamiento de la evidencia es fundamental y su existencia fue confirmada por el 67% de los encuestados y la necesidad de estos es porque trae múltiples beneficios entre los cuales podemos mencionar una mejor recolección de la evidencia digital así como un mejor tratamiento de ésta, lo cual permitiría a la fiscalía tener bases más solidas para poder fundamentar sus acusaciones en base a la evidencia digital presentada. Además se beneficia por la trasparencia del manejo que tendría la evidencia permitiendo al Juez confiar en las pruebas que se presentan en un juicio. A pesar que la mayoría menciono conocer sobre esta existencia, aun no son todos, y esto trae consigo problemas ya que son los peritos informáticos los que realizan los análisis a las evidencias recolectadas y si ellos desconocen sobre estos estándares, no podrán realizar su trabajo en base a protocolos previamente establecidos de cómo se deben realizar los procesos correctamente, dando lugar a poner en duda el análisis realizado por éstos y la validez de la evidencia presentada ante un juez que ayude a determinar cómo ocurrieron los hechos.

La necesidad de realizar capacitaciones es fundamental para que el profesional que ejerce en esta área pueda conocer las nuevas tecnologías así como herramientas que le permitan realizar su trabajo, las encuestas nos revelan que solo el 34% recibe capacitaciones en menos de seis meses, de esta

forma actualiza sus conocimientos de los nuevos delitos que van surgiendo y analizarlos a través de herramientas más recientes y confiables permitiéndole presentar dictámenes más precisos y transparentes.

La falta de capacitaciones o de preparación que tenga el experto afectara negativamente en el desarrollo de los casos ya que el 67% ha enfrentado dificultades a la hora de utilizar la informática forense en delitos informáticos, haciendo invalido el análisis realizado a la evidencia digital, aumentando la impunidad de los delincuentes por falta de pruebas y perjudicando al sistema judicial para ejercer su labor de hacer valer la justicia y esclarecer los hechos delictivos, castigando a los responsables de cometerlos.

La justificación de los encuestados fue referida a dos factores primordiales que les impidieron la resolución de este tipo de casos, la tecnología y la falta de conocimientos. Los problemas por el factor tecnológico es importante darle solución, debido a que los cambios constantes de medios de almacenamiento permiten ir creando nuevos dispositivos donde almacenar la evidencia y el profesional informático de hoy en día debe comprender y poder utilizar estos dispositivos de almacenamiento masivo que existe en el mercado para realizar análisis y posteriormente dar los resultados correctos.

Además la falta de metodologías y conocimientos es otro elemento que imposibilito el poder resolver un caso, ya que al no contar con el conocimiento sobre las metodologías y técnicas necesarias para realizar y justificar el análisis realizado a la evidencia, puede impedir que ésta sea aceptada en un juicio y evitando realizar una correcta investigación para llegar a determinar quiénes son los responsables de un hecho y como se cometió el delito.

Un aporte positivo a esta investigación fue que dos peritos informáticos explicaron los elementos necesarios para formar un laboratorio básico en la implementación en universidades o centros de capacitación, estos elementos son:

- métodos de criptografía para poder obtener contraseñas de archivos de cualquier índole.
- Contar con software diseñado para el tratamiento y manejo de la evidencia digital, con el fin de realizar un buen análisis y cuidar la cadena de custodia de la evidencia.
- Equipo especializado para el procesamiento de datos, esto se debe a que la tecnología va cambiando con el tiempo, y también paralelamente lo tiene que hacer el equipo que permite hacer el análisis de la evidencia digital.

IV. ANALISIS SOBRE LA COMPARACION ENTRE PERITOS INFORMATICOS NACIONALES E INTERNACIONALES

Al realizar la comparación entre los peritos nacionales e internacionales, revela que todos los peritos encuestados dijeron conocer el término informática forense, lo cual indica que este tema está siendo abordado y estudiado por distintos países incluyendo el nuestro. El estudio nos permite conocer que hay una diferencia entre los conocimientos de los peritos internacionales con los nacionales, ya que todos los internacionales dijeron que su nivel de conocimiento es amplio en el tema, no siendo este el caso de los peritos nacionales, en donde el nivel de conocimiento se encuentra dividido desde el qué dice tener solo conocimientos básicos hasta el que manifiesta contar con bases solidas en éste. Esta diferencia de conocimientos refleja que en el país aun los peritos informáticos no tienen una amplia comprensión del tema. Esta diferencia de conocimientos se le atribuye a que los peritos internacionales pueden realizar sus capacitaciones dentro de sus países de origen permitiéndoles conocer cómo utilizarla directamente en su entorno, mientras que los nacionales tienen que realizar sus capacitaciones en otros países o de forma autodidacta lo cual no garantiza que el conocimiento adquirido por sus propios medios sea el idóneo ya que esto no les permite conocer cuales temas son los que realmente un perito debe abarcar, cuales son las tendencias de crímenes informáticos, el conocimiento de nuevas herramientas y sus beneficios, etc.

El estudio nos muestra que los expertos internacionales así como los nacionales comparten la idea de que un perito informático debe conocer de distintas disciplinas relacionadas con la informática, desde el manejo de bases de datos, redes, software, sistemas operativos hasta el conocimiento de leyes para conocer el marco legal en el que se desenvuelven.

AL realizar la comparación entre la capacidad de uso de distintas herramientas informáticas forenses, los peritos internacionales demostraron un alto conocimiento de la existencia de herramientas que le permiten desarrollar un mejor trabajo, mientras que los peritos nacionales no opinaron al respecto, esto genera la incertidumbre de que si realmente conocen y utilizan herramientas informáticas forenses como apoyo al desarrollo de su trabajo, esto puede ser por las razones anteriormente expuestas sobre el grado de conocimiento que poseen sobre informática forense.

El conocimiento de estándares para el tratamiento de la evidencia y así como para la aplicación de la informática forense, esta compartido por ambas clases de peritos, es decir el estudio que ellos han realizado les permite conocer que existen estándares, porque en ambas poblaciones se observo la misma tendencia de que la mitad conoce de estándares y la otra no, es de cuestionar si los peritos nacionales conocen al respecto de forma autodidacta o han recibido capacitaciones que garanticen su certificación como informático forense y su conocimiento, ya que como anteriormente se expuso, el grado de conocimiento entre ambas poblaciones es distinto.

Los peritos internacionales demuestran estar interesados en capacitarse constantemente, es por esto que buscan de instituciones que les permitan certificarse en el tema ya que para ellos les es necesario conocer los nuevos avances en la materia y así poder desempeñar su trabajo de la mejor manera y con los mejores resultados. En cambio los peritos nacionales se están conformando con tener conocimientos de forma autodidacta y no a través de instituciones que respalden sus conocimientos.

El grado de conocimiento que tienen los peritos internacionales en el tema, les permite tener mayores criterios para poder seleccionar como y que medios se utilizaran a la hora de realizar el análisis a la evidencia digital, es por este motivo que la mayoría de ellos no ha enfrentado casos en los cuales no han podido resolverlos. En contraparte los peritos nacionales al no tener conocimientos

sólidos en el tema, se les dificulta el poder saber que herramienta aplicar para analizar la evidencia es por este motivo que ellos enfrentan más casos sin resolver.

Y esto es comprobado porque los peritos internacionales solo enfrentan dos tipos de dificultades, en cambio los peritos nacionales presentan más factores que les dificulta el poder realizar su trabajo, ya que no solo es por falta de metodologías o conocimientos sino también por la falta de tecnologías o por las leyes que no respaldan el uso de la informática forense en el esclarecimiento de un delito impidiendo así su esclarecimiento y fomentando la impunidad en este tipo de casos.

V. ANÁLISIS GENERAL PARA LA POBLACIÓN DE UNIVERSIDADES

Según datos obtenidos por medio del cuestionario pasado a la población docente de las universidades, se obtuvo que el 49% tienen conocimiento sobre esta temática, pero este conocimiento es relativamente bajo ya que se encuentra en un rango de 0 a 25%; esto muestra que solo tienen los principios básicos, dificultando poder impartir conocimiento a los estudiantes en su proceso de formación. Los docentes que poseen conocimiento sobre informática forense, es por iniciativa propia, siendo el medio más utilizado hoy en día para obtener dicho conocimiento el internet, siendo esta una fuente no muy confiable en la mayoría de información, otra forma ha sido a través de revistas, películas y series de televisión con relación a esta temática.

Por tal razón las universidades no poseen una asignatura como tal para impartir informática forense y esto es reflejado en los resultados, el poco conocimiento que se imparte es debido a que los docentes no poseen bases solidas sobre la temática, dicho conocimiento es impartido de manera superficial en asignaturas que tienen que ver con seguridad de sistemas informáticos y redes computacionales.

La población en general considera necesario que se imparta conocimientos sobre informática forense a los futuros profesionales, un 73% está de acuerdo en la creación de una asignatura en la cual se imparta este conocimiento, debido a que se trata de una temática nueva estos evalúan que debería ser una asignatura electiva por ser un área informática poco estudiada y utilizada hoy en día en el país.

Algunas razones por las que evalúan la necesidad de crear dicha asignatura son:

- Brindar técnicas y metodologías utilizadas en informática forense.
- Ayudar al crecimiento profesional de los estudiantes, ya que cada vez se ven más casos en los que se necesita de expertos en computación para validar la información.
- Ayudar al progreso del país en relación a tecnología informática.
- Brindar una base técnica a la carrera de computación con respecto al tratamiento de información sobre la evidencia digital, siendo esta un área de actualidad que dentro de poco será de mucha importancia en la toma de decisiones judiciales en nuestro país.
- Ayudar a la seguridad informática en la vulnerabilidad de redes computacionales porque hoy en día suceden delitos informáticos cuya complejidad requiere personal especializado por lo que es necesario se imparta este conocimiento.
- Ser de utilidad para evitar cualquier problema en una institución cuya información sea de gran valor.

Por otra parte el 27% restante de la población considera que no es necesaria la creación de una asignatura como tal para impartir este conocimiento, en este grupo hay dos opiniones:

1. Los docentes manifiestan que la temática por ser poco demandada en el país puede impartirse en otras asignaturas tales como: seguridad informática, auditoria de sistemas informáticos e ingeniería de software.
2. Los docentes manifiestan que por la complejidad de la temática, es necesario hacer una especialización que les permita obtener a los estudiantes conocimientos tanto teóricos como prácticos de informática forense y su relación con la legislación.

Las facultades que imparten carreras de informática presentan la limitante de no tener recurso tecnológico informático, ya que no poseen software ni hardware especializado para implementar un laboratorio de informática forense, sin embargo el 15% de la población manifiesta que la institución posee el recurso económico para obtener la tecnología necesaria en caso de implementar un laboratorio de este tipo.

Por la falta de recurso tecnológico y recurso humano capacitado en las instituciones de educación superior no se imparte conocimiento de informática forense a los futuros profesionales que se están preparando actualmente.

VI. ANÁLISIS GENERAL PARA LA POBLACIÓN DE POLICÍA NACIONAL CIVIL

A través de la investigación realizada en las divisiones policiales, se desconoce si éstas poseen la capacidad de hacer frente a los delitos informáticos que sufre gran parte de la población, ya que en la actualidad se desconoce si estas divisiones tienen personal especializado, hardware, software y manuales de procedimientos que les permitan realizar de manera adecuada investigaciones donde se ve involucrado un hecho delictivo de carácter informático.

Esto en su gran mayoría favorece a los delincuentes, porque estos valiéndose de la incapacidad de las instituciones investigadoras de este tipo de delitos, siguen realizándolos sin que puedan ser detectados, por lo que la mayoría de estos delitos quedan impunes.

Las consecuencias de esta problemática se reflejan en la población salvadoreña ya que son posibles víctimas de amenazas, estafas, entre otros que en la mayoría de los casos no se denuncia porque no se conoce de una institución que pueda brindar la ayuda para resolver el problema que sufren.

La autoridad competente en esta área debe considerar los avances que las sociedades tienen ya que éstas van cambiando constantemente en todas las áreas, la tecnología hoy en día es la que cambia a un ritmo acelerado, las sociedades que no se adaptan a ese cambio sufren las consecuencias, como las que actualmente sufre nuestro país, porque se ha estancado en el desarrollo de las áreas de educación y seguridad, por lo anteriormente expuesto se debe iniciar capacitando, instruyendo a los encargados de la seguridad y los entes que se ven involucrados a resolver los delitos informáticos que sufre la población, esto a través de la aplicación de medidas para reducir los delitos informáticos, una de estas es la aplicación de la informática forense, siendo ésta una ciencia en la cual lo principal es la obtención, la preservación, análisis y presentación de la evidencia digital encontrada en una escena del crimen, de manera tal que una vez expuesta en un juicio esta no genere duda de su procedencia.

VII: ANÁLISIS GENERAL PARA LA POBLACIÓN DE FISCALÍA GENERAL DE LA REPÚBLICA

Siendo La Fiscalía General de la República una institución que tiene entre sus funciones defender a la sociedad, dirigir investigaciones de delitos con la colaboración de la Policía Nacional Civil, promover el enjuiciamiento y castigo de los sospechosos por delitos de atentados contra las autoridades y el desacato entre otras.

Dentro de las funciones mencionadas anteriormente la primordial es defender a la sociedad de los atropellos a los que puedan estar expuestos, uno de estos es ser víctimas de delitos informáticos, sin embargo esta institución se ve sin argumentos para hacer frente a la cantidad de este tipo de delitos que se dan en el país, debido a que solo se cuenta con un fiscal encargado de dirigir las investigaciones de casos de delitos informáticos junto con la policía.

Se encuesto al fiscal encargado de las investigaciones de delitos informáticos y según los resultados se conoció que no ha recibido capacitaciones sobre el manejo de evidencia digital, lo cual representa una debilidad en el proceso de la investigación.

Otro dato que llama la atención es la forma de cómo el fiscal se ha preparado para hacer frente a este tipo de delitos, siendo su preparación autodidactica a través de internet, sin embargo la información que se obtiene de internet no es siempre confiable. La tecnología hoy en día juega un papel importante en el desarrollo de los países, para ello debe existir disponibilidad de conocimiento, esto a través de capacitaciones constantes en base a los cambios que se vayan dando.

A todo lo anterior no podemos excluir la legislación que actualmente existe en nuestro país, ya que no se tienen leyes propias para juzgar a personas involucradas en este tipo de hechos delictivos.

VIII: MATRIZ DE PUNTOS COINCIDENTES DEL ANALISIS.

Poblaciones / criterios	Jueces	Abogados	Peritos	Policia Nacional Civil	Fiscalia General de la Republica
Conocimiento sobre IF[80].	75%	25%	75%	----	25%
Conocimiento de evidencia digital	75%	50%	100%	----	75%
Delitos informaticos con mayor auje	pirateria	Pirateria	Pirateria	----	Pirateria
Nivel de aplicación de IF.	25%	25%	50%	----	25%
Falta de tecnologia	----	----	75%	----	----
Falta de leyes en el pais.	90%	90%	90%	----	90%

Como resultado de los analisis se puede determinar el grado de conocimiento sobre la informatica forense y los elementos que estan involucrados en un delito informatico, como puntos de coincidencia las instituciones involucradas y los elementos presentados muestra que nuestro pais no posee la capacidad actuamente para hacer frente a los delitos informacos. Como se puede notar la institucion que no proporciono informacion es la primera en llegar a la escena del crimen siendo esto un problema por no tener esta el conocimiento de cómo tratar el tipo de evidencia en este caso, la evidencia digital.

[80] IF: Informática Forense.

F- COMPROBACIÓN DE HIPOTESIS

I. ENUNCIADO DEL PROBLEMA

¿En qué medida el desconocimiento sobre la aplicación de la informática forense; afecta el esclarecimiento de los hechos delictivos informáticos en El Salvador?

II. HIPÓTESIS DEL ESTUDIO.

En este apartado se enuncian las hipótesis, las cuales ayudaran a resolver el problema que se ha identificado.

a. GENERAL.

"La aplicación de la informática forense en los procesos judiciales; favorecerá el esclarecimiento en el 75% de los delitos informáticos"

b. HIPÓTESIS NULA Ho.

"La aplicación de la informática forense en los procesos judiciales; no alterará el esclarecimiento de los delitos informáticos".

c. AUXILIARES

1. "La falta de herramientas informáticas forenses en las instituciones policiales, determina el 80% de la incidencia de fraudes que se realizan a través de Internet".

2. "La aplicación de una metodología de recolección y análisis de evidencias digitales, causará un rendimiento del 95% en el proceso de obtención de esta".

3. "La falta de personal calificado en informática forense, determina el 85% de la ineficiencia en la resolución de delitos informáticos".

"La debilidad de la legislación salvadoreña permite que el 85% de los delitos informáticos no sean esclarecidos en su totalidad".

d. OPERACIONALIZACIÓN DE LAS VARIABLES[81]

VARIABLES	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	INSTRUMENTOS
Aplicación de informática forense. (variable independiente)	*Aplicación de herramientas forenses informáticas, metodologías para guardar la evidencia digital encontrada en la escena del crimen, aplicación de un marco legal de delitos informáticos.*	*Alto nivel de aplicación de la informática forense.*	1. Conocimiento de la informática forense. 2. Código penal reformado. 3. Uso de leyes. 4. Uso de tecnología. 5. Uso de recurso humano calificado. 6. Manejo de técnicas y herramientas informáticas.	Encuesta, Entrevista y Cuestionario
		Bajo nivel de aplicación de informática forense.	1. Desconocimiento de la informática forense. 2. Código penal sin reformas. 3. Falta de leyes. *4.* Falta de tecnología, recurso humano calificado, técnicas y herramientas informáticas.	
Esclarecimiento de delitos informáticos. (variable dependiente)	*Solución apegada a la justicia según los métodos de evaluación de evidencia presentada en el juicio en el cual se evalúa un caso de delito informático.*	*Esclarecimiento favorable (culpabilidad o inocencia)*	*1. Manejo adecuado de las metodologías de recolección de evidencia digital.* *2. Interpretación adecuada de las leyes.*	Encuesta, Entrevista y Cuestionario

[81] Fuente: Ver apartado Referencia Bibliográfica - I libros: numeral 17 y 18

III. COMPROBACION DE HIPOTESIS[82]

a. PRUEBA DE CHI CUADRADO x^2

Esta prueba de significación estadística nos permite encontrar relación o asociación entre dos variables de carácter cualitativo que se presentan únicamente según dos modalidades (dicotómicas).

Chi cuadrado x^2 sirve para determinar si los datos obtenidos de una muestra presentan variaciones estadísticamente significativas respecto de la hipótesis nula *Ho*.

Cuando formulamos la hipótesis general, simultáneamente definimos la hipótesis nula, que niega nuestra hipótesis general. De acuerdo a la hipótesis nula las variaciones en la variable independiente no tienen correspondencia con las variaciones que pudiere haber de la variable dependiente. Es decir que existe "independencia estadística".

Para la aplicación del chi cuadrado es necesario, antes realizar dos pasos. Por una parte, establecer el nivel de significación (α) con el cual vamos a trabajar, y determinar los grados de libertad de nuestra muestra.

El nivel de significación es arbitrario y se fija de antemano, para nuestro estudio se trabajara con el 3%. Los grados de libertad se establecen en función de la cantidad de celdas que tenemos (cuatro para muestro caso), producto del cruce de dos variables.

b. GRADOS DE LIBERTAD

Se refiere a la posibilidad que se tiene de establecer, en una distribución dada, valores arbitrarios sin modificar el marginal de dicha distribución, la fórmula para calcular los grados de libertad es:

Gl= (F-1) (C-1), En donde, F= número de filas y C= número de columnas.

c. DESCRIPCIÓN Y JUSTIFICACIÓN DE LA PRUEBA ESTADÍSTICA QUE SE UTILIZARA PARA PROBAR LAS HIPÓTESIS EN ESTUDIO

Se utilizo la prueba estadística chi-cuadrado x^2.

La razón por la que utilizamos chi-cuadrado x^2 es por que ésta nos permitió evaluar dos variables, además a través de esta prueba comparamos los valores esperados contra valores observados, es decir, que permitió comparar los indicadores teóricos contra los valores empíricos contenidos en la investigación.

Al aplicar la formula de chi cuadrado x^2 a los datos recolectados, los resultados se comparan con el valor de chi cuadrado tabla ${x^2}_t$. Si $x^2 > {x^2}_t$, entonces se rechaza la hipótesis nula *Ho* y se acepta la general; si $x^2 < {x^2}_t$, se acepta la hipótesis nula *Ho*.

[82] Fuente: Ver apartado Referencia Bibliográfica- II Sitios web: numeral 45,46 y 47.

Formula:

$$x^2 = \sum_i \frac{(fOi - fEi)^2}{fEi}$$ (Ecuación 1)

En donde:

x^2= valor del chi cuadrado.

fO= Valores Observados o reales.

fE = Valores Esperados o teóricos.

$\sum_i$ = Sumatoria de puntaje.

Para calcular valores esperados:

$$fE = \{ tf \ x(tc)/total \}$$ (Ecuación 2)

Donde:

tf: total de filas.

tc: total de columna.

total: total global

IV. POBLACIONES

Las poblaciones de las cuales se obtuvieron datos para la comprobación de la hipótesis del estudio se presentan a continuación en la ***tabla N° 24.***.

POBLACIÓN	ENCUESTADOS
Peritos Informáticos	3
Abogados	96
Jueces	10
Fiscales	1
TOTAL	110

Tabla N°24: Poblaciones que se tomaron en cuenta en la comprobación de la hipótesis.

En este apartado no se ha considerado la población de las universidades, ya que no esta involucrada en la aplicación de la informática forense para esclarecer los delitos informáticos.

V. PROCEDIMIENTO ESTADÍSTICO PARA COMPROBAR LAS HIPÓTESIS

El método estadístico para comprobar la hipótesis es chi-cuadrado x^2 por ser una prueba que permitió medir aspectos cualitativos y cuantitativos de las respuestas que se obtuvieron del instrumento administrado y medir la relación que existe entre las variables de las hipótesis en estudio.

El valor de chi-cuadrado se calculará a través de la formula presentada anteriormente, ecuación 1, el criterio para la comprobación de la hipótesis se define así: si $x^2 > x^2{}_t$; se acepta la hipótesis general y se rechaza la hipótesis nula *Ho*; en caso contrario se rechaza la general.

A continuación se presenta la ***tabla N° 25*** que muestra los valores obtenidos por medio de las encuestas, dichos valores se obtuvieron para las variables definidas como independiente (Aplicación de la informática forense) y dependiente (esclarecimiento de delitos informáticos); variables definidas previamente en el anteproyecto de esta investigación, los datos se han obtenido de la manera siguiente de la pregunta 1 ***Anexo N° 11***, dirigida a los abogados, jueces, fiscalía y peritos; se obtuvo de respuesta 72 a favor y 38 en contra; y de la pregunta 4 ***Anexo N° 11*** dirigida a jueces, fiscalía y abogados, 78 a favor y 9 en contra; respectivamente.

Tabla de valores.

OBSERVADOS	SI	NO	TOTAL
Aplicación de Informática forense(VI)	72	38	110
Esclarecimiento de delitos informáticos(VD)	78	9	87
TOTAL	150	47	197

Tabla N°25: Valores observados para las variables dependiente e independiente.

Para calcular los valores esperados se ha hecho uso de la ecuación 2, cuyos resultados se muestran en la ***tabla N° 26*** a continuación:.

ESPERADOS	SI	NO
Aplicación de Informática forense(VI)	83.7563[83]	26.2437[84]
Esclarecimiento de delitos informáticos(VD)	66.2437	20.7563

Tabla N°26: Valores esperados para las variables dependiente e independiente

Sustituyendo valores en la ecuación 1, se tienen:

[83] sustituyendo valores en la ecuación 2 se obtiene: $fE = \{ tf\ x(tc)/total \}$ {(110)x(150)/197}=83.7563.

[84] {(110)x(47)/197}=26.2437.

$$x^2 = \frac{72 - 83.7563\ ^2}{83.7563} + \frac{38 - 26.2437\ ^2}{26.2437} + \frac{78 - 66.2437\ ^2}{66.2437} + \frac{9 - 20.7563\ ^2}{20.7563}$$

$$x^2 = 1.6502 + 5.2664 + 2.0864 + 6.6587$$

$$\underline{\boldsymbol{x^2 = 15.6617}}$$

La obtención del valor de chi cuadrado tabla, se hizo mediante el siguiente procedimiento.

La tabla de chi cuadrado tiene dos entradas:

- *Alfa* (α): este valor hace referencia al nivel de confianza, para el caso en estudio es de 97%, el valor de alfa es de 0.03, lo cual corresponde al complemento porcentual de la confianza.
- Grados de Libertad (Gl): Es un estimador del número de categorías independientes en la prueba de independencia o experimento estadístico. Se encuentran mediante la fórmula Gl= (F-1) (C-1).
- Obtención del grado de libertad.

Estos se obtiene aplicando la formula.

Gl= (F-1) (C-1)

En donde:

F= 2 y C= 2

Gl= 1

e= 3%.

Debido a que en la tabla de distribución de Chi cuadrado no hay un valor para e= 3%, este se obtuvo mediante interpolación ($x^2{}_t$); el proceso se hizo de la siguiente manera:

De la tabla de distribución de chi cuadrado, ***Anexo N° 12,*** se obtiene los siguientes datos que se muestran en la ***tabla N° 27***.

GL	NIVEL DE CONFIANZA	VALOR ALFA
1	95%	3.84
1	97%	"x"incognita
1	97.5%	5.02

Tabla N°27: Valores de Chi cuadrado para Alfa.

Interpolación.

$$\frac{97.5\% - 95\%}{5.02 - 3.84} = \frac{97.5\% - 97\%}{5.02 - x}$$

$$\frac{2.5\%}{1.18} = \frac{0.5\%}{5.02 - x}$$

$$12.55\% - x2.5\% = 0.59\%$$

$\underline{x = 4.784}$; Valor Chi cuadrado tabla, para un nivel de confianza del 97%.

Dado que el valor de x^2(15.6617) $> x^2{}_t$ (4.784) por medio de interpolación, se rechaza la hipótesis nula y se acepta la hipótesis general, por lo que se determina que la aplicación de la informática forense influye en el 75% del esclarecimiento de delitos informáticos en los procesos judiciales.

CAPITULO 4

Diagnóstico de la Situación Actual de la Informática Forense en El Salvador

CAPITULO 4: DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA INFORMATICA FORENSE EN EL SALVADOR

A- INDICADORES SOBRE LA INFORMATICA FORENSE EN EL SALVADOR

I. CONCEPTO DE INDICADOR[85]

Los indicadores son elementales para evaluar, dar seguimiento y predecir tendencias de la situación de un país, un estado o una región en lo referente a su economía, sociedad, desarrollo humano, etc., así como para valorar el desempeño institucional encaminado a lograr las metas y objetivos fijados en cada uno de los ámbitos de acción de los programas de gobierno.

La comparabilidad del desarrollo económico y social es otra de las funciones de los indicadores, ya que estamos inscritos en una cultura donde el valor asignado a los objetos, logros o situaciones sólo adquiere sentido respecto a la situación de otros contextos, personas y poblaciones, es decir, es el valor relativo de las cosas lo que les da un significado.

Existen diferentes definiciones de indicadores, pero todas coinciden en las siguientes:

- Un indicador: es una herramienta o instrumento importante para la producción y generación de información científica y técnica.
- Un indicador: Transforma la información en acciones concretas que van desde diagnósticos hasta la elaboración de estrategias, facilitando los procesos de planificación y desarrollo.
- Un indicador: es una expresión numérica que permite la medición de diferentes características de un sistema específico y sus variables asociadas.

II. TIPOS DE INDICADORES[86]

Existen diferentes tipos de indicadores dependiendo del fenómeno que se estudie ya que estos se construyen con el objetivo de simplificar, representar y cuantificar un fenómeno concreto y proporcionar información sobre el estado y evolución que éste ha tenido en un espacio y tiempo determinado. Los indicadores no cambian la realidad, pero sí ayudan a formar la manera en que se percibe y sirven para formar un concepto de desarrollo en común. Proveen información que puede indicar una necesidad de ajustes y correcciones a políticas, metas, prioridades, programas, actitudes, y comportamientos.

Los indicadores se pueden clasificar, atendiendo a las características del fenómeno estudiado en los siguientes:

a) Indicadores Económicos

b) Indicadores Sociales

c) Indicadores Institucionales

d) Indicadores Ambientales

[85] Fuente: Ver apartado Referencias Bibliográficas- II: Sitios Web: numeral 37.
[86] Fuente Ver apartado Referencias Bibliográficas- VII: Tesis: numeral 1

Para nuestro trabajo se utilizaran indicadores sociales debido al fenómeno de estudio seleccionado, ya que está relacionado con los problemas que enfrenta la sociedad salvadoreña y en específico lo que atañe a delitos informáticos y el uso de la informática forense en el esclarecimiento de éstos.

a. INDICADORES SOCIALES

Los indicadores sociales proporcionan información sobre aspectos vinculados con la calidad de vida y el bienestar de la población por lo cual constituyen instrumentos fundamentales para dar respuesta a problemas sociales y para la toma de decisiones de política pública.

En el marco de desarrollo social, cobra importancia la utilización de los indicadores sociales ya que aportan evidencia empírica para la realización de diagnósticos, implementación de políticas públicas, formulación de programas y proyectos. A pesar de su relevancia, los indicadores sociales han sido menos explorados que los económicos y técnico-productivos, en parte por ser fenómenos más complejos y por ende, de difícil medición.

De esta manera, como un marco teórico para la selección y construcción de éstos, se presentan a continuación algunas definiciones de indicador social, sus áreas o campos de aplicación y una clasificación de los distintos tipos de indicadores sociales.

a.1. DEFINICIONES Y ÁREAS DE UTILIZACIÓN

A pesar de que el término "indicador social" es ampliamente utilizado, existen escasas definiciones del mismo. Generalmente, los indicadores sociales son utilizados como medidas de cambio en dimensiones sociales**.**

Así, los indicadores sociales, han sido definidos como "Indicadores referidos a variables sociológicas; esto es, que buscan describir de manera agregada las características y procesos, observables o no, de poblaciones o grupos sociales"[87].

También, se define a los indicadores sociales como "instrumentos analíticos que permiten mejorar el conocimiento de distintos aspectos de la vida social en los cuales estamos interesados, o acerca de los cambios que están teniendo lugar".

Algunas de las aplicaciones de los indicadores sociales mencionadas son: descripción de una situación social; medición de cambios de una situación dada, proyecciones y tendencias; seguimiento y evaluación de una acción social como instrumentos para la toma de decisiones.

Algunos de los indicadores más utilizados para estas áreas pueden ser: población, vivienda y servicios básicos, salud, educación, etc. Asimismo, la unidad de análisis puede ser la persona, el hogar, la vivienda, etc. De esta manera, se puede observar que los indicadores pueden referirse, según la amplitud de la unidad de análisis, a individuales o colectivos (conjunto de individuos, organizaciones o instituciones, localidades, países, etc.).

[87] Fuente: Ver apartado Referencias Bibliográficas- II: Sitios Web: numeral 38.

a.2 CLASIFICACIÓN DE INDICADORES[88]

Los indicadores pueden ser clasificados en: Indicadores cualitativos y cuantitativos; absolutos y relativos; simples y compuestos; inter medios y finales.

a.2.1 INDICADORES CUANTITATIVOS Y CUALITATIVOS

Mientras que los indicadores cuantitativos se refieren a aspectos tangibles de la realidad, los indicadores cualitativos describen características intangibles. Los indicadores cuantitativos parten de observaciones objetivas y verificables como por ejemplo número de productores, ingresos, población NBI, etc. En cambio, los indicadores cualitativos se refieren a percepciones, valores, opiniones y vivencias subjetivas como por ejemplo grado de satisfacción con el trabajo grupal, grado de participación en el proyecto, grado de satisfacción con los resultados alcanzados por el proyecto, grado de satisfacción con el desempeño del técnico, etc.

La elección de indicadores cualitativos o cuantitativos depende de los objetivos del proyecto como así también de la disponibilidad de datos y recursos. Una de las principales diferencias entre ambos indicadores radica en el formato de los datos que se utilizan para la construcción de los mismos: mientras que los indicadores cuantitativos derivan de métodos que recogen información principalmente en formato numérico o en categorías pre-codificadas, la información utilizada para construir indicadores cualitativos proviene mayoritariamente de textos descriptivos sin y con poca categorización . La utilización combinada de indicadores cuantitativos y cualitativos brindaría información más completa de las experiencias, situaciones y procesos que se buscan conocer y comprender.

a.2.2 INDICADORES ABSOLUTOS Y RELATIVOS

Los indicadores pueden ser expresados en los términos absolutos en que se realiza la medición (por ejemplo, población total) o relativos, es decir, derivados mediante un proceso de cálculo que relacione dicha medición con otras magnitudes (por ejemplo, tasa de crecimiento de la población).

Las medidas más frecuentemente utilizadas para expresar indicadores en términos relativos son: medias, relaciones o ratio, proporciones o porcentajes y tasas.

- La media**:** es el promedio de dos o más valores. La media simple de un conjunto de valores es la suma de todos los valores divididos entre el número de esos valores. Por ejemplo, el promedio de edad de los integrantes de un grupo de Cambio Rural.
- Un ratio**:** es una comparación entre dos cantidades que se miden en una misma unidad. Se expresa como un valor dividido entre otro. El resultado no tiene unidades; las unidades del denominador y el numerador se cancelan mutuamente".
- Una proporción: es la relación de una parte o subconjunto con el todo. Es un tipo de relación en la que el denominador es una cantidad que representa el conjunto total de un grupo de estudio y el numerador es un subconjunto de éste.
- Se denomina tasa: al cociente de un numerador y un denominador que se expresan en diferentes unidades.

[88] Fuente: Ver apartado Referencias Bibliográficas- II: Sitios Web: numeral 44.

III. LOS INDICADORES SOCIALES PARA LA FORMULACIÓN DE PROYECTOS[89]

En el marco de la formulación, seguimiento o monitoreo y evaluación de proyectos, los indicadores se utilizan para el diagnóstico de la situación inicial, la cuantificación del cumplimiento de metas establecidas y la medición de impacto. Cabe destacar que el uso de indicadores en la formulación e implementación de proyectos es imprescindible para el seguimiento y evaluación externos así como internos.

Un proyecto constituye tanto una respuesta a un problema, como un proceso, una metodología de trabajo y una forma de gestión o asignación de recursos.

Los proyectos cuentan con una población objetivo, una localización espacial, un tiempo de inicio y de finalización y recursos asignados para el desarrollo de las actividades y objetivos planteados.

A continuación se presenta la clasificación de indicadores utilizados en la formulación de proyectos y luego algunas recomendaciones para su selección y construcción.

a. TIPOS DE INDICADORES UTILIZADOS EN LA FORMULACIÓN DE PROYECTOS

Para la formulación de proyectos se propone indicadores de actividades, de producto y de impacto.

A continuación se describe cada uno de ellos para su mayor comprensión:

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 la cantidad de 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.

Estos tres tipos de indicadores son los que se utilizaran para la creación de los indicadores sociales que permitirán el posterior análisis de la informática forense en El Salvador.

[89] Fuente: Ver apartado Referencias Bibliográficas- II: Sitios Web: numeral 44

IV .DIAGRAMA DE LA METODOLOGÍA PARA LA CREACIÓN DE INDICADORES DEL ESTUDIO Y ANÁLISIS DE INFORMÁTICA FORENSE.

En la ***figura Nº5*** se presenta la metodología para la creación de indicadores del estudio y análisis de informática forense

Figura N°5: Metodología para la creación de indicadores del estudio y análisis de informática forense

Fuente: Elaboración propia.

V. METODOLOGÍA UTILIZADA PARA LA CREACION DE LOS INDICADORES SOCIALES APLICADOS AL ESTUDIO DE LA INFORMATICA FORENSE EN EL SALVADOR

Para el presente proyecto y la generación de indicadores del mismo, se realizo en base a los indicadores sociales para la formulación de proyectos: actividad, producto e impacto, para evaluar y monitorear el desarrollo de la informática forense en el área Metropolitana de San Salvador, permitiendo la creación de indicadores propios para la investigación teniendo como base los resultados obtenidos a través del uso de las encuestas realizadas para las poblaciones de peritos nacionales, jueces, abogados y fiscales. Para llevar a cabo el análisis de la situación actual de la informática forense, se han seleccionado cuatro variables importantes que están en función de los principales problemas que enfrenta la informática forense en el país:

- Leyes
- Evidencia digital
- Recurso humano
- Herramientas y metodología de informática forense.

Cada una de estas variables está representada por una serie de indicadores que muestran la magnitud y dimensión de los problemas sociales que atañen a este tema. Estos indicadores son el resultado de un proceso de selección y valoración de los integrantes del grupo, como ya se menciono anteriormente se partirá de la base de los indicadores sociales para la formulación de proyectos y la información propia.

A continuación se describen las etapas metodológicas para la selección, diseño y creación de los indicadores sociales.

a. CRITERIOS PARA LA SELECCIÓN DE INDICADORES SOCIALES[90]

La elección de los indicadores depende de los objetivos del proyecto, deben medir lo que es importante y atribuible a la acción del mismo. Es decir, deben medir el cambio atribuible al proyecto. En esta dirección, se afirma que en la medida en que los objetivos estén bien definidos, la construcción de los indicadores resultará más sencilla.

Asimismo, se recomienda que la definición de indicadores sea acordada con los beneficiarios e involucrados con el fin de obtener mayor aceptación sobre los avances y resultados obtenidos a lo largo del proceso[91].

A continuación se describen los criterios que deberían cumplir los indicadores.

- **Específico o preciso:** corresponde a los objetivos del proyecto.
- **Mensurable o medible**: indicadores que basan su cálculo en datos básicos disponibles, cuya obtención se puede repetir sin dificultad en el futuro.
- **Realizable**: probabilidad de alcanzar el indicador.
- **Relevante o pertinente**: apropiado para medir el objetivo.
- **Enmarcado en el tiempo**: expresar plazos de inicio y finalización para alcanzar las metas.

[90] Fuente Ver apartado Referencias Bibliográficas - VII: Tesis: numeral 1.
[91] Fuente Ver apartado Referencias Bibliográficas - II: Sitios Web: numeral 39.

Por otra parte, a los criterios anteriores se suele agregar que los indicadores deberían ser:

- **Fiables:** deben generar confianza no sólo entre los productores de información sino también entre los usuarios de la misma, arrojan las mismas conclusiones si la medición se realiza en forma repetida o a partir de diversas fuentes.
- **Fáciles de interpretar:** no deben dar lugar a interpretaciones ambiguas, deben ser simples y claros.
- **Focalizados:** deben ser medibles y debe especificar el grupo objetivo, la cantidad, la calidad, el tiempo y el lugar (localización).
- **Económicos y accesibles**: economía de costos en su recopilación y disponibilidad de acceso a las fuentes.
- **Comparables:** indicadores que permiten las comparaciones entre distintos países, áreas geográficas, grupos socioeconómicos y años.

Una forma de realizar la selección de estos indicadores, es utilizando los indicadores para la formulación de proyectos, es decir, para cada variable o problema se seleccionan indicadores que responden a las categorías de Actividad, Producto e Impacto, de acuerdo a la información que se quiere obtener del mismo, una manera de hacerlo es definir criterios evaluativos para obtener indicadores que sean viables de acuerdo a la información disponible de la realidad social y jurídica del país.

Los criterios utilizados para seleccionar los indicadores que pertenecen a cada categoría de Actividad, Producto e Impacto (A-P-I) son los siguientes:

a) Evaluación de los datos:

Dentro de este criterio es necesario evaluar los siguientes elementos:

- Calidad de los datos
- Confiabilidad de los datos
- Recopilación de los datos
- Escala espacial y temporal

b) Características de los indicadores

- Mensurabilidad
- Pertinencia
- Representatividad
- Sensibilidad al cambio
- Conexiones causales claras

c) Utilidad para los usuarios

- Validez
- Cantidad limitada

- Claridad en el diseño
- Aplicabilidad y predicción.

Los indicadores sirven para darle seguimiento a un fenómeno o aspecto de la realidad en distintos momentos del tiempo. No hay que olvidar que un indicador si no cumple con un objetivo específico para el investigador, no tiene sentido su construcción y este representa un costo social.

b. IDENTIFICACIÓN Y SELECCIÓN DE LOS INDICADORES SOCIALES PARA EVALUAR LA INFORMATICA FORENSE EN EL SALVADOR

Los indicadores sociales que han sido seleccionados para evaluar y monitorear la situación social de la informática forense en el área metropolitana de San Salvador, han sido el resultado de un proceso de selección y evaluación, en base a los criterios expuestos en el apartado anterior.

Los criterios a sustentar por cada indicador creado son: Eficacia, eficiencia, simplificación y transparencia.

Se entenderá por los siguientes criterios:

- Eficacia: es la capacidad de lograr el efecto deseado o esperado.
- Eficiencia: es la capacidad de lograr el efecto deseado con el mínimo de recursos posibles.
- Simplificación: realizar las actividades de manera sencilla.
- Transparencia: mostrar las actividades tal cual son.

Las variables que se evalúan en este estudio son: Leyes, Evidencia digital, Recurso Humano, Herramientas y metodología. Cada una de estas variables nos brindan información relevante sobre el estado actual de la informática forense y la relación que existe con estas variables. Además, estas cuatro variables nos permiten tener un panorama integral del funcionamiento de la informática forense utilizada como herramienta en el esclarecimiento de un caso por delitos informáticos.

Las instituciones a nivel nacional que sirvieron de apoyo para la construcción de los indicadores son: Asociación de Ciencias Forenses El Salvador (ACFES), Fiscalía General de la República, Procuraduría General de la República, Centro Judicial Isidro Menéndez, INTERPOL.

c. DISEÑO Y CONTRUCCION DE LOS INDICADORES SOCIALES

En este apartado se presentan el diseño y la construcción de los indicadores propios para esta investigación sobre El Estudio de la informática forense en El Salvador.

c.1-DISEÑO DE LOS INDICADORES SOCIALES[92]

A continuación se muestran los pasos para la elaboración del diseño de los indicadores.

- *Establecer los indicadores sociales.*

  El desarrollo de los indicadores sociales se detalla en la sección **anterior b**. **Identificación y selección de los indicadores sociales para evaluar la informática forense en el salvador.**

- *Definir las partes que conforman cada indicador y diseñar la medición*
  - NOMBRE DEL INDICADOR: describe el factor o situación que origina el resultado de lo que se ha de controlar.
  - UTILIZACION: describe el objetivo que se quiere obtener con la medición de los resultados.
  - FORMULA: es el cálculo o medio de donde se obtienen los resultados a obtener.
  - UNIDAD DE MEDIDA: indica en que unidades se interpretara el indicador.
  - ORIGEN DE LA INFORMACION: las fuentes de donde se sacaron estos datos.
  - CRITERIO A RESPALDAR: indica que criterios se están afectando con el control de los resultados para el buen uso de los recursos.
  - CATEGORIZACIÓN: es una escala de valores establecida en la cual se indica que rangos se consideran malos, regulares y buenos dependiendo del objetivo del indicador.
  - INTERPRETACIÓN: es la explicación de que significado tendría si el valor del indicador se acercar a los valores presentados en la escala.
  - FRECUENCIA: establece el tiempo sugerido en el cual se tendría que volver hacer la medición de cada indicador.
- *Medir, aprobar, y ajustar el sistema de indicadores.*
  - Pertinencia del indicador
  - Fuentes de información seleccionadas

c.2- CONTRUCCION DE LOS INDICADORES SOCIALES

En este apartado se presenta el marco teórico, la construcción y la presentación de los indicadores sociales creados para el estudio de la informática forense en el área Metropolitana de San Salvador.

c.2.1- MARCO TEÓRICO PARA LA CONSTRUCCION Y SELECCIÓN DE INDICADORES SOCIALES[93]

A continuación se describe como se lleva a cabo ese proceso de construcción de indicadores haciendo referencia en primer lugar a la pirámide de información[94] que se presenta en la ***figura N°6***.

[92] Fuente Ver apartado Referencias Bibliográficas- VII: Tesis: numeral 2.
[93] Fuente Ver apartado Referencias Bibliográficas- VII: Tesis: numeral 1.
[94] Fuente Ver apartado Referencias Bibliográficas- I:Libros: numeral 13.

Pirámide de información

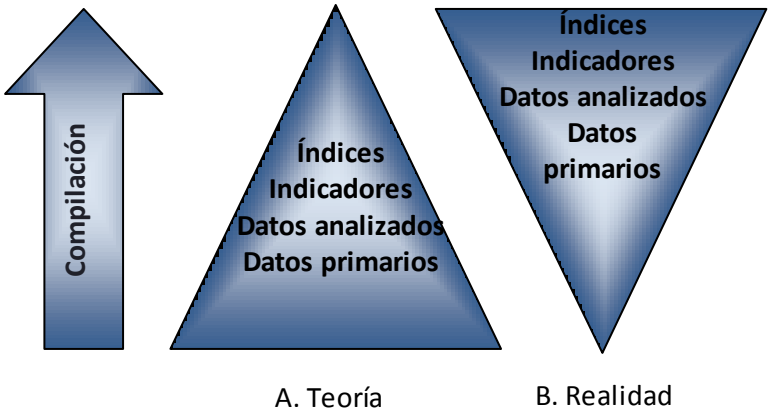


Figura N°6: Pirámide de la información

La pirámide de información es utilizada para mostrar cómo se estructura un sistema de indicadores, a partir de una amplia base de datos primarios disponibles en el ambiente, que al ser analizados y sistematizados facilitan la elaboración de indicadores. Este proceso de análisis y síntesis se aplica en cualquier dimensión de análisis de la realidad que se quiera estudiar tomando en cuenta que debe seleccionarse una metodología adecuada para la selección de datos que servirán de base para la creación de indicadores, mientras mayor sea la disponibilidad de datos y estadísticas, más eficaz será el proceso de agregación, síntesis y desarrollo de los indicadores que se seleccionen.

En la parte A de la ***figura Nº 6***, se presenta la situación teórica de cómo deberían comportarse el proceso de información síntesis agregación de indicadores, sin embargo la realidad puede ser distinta. Especialmente en países como el nuestro, donde no se cuenta con un sistema de información estadística confiable que genere y produzca información precisa, oportuna y disponible para los diferentes sectores que la requiera y así hacer eficiente y eficaz la toma de decisiones.

La dificultad del acceso a datos confiables, la ausencia de metodologías comunes para la elaboración de información y la falta de marcos conceptuales que permitan el desarrollo y uso de indicadores económicos, sociales, ambientales, etc., a nivel nacional y regional, son algunas de las razones más importantes de que la pirámide de información tome la forma invertida como lo muestra la parte B de la ***figura Nº 6***, ya que en la realidad nos encontramos con un gran número de indicadores respaldados por una escasa información disponible y confiable, que apoyen la generación de esta información.[95]

El desarrollo de indicadores y la generación de información para la toma de decisiones requiere definir qué indicadores utilizar y cómo medirlos, de acuerdo a los objetivos establecidos de la investigación y del problema de estudio.

[95] Fuente Ver apartado Referencias Bibliográficas- I:Libros: numeral 13.

c.2.2- CONSTRUCCIÓN DE INDICADORES SOCIALES PARA CADA VARIABLE[96]

La construcción de estos indicadores se fundamenta en la recolección de información de fuentes primarias y secundarias a través del uso de encuestas, visitas de campo y de la observación directa de cada población.

Los Modelos que se utilizaron para la construcción de los indicadores fueron: para su definición en base a cada variable y para la descripción de cada indicador diseñado. Los cuales se presentan a continuación en las ***tablas Nº 28 y 29.***:

Construcción de indicadores por cada variable:

NOMBRE DE LA VARIABLE: Leyes, Recurso Humano, Herramientas y metodologías y Evidencia Digital.

TIPO DE INDICADOR: Actividad, Producto e Impacto.

NOMBRE DE INDICADOR	FORMULA	UTILIZACION	CRITERIO A RESPALDAR

Tabla N°28: Esquema utilizado para la presentación de los indicadores creados en esta investigación.

Descripción de cada a indicador:

Nombre Indicador	
Utilización	
Fórmula:	
Unidad de Medida	
Origen de la información:	
Criterios a respaldar:	
Categorización	
Interpretación	
Frecuencia	

Tabla N°29: Esquema utilizado para la descripción de los indicadores creados en esta investigación.

[96] Fuente Ver apartado Referencias Bibliográficas- VII: Tesis: numeral 2.

Donde:

- **Utilización:** se refiere al objetivo que se pretende alcanzar con ese indicador.
- **Formula:** es la formula ocupada para crear ese indicador.
- **Unidad de medida:** son las unidades en que estará dado el valor del indicador, ya sea numérico o porcentaje.
- **Origen de la información:** especifica de donde son tomados los datos para la construcción del indicador.
- **Criterios a respaldar:** indican los criterios que son respaldados por ese indicador y la explicación del porque los respalda.
- **Categorización:** es una escala de valores establecida en la cual se indica que rangos se consideran malos, regulares y buenos dependiendo del objetivo del indicador.
- **Interpretación:** es la explicación de que significado tendría si el valor del indicador se acercar a los valores presentados en la escala.
- **Frecuencia:** establece el tiempo sugerido en el cual se tendría que volver hacer la medición de cada indicador.

VI. PRESENTACIÓN DE LOS INDICADORES

a. CLASIFICACION DE INDICADORES SEGÚN EL CRITERIO QUE RESPALDA

Se elaboraron 12 indicadores sociales para medir el avance de la informática forense en el área metropolitana de San Salvador. A continuación se presenta la ***tabla Nº 30*** consolidando los indicadores y el criterio que cada uno de ellos respalda.

Nombre del Criterio / Nombre del Indicador	EFICIENCIA	EFICACIA	SIMPLIFICACION	TRANSPARENCIA
1. Reformas al código penal			✓	
2. Conocimiento de informática forense			✓	✓
3. Instituciones certificadoras				✓
4. Capacitación a nivel nacional			✓	
5. Utilización de herramientas	✓		✓	✓
6. Estándares aplicación de informática forense	✓			✓
7. Factor tecnología en la aplicación de la informática forense	✓			
8. Factor metodología en la aplicación de la informática forense	✓			
9. Conocimiento de la evidencia digital			✓	✓
10. Validez de la evidencia digital				✓
11. Cadena de custodia		✓		✓
12. Delitos por peritos		✓		
TOTAL	**4**	**2**	**5**	**7**

Tabla N° 30: Cuadro resumen de los indicadores creados junto con el criterio que respaldan.

b. INDICADORES CREADOS PARA LA INVESTIGACION

A continuación se presentan los indicadores creados para la presente investigación:

1. **LEYES**

➢ **INDICADOR DE PRODUCTO**

NOMBRE DE INDICADOR	FORMULA	UTILIZACION	CRITERIO A RESPALDAR
Reformas al código penal	$$RCP = \frac{\sum \text{de jueces y abogados que conocen sobre reformas al código penal}}{\sum \text{de jueces y abogados estudiados}} x100$$	Determinar el nivel de actualización que tiene el código penal para hacer frente a delitos informáticos mediante las reformas a éste.	Simplificación

2. RECURSO HUMANO

➢ **INDICADOR DE ACTIVIDAD**

NOMBRE DE INDICADOR	FORMULA	UTILIZACION	CRITERIO A RESPALDAR
Conocimiento de informática forense	$CIF = \frac{\sum \text{de jueces, abogados, fiscales y peritos que conocen sobre informática forense}}{\text{dejueces, abogados, fiscales y peritos estudiados}}$	dir el conocimiento que se tiene de la informática forense por parte de todos los involucrados en la resolución de un caso por delito informático.	Simplificación, transparencia.
Instituciones certificadoras	$IC = \frac{\text{Numero de peritos que conocen de instituciones certificadoras}}{\text{Total peritos estudiados}} x100$	Conocer el porcentaje de los peritos que conocen instituciones certificadoras de informática forense en el país.	Transparencia,
Capacitación a nivel nacional	$CNN = \frac{\text{Numero de peritos capacitados en el país}}{\text{Total peritos estudiados}} x100$	Medir el avance de la informática forense en El Salvador con respecto a su conocimiento por parte de los peritos.	Simplificación.

3. HERRAMIENTAS Y METODOLOGÍA DE INFORMÁTICA FORENSE

INDICADOR DE ACTIVIDAD

NOMBRE DE INDICADOR	FORMULA	UTILIZACION	CRITERIO A RESPALDAR
Utilización de herramientas	$UH = \frac{\text{Numero de peritos que usan herramientas}}{\text{Total peritos estudiados}} x100$	Conocer el porcentaje de peritos que hacen uso de herramientas informáticas forenses.	Transparencia, simplificación, eficiencia.
Estándares aplicación de informática forense	$EAIF = \frac{\text{Numero de peritos con conocimientos sobre estándares de informática forense}}{\text{Total peritos estudiados}} x100$	Evaluar el conocimiento de los peritos informáticos forenses con respecto a estándares para garantizar la validez de la aplicación de la informática forense en el análisis de evidencia.	Eficiencia, transparencia.

➢ **INDICADOR DE PRODUCTO**

NOMBRE DE INDICADOR	FORMULA	UTILIZACION	CRITERIO A RESPALDAR
Factor tecnología en la aplicación de la informática forense	$FTAIF = \frac{\text{Factores de tecnología escogidos por los peritos}}{\text{total peritos estudiados}} x100$	terminar la incidencia que el factor tecnológico tiene sobre la aplicación de la informática forense.	Eficiencia.
Factor metodología en la aplicación de la informática forense	$FMAIF = \frac{\text{Factores de metodología escogidos por los peritos}}{\text{Total peritos estudiados}} x100$	terminar la incidencia que el factor de metodológica tiene sobre la aplicación de la informática forense.	Eficiencia.

4. EVIDENCIA DIGITAL

➢ **INDICADOR DE ACTIVIDAD**

NOMBRE DE INDICADOR	FORMULA	UTILIZACION	CRITERIO A RESPALDAR
Conocimiento de evidencia digital	$CED = \frac{\text{Numero de jueces y abogados que conocen evidencia digital}}{\sum \text{de jueces y abogados estudiados}} x100$	edir el conocimiento que se tiene de la evidencia digital por parte de los jueces y abogados que están involucrados en la resolución de un caso por delito informático.	Simplificación, transparencia.

➢ **INDICADOR DE PRODUCTO**

NOMBRE DE INDICADOR	FORMULA	UTILIZACION	CRITERIO A RESPALDAR
Validez de la evidencia digital	$VED = \frac{\sum \text{de jueces que confían en la evidencia digital}}{\sum \text{de jueces estudiados}} x100$	Conocer el grado de confiablidad que tienen los jueces en la evidencia digital para el esclarecimiento de delitos informáticos.	Transparencia

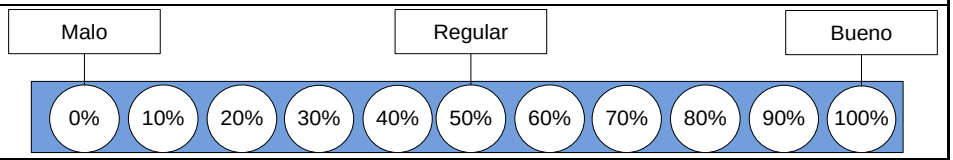
➢ **INDICADOR DE IMPACTO**

NOMBRE DE INDICADOR	FORMULA	UTILIZACION	CRITERIO A RESPALDAR
Cadena de custodia	$CC = \frac{\sum \text{jueces que seleccionaron el factor cadena de custodia}}{\text{de jueces estudiados}} X100$	Evaluar el grado de incidencia e importancia que tiene el romper la cadena custodia en la manera y la necesidad de realizar una eficaz recolección y seguimiento de la evidencia digital durante su análisis.	Eficacia, transparencia.

VII. DESCRIPCIÓN DE INDICADORES

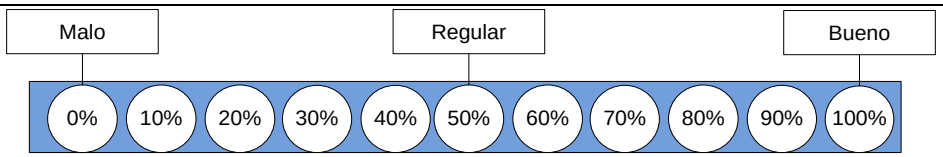
LEYES

- **INDICADOR DE PRODUCTO**

Nombre Indicador: Reformas al código penal	
Utilización	Determinar el nivel de actualización que tiene el código penal para hacer frente a delitos informáticos mediante las reformas a éste.
Fórmula:	$$RCP = \frac{\sum \text{de jueces y abogados que conocen sobre reformas al código penal}}{\sum \text{de jueces y abogados estudiados}} x100$$
Unidad de Medida	Porcentaje
Origen de la información:	Total de jueces y abogados que conocen sobre reformas al código penal entre el total de jueces y abogados encuestados.
Criterios a respaldar:	**Simplificación**: Debido a que si existen reformas al código penal que tipifiquen a los delitos informáticos como tal, se podrán resolver con mayor facilidad casos por este tipo de delitos.
Categorización	
Interpretación	Mientras mas cercano este al 100% mejor será la evaluación de este indicador, ya que reflejara el crecimiento sobre la actualización del código penal en materia de delitos informáticos a través del tiempo.
Frecuencia	Anual

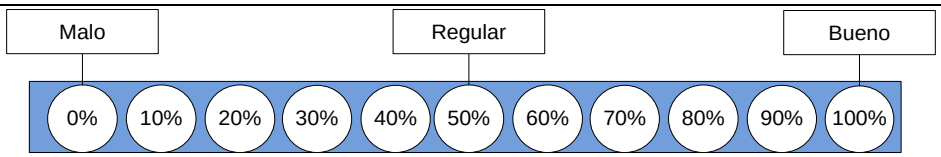
RECURSO HUMANO

- **INDICADORES DE ACTIVIDAD**

Nombre Indicador: Conocimiento de informática forense	
Utilización	Medir el conocimiento que se tiene de la informática forense por parte de todos los involucrados en la resolución de un caso por delito informático.
Fórmula:	$$CIF = \frac{\sum \text{de jueces, abogados, fiscales y peritos que conocen sobre informática forense}}{\text{de jueces, abogados, fiscales y peritos estudiados}}$$
Unidad de Medida	Porcentaje
Origen de la información:	Total de jueces, abogados, peritos y fiscales que conocen sobre informática forense entre el Total de jueces, abogados, peritos y fiscales.
Criterios a respaldar:	**Simplificación:** Debido a que este conocimiento les ayudara a poder realizar sus labores de mejor manera. **Transparencia:** Debido a que el tener conocimiento de cómo se hacen las cosas en la informática forense, trae como consecuencia un proceso transparente.
Categorización	
Interpretación	Mientras mas cercano este al 100% mejor será la evaluación de este indicador, ya que reflejara el crecimiento del conocimiento que se tiene sobre la informática forense a través del tiempo en el país.
Frecuencia	Anual

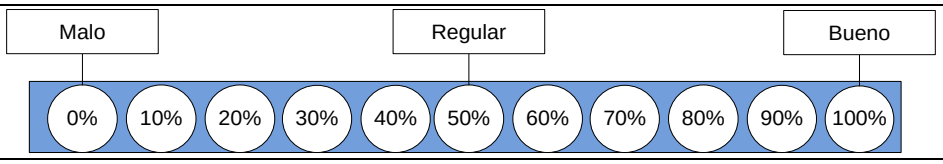
HERRAMIENTAS Y METODOLOGÍA DE INFORMÁTICA FORENSE

INDICADOR DE ACTIVIDAD

Nombre Indicador: Utilización de herramientas	
Utilización	Conocer el porcentaje de peritos que hacen uso de herramientas informáticas forenses.
Fórmula:	$$UH = \frac{\text{Numero de peritos que usan herramientas}}{\text{Total peritos estudiados}} x100$$
Unidad de Medida	Porcentaje
Origen de la información:	Numero de peritos que si usan herramientas entre Total de peritos encuestados.
Criterios a respaldar:	**Transparencia:** Porque sin importar cuantos peritos estén involucrados en el análisis de la evidencia, al hacer uso de herramienta los resultados serán los mismos. **Simplificación:** Porque el uso de herramientas facilita la labor del perito en el análisis de la evidencia. **Eficiencia:** Porque permite analizar la evidencia de manera correcta con los recursos necesarios.
Categorización	
Interpretación	Mientras mas cercano este al 100% mejor será la evaluación de este indicador, ya que reflejara un crecimiento en la utilización de herramientas especializadas en informática forense por parte de los peritos a través del tiempo.
Frecuencia	Anual

EVIDENCIA DIGITAL

- **INDICADOR DE ACTIVIDAD**

Nombre Indicador: Conocimiento de evidencia digital	
Utilización	Medir el conocimiento que se tiene de la evidencia digital por parte de los jueces y abogados que están involucrados en la resolución de un caso por delito informático.
Fórmula:	$$CED = \frac{\text{Numero de jueces y abogados que conocen evidencia digital}}{\sum \text{de jueces y abogados estudiados}} x100$$
Unidad de Medida	Porcentaje
Origen de la información:	Número de jueces y abogados que conocen evidencia digital, Total de jueces y abogados encuestados.
Criterios a respaldar:	**Simplificación:** Debido a que este conocimiento les ayudara a poder realizar sus labores de mejor manera. **Transparencia:** Debido a que el tener conocimiento de cómo se hacen las cosas en la informática forense y en específico sobre la evidencia digital, trae como consecuencia un proceso transparente.
Categorización	
Interpretación	Mientras mas cercano este al 100% mejor será la evaluación de este indicador, ya que reflejara el crecimiento del conocimiento que se tiene sobre la evidencia digital a través del tiempo en el país.
Frecuencia	Anual

Para detalle de todos los indicadores y el manejo de estos ver CD apartado INDICADORES.

B- DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LA INFORMATICA FORENSE EN EL SALVADOR

I. INTRODUCCIÓN

El desarrollo de resolución de un caso por delito informático inicia con la investigación que llevan a cabo la Fiscalía General de la República junto con la Policía Nacional Civil, la Policía Nacional Civil tiene como objetivo fundamental guardar la cadena de custodia de la evidencia digital secuestrada en la escena del crimen, para evitar que esta sea refutada por el juez, dicha evidencia es llevada a la División Policía Técnico Científica para su análisis y obtención de informes con sus respectivas conclusiones.

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.

Para conocer la situación actual sobre la informática forense a través del "Estudio y Análisis sobre la informática forense en El Salvador", se utilizo la información recolectada de las poblaciones: jueces, abogados, fiscales, Policía Nacional Civil, peritos informáticos y Universidades; dando como resultado el siguiente diagnostico:

II. DIAGNOSTICO SOBRE LA SITUACIÓN ACTUAL DE LA INFORMÁTICA FORENSE EN EL SALVADOR EN EL 2008

CONOCIMIENTO SOBRE INFORMÁTICA FORENSE

El trabajo en conjunto que hacen estas instituciones es necesario para el esclarecimiento de delitos informáticos y lo que es aun más importante es mostrar pruebas que permitan culpar y juzgar a un criminal, según muestra el indicador "Conocimiento de Informática Forense" solo el 65.4% de las entidades involucradas directamente tienen el conocimiento de informática forense lo que indica que existe un desarrollo de esta ciencia pero este no es lo suficiente por lo cual es necesario capacitar a jueces, abogados, peritos y fiscales, para que obtengan conocimientos y les permita llevar a cabo sus actividades de forma transparente teniendo en cuenta la importancia de su aplicación y el beneficio que proporciona. Además de disminuir la desconfianza que se pueda tener con respecto a su aplicación, ya que la evidencia tratada puede ser fácilmente alterada.

A pesar del porcentaje de conocimiento que se posee, este es limitado y teórico, por lo que esta categorización refleja un estado "regular" con respecto a su medición en base al conocimiento de las entidades estudiadas sobre el tema.

REALIZACIÓN ACTUAL DE PROCEDIMIENTOS EN INVESTIGACIÓN DE DELITOS INFORMÁTICOS

Un elemento importante para la aplicación de la informática forense es el Perito informático, porque es quién aplica las metodologías y utiliza las herramientas forenses para el análisis de la evidencia digital, por lo que la necesidad de capacitar al personal es indispensable, el estudio muestra que de

tres peritos encuestados solo dos de ellos han sido capacitados en esta área, además se observa que de estos solo el 33.3% utilizan herramientas forenses para realizar los peritajes como se puede observar en el indicador "Utilización de herramientas", sin embargo los peritos restantes utilizan herramientas forenses libres y también se auxilian de otras herramientas para el desarrollo de sus actividades, porque las instituciones para las que laboran no cuentan con recurso tecnológico apropiado para realizar análisis forenses a las evidencias; como lo manifiesta en el análisis que se realizo en la unidad de INTERPOL.

En el esclarecimiento de delitos no solo participan los peritos sino también los Fiscales ya que son ellos los encargados de dirigir la investigación de los hechos ocurridos, por lo cual es importante que el fiscal tenga conocimiento sobre informática forense para que le indique al perito el trabajo que debe realizar sobre la evidencia.

Una vez finalizado el análisis a la evidencia, el perito le entrega los resultados al fiscal, defensor y al juez encargado del caso, para que este análisis sirva de prueba en un juicio y se pueda llegar a un veredicto final confiable y veraz que permite el esclarecimiento del delito.

Actualmente no se aplica informática forense para el esclarecimiento de delitos informáticos, según los resultados de las entidades estudiadas y también porque se desconoce si se aplica en la división policial técnico científica, esto significa que según nuestro estudio, el estado de esta categorización es "deficiente" porque no se está aplicando.

LA PREPARACIÓN DEL RECURSO HUMANO

Las capacitaciones recibidas por los peritos informáticos han sido a nivel internacional en países como España, Guatemala, Puerto Rico, Canadá, México y EE.UU. por lo que se ve que hay interés por parte de las instituciones de obtener conocimiento sobre como enfrentar los nuevos tipos de delitos que se están realizando. Pero también en nuestro país han recibido capacitaciones sobre informática forense de parte de la Academia Nacional de Seguridad Publica. Cabe aclarar que esta institución únicamente brinda capacitaciones a lo elementos policiales encargados de realizar el análisis de evidencia digital, de esta forma se está contribuyendo gradualmente al desarrollo de esta ciencia. Esta institución debe de apoyar a los expertos informáticos brindando conocimiento sobre la utilización de herramientas que les permitan el uso de estándares para ejecutar un trabajo transparente y lo más importante es el factor de tecnología. La proporción de cambios tecnológicos con relación al tiempo es muy alta esto quiere decir que tenemos el desarrollo de mas tecnología en menor tiempo y a menor costo, es necesario que los expertos informáticos logren una armonía entre el conocimiento con las tecnologías emergentes y como éstas se prestan para una mala utilización**.**

La preparación que tienen los jueces con respecto a la informática forense ha sido por medio de capacitaciones y por iniciativa propia ya que son ellos los responsables de juzgar y dictaminar sentencia en un juicio por lo tanto se requiere que ellos tenga conocimientos sobre informática forense debido a que la comprobación de cómo fue cometido un delito de tipo informático, solo se puede realizar con la ayuda de herramientas, tecnologías y metodologías propias que la informática forense proporciona.

La forma en que los fiscales y abogados se han preparado con respecto a informática forense es por iniciativa propia, ya que no se les ha proporcionado capacitaciones y se ven en la necesidad de obtener conocimiento sobre este tópico para realizar sus actividades de la mejor manera posible (libros, internet, etc.) para hacerle frente a los delitos de tipo informático que suceden en el país.

El estado de la categorización de preparación de recurso humano respecto a la aplicación de informática forense es "regular" por el hecho de que hay una preparación, pero es mínima porque no todos los peritos informáticos se están capacitando y por la falta de capacitaciones tanto a fiscales y abogados.

TECNOLOGÍA Y METODOLOGÍAS

La falta de conocimiento sobre metodologías y herramientas necesarias para realizar y justificar el análisis de la evidencia digital, puede impedir su aceptación en un juicio, lo que conlleva a que en la investigación no se pueda determinar los responsables de un hecho y de qué manera se cometió, haciendo invalido el análisis realizado a la evidencia digital, aumentando la impunidad de los delincuentes por falta de pruebas y perjudicando al sistema judicial para ejercer su labor de hacer valer la justicia y esclarecer los hechos delictivos informáticos. Según los peritos encuestados se han visto en casos donde no han podido resolverlos, es decir proporcionar el análisis de la evidencia digital que se les ha solicitado, esto sucede por la falta de tecnología y conocimiento sobre metodologías utilizadas en informática forense, como se contempla en los indicadores "Factor Tecnología en la aplicación de informática forense" con un valor del 66.7% y el "Factor Metodología en la aplicación de la informática forense" con un 33.3%.

El estado que presenta actualmente la categoría de falta de tecnologías y falta de conocimiento sobre metodologías de informática forense en su aplicación es "deficiente", porque indica que hay limitantes para las investigaciones de delitos informáticos, por lo tanto aumenta la impunidad para los delincuentes.

VALIDEZ Y CONFIABILIDAD DE LA EVIDENCIA DIGITAL

El elemento trascendental para que se pueda aplicar la informática forense es la evidencia digital; el conocimiento de evidencia digital que se tiene por las entidades involucradas en el tema es de un 81.1% como lo muestra el indicador "Conocimiento de Evidencia Digital", lo cual es beneficioso pero solo el 50% de los jueces confían en ella en el rango de 76% a 100%, sin embargo el nivel de confianza que tienen los abogados en la evidencia digital están entre un 26% a 50% como se muestra el análisis de las entrevistas; esta desconfianza se debe a muchos elementos la principal se enmarca con un 70% de fallas en la cadena de custodia como se contempla en el indicador "Cadena de Custodia", lo cual indica que la evidencia fue manipulada de alguna forma para alterar el análisis de ésta, afectando la resolución que se pueda tomar en un juzgado.

Según el análisis realizado, se tiene conocimiento sobre evidencia digital por parte de las entidades estudiadas, pero no en su totalidad. Además el estado que representa la valides y confiabilidad que tiene la evidencia digital para los jueces es "regular", esto se tiene como resultado porque aun se tiene desconfianza de la aplicación de informática forense para el análisis de evidencias digitales, debido al desconocimiento que aun se tiene en esta área.

RELACIÓN DE LA INFORMÁTICA FORENSE CON LAS LEYES

Un dato que expone el presente proyecto es que no hay reformas al código penal lo cual es negativo en diversas formas entre las cuales podemos mencionar: Delitos no tipificados, falta de respaldo por parte de las autoridades, sentencias inciertas a los imputados, seguimiento a casos, etc. Lo cual nos

lleva que el presente trabajo puede ser una pieza de correspondencia hacia las instituciones pertinentes para retomar el tema para beneficio de todos ya que de las personas involucradas solo el 10.4% afirma que existen documentos para reformas hacia la ley, como se aprecia en el indicador "Reformas al Código Penal".

La legislación salvadoreña posee muchos vacios para afrontar delitos relacionados con las tecnologías de información, lo cual impide sancionar al delincuente, porque no existen leyes específicas que aborden y tipifiquen estas conductas ilícitas como delitos. Por lo que tanto jueces como abogados reconocen la necesidad que existe de fortalecer la legislación de nuestro país, para poder actuar ante la nueva forma de operar de los delincuentes y así evitar que este tipo de delitos sigan ocurriendo.

El estado que presenta esta categorización en la actualidad es "deficiente" debido a que las leyes en nuestro país aun no contemplan una tipificación de los delitos informáticos, ni de la aplicación de informática forense como herramienta para el esclarecimiento de este tipo de delitos.

EL APORTE DE LAS UNIVERSIDADES A ESTA TEMÁTICA

Aunque estas instituciones no están directamente involucradas en la aplicación de informática forense para el esclarecimiento de casos por delitos informáticos, se han considerado para el estudio por ser las encargadas de formar a futuros profesionales, en este caso futuros ingenieros o licenciados en informática, ya que los expertos en aplicar la informática forense son profesionales en el área de informática, pero también deben conocer sobre leyes relacionadas con el tipo de delito que se este investigando.

El 49% de los catedráticos de las carreras de ingeniería y licenciatura en informática poseen conocimiento sobre informática forense, pero este conocimiento es relativamente bajo ya que se encuentra en un rango de 0 a 25%; esto muestra que solo tienen los principios básicos, dificultando poder impartir conocimiento a los estudiantes en su proceso de formación, por lo que consideran necesario que se imparta conocimientos sobre informática forense a los futuros profesionales. Algunas razones por las que evalúan la necesidad de impartir este conocimiento son: Brindar técnicas y metodologías utilizadas en informática forense, Ayudar al crecimiento profesional de los estudiantes, ya que cada vez se ven más casos en los que se necesita de expertos en computación para validar la información y Ayudar al progreso del país en relación a tecnología informática.

El desconocimiento de informática forense es una debilidad que presentan las instituciones de educación superior, ya que actualmente no se imparten conocimientos a los estudiantes en esta área. Por lo tanto el estado que presenta esta categorización es "deficiente".

En conclusión la informática forense en El Salvador se encuentra en su etapa inicial, ya que no se tiene un avance de ésta como una ciencia formal que pueda brindar el apoyo necesario para el esclarecimiento de delitos informáticos debido a que en la evaluación de las categorías anteriores el 57.14% de éstas se encuentra en un estado "DEFICIENTE" y el 42.86% representan un estado "REGULAR" con respecto al conocimiento y aplicación de la informática forense.

El presente estudio da a conocer que la responsabilidad del desarrollo de la informática forense no solo le compete al área policial con el uso de tecnologías, metodologías y el contar con personal capacitado, sino que también recae en el área judicial porque son éstos los entes encargados de crear las leyes necesarias para tipificar los delitos informáticos y respaldar el uso de informática forense.

CAPITULO 5

ELEMENTOS INVOLUCRADOS EN LA APLICACIÓN DE LA INFORMATICA FORENSE

CAPITULO 5: ELEMENTOS INVOLUCRADOS EN LA APLICACIÓN DE LA INFORMÁTICA FORENSE

A- METODOLOGÍAS UTILIZADAS EN INFORMATICA FORENSE

Para la aplicación de informática forense se hace necesario el uso de herramientas informáticas forenses, estándares de aplicación y metodologías, por esta razón el recurso humano encargado de su aplicación debe estar capacitado en esta ciencia, garantizando de esta manera que el proceso de análisis forense de evidencias digitales se realice de manera correcta y transparente. El proyecto en estudio muestra una serie de metodologías utilizadas por expertos en la aplicación de informática forense, estas se muestran a continuación:

I. METODOLOGIA[97]: CERTIFICACIÓN GLOBAL DEL ASEGURAMIENTO DE LA INFORMACIÓN (GIAC[98])

Esta metodología para la realización de una exanimación forense de la computadora consiste en cuatro fases, que se pueden observar en la ***Figura N° 7***. Durante cada fase, se recogen los datos que sirven de fundamento para las siguientes fases.

Figura N° 7: Diagrama de la Metodología GIAC

El proceso que se lleva a cabo al aplicar esta metodología incluye lo siguiente:

Se detallan a continuación cada una de las fases que conforman la metodología (GIAC).

- **Recolección de evidencia:**

  Se recoge, fotografía y se hacen copias forenses de la evidencia física mientras tanto, se asegura que este protegida la integridad de la evidencia. También se realizan los procedimientos sobre las copias forenses obtenidas de la evidencia y prepararlas para el análisis. Se recoge la información detallada sobre el contenido de las copias forenses y los sistemas de ficheros que las contienen.

[97] Ver apartado Referencia Bibliográfica II: Páginas Web numeral 48
[98] Por sus siglas en ingles: *Global Information Assurance Certification (GIAC)*

- **Construcción y análisis de la línea de tiempo[99] (cronología de los eventos):**

  Se crea otra vista de la actividad del sistema de ficheros que detalle lo ocurrido en el sistema. Una línea de tiempo es una cronología de los archivos manipulados según la hora registrada por el sistema, indicando qué sucedió en el sistema y cuando, para utilizarlo posteriormente en la identificación de las actividades del interés.

- **Análisis de los medios:**

  La fase de análisis de los medios contiene la mayor y la más importante parte del trabajo en una exanimación. Se analizo las copias forenses creadas durante la colección de la evidencia. En esta fase, también identifican las palabras y frases de interés para la posterior investigación. Se recupera cualquier archivo eliminado del sistema contenido en la copia creada y de manera tentativa determinar el tipo de archivo eliminado. Después se analizan los archivos recuperados y se comprueba si tenían cualquier relación con en el incidente investigado.

- **Reporte forense**:

  La tarea final es divulgar los resultados encontrados y determinar la relación de la evidencia encontrada en la escena del crimen con el delito investigado, para así establecer cualquier implicación potencial tanto a nivel policial como legal que tiene la evidencia. La meta es comunicar con eficacia esta información y proporcionar las recomendaciones para tomar las respectivas acciones de seguimiento.

II. METODOLOGÍA DE EXAMEN Y ANÁLISIS DE DATOS.

Esta metodología está orientada a ayudar al investigador, como consecuencia del aumento de la capacidad de los dispositivos de almacenamiento, al igual que el incremento en la heterogeneidad de la información en ellos contenida, la labor del investigador en computación forense se ha tornado cada vez más compleja.

Debido a lo anterior, existe una necesidad imperiosa de construir herramientas y concebir guías metodológicas adecuadas que apoyen y sistematicen esta labor.

Las etapas que propone este modelo son:

- Identificación: reconocer un incidente mediante indicadores y determinar su tipo. Esto no esta incluido dentro del análisis forense, pero es significativo en los siguientes pasos.
- Preparación: preparar las herramientas, técnicas, autorizaciones de monitoreo y soporte administrativo.

[99] Ver apartado Glosario de Términos para su mayor comprensión

- Estrategia de acercamiento: formular de manera dinámica una estrategia basada en el impacto sobre la tecnología en cuestión. La idea es obtener el máximo de evidencia minimizando el impacto en la víctima.
- Preservación: aislar, asegurar y preservar el estado de la evidencia física y digital. Esto incluye evitar que personas usen los dispositivos digitales, o que algún otro dispositivo electromagnético se use dentro de un determinado radio.
- Colección: almacenar la escena física y duplicar las evidencias digitales utilizando procedimientos aceptados y estandarizados.
- Examinación: búsqueda sistemática en profundidad de evidencia relacionada con el crimen. Se enfoca en identificar y localizar evidencia potencial, posiblemente dentro de lugares no convencionales.
- Construir documentación detallada para el análisis.
- Análisis: determina la significancia de las evidencias, reconstruye los fragmentos de datos y genera conclusiones basadas en las evidencias encontradas. Un detalle del análisis es que puede no requerir grandes habilidades técnicas para su desarrollo, es por esto que una gran cantidad de personas puede trabajar en esta etapa.
- Presentación: resume y provee una explicación de las conclusiones. Se puede escribir en términos legales utilizando una terminología abstracta, la que debe hacer referencia a detalles específicos.

Este modelo se centra en las fases de examen y análisis, en particular, propone una guía metodológica que a partir de la imagen binaria de datos (un resultado específico de la etapa de recolección) permite hallar de forma sistemática la evidencia digital relacionada con el caso que se investiga, esta metodología se presenta en la ***figura N° 8***.

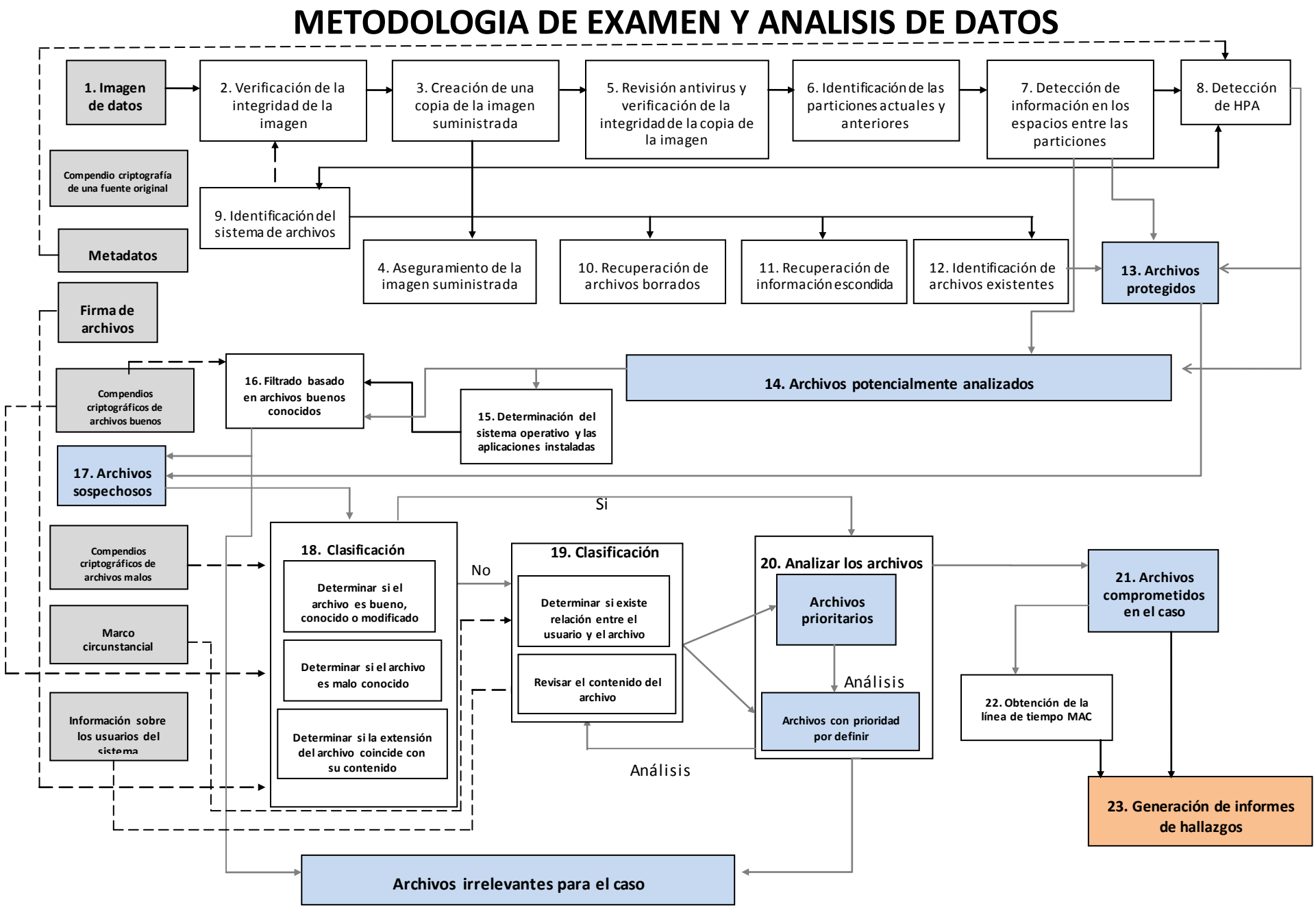


Figura N° 8. Diagrama de la metodología de examen y análisis de datos

Para realizar un análisis de datos forense es necesario seguir una serie de pasos para la obtención de la evidencia. A continuación se propone una guía metodológica que reúne y organiza una serie de actividades conducentes a la obtención de tal evidencia.

En el caso de la guía metodológica propuesta es necesario definir un conjunto de elementos requeridos que constituyen la información inicial para seguirla. Estos elementos son:

- Imágenes binarias de los dispositivos de almacenamiento digital comprometidos en el caso con sus respectivos compendios criptográficos.
- Descripción del caso ilustrando el marco circunstancial.
- Meta-datos de cada una de las imágenes, es decir, todo tipo de información necesaria para determinar las características de la imagen, en particular, la existencia de un HPA (*Host Protected Área*), concepto que se explicará más adelante.

El objetivo de esta guía metodológica es obtener un informe de hallazgos que describa la evidencia hallada y la forma como se obtuvo.

DESCRIPCIÓN DE LOS PASOS

Creación del archivo de hallazgos

Consiste en la creación y aseguramiento de un documento, ya sea físico o electrónico, que permita llevar un historial de todas las actividades que se llevan a cabo durante el proceso, y de los hallazgos encontrados, de modo que se tenga un resumen que permita hacer la reconstrucción del caso tiempo después de que este haya sido analizado.

A continuación se describen los pasos de la metodología examen y análisis de datos de la ***figura N° 8*** anteriormente expuesta.

1. **Imagen de datos**

   Consiste en la recepción de las imágenes de datos que conciernen al caso en investigación.

2. **Verificación de integridad de la imagen.**

   Para cada imagen suministrada se debe calcular su compendio criptográfico (MD5), comparándolo luego con el de la fuente original. Si la comparación arroja un resultado negativo se debe rechazar la imagen proveído en el primer paso.

3. **Creación de una copia de la imagen suministrada.**

   En un análisis de datos nunca se debe trabajar sobre la imagen original suministrada, sino sobre su copia.

4. **Aseguramiento de la imagen suministrada.**

   Se debe garantizar que la imagen suministrada no sufra ningún tipo de alteración, con el fin de conservación de la cadena de custodia y del mantenimiento de la validez jurídica de la evidencia.

5. **Revisión antivirus y verificación de la integridad de la copia de la imagen.**

   Una vez se ha obtenido la copia de la imagen, es necesario asegurar que no tenga ningún tipo de virus conocido. Luego se debe verificar la integridad de la copia, de la misma forma como se hizo con la original (paso 2). De hecho, esta actividad es de tipo transversal en la metodología, es decir, debe realizarse periódicamente durante el proceso de análisis de datos, de modo tal que se garantice la integridad de los datos desde el comienzo, hasta el fin de la investigación.

6. **Identificación de las particiones actuales y anteriores (las que sea posible recuperar).**

   La identificación de las particiones en un dispositivo es de vital importancia, ya que reconocerlas implica la identificación de su sistema de archivos, mediante el cual se pueden reconocer características especiales de la organización de la información y se puede definir la estrategia de recuperación de archivos adecuada.

7. **Detección de información en los espacios entre las particiones.**

   Cuando se detectan datos en estas zonas de la imagen, se debe proceder a hacer un análisis para determinar si representan algún tipo de información relevante para la investigación. En caso de estar protegidos, estos archivos serán tenidos en cuenta en la fase de la identificación de archivos protegidos, de lo contrario, se incluirán en el conjunto de archivos potencialmente analizables.

8. **Detección de un HPA[100].**

   Este paso debe realizarse solo si en los Meta-datos se indica la existencia del HPA, ya que de otro modo es imposible de identificar. En el caso en que exista, se debe seguir el mismo procedimiento del paso anterior.

9. **Identificación del sistema de archivos.**

   Para cada una de las particiones identificadas en el paso 6, debe identificarse su sistema de archivos, con el fin de escoger la forma de realizar las actividades posteriores del análisis de datos.

10. **Recuperación de los archivos borrados.**

    Durante esta actividad se deben tratar de recuperar los archivos borrados del sistema de archivos, lo que es conveniente dado el frecuente borrado de archivos para destruir evidencia.

    Dependiendo de las características técnicas y del estado del sistema de archivos puede no ser posible la recuperación de la totalidad de los archivos eliminados, por ejemplo si estos han sido sobre escritos, o si se han utilizado herramientas de borrado seguro para eliminarlos.

    Los archivos recuperados exitosamente formarán parte de los archivos potencialmente analizables, exceptuando los archivos identificados como protegidos que serán tenidos en cuenta durante la fase de identificación de archivos protegidos.

11. **Recuperación de información escondida.**

    En esta etapa se debe examinar exhaustivamente el *slack space*[101], los campos reservados en el sistema de archivos y los espacios etiquetados como dañados por el sistema de archivos.

    Al igual que en la fase 10, los archivos protegidos también se tendrán en cuenta durante la fase de análisis de éste tipo de archivos.

[100] Ver apartado Glosario de Términos para su mayor comprensión.
Ver apartado Referencia Bibliográfica II: Páginas Web numeral 49.
[101] Ver apartado Glosario de Términos para su mayor comprensión.

12. **Identificación de archivos existentes.**

    Seguidamente, se clasifican los archivos restantes entre protegidos y no protegidos, donde estos últimos harán parte de los archivos potencialmente analizables, mientras los primeros harán parte la fase de análisis de archivos protegidos.

13. **Identificación de archivos protegidos.**

    Esta es la fase de consolidación de archivos protegidos identificados en las fases anteriores. Durante esta fase se pretende descifrar o romper tal protección en estos archivos, con el fin de adicionarlos al conjunto de archivos potencialmente analizables. Los archivos cuya protección no pudo ser vulnerada formarán parte del conjunto de archivos sospechosos.

14. **Consolidación de archivos potencialmente analizables.**

    Durante esta fase se reúnen todos los archivos encontrados durante las fases de: recuperación de archivos borrados, recuperación de información escondida, identificación de archivos no borrados e identificación de archivos protegidos.

15. **Determinación del sistema operativo y las aplicaciones instaladas.**

    Al determinar el sistema operativo y las aplicaciones instaladas, se está en la capacidad de obtener la lista de compendios criptográficos de los archivos típicos del sistema operativo y de las aplicaciones, para verificar posteriormente la integridad de los estos archivos de encontrarse en la imagen sometida a análisis.

16. **Filtrado basado en archivos buenos conocidos.**

    Con la lista de compendios criptográficos obtenida en el paso anterior, se procede a verificar la integridad de los archivos en la imagen que aparecen en tal lista. Si dicha comprobación es exitosa, éste se considera "bueno" y por lo tanto es descartado del proceso de análisis.

17. **Consolidación de archivos sospechosos[102].**

    Como resultado del filtrado de "buenos" conocidos, se obtiene un conjunto de archivos susceptibles a análisis, este conjunto se llamará archivos sospechosos.

18. **Primera Clasificación.**

    Divide los archivos sospechosos en:

    - Archivos "buenos" modificados: Son identificados en la fase de filtrado como archivos buenos cuya versión original (descrita por la lista obtenida en el paso 15) ha sido modificada.
    - Archivos "malos": Se obtienen a partir de la comparación de los archivos sospechosos contra los compendios criptográficos de archivos "malos" relacionados con el sistema operativo particular. Estos archivos representan algún tipo de riesgo para el sistema en el que se encuentran o se ejecutan, por ejemplo: troyanos, *backdoors*[103] *y virus*, entre otros.
    - Archivos con extensión modificada: Aquellos cuya extensión no es consistente con su contenido.

    Los archivos que cumplen alguna de las anteriores características se convierten en archivos prioritarios para el análisis. Los que no cumplen con estas características se someten a la siguiente etapa de clasificación.

[102] Ver apartado Glosario de Términos para su mayor comprensión.
[103] Ver apartado Glosario de Términos para su mayor comprensión.

19. **Segunda Clasificación.**

    Esta clasificación toma archivos que no han sido considerados de máxima prioridad, los examina y los evalúa respecto a dos criterios: relación de los archivos con los usuarios involucrados en la investigación y contenido relevante para el caso, derivado del marco circunstancial.

    El resultado de esta clasificación es seleccionar como prioritarios para el análisis a los archivos que sean identificados bajo los anteriores criterios.

20. **Analizar los archivos.**

    Este proceso se basa en la discriminación de los archivos prioritarios con respecto a su relevancia con el caso y el criterio del investigador.

    Es importante resaltar que los procesos de la segunda clasificación y análisis, pueden ser iterativos con el fin de obtener más cantidad de evidencia pertinente. En cada iteración cada archivo de alta prioridad puede ser descartado o catalogado como archivo comprometido en el caso, y los archivos con poca prioridad son sometidos a una nueva iteración.

    Este proceso cesa cuando el investigador, a partir de su criterio y experiencia, considera suficiente la evidencia recolectada para resolver el caso, o por que se agotan los datos por analizar.

21. **Archivos comprometidos con en el caso.**

    Es el conjunto de archivos que forman parte de la evidencia del caso.

22. **Obtención de la línea de tiempo definitiva.**

    Se procede a realizar la reconstrucción de los hechos a partir de los atributos de tiempo de los archivos, lo que permite correlacionarlos enriqueciendo la evidencia.

    Es importante resaltar que en algunas ocasiones, y dependiendo del sistema de archivos del volumen analizado, puede ser imposible realizar un análisis temporal, situación que como todos los hallazgos, debe ser consignada en el informe.

23. **Generación del informe**

    Se elabora el informe de hallazgos, que contiene una descripción detallada de los hallazgos relevantes al caso y la forma como fueron encontrados, apoyándose en la documentación continua de la aplicación metodológica.

Para conocer mas metodologías que se utilizan para aplicar la informática forense ver CD apartado METODOLOGIAS

B- HERRAMIENTAS INFORMÁTICO FORENSE

El análisis forense informático es una ciencia que está tomando valor para diversos ámbitos, ya sea desde casos cotidianos por ejemplo robo de identidad, clonación de tarjetas hasta casos en empresas como robo de información o mala manipulación de la información.

Para todos estos eventos el encargado de realizar el análisis forense necesita de herramientas que faciliten esta tarea, a continuación se presenta una serie de herramientas informáticas forenses comerciales como gratuitas que son utilizadas en el análisis forense informático.

I. APLICACIONES COMERCIALES

a. ENCASE FORENSIC

Véase la ***tabla N° 31***para una mayor comprensión de la herramienta forense Encase Forensic.

Descripción del producto.	Requerimiento de sistema mínimos recomendables[104].
EnCase Forensic es el estándar de la industria en tecnología de investigación forense informática. Con una interfaz gráfica del usuario intuitiva, análisis superior, soporte mejorado de correo electrónico/Internet y motor potente de scripting, EnCase proporciona a los investigadores una herramienta única, capaz de realizar investigaciones complejas y a gran escala de principio a fin. Funcionarios encargados del cumplimiento de la ley, investigadores gubernamentales/corporativos y consultores en todo el mundo se benefician de la potencia de EnCase Forensic.	**Software.** Windows 2000, XP ó 2003 Server **Hardware** - Procesador Intel de 3 GHz o superior recomendado. - 1 GB de RAM (se recomienda 2 GB o más) - Puertos USB. Se recomienda un amplio espacio de almacenamiento de datos para admitir la adquisición de archivos de evidencia.

Tabla N° 31: Descripción y Requerimientos de Encase

[104] Ver apartado Referencia Bibliográfica II: Páginas Web numeral 69.

a.1. CARACTERÍSTICAS DE ENCASE FORENSIC

Las dos características principales que hacen de EnCase una herramienta software única son la variedad de sistemas operativos y sistemas de archivos que admite. Para cada sistema operativo existen varios sistemas de archivos que pueden utilizarse en un equipo. El sistema operativo y el sistema de archivos son elementos distintos pero tienen una estrecha relación en cuanto a cómo almacenan la información y cómo el sistema operativo interactúa con el sistema de archivos. La capacidad de analizar con profundidad un amplio rango de sistemas operativos y sistemas de ficheros es un componente crítico en las investigaciones. EnCase tiene la capacidad de analizar todos los sistemas de archivos, para los cuales se ha desarrollado un Servlet[105] (actualmente Windows, Linux, Solaris, AIX y OSX; está en camino el soporte de más sistemas). Además, EnCase puede interpretar otros sistemas de archivos para los cuales actualmente no existe un Servlet desarrollado.

- Sistemas Operativos: Windows 95/98/NT/2000/XP/2003 Server, Linux Kernel 2.4 y superior, Solaris 8/9 en 32 y 64 bits, AIX, OSX.
- Sistemas de archivos: FAT12/16/32, NTFS, EXT2/3 (Linux), Reiser (Linux), UFS (Sun Solaris), AIX Journaling File System (JFS y jfs), LVM8, FFS (OpenBSD, NetBSD y FreeBSD), Palm, HFS, HFS+ (Macintosh), CDFS, ISO 9660, UDF, DVD y TiVo 1 y 2.

En exclusiva soporta la realización de imágenes y el análisis de RAID, de tipo software y hardware. El análisis forense de RAID es casi imposible fuera del entorno de EnCase.

- Soporte para discos dinámicos de Windows 2000/XP/2003 Server.
- Capacidad para previsualizar dispositivos Palm.
- Capacidad para interpretar y analizar VMware[106], Microsoft Virtual PC, e imágenes de DD[107] y Safeback[108] v2.

a.1.1. Características de encase:

- **Copiado comprimido de discos fuente.** Encase emplea un estándar sin pérdida (loss-less) para crear copias comprimidas de los discos origen. Los archivos comprimidos resultantes, pueden ser analizados, buscados y verificados, de manera semejante a los normales (originales). Esta característica ahorra espacio en el disco, permitiendo trabajar en una gran diversidad de casos al mismo tiempo, examinando la evidencia y buscando en paralelo.
- **Búsqueda y análisis de múltiples partes de archivos adquiridos.** EnCase permite al examinador buscar y analizar múltiples partes de la evidencia. Muchos investigadores involucran una gran cantidad de discos duros, discos extraíbles, discos "Zip" y otros tipos de dispositivos de almacenamiento de la información. La evidencia se clasifica, si esta comprimida o no, y puede ser colocada en un disco duro y ser examinada en paralelo por el especialista.

[105] Ver apartado Glosario de términos para su mayor comprensión
[106] Ver apartado Glosario de Términos para su mayor comprensión.
[107] Ver apartado Glosario de términos para su mayor comprensión.
[108] Ver apartado Glosario de Términos para su mayor comprensión.

- **Diferente capacidad de almacenamiento.** Los datos pueden ser colocados en diferentes unidades, como Discos duros IDE o SCSI, drives ZIP, y Jazz. Los archivos pertenecientes a la evidencia pueden ser comprimidos o guardados en CD-ROM manteniendo su integridad forense intacta.
- **Varios campos de ordenamiento, incluyendo estampillas de tiempo.** EnCase permite al especialista ordenar los archivos de la evidencia de acuerdo a 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 y extensiones.
- **Análisis compuesto del documento.** EnCase permite la recuperación de archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el slack interno y los datos del espacio unallocated.

a.1.2. Búsqueda automática y análisis de archivos de tipo Zip y archivos adjuntos al correo electrónico.

- **Análisis electrónico del rastro de intervención.** Sellos de fecha, sellos de hora, registro de accesos y la actividad de comportamiento reciclado son a menudo puntos críticos de una investigación por computadora. EnCase proporciona los únicos medios prácticos de recuperar y de documentar esta información de una manera no invasora y eficiente.
- **Soporte de múltiples sistemas de archivo.** EnCase reconstruye los sistemas de archivos forenses en DOS, Windows (todas las versiones), Macintosh (MFS, HFS, HFS+), Linux, UNIX (Sun, Open BSD), CD-ROM, y los sistemas de archivos DVD-R.

  Vista de archivos y otros datos en el espacio Unallocated. EnCase provee una interfaz tipo Explorador de Windows y una vista del Disco Duro de origen, también permite ver los archivos borrados y todos los datos en el espacio Unallocated. También muestra el Slack File con un color rojo después de terminar el espacio ocupado por el archivo dentro del cluster, permitiendo al investigador examinar inmediatamente y determinar cuándo el archivo reescrito fue creado. Los archivos Swap y Print Spooler[109] son mostrados con sus estampillas de datos para ordenar y revisar.
- **Integración de reportes.** EnCase genera el reporte del proceso de la investigación forense como un estimado. En este documento realiza un análisis y una búsqueda de resultados, en donde se muestra el caso incluido, la evidencia relevante, los comentarios del investigador, favoritos, imágenes recuperadas, criterios de búsqueda y tiempo en el que se realizaron las búsquedas.

a.2. COSTO DE ENCASE

- Gobierno y Educación $2,850.00
- Sector Privado $3,600.00

[109] Ver apartado Glosario de Términos para su mayor compresión.

b. WINHEX

En la ***tabla N° 32*** se presenta información sobre esta herramienta.

Descripción del producto	Requerimientos mínimos de sistema.
WinHex es un editor hexadecimal universal, apropiado para informática forense, recuperación de archivos, peritaje informático, procesamiento de datos de bajo nivel y seguridad informática.	**Software** Windows XP ó 2003 Server **Hardware** - Procesador Intel o AMD de 2.1 GHz o superior recomendado. - 512 MB de RAM (se recomienda 1 GB o más) - Amplio espacio de almacenamiento de datos.

Tabla N° 32: Descripción y Requerimientos de WinHex

b.1. CARACTERÍSTICAS PRINCIPALES DE WINHEX

- Editor de disco por FAT, NTFS, Ext2/3, ReiserFS[110], Reiser4, UFS, CDFS, UDF.
- Función de interpretación de los discos RAID[111] y los sistemas dinámicos
- Diversas técnicas de recuperación de datos.
- Editor de RAM, una manera de editar RAM y la memoria virtual de otros procesos
- Intérprete de Datos que reconoce hasta 20 tipos distintos de datos
- Edición de estructuras de datos mediante plantillas
- Concatenar, partir, unir, analizar y comparar archivos
- Funciones de búsqueda y reemplazo especialmente flexibles
- Imágenes y backups de discos (comprimibles o divisibles en archivos de 650 MB)
- Obtención de imágenes de discos y clonación de discos.
- Cifrado de 128 bits, MD5, digestos de 256 bits, CRC32, sumas de control
- interfaz de programación (API) y scripts
- Encriptación AES[112] de 256 bits, checksums, CRC32, digests (MD5, SHA-1)
- Borrado irreversible de datos confidenciales/privados
- Importación de todos los formatos de portapapeles

[110] Ver apartado Glosario de Términos para su mayor comprensión.
[111] Ver apartado Glosario de Términos para su mayor comprensión.
[112] Ver apartado Glosario de términos para su mayor comprensión

- Formatos de conversión: Binario, Hex, ASCII.
- Juego de caracteres: ANSI ASCII, IBM ASCII, EBCDIC
- Ver y manipular los archivos que normalmente no se pueden editar
- Ocultación de datos o descubrimiento de datos ocultos.

b.2. AMBIENTE DE WINHEX

A continuación se presenta el entorno de WinHex en la ***figura N°9***.

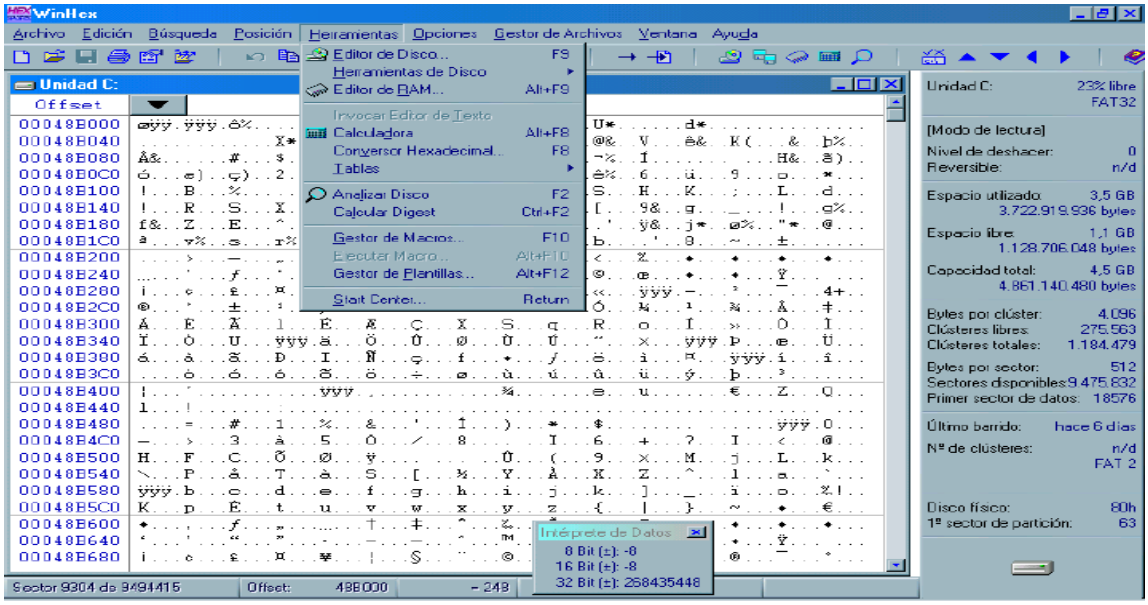


Figura N° 9: Entorno de WinHex

b.3. COSTO DE WINHEX

$50.00

Para conocer mas de herramientas informaticas ver CD apartado HERRAMIENTAS INFORMATICAS

C- FORMATOS DE INFORMES PERICIALES UTILIZADOS EN INFORMATICA FORENSE

I. FORMATOS DE REPORTE DE CADENA DE CUSTODIA UTILIZADOS EN INFORMÁTICA FORENSE

El resguardo de la cadena de custodia es un elemento muy importante dentro del análisis que se realiza a cualquier tipo de evidencia encontrada en la escena del crimen, ya que es un conjunto de procesos y documentación que permiten acreditar e identificar sin ningún tipo de dudas a la evidencia y asegurar que la recolección de la misma se ha realizado siguiendo los procedimientos legalmente establecidos.

Por lo cual se hace necesario el contar con formatos ya establecidos de cómo llevar a cabo dicho procedimiento. Es por esta razón que a continuación se presentan dos tipo de formatos para la cadena de custodia.

a. FORMATO N°1: CADENA DE CUSTODIA

En este apartado se muestra tanto el formato de la cadena de custodia como la descripción de cada uno de los elementos que la conforman.

a.1. FORMATO DEL FORMULARIO DE CADENA DE CUSTODIA

A continuación se presentan un formatos de cadena de custodia, ***Figura N° 10***.

(ABRIR SOLO POR EL PERSONAL AUTORIZADO)

Presentado por la Agencia: _____

Caso N°: _____ Elemento N°: _____

Fecha de Recolección: _____ Hora de Recolección: _____

Recogido por: _____ Insignia N°: _____

Descripción Adjunta de la Evidencia _____

_____

_____

Lugar Donde fue Recogida: _____

_____

_____

Tipo de Ofensa: _____

Nombre completo de la víctima:

_____

Nombre completo del sospechoso:

_____

Bolsa sellada por: _____ Paquete N°: _____

– **CADENA DE CUSTODIA** –

De	Para	Fecha

Figura N° 10: Formato de cadena de custodia.

a.2. DESCRIPCIÓN DEL FORMATO DE CADENA DE CUSTODIA

A continuación, en la ***tabla N° 33***, se describen las partes por las cuales está constituido el informe de la cadena de custodia anteriormente expuesto:

Presentado por la agencia	:	Entidad policial responsable de hacer el levantamiento de la evidencia en la escena del crimen.
Caso N°	:	Identificador único con el cual se enumera al caso investigado
Elemento N°	:	Subindicador con el cual se enumera al caso investigado.
Fecha de recolección	:	Fecha en la cual fue recolectada la evidencia.
Hora de recolección	:	Hora en la cual fue recolectada la evidencia.
Recogido por	:	Nombre del elemento policial encargado de recolectar la evidencia.
Insignia N°	:	Número de placa del elemento policial encargado de la recolección de la evidencia.
Descripción adjunta de la evidencia	:	Descripción realizada por el elemento policial sobre la evidencia recolectada y así proporcionar información que se considere relevante para la realización del posterior análisis.
Lugar donde fue recogida	:	Sitio especifico de la escena del crimen donde se realizó la recolección de la evidencia.
Tipo de ofensa	:	Tipo de delito que se presume fue cometido en la escena del crimen.
Nombre completo de la victima	:	Nombre de la persona afectada por el delito.
Nombre completo del sospechoso	:	Nombre de la persona responsable de haber cometido el ilícito.
Bolsa sellada por	:	Nombre del elemento policial responsable de rotular la evidencia embalada.
Paquete N°	:	Identificador numérico que especifica el paquete donde esta almacenada toda la evidencia recolectada.
De	:	Nombre remitente responsable que solicita el análisis a la evidencia recolectada.
Para	:	Nombre del destinatario donde se realizara el posterior análisis a la evidencia.
Fecha	:	Fecha en la cual es enviada la evidencia para su análisis. (Inicio de la cadena de custodia)

Tabla N° 33: Descripción de los campos contenidos en el formulario de cadena de custodia del primer formato.

b. FORMATO N°2: CADENA DE CUSTODIA

En este apartado se muestra tanto el formato de la cadena de custodia como la descripción de cada uno de los elementos que la conforman.

b.1 FORMATO DE CADENA DE CUSTODIA

A continuación se presenta el formato de cadena de custodia en ingles, ***Figura N°11***, pero posteriormente, en la parte de la descripción del formato se traducen cada uno de los términos expuesto.

Este formato fue retomado de una de las herramientas informáticos forenses que fueron referidas por los peritos informáticos forenses internacionales, cuando se llevo a cabo la encuesta, como parte de las herramientas que ellos utilizan en sus análisis periciales. El nombre de esta herramienta es HELIX[113] y esta aplicación le proporciona su propio modelo de cadena de custodia al perito mientras éste realiza sus labores trabajando de manera conjunta con HELIX.

[113] Ver apartado Referencia Bibliográfica II: Páginas Web numeral 71.

Formato de cadena de custodia generado por HELIX

COC-200827001-.pdf

Figura N° 11: Formato de cadena de custodia generada por Hélix.

b.2 DESCRIPCIÓN DEL FORMATO DE CADENA DE CUSTODIA

A continuación, en la ***tabla N° 34***, se presenta la descripción de los elementos que conforman el formulario anteriormente presentado de la cadena de custodia:

Caso No (Case No)	:	Identificador único con el cual se enumera al caso investigado
Página (Page)	:	Número de página actual.
De (Of)	:	Número de páginas totales que contiene el informe.
DETALLES DE MEDIOS ELECTRÓNICOS/COMPUTACIONALES (Electronic media/computer details)		
Elemento No (Item No)	:	Identificador con el que se enumera el dispositivo de almacenamiento embalado en la escena del crimen para realizar su posterior análisis.
Descripción (Description)	:	Descripción de las características físicas del dispositivo de almacenamiento incautado.
Fabricante (Manufacturer)	:	Nombre del fabricante del dispositivo de almacenamiento.
Modelo No (Model No)	:	Número del modelo del dispositivo de almacenamiento.
Serie No (Serial No)	:	Número de serie del dispositivo de almacenamiento.
DETALLES DE LA IMAGEN (Image details)		
Fecha/ Hora (Date/ Time)	:	Fecha y hora de la creación de la imagen del dispositivo de almacenamiento a ser analizado.
Creado por (Created by)	:	Nombre del responsable de la creación de la imagen del dispositivo de almacenamiento.
Método usado (Method used)	:	Nombre del método utilizado para la generación de la imagen del dispositivo de almacenamiento.
Nombre de la imagen (Image name)	:	Nombre asignado a la imagen creada del dispositivo de almacenamiento.
Segmentos (Segments)	:	Numero de segmentos con los cuales cuenta el dispositivo de almacenamiento.
Dispositivo de almacenamiento (Storage drive)	:	Nombre y tipo del dispositivo de almacenamiento.
HASH (HASH)	:	Número HASH con el cual se identifica unívocamente a la imagen creada del dispositivo de almacenamiento.
CADENA DE CUSTODIA (Chain of custody)		
Seguimiento No (Tracking No)	:	Número de seguimiento asignado a la cadena de custodia del dispositivo de almacenamiento incautado.
Fecha/ Hora	:	Fecha en la cual es enviada la evidencia para su análisis. (Inicio de la cadena de

(Date/ Time)		custodia)
Remitente (From)		
Nombre/ Organización (Name / Org)	:	Nombre de la persona o de la organización remitente que solicita el análisis del dispositivo de almacenamiento incautado.
Destinatario (To)		
Nombre/ Organización (Name / Org)	:	Nombre de la persona o de la organización destinatario donde se realizara el posterior análisis del dispositivo de almacenamiento incautado.
Motivo (Reason)	:	Razones por las cuales se transfiere la evidencia, el dispositivo de almacenamiento para ser analizado, de un lugar a otro.

Tabla N° 34: Descripción de los campos contenidos en el formulario de cadena de custodia generado por Hélix.

II. FORMATOS DE INFORMES PERICIALES UTILIZADOS EN INFORMÁTICA FORENSE[114]

En esta sección se aborda el tema de que es y que contiene un informe pericial, además se expondrán dos ejemplos de informes proporcionados por 2 peritos internacionales los cuales han sido presentados por ellos cuando han realizado análisis a la evidencia digital para un juicio.

a. QUE ES UN INFORME PERICIAL

El informe pericial es el documento redactado por el perito informático, en el que se exponen las conclusiones obtenidas por el experto, tras la investigación de un caso de delito informático**.**

b. CONTENIDO DE UN INFORME PERICIAL

El Informe pericial debe incluir:

- Los datos del cliente.
- Los objetivos de la investigación.
- La declaración previa del perito informático, en la que se establecen los principios de profesionalidad, veracidad e independencia.
- Documentación sobre el proceso de adquisición de pruebas.
- Detalle de las acciones que el perito informático lleva a cabo durante la investigación.
- Resultados de la investigación informática y conclusiones.

c. PROCESO DE ELABORACIÓN DE UN INFORME PERICIAL

La elaboración del informe consta a su vez de tres fases, las cuales se han representado por medio de un Flujograma el cual explica la secuencia de pasos que se siguen para su elaboración:

Explicación de la secuencia seguida en el Flujograma:

- El proceso inicia con la Fase 1, cuando la evidencia recolectada en la escena del crimen es entregada al perito para que éste realice el posterior análisis.
- Luego el perito certifica que la evidencia este correctamente embalada para verificar si no ha sido anteriormente contaminada antes de realizar el análisis y verifica que la cadena de custodia no haya sido quebrantada durante el proceso de recolección de la misma.
- Si estos dos elementos se han trabajado correctamente el perito recoge la evidencia y pasa a la Fase 2 donde se realiza el análisis. Una vez concluida la Fase 2 el perito pasa a la Fase 3 donde se elabora el informe pericial con la explicación del análisis realizado y las conclusiones a las cuales se llego. Para luego ser entregado al Fiscal encargado del caso o a la entidad competente que ha

[114] Ver apartado Referencia Bibliográfica II: Páginas web numeral 72.

solicitado el análisis de la evidencia digital y finaliza el proceso de la elaboración del informe pericial.

- De lo contrario, si la cadena de custodia fue quebrantada y/o la evidencia no está embalada correctamente, el perito no acepta la evidencia que se le entrega y le notifica a su superior para que se realicen las averiguaciones y se brinden las explicaciones pertinentes.

A continuación, en la ***figura N° 12***, se presenta el Flujograma con la explicación anteriormente brindada y posteriormente se describen con mayor dellate las fases anteriormente mencionadas:

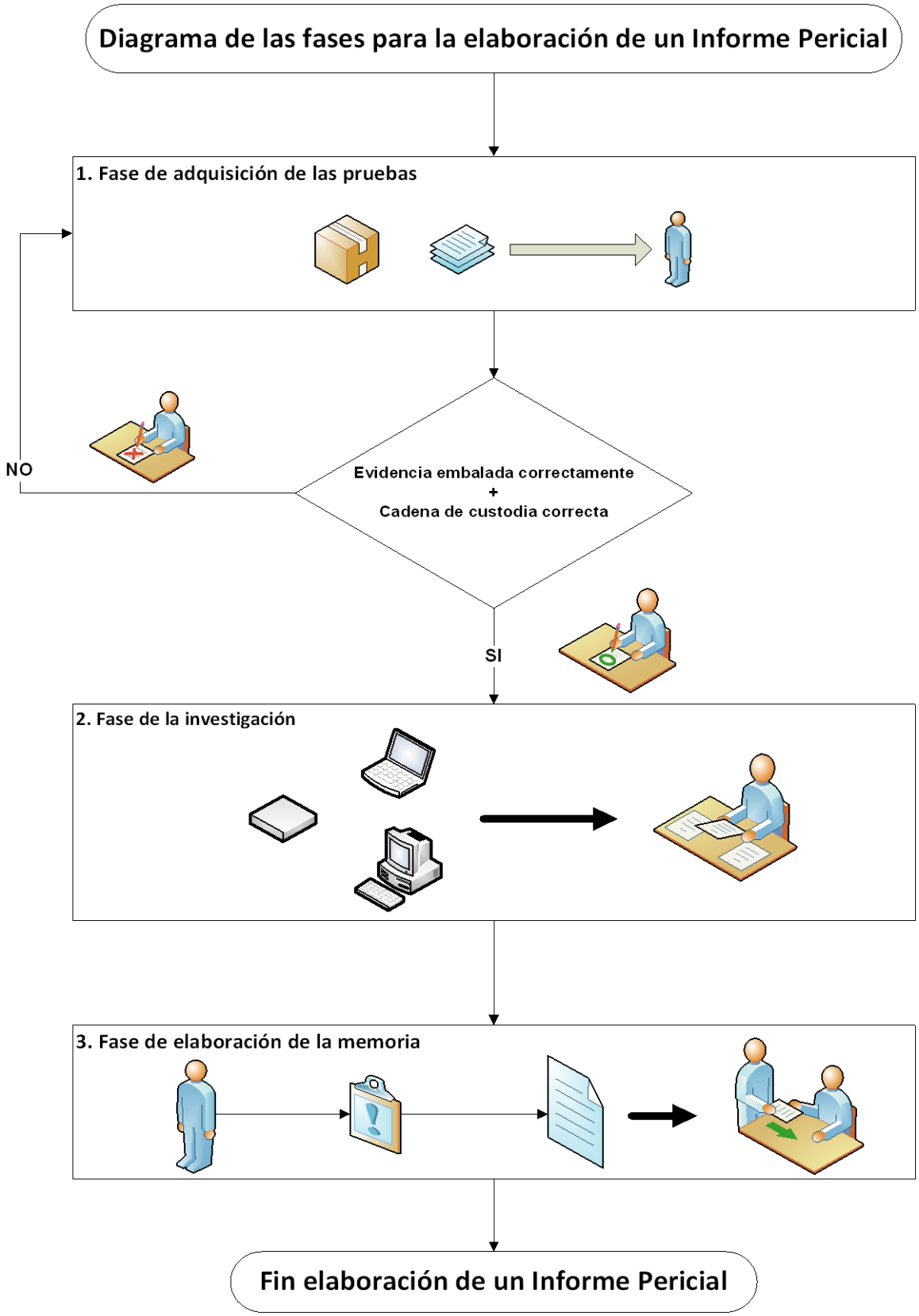


Figura N° 12: Flujograma de las fases a seguir para la elaboración de un informe pericial.
Fuente: Elaboración propia.

1. **Fase de adquisición de las pruebas:**

   Recogida de todos elementos que van a intervenir en la investigación. Es importante que el proceso de intervención de los equipos informáticos se lleve a cabo con todas las garantías para las partes. La documentación del proceso de adquisición de las pruebas es una información que debe formar parte del informe pericial.

2. **Fase de la investigación:**

   El perito informático realiza un análisis exhaustivo de los equipos informáticos, especialmente de las unidades de almacenamiento de datos en busca de todos aquellos elementos que puedan constituir prueba o evidencia electrónica en el caso en cuestión.

   Constarán en el informe todos las acciones realizadas durante la fase de investigación, como las herramientas empleadas para la adquisición de la evidencia electrónica y el detalle y resultado de los procesos efectuados sobre el dispositivo o unidad que se está analizando.

3. **Fase de elaboración de la memoria:**

   Tras el minucioso estudio de la información almacenada en los dispositivos, intervenidos en la fase de adquisición de pruebas, el perito informático analiza los resultados obtenidos con el fin de extraer las conclusiones finales de la investigación.

   En esta última fase, el perito informático recopila la información que ha obtenido durante todo el proceso de investigación y redacta el informe o memoria que se presentará ante los Tribunales. En algunas ocasiones, un buen informe pericial elaborado con veracidad y exactitud ha llevado a que ambas partes ofendidas hayan llegado a un acuerdo, sin que el juicio llegue a celebrarse.

d. EJEMPLO N°1: CONTENIDO DEL INFORME PERICIAL MOSTRADO EN ESPAÑA[115]:

Partes del informe pericial.

El informe pericial debe de indicar con cuantas hojas está conformado.

Ejemplo: El presente informe consta de hojas numeradas de 1 a X.

d.1. IDENTIFICACIÓN

En la etapa de identificación el informe deberá de contener:

- Nombre e identificación del investigador encargado del informe.
- De quien recibe los elementos para realizar el informe forense.
- Petición de que Juzgado.
- Acusación realizada en el juzgado.
- Interrogantes formuladas relacionadas con la evidencia.

Ejemplo:
El presente informe pericial es realizado por José Pérez, Informático forense, con PLACA xxxxxx-x.

Recibe la evidencia a través de David Pérez de la PNC, División Contra el Crimen, con PLACA xxxxxx-x.

A petición del Juez del Juzgado de Primero de Instrucción de San Salvador de Asuntos Civiles, por la causa de pornografía infantil.

Se ha encomendado dar respuesta a las siguientes interrogantes:

1. *Determinar el contenido de los medios de almacenamiento decomisados al imputado.*
2. *.*
3. *.*
4. *.*
5. *Cualquier otro dato que considere necesario para el buen proveer de la sala.*

[115] Proporcionado por experto informático de España

d.2 METODOLOGÍA

La etapa de la metodología debe de contener lo siguiente:

- Descripción del la evidencia que recibe *(Autenticidad de la evidencia, documentación adjunta a la evidencia, integridad de la evidencia)*.
- Documentar los procedimientos realizados.
- La metodología empleada para tratar la evidencia en esta etapa debe de incluir una breve descripción del proceso realizado *(Ejemplo: RFC3227)*
- Herramientas utilizadas.

***Ejemplo**: Se realizo una copia de la evidencia trabajando con los siguientes archivos, con sus respectivos algoritmos hash:*

PR2008-xxxxxxxx.md5	*PR = Pre-imagen del elemento N °xxxxx.*	*Hash 011120021f255sa0215s*
DI2008- xxxxxxxx*.img*	*DI = Imagen del elemento N °xxxxx.*	*Hash 011120021f255sa0215s*
PO2008- xxxxxxxx*.md5*	*PO = Imagen final del estudio de los elementos N °xxxxx.*	*Hash 011120021f255sa0215s*

d.3. RESULTADOS

El investigador debe dar a conocer en esta etapa:

- Estado: El estado del caso Abierto o Cerrado.
- Sumario de lo encontrado: Descripción y el contenido de los elementos de los dispositivos de almacenamiento estudiados, con una breve descripción de su contenido.
- Detalles de lo encontrado: dirección física de los archivos que son parte de las preguntas planteadas al inicio del reporte.
- Glosario: una lista de los elementos encontrados.
- Reporte de los elementos utilizados: Cuantos discos fueron usados para elaborar la copia, si se utilizo otros dispositivos de almacenamiento que contienen evidencia, etc. (estos elementos deben estar debidamente rotulados y documentados).

Ejemplo:

1. Estado: *Cerrado.*

2. Sumario de lo encontrado:

■ *327 archivos con imágenes de menores de edad en actividades sexuales.*
■ *34 Videos relacionados con actividades de menores de edad en actividades sexuales.*

3. Elementos Analizados:

Caso N°:	***Descripción del caso:***
XXXXXXXXX	*Disco duro de laptop, Capacidad de 30Gb, Marca XXXX, Modelo ABCDE, Serial # 123456789*

4. Detalles encontrados.

■*Se encontró en el disco duro Modelo ABCDE, Serial # 3456ABCD, De la Marca XXXXX, fichada con el caso 123*

1. *El examen del disco duro revelo el sistema operativo Microsoft Windows® 98.*
2. *En el Directorio C:\JOHN DOE\PERSONAL\FAV PICS\, se encontró 327 archivos de imagen, con formato *.jpg, estos archivos contienen material explicito de actividades sexuales de menores de edad… última fecha de acceso aaaa/mm/dd….*
3. .
4. .

5. Glosario:

6. Elementos utilizados: *se realizaron dos copias de la evidencia utilizando dos discos de 30Gb de capacidad, Marca XXXX, Modelo ABCDE, Serial # 123456789 …*

d.4 CONCLUSIONES

En dicha etapa el investigador debe de dar a conocer las respuestas a las interrogantes planteadas en la etapa I.

Ejemplo

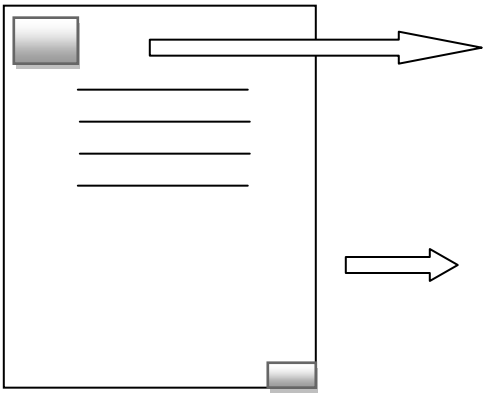
1. Determinar el contenido de los medios de almacenamiento decomisados al imputado contienen material pornográfico de carácter infantil.
R/ Se logro encontrar fotografías así como videos que presentan escenas sexuales en la que se ha involucrado menores de edad……

e. EJEMPLO N°2: CONTENIDO DEL INFORME PERICIAL MOSTRADO EN ARGENTINA[116]:

e.1 ETAPA I: CARACTERÍSTICAS DEL INFORME PERICIAL

El informe pericial inicia con la ubicación del juzgado que solicita el informe pericial en la esquina superior izquierda de la siguiente manera:

Ejemplo:



Juzgado Primero de Instrucción de San Salvador de Asuntos Civiles. Centro Judicial Isidro Menéndez

Numeración de páginas y cuantas son en total. (Ejemplo: 2 de 18)

Posteriormente el encabezado del documento el cual puede ser el siguiente:

Ejemplo: *Perito en Análisis de sistemas contesta pedido de explicaciones.*

e.2 ETAPA II: INFORMACIÓN DEL EXPERTO Y DEL CASO A INVESTIGACIÓN

- Los datos del experto en informática (Ubicación geográfica, documentos que demuestren la calidad de experto en el tema, documentos de identidad personal)
- Designación del caso en el cual realizara la experticia.
- A que institución representa (Ejemplo Fiscalía, PNC, Procuraduría)
- Detalle de las acciones que el perito realizara durante la investigación.

Ejemplo:
Pedro Pérez, Ingeniero en Sistemas informáticos, Máster en Sistemas Inteligentes, Matricula de Profesional XXXX-XX del consejo de Ingenieros Informáticos, labora en Departamento XXXXXX de la Policía Nacional Civil con dirección xxx-xxxx, San Salvador El Salvador, designado como perito de oficio en el caso titulado "XXXX-XXXX". Representante de la Policía Nacional Civil.
Que tramita por ante este Tribunal, me presento y expongo:

1) Que vengo en tiempo y forma a contestar los pedidos de explicaciones a mi dictamen pericial formulado por ambas partes en litigio.

2) Que metodológicamente iré reproduciendo uno a uno los pedidos de explicaciones de cada una de las partes, para luego responderlos a continuación…..

[116] Proporcionado por experto informático de Argentina.

e.3 ETAPA III: ADQUISICIÓN Y DOCUMENTACIÓN

En esta sección se generan las preguntas que se espera pueda contestar el experto en el área, se recogen todos los elementos que intervienen en la investigación.

mplo:

1. *En la evidencia encontrada puede establecer la relación de las extorciones cometidas, fraudes y piratería realizada por José Pérez a la empresa XYZ.*
2. .
3. .
4. .

e.4 ETAPA IV: INVESTIGACIÓN

El perito informático ejecutara un estudio y profundo de los equipos informáticos, especialmente de las unidades de almacenamiento de datos (discos duros, unidades de CD/DVD, USB, etc.) en busca de todos aquellos elementos que puedan constituir prueba o evidencia electrónica en el caso en cuestión.

Construirá un informe que mencionen las acciones realizadas durante la fase de investigación, como las herramientas empleadas para la adquisición de la evidencia electrónica y el detalle y resultado de los procesos efectuados sobre el dispositivo o unidad que se está analizando.

e.5 ETAPA V: CONCLUSIONES

El investigador brinda respuestas a las interrogantes que se formularon al principio de la investigación y las que se les pide que realice los acusadores o defensores.

e.6 ETAPA VI: PETICIONES DEL PERITO (OPCIONALES)

En esta etapa el investigador puede gestionar sus servicios profesionales.

Ejemplo:

a) *se tenga por presentado en tiempo y forma estas las aclaraciones y explicaciones a mi dictamen pericial,*

b) *Se tengan presentes las mencionadas explicaciones y aclaraciones.*

c) *Oportunamente se regulen mis honorarios profesionales fijándolos en el máximo que autoriza la Ley, merituando, importancia, extensión y calidad del presente dictamen, como así también el valor para administrar justicia que ha tenido para dictar sentencia.*

III. PROPUESTAS DE FORMATOS DE INFORMES DE CADENA DE CUSTODIA Y PERICIALES

En esta sección se presentan propuestas de los formatos para la elaboración de informes tanto para la cadena de custodia como para la elaboración del informe pericial, estos formatos se elaboraron con la cooperación de los peritos internacionales que nos proporcionaron los ejemplos de los formatos anteriormente descritos en el apartado I y II de este mismo capitulo y acoplándolos al entorno de nuestro país. Además se presenta la descripción de cada campo que contienen los informes.

a. PROPUESTA DE INFORME DE CADENA DE CUSTODIA

a.1. FORMATO DEL INFORME DE CADENA DE CUSTODIA

A continuación, en la ***tabla N° 35***, se presenta el formato propuesto en esta investigación sobre el informe de cadena de custodia y en la ***tabla N° 36*** se presenta la descripción contenidos en dicho formato:

EVIDENCIA ELECTRÓNICA FORMULARIO DE CADENA DE CUSTODIA

Presentado por la División:

ABRIR SOLO PERSONAL AUTORIZADO

Caso N°:		**Página:**	**De:**
Fecha de Recolección:		**Hora de Recolección:**	
Recogida por: Apellidos	**Nombres**	**Número de insignia:**	
Lugar de la Recolección:			
Tipo de Ofensa:			
Nombre completo de la víctima: Apellidos	**Nombres**		
Nombre completo del sospechoso: Apellidos	**Nombres**		
Bolsa sellada por: Apellidos	**Nombres**	**Número de Insignia:**	
Número del paquete:			

DETALLES DE MEDIOS ELECTRÓNICOS/COMPUTADORAS

Número del elemento:	**Descripción:**	
Fabricante:	**Número de modelo:**	**Número de serie:**

DETALLES DE LA IMAGEN

Creado por:	

Apellidos		Nombres	
Fecha/ Hora:	**Método usado:**	**Nombre de la imagen:**	**Segmentos:**
Dispositivo de almacenamiento:		**HASH:**	

CADENA DE CUSTODIA				
Número de seguimiento:	**Fecha/ Hora:**	**Remitente:**	**Destinatario:**	**Motivos:**
	Fecha	**Organización/Apellido-Nombre:**	**Organización/Apellido-Nombre:**	
	Hora	**Firma:**	**Firma:**	
	Fecha	**Organización/Apellido-Nombre:**	**Organización/Apellido-Nombre:**	
	Hora	**Firma:**	**Firma:**	
	Fecha	**Organización/Apellido-Nombre:**	**Organización/Apellido-Nombre:**	
	Hora	**Firma:**	**Firma:**	
	Fecha	**Organización/Apellido-Nombre:**	**Organización/Apellido-Nombre:**	
	Hora	**Firma:**	**Firma:**	
	Fecha	**Organización/Apellido-Nombre:**	**Organización/Apellido-Nombre:**	
	Hora	**Firma:**	**Firma:**	

Descripción adjunta de la Evidencia:

Tabla N° 35: Formato propuesta de informe de cadena de custodia.

a.2. DESCRIPCIÓN DEL INFORME DE CADENA DE CUSTODIA

NOMBRE DEL CAMPO		DESCRIPCIÓN
Presentado por la agencia	:	Entidad policial responsable de hacer el levantamiento de la evidencia en la escena del crimen.
Caso N°	:	Identificador único con el cual se enumera al caso investigado
Página	:	Número de página actual.
De	:	Número de páginas totales que contiene el informe.
Fecha de recolección	:	Fecha en la cual fue recolectada la evidencia.
Hora de recolección	:	Hora en la cual fue recolectada la evidencia.
Recogido por	:	Nombre del elemento policial encargado de recolectar la evidencia.
Insignia N°	:	Número de placa del elemento policial encargado de la recolección de la evidencia.
Lugar de la Recolección	:	Sitio especifico de la escena del crimen donde se realizó la recolección de la evidencia.
Tipo de ofensa	:	Tipo de delito que se presume fue cometido en la escena del crimen.
Nombre completo de la victima	:	Nombre de la persona afectada por el delito.
Nombre completo del sospechoso	:	Nombre de la persona responsable de haber cometido el ilícito.
Bolsa sellada por	:	Nombre del elemento policial responsable de rotular la evidencia embalada.
Paquete N°	:	Identificador numérico que especifica el paquete donde esta almacenada toda la evidencia recolectada.
DETALLES DE MEDIOS ELECTRÓNICOS/COMPUTADORAS		
Número del Elemento	:	Identificador con el que se enumera el dispositivo de almacenamiento embalado en la escena del crimen para realizar su posterior análisis.
Descripción	:	Descripción de las características físicas del dispositivo de almacenamiento incautado.
Fabricante	:	Nombre del fabricante del dispositivo de almacenamiento.
Número de Modelo	:	Número del modelo del dispositivo de almacenamiento.
Número de Serie	:	Número de serie del dispositivo de almacenamiento.
DETALLES DE LA IMAGEN		
Creado por	:	Nombre del responsable de la creación de la imagen del dispositivo de almacenamiento.
Fecha/ Hora	:	Fecha y hora de la creación de la imagen del dispositivo de almacenamiento a ser analizado.
Metodo usado	:	Nombre del método utilizado para la generación de la imagen del dispositivo de almacenamiento.
Nombre de la imagen	:	Nombre asignado a la imagen creada del dispositivo de almacenamiento.
Segmentos	:	Numero de segmentos con los cuales cuenta el dispositivo de almacenamiento.
Dispositivo de almacenamiento	:	Nombre y tipo del dispositivo de almacenamiento.
HASH	:	Número HASH con el cual se identifica unívocamente a la imagen creada del dispositivo de almacenamiento.

NOMBRE DEL CAMPO		DESCRIPCIÓN
CADENA DE CUSTODIA		
Número de Seguimiento	:	Número de seguimiento asignado a la cadena de custodia del dispositivo de almacenamiento incautado.
Fecha/ Hora	:	Fecha en la cual es enviada la evidencia para su análisis. (Inicio de la cadena de custodia)
Remitente		
Nombre/ Organización	:	Nombre de la persona o de la organización remitente que solicita el análisis del dispositivo de almacenamiento incautado.
Destinatario		
Nombre/ Organización	:	Nombre de la persona o de la organización destinatario donde se realizara el posterior análisis del dispositivo de almacenamiento incautado.
Motivo	:	Razones por las cuales se transfiere la evidencia, el dispositivo de almacenamiento para ser analizado, de un lugar a otro.
Firma	:	Firma de la persona remitente y destinatario a la hora de recibir la evidencia.
Descripción adjunta de la evidencia	:	Descripción realizada por el elemento policial sobre la evidencia recolectada y así proporcionar información que se considere relevante para la realización del posterior análisis.

Tabla N° 36: Descripción de los campos contenidos en el formulario de cadena de custodia propuesto.

b. PROPUESTA DE INFORME PERICIAL

b.1. FORMATO Y DESCRIPCIÓN DEL INFORME PERICIAL

A continuación se presenta el formato propuesto en esta investigación sobre el informe pericial como guía para la utilización de éste en la presentación del análisis realizado a la evidencia digital por parte del perito.

b.1.1 ENCABEZADO

El informe pericial debe de indicar con cuantas hojas está conformado.

> ***Ejemplo:***
> *El presente informe consta de hojas numeradas de 1 a X.*

b.1.2 IDENTIFICACIÓN

En la etapa de identificación el informe deberá de contener:

- Nombre e identificación del investigador encargado del informe (Ubicación geográfica, documentos que demuestren la calidad de experto en el tema, documentos de identidad personal)
- A que institución representa (Ejemplo Fiscalía, PNC, Procuraduría)
- De quien recibe los elementos para realizar el informe forense.
- Petición de que Juzgado.

- Acusación realizada en el juzgado.
- Detalle de las acciones que el perito realizara durante la investigación.

> ***Ejemplo:***
> *Pedro Pérez, Ingeniero en Sistemas informáticos, Máster en Sistemas Inteligentes, Matricula de Profesional XXXX-XX del consejo de Ingenieros Informáticos con numero de INSIGNIA XXXX, labora en Departamento XXXXXX de la Policía Nacional Civil con dirección xxx-xxxx, San Salvador El Salvador, designado como perito de oficio en el caso titulado "XXXX-XXXX".*
> *Representante de la Policía Nacional Civil.*
> *Recibo la evidencia a través de David Pérez de la PNC, División Contra el Crimen, con INSIGNIA xxxxxx-x.*
> *A petición del Juez del Juzgado de Primero de Instrucción de San Salvador de Asuntos Civiles, por la causa de pornografía infantil.*
> *Que tramita por ante este Tribunal, me presento y expongo:*
> *1) Que vengo en tiempo y forma a contestar los pedidos de explicaciones a mi dictamen pericial formulado por ambas partes en litigio.*
> *2) Que metodológicamente iré reproduciendo uno a uno los pedidos de explicaciones de cada una de las partes, para luego responderlos a continuación…..*

b.1.3 ADQUISICIÓN Y DOCUMENTACIÓN

En esta sección se generan las preguntas que se espera pueda contestar el experto en el área, se recogen todos los elementos que intervienen en la investigación.

> ***Ejemplo:***
> *En la evidencia encontrada puede establecer la relación de tenencia de pornografía infantil al imputado Juan Pérez.*
>
> 1. .
> 2. .

b.1.4 METODOLOGÍA

La etapa de la metodología debe de contener lo siguiente:

- Descripción del la evidencia que recibe *(Autenticidad de la evidencia, documentación adjunta a la evidencia, integridad de la evidencia).*
- Documentar los procedimientos realizados.
- La metodología empleada para tratar la evidencia en esta etapa debe de incluir una breve descripción del proceso realizado *(Ejemplo: RFC3327)*
- Herramientas utilizadas.

Ejemplo:
Se realizo una copia de la evidencia trabajando con los siguientes archivos, con sus respectivos algoritmos hash:

PR2008-xxxxxxxx.md5	*PR = Pre-imagen del elemento N °xxxxx.*	*Hash 011120021f255sa0215s*
DI2008- xxxxxxxx.*img*	*DI = Imagen del elemento N °xxxxx.*	*Hash 011120021f255sa0215s*
PO2008- xxxxxxxx.*md5*	*PO = Imagen final del estudio de los elementos N °xxxxx.*	*Hash 011120021f255sa0215s*

b.1.5 INVESTIGACIÓN

El perito informático ejecutara un estudio y profundo de los equipos informáticos, especialmente de las unidades de almacenamiento de datos (discos duros, unidades de CD/DVD, USB, etc.) en busca de todos aquellos elementos que puedan constituir prueba o evidencia electrónica en el caso en cuestión.

Construirá un informe que mencionen las acciones realizadas durante la fase de investigación, como las herramientas empleadas para la adquisición de la evidencia electrónica y el detalle y resultado de los procesos efectuados sobre el dispositivo o unidad que se está analizando.

b.1.6 RESULTADOS

El investigador debe dar a conocer en esta etapa:

- Estado: El estado del caso Abierto o Cerrado.
- Sumario de lo encontrado: Descripción y el contenido de los elementos de los dispositivos de almacenamiento estudiados, con una breve descripción de su contenido.
- Detalles de lo encontrado: dirección física de los archivos que son parte de las preguntas planteadas al inicio del reporte.
- Glosario: una lista de los elementos encontrados.
- Reporte de los elementos utilizados: Cuantos discos fueron usados para elaborar la copia, si se utilizo otros dispositivos de almacenamiento que contienen evidencia, etc. (estos elementos deben estar debidamente rotulados y documentados).

Ejemplo:
1. Estado: *Cerrado.*

2. Sumario de lo encontrado:
■ *327 archivos con imágenes de menores de edad en actividades sexuales.*
■ *34 Videos relacionados con actividades de menores de edad en actividades sexuales.*

3. Elementos Analizados:

Caso N°:	***Descripción del caso:***
XXXXXXXXX	*Disco duro de laptop, Capacidad de 30Gb, Marca XXXX, Modelo ABCDE, Serial # 123456789*

4. Detalles encontrados.

■*Se encontró en el disco duro Modelo ABCDE, Serial # 3456ABCD, De la Marca XXXXX, fichada con el caso 123*

1. *El examen del disco duro revelo el sistema operativo Microsoft Windows® 98.*
2. *En el Directorio C:\JOHN DOE\PERSONAL\FAV PICS\, se encontró 327 archivos de imagen, con formato *.jpg, estos archivos contienen material explicito de actividades sexuales de menores de edad… última fecha de acceso aaaa/mm/dd….*
3. .
4. .

5. Glosario:

6. Elementos utilizados: *se realizaron dos copias de la evidencia utilizando dos discos de 30Gb de capacidad, Marca XXXX, Modelo ABCDE, Serial # 123456789 …*

b.1.7 CONCLUSIONES

El investigador brinda respuestas a las interrogantes que se formularon al principio de la investigación y las que se les pide que realice los acusadores o defensores.

Ejemplo

1. *Determinar el contenido de los medios de almacenamiento decomisados al imputado contienen material pornográfico de carácter infantil.*

   R/ Se logro encontrar fotografías así como videos que presentan escenas sexuales en la que se ha involucrado menores de edad……

D- PROPUESTA DE CONTENIDOS TEMÁTICOS PARA CAPACITACIONES EN INFORMATICA FORENSE DIRIGIDA A PROFESIONALES EN SISTEMAS INFORMÁTICOS Y PROFESIONALES EN DERECHO

El recurso humano es un elemento muy importante para la aplicación de la informática forense, este debe tener conocimientos amplios de esta ciencia y a la vez conocer sobre la legislación que involucra las investigaciones de delitos informáticos y la tipificación de estos en el código penal. Las investigaciones forenses requieren la colaboración de instituciones encargadas de velar por la seguridad de la sociedad, por lo que el personal involucrado en el esclarecimiento de casos por delitos informáticos deben capacitarse con conocimiento en herramientas que sean capaces de poder determinar a los culpables del delito, es por esta razón que se brinda por medio del presente proyecto dos propuestas de contenido temático sobre informática forense dirigidas a los profesionales de sistemas informáticos y a los profesionales en el área de derecho. Los temarios propuestos tratan de las conceptualizaciones básicas de informática forense, debido a que esta ciencia es nueva en nuestro país y no se tiene un conocimiento amplio de ella.

I. PROPUESTA DE CONTENIDO TEMÁTICO DE INFORMÁTICA FORENSE PARA PROFESIONALES EN SISTEMAS INFORMATICOS.

DESCRIPCION

Es necesario que los estudiantes conozcan las metodologías que son utilizadas en la aplicación de la informática forense para determinar la manera de actuar de personas malintencionadas que hacen uso inadecuado de las tecnologías informáticas, así como las herramientas y personal capacitado en el área. Dentro del contenido esta comprendido una serie de temas a desarrollar que fundamentaran al estudiante en la manera correcta de accionar ante una situación delictiva informática.

OBJETIVO GENERAL

Fundamentar al estudiante en el área de informática forense, además de dar a conocer la interrelación existente que se tiene tanto la informática como la legislación, así como el conocimiento de metodologías y herramientas que se utilizan en el proceso de aplicación de la informática forense.

CONTENIDO DE PROGRAMA SOBRE INFORMÁTICA FORENSE[117]

UNIDAD I: GENERALIDADES SOBRE DELITOS INFORMATICOS Y EVIDENCIA DIGITAL

Descripción: En esta unidad se presentaran todas las generalidades sobre delitos informáticos, mostrando de esta manera cual es la causa por la que se hace necesario la aplicación de informática forense, es importante que se dé a conocer que esta ciencia entra en acción una vez se ha cometido un delito de este tipo. La evidencia digital es un elemento importante para la aplicación de la informática forense, por lo que también se muestra en qué consiste y su importancia.

Para una mejor comprensión de lo expuesto anteriormente se desarrollaran los siguientes temas:

1.1. Que es forense

Objetivo: Explicar el significado del término forense y de que manera es utilizado en el área de informática, para tener una mejor comprensión del término informática forense.

1.2. Delitos informáticos

Objetivo: Mostrar en que consisten los delitos informáticos y los efectos que se tienen después de que se han cometido.

1.3. Evidencia digital

Objetivo: Presentar la definición de evidencia digital y comprender que es un elemento muy importante en el desarrollo de la aplicación de la informática forense.

1.4. Importancia de la evidencia digital

Objetivo: Tratar de forma adecuada la evidencia digital ya que es la parte fundamental para la aplicación de la informática forense.

1.5. Tratamiento de la evidencia digital

Objetivo: Conocer cual es el tratamiento que se le debe dar a la evidencia digital desde el momento en que ésta es secuestrada.

1.6. Tipos de evidencia.

Objetivo: Mostrar a los estudiantes los tipos de evidencia que se analizan a través de informática forense, porque no es solo secuestrar la evidencia física si no también hay que considerar la evidencia volátil.

1.7. Leyes salvadoreñas contra los delitos informáticos

Objetivo: Presentar el marco legal dentro del cual están contemplados algunos artículos que condenan los delitos informáticos.

[117] Ver apartado Referencia Bibliográfica II: Páginas Web numeral 73.

Punto de control:

Al finalizar la unidad, realizar un resumen del contenido visto en la Unidad I: Generalidades sobre delitos informáticos y evidencia digital

UNIDAD II: INTRODUCCION A LA INFORMATICA FORENSE

Descripción: En esta unidad se presentara de forma general en que consiste la informática forense, su importancia y los elementos que están sujetos al análisis forense, además de mostrar el tratamiento que se le debe dar a la cadena de custodia.

Los temas a desarrollar en esta unidad son los siguientes:

2.1. ¿Qué es la informática Forense?

Objetivo: Presentar las definiciones de informática forense, para que los estudiantes sepan en que consiste esta ciencia.

2.2. Importancia de la informática forense.

Objetivo: Mostrar la importancia de aplicación de la informática forense para ayudar a determinar de que manera se cometió un delito informático.

2.3. Unidades de almacenamiento

Objetivo: Presentar la importancia que tiene el análisis de las unidades de almacenamiento en la informática forense.

2.4. Secuestro del equipo[118]

Objetivo: Saber en qué consiste el secuestro del equipo, quienes lo realizan y de que manera, esto para que los estudiantes se informen de los procesos que se hacen para las investigaciones de delitos informáticos.

2.5. Cadena de custodia

Objetivo: Conocer en que consiste la cadena de custodia y la importancia de que esta no sea interrumpida porque de lo contrario cualquier elemento probatorio puede contaminarse e impedir su validez en los tribunales de justicia en los que se presente como prueba.

Punto de control:

Al finalizar la unidad, realizar un resumen del contenido visto en la Unidad II: Introducción a la informática forense.

UNIDAD III: ANALISIS DE LA EVIDENCIA DIGITAL

[118] Ver apartado Glosario de Términos para su mayor comprensión.

Descripción: Comprende la aplicación de técnicas, herramientas y metodologías propias de la informática forense a evidencias digitales que se han obtenido de la escena del crimen y la importancia de la presentación del informe pericial, el cual se presentara como prueba válida en un juicio.

Los temas a desarrollar en esta unidad son los siguientes:

3.1. Metodología del análisis forense

Objetivo: Brindar información sobre la metodología que se lleva a cabo para realizar el análisis forense a los equipos que se hayan secuestrado.

3.2. Identificar la evidencia digital

Objetivo: Evaluar cuales son los elementos que estuvieron involucrados en la realización del delito informático, para tener una noción de cual es le evidencia que se secuestrara.

3.3. Preservación de la evidencia digital

Objetivo: Dar a conocer en que consiste durante el proceso forense la manipulación de la evidencia, en la escena del crimen se debe de recoger la evidencia y proceder inmediatamente a embalarla, además de hacer un registro sobre esta.

3.4. Análisis de evidencia digital

Objetivo: Mostrar en que consiste el análisis de la videncia digital, de la cual se obtendrá un informe en el cual se presentara los detalles de cómo fue manipulada cuando se cometió el delito informático.

3.5. Análisis de sistemas vivos

Objetivo: Presentar en que consiste el análisis en vivo de las evidencias, ya que es muy importante analizar el equipo informático tal como fue encontrado en el momento de llegar a la escena del crimen.

3.6. Análisis de sistemas muertos

Objetivo: Brindar información para conocer en que consiste el análisis de sistemas muertos dentro del proceso de aplicación de la informática forense.

3.7. Herramientas Forenses

Objetivo: Presentar información sobre las herramientas forenses que son utilizadas en la aplicación de la informática forense.

3.8. Presentar la evidencia

Objetivo: Informar a los estudiantes que la evidencia digital esta sujeto a un análisis judicial por lo que esta es presentada a un juez.

Punto de control:

Al finalizar la unidad, realizar un resumen del contenido visto en la Unidad III: Análisis de la evidencia digital.

UNIDAD IV: CASO EJEMPLIFICADOR

Descripción: El objetivo de esta unidad es presentar un caso práctico, en donde se muestre el proceso de la aplicación de informática forense.

REFERENCIA BIBLIOGRAFICA

LIBROS

1. Órgano Legislativo de El Salvador; CODIGO PENAL El Salvador Estado: VIGENTE; Imprenta Nacional, El Salvador, 1997.
2. Mohay G.; COMPUTER AND INTRUSION FORENSICS; Artech House, Londres Inglaterra, 2003.
3. Eoghan Casey; Handbook of computer crime investigation, forensic tools and technology; Elsevier Academic Press, 2005

SITIOS WEB

Unidad I:

" Generalidades sobre delitos informaticos y evidencia digital"

Tópico 1.1

1. http://www.entomologiaforense.unq.edu.ar/intro_es.htm

tópico 1.2

1. http://www.elpais.com/articulo/elpcibpor/20060119elpcibpor_1/Tes/informaticos/forenses/hacen/imprescindibles/delitos/guante/blanco
2. http://www.fgr.cu/Biblioteca%20Juridica/Derecho%20y%20Delitos%20Informaticos/Delitos%20Inform%E1ticos%20M%E9xico.pdf
3. http://www.ie.itcr.ac.cr/marin/mpc/virus/02.Delitos%20Inform%E1ticos2.pdf

tópico 1.3

1. http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml
2. http://www.dragonjar.org/recoleccion-de-evidencias-forenses-en-sistemas-vivos.xhtml
3. http://www.ncjrs.gov/pdffiles1/nij/187736.pdf
4. http://science.kennesaw.edu/~rda7838/ISA4350Files/ForensicsCheapProceedings.pdf

tópico 1.4

1. http://www.acis.org.co/index.php?id=856
2. http://www.urru.org/papers/RRfraude/DrJeimyCano.pdf

Tópico 1.5

1. http://www.belt.es/expertos/HOME2_experto.asp?id=3989
2. http://www.areino.com/forensics-1/

tópico 1.6

1. http://www.virusprot.com/Archivos/Eviden-GECTI03.pdf

tópico 1.7

1. El Código Penal. UTILIZACION DE MENORES CON FINES PORNOGRAFICOS Y EXHIBICIONISTAS. Art. 173
2. El Código Penal. DE LOS DELITOS RELATIVOS A LA INTIMIDAD, VIOLACION DE COMUNICACIONES PRIVADAS. Art. 184.
3. El Código Penal. VIOLACION AGRAVADAS DE COMUNICACIONES. Art. 185
4. El Código Penal. DISPOSICION COMUN, EXCLUCION DE DELITOS. Art. 191
5. El Código Penal. ESTAFA AGRAVADA. Art. 216, Nº 5
6. El Código Penal. DAÑOS AGRAVADOS. Art. 222, Nº 2
7. El Código Penal. DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL, VIOLACION DE DERECHOS DE AUTOR Y DERECHOS CONEXOS. Art. 226

UNIDAD II:

"Introduccion a la informatica forense"

Tópico 2.1 El Código Penal. INFIDELIDAD COMERCIAL. Art. 230.

1. http://www.nexos-software.com.co/Articulo_17.htm
2. http://www.forensic-es.org/contenido/07/10/las-puertas-de-una-nueva-especializaci%C3%B3n:-la-inform%C3%A1tica-forense.-alberto-david-aira
3. http://www.javierpages.com/inforenses/index.php/inforenses?cat=30
4. http://www.elhacker.net/InfoForenseWindows.htm
5. http://www.microsoft.com/spain/empresas/legal/forensic.mspx
6. http://www.experticia.net/blog/index.php?/categories/15-INFORMATICA-FORENSE
7. http://www.tudiscovery.com/crimen/ciencia_forense/index.shtml
8. http://www.criptored.upm.es/guiateoria/gt_m180b.htm

tópico 2.2

1. http://www.netzweb.net/html/print/segurid/forense/intro.pdf
2. http://www.ticsevolution.com/informatica-forense-28-p.html

tópico 2.3

1. http://www.configurarequipos.com/doc336.html

tópico 2.4

1. http://www.borrmart.es/articulo_redseguridad.php?id=1376&numero=27
2. http://www.alfa-redi.org/rdi-articulo.shtml?x=6216

tópico 2.5

1. http://www.cadenadecustodia.com/
2. http://www.csj.gob.sv/LINEAS%20JURISPRUDENCIALES.nsf/4b925d1337d3ea22062569cb00706b69/64a3b48d2a82688d0625695e007369c6?OpenDocument

UNIDAD III:

Analisis de la evidencia digital

tópico 3.1

1. http://ocw.ua.es/Humanidades/el-ingles-y-el-espanol-en-la-linguistica-forense/metodologia/
2. http://homepages.mty.itesm.mx/al617903/ComputerForensics.doc

tópico 3.2

1. http://www.e-fense.com/helix/Docs/Forensic%20Examination%20of%20Digital%20Evidence.pdf

tópico 3.3

1. http://www.e-fense.com/helix/Docs/Jesse_Kornblum.pdf

tópico 3.4

1. http://www.e-fense.com/helix/Docs/Recycler_Bin_Record_Reconstruction.pdf
2. http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf
3. http://www.epa.gov/QUALITY/qs-docs/g6-final.pdf
4. http://www.cienciaforense.cl/csi/index2.php?option=com_content&do_pdf=1&id=39
5. http://www.cienciaforense.cl/csi/content/view/39/2/
6. http://vtroger.blogspot.com/2008/07/anlisis-forense-de-elementos-borrados_14.html

tópico 3.5

1. http://www.tecnoseguridad.net/anlisis-forense-de-elementos-enviados-a-la-papelera-de-reciclaje/
2. http://vtroger.blogspot.com/2008/06/recoleccin-de-evidencias-forenses.html
3. http://seguinfo.wordpress.com/2008/06/28/recoleccion-de-evidencias-forenses-sistema-vivo/

tópico 3.6

1. http://www.eset-la.com/press/informe/virtumonde_cronica_muerte_anunciada.pdf
2. http://www.tecnoseguridad.net/anlisis-forense-de-elementos-enviados-a-la-papelera-de-reciclaje/

tópico 3.7

1. http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/060.pdf
2. http://inza.wordpress.com/2006/11/28/herramientas-de-informatica-forense-para-recuperar-datos-de-disco-duro/
3. http://vtroger.blogspot.com/2008/01/suite-completa-para-informtica-forense.html

tópico 3.8

1. http://idicperitos.blogspot.com/

DOCUMENTOS ELECTRÓNICOS

1. Juan David Gutiérrez*; "*Informática Forense" (documento pdf), 2006 < http://cicsa.uaslp.mx/ProgrAcadem/FacDerecho/MtraMaGpe/Documentos/exposiciones2007/cap1/teoria%20general%20del%20proceso%20cap%201.doc >; 9/Abril/2008

2. Jim McMillan*; "*Informática Forense" (documento doc), 2000 < http://www.giac.org/practical/Jim_McMillan_GSEC.doc >;9/Abril/2008

3. Santiago Acurio Del Pino*; "*Introducción a la informática forense" (documento doc), 2005 < http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf >;10/Abril/2008

4. **Evidencia Digital.** Jeimy J. Cano; "Buenas prácticas en la administración de la Evidencia digital" (documento pdf), 2006 <http://gecti.uniandes.edu.co/docs/buenas%20practica%20evidencia%20digital%20jcano.pdf>;15/Abril/2008.

REVISTAS ELECTRÓNICAS

1. **Evidencia Digital** Jeimy José Cano Martínez*; "*Admisibilidad de la Evidencia Digital: Algunos elementos de revisión y análisis" (documento web), 2003 < http://www.alfa-redi.org/rdi-articulo.shtml?x=1304 >;31/Marzo/2008

II. PROPUESTA DE CONTENIDO TEMÁTICO DE INFORMÁTICA FORENSE PARA PROFESIONALES DE DERECHO.

DESCRIPCION

Es necesario que los estudiantes conozcan en qué consiste la aplicación de la informática forense y la relación que esta tiene para ayudar al esclarecimiento de delitos informáticos, además de la importancia que tiene que el proceso de esta aplicación se realice conforme a la utilización de herramientas, estándares y metodologías propias de esta ciencia. Dentro del contenido está comprendido una serie de temas a desarrollar que fundamentaran al estudiante tanto en la informática forense como en los roles que los profesionales del derecho deben de cumplir ante una situación de investigación sobre este tipo de delitos.

OBJETIVO GENERAL

Fundamentar al estudiante de derecho en el área de informática forense, además de dar a conocer la interrelación existente que tiene esta ciencia con la legislación y de esta manera obtengan conocimiento sobre el funcionamiento de la informática forense.

CONTENIDO DE PROGRAMA SOBRE INFORMÁTICA FORENSE[119]

UNIDAD I: INFORMÁTICA FORENSE

Descripción: En esta unidad se presentara de forma general los elementos que conforman la informática forense, así como también los roles de las personas involucradas en su aplicación y definiciones de términos utilizados. Además se pretende dar a conocer para que se utiliza esta ciencia, en que consiste, cual es su finalidad, metodologías que se utilizan y cual es su forma de proceder y el porqué de ésta.

Los temas a desarrollar en esta unidad son los siguientes:

1.1. ¿Que es informática forense?

Objetivo: Presentar las definiciones de informática forense, para que los estudiantes sepan en que consiste esta ciencia.

1.2. ¿Dónde se aplica?

Objetivo: Conocer donde y cuando se aplica la informática forense, para proceder de forma correcta en la obtención de evidencia.

1.3. Objetivos de la informática forense

Objetivo: Presentar los objetivos que tiene como finalidad la informática forense, para que se tenga bien claro los resultados que se obtendrán al aplicar esta ciencia.

1.4. Evidencia digital o informática

Objetivo: Presentar la definición de evidencia digital y comprender que es un elemento muy importante en el desarrollo de la aplicación de la informática forense.

1.5. Obtención de evidencia en distintos ámbitos

Objetivo: Considerar la importancia de aplicar métodos y técnicas adecuadas para la obtención de evidencia digital y evitar así romper la cadena de custodia que se lleva a cabo en todo el proceso de aplicación de informática forense.

1.6. Roles del perito

Objetivo: Dar a conocer los roles o funciones que llevan a cabo los peritos informáticos en el proceso de aplicación de la informática forense.

[119] Esta información fue brindada por Ing. Gustavo Presman. Para mayor detalle, Ver apartado Referencia Bibliográfica VI: Referencia de Fuentes personales numeral 2.

1.7. Autenticación de evidencia

Objetivo: Mostrar la autenticación de la evidencia digital en la cual se aplique la informática forense, esto se logra utilizando procedimientos, metodologías y herramientas adecuadas, que hacen constar que la evidencia tratada no ha sido modificada.

1.8. Rol del abogado(fiscal, juez, defensor)

Objetivo: Presentar en que consiste el rol del abogado en el proceso de aplicación de la informática forense, debido a que esta ciencia esta ligada aspectos judiciales.

1.9. Evaluación de la evidencia informática

Objetivo: Conocer en que consiste la evaluación de la evidencia digital, esto debido a que el informe final de la aplicación de informática forense esta sujeto a análisis judicial.

Punto de control:

Al finalizar la unidad, realizar un resumen del contenido visto en la Unidad I: Informática forense.

UNIDAD II: ESCENA DEL CRIMEN

Descripción: Esta unidad trata sobre como se debe de accionar en el lugar donde se cometió el delito informático, con la adquisición y preservación de las evidencias que se encuentren, ade más de hacer un análisis previo de la situación encontrada y obtener imágenes que ayudaran en un cierto momento a recrear la escena del delito.

Los temas a desarrollar en esta unidad son los siguientes:

2.1. Preservación de la evidencia

Objetivo: Dar a conocer en que consiste durante el proceso forense la manipulación de la evidencia, en la escena del crimen se debe de recoger la evidencia y proceder inmediatamente a embalarla, además de hacer un registro sobre esta.

2.2. Riesgos de destrucción o alteración de la videncia

Objetivo: Conocer cuales factores pueden ocasionar alteraciones en las evidencias que se estén analizando, ya que estas pueden ser fáciles de manipular.

2.3. Dispositivos internos en la PC, Bloqueo de acceso, Posibilidad de alteración o borrado y acceso malicioso remoto o físico.

Objetivo: Tratar estos elementos de manera cuidadosa porque son los que ayudaran a esclarecer la forma en que fueron manipulados por la persona que cometió el delito.

2.4. Análisis Previo

Objetivo: Mostrar la importancia de hacer un informe, en el cual se detalle los elementos que fueron encontrados en la escena del crimen.

2.5. Antecedentes del caso, Planos, croquis, esquemas y testimonios

Objetivo: Recolectar todo tipo de información que ayude a la investigación del delito, pero basado siempre en el lugar de los hechos.

2.6. Análisis de sistemas vivos

Objetivo: Presentar en que consiste el análisis en vivo de las evidencias, ya que es muy importante analizar el equipo informático tal como fue encontrado en el momento de llegar a la escena del crimen.

Punto de control:

Al finalizar la unidad, realizar un resumen del contenido visto en la Unidad II: Escena del crimen.

UNIDAD III: PUNTOS DE PERICIA

Descripción: Consiste en los puntos que se trataran durante la pericia forense que se realizara a las evidencias digitales que se obtendrán de la escena del crimen, se podrá conocer el proceso de informática forense desde el momento que se decomisa la evidencia hasta el momento de presentar el informe final a un juez.

Los temas a desarrollar en esta unidad son los siguientes:

3.1. Adquisición de la evidencia informática

Objetivo: Mostrar la forma de accionar de las autoridades correspondientes al momento de obtener evidencia que permita conocer como sucedieron los hechos.

3.2. Monitoreo de tráfico

Objetivo: Investigar todas las posibles formas que los delincuentes pueden utilizar para realizar un delito informático, lo que conlleva a vigilar las conexiones de red, es decir buscar pruebas del accionar de estos a través de internet.

3.3. Lugar de ubicación de la prueba

Objetivo: Observar el lugar de ubicación de la prueba, para poder deducir de que manera pudo ocurrir el delito.

3.4. Cadena de custodia

Objetivo: Conocer en que consiste la cadena de custodia y la importancia de que esta no sea interrumpida porque de lo contrario cualquier elemento probatorio puede contaminarse e impedir su validez en los tribunales de justicia en los que se presente como prueba.

Punto de control:

Al finalizar la unidad, realizar un resumen del contenido visto en la Unidad III: Puntos de pericia.

UNIDAD IV: ANÁLISIS FORENSE DE LA EVIDENCIA INFORMÁTICA

Descripción: Comprende la aplicación de técnicas, herramientas y metodologías propias de la informática forense a evidencias digitales que se han obtenido de la escena del crimen, y la importancia de la presentación del informe pericial, el cual se presentara como prueba válida en un juicio.

Los temas a desarrollar en esta unidad son los siguientes:

4.1. Copias de trabajo

Objetivo: Realizar copias de trabajo durante la aplicación de informática forense ayuda a preservar la evidencia, de manera que se puede trabajar sobre copias intactas de la original.

4.2. Herramientas comerciales y de software libre

Objetivo: Dar a conocer una enorme gama de herramientas informáticas forenses por medio de las cuales se llega a un análisis de cómo sucedieron los hechos.

4.3. Copia Forense e imagen forense

Objetivo: Mostrar que significa copia e imagen forense y su importancia en el análisis forense.

4.4. Firmas digitales[120]

Objetivo: Mostrar en que consisten, su funcionamiento, aplicación y comprobación de las firmas digitales en el proceso de análisis de la evidencia digital.

4.5. Bases de datos de hashes de: Programas, Sistemas Operativos y Fotos ó videos de pedofilia

Objetivo: Aplicar informática forense para detectar cualquier tipo de anomalía y luego presentar un informe que especifique lo sucedido, ya sea instrucciones a sistemas o robo de información de base de datos.

[120] Ver apartado Glosario de Términos para su mayor comprensión.

4.6. Alteraciones. Fecha y hora

Objetivo: Ayudar a determinar por medio de un informe pericial si una información determinada ha sido alterada.

4.7. Tipo de archivos, Contenido, Formateado y Borrado.
Objetivo: Presentar la información que esta sujeta a la aplicación de informática forense.

4.8. Informe pericial

Objetivo: Mostrar en que consiste el informe pericial, su estructura y cual es su finalidad en la informática forense.

Punto de control:

Al finalizar la unidad, realizar un resumen del contenido visto en la Unidad IV: Análisis forense de la evidencia informática.

UNIDAD V: MARCO NORMATIVO LEGAL

Descripción: Esta unidad comprende el marco legal salvadoreño en el cual están contemplados algunos artículos que condenan los delitos informáticos, la informática forense sirve como el medio para la obtención de evidencia que sirva para esclarecer estos tipos de delitos. Se presentan a continuación algunos artículos contemplados en el código penal sobre delitos informáticos.

5.1. El Código Penal. UTILIZACION DE MENORES CON FINES PORNOGRAFICOS Y EXHIBICIONISTAS. Art. 173
5.2. El Código Penal. DE LOS DELITOS RELATIVOS A LA INTIMIDAD, VIOLACION DE COMUNICACIONES PRIVADAS. Art. 184
5.3. El Código Penal. VIOLACION AGRAVADAS DE COMUNICACIONES. Art. 185
5.4. El Código Penal. DISPOSICION COMUN, EXCLUCION DE DELITOS. Art. 191
5.5. El Código Penal. ESTAFA AGRAVADA. Art. 216, Nº 5
5.6. El Código Penal. DAÑOS AGRAVADOS. Art. 222, Nº 2
5.7. El Código Penal. DE LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL, VIOLACION DE DERECHOS DE AUTOR Y DERECHOS CONEXOS. Art. 226
5.8. El Código Penal. INFIDELIDAD COMERCIAL. Art. 230.

Punto de control:

Al finalizar la unidad, realizar un resumen del contenido visto en la Unidad V: Marco normativo legal.

REFERENCIA BIBLIOGRAFICA

LIBROS

1. Órgano Legislativo de El Salvador; CODIGO PENAL El Salvador Estado: VIGENTE; Imprenta Nacional, El Salvador, 1997.
2. Mohay G.; COMPUTER AND INTRUSION FORENSICS; Artech House, Londres Inglaterra, 2003.
3. Eoghan Casey; Handbook of computer crime investigation, forensic tools and technology; Elsevier Academic Press, 2005

SITIOS WEB

UNIDAD I:

"Informática forense"

Tópico 1.1

1. http://www.nexos-software.com.co/Articulo_17.htm
2. http://www.forensic-es.org/contenido/07/10/las-puertas-de-una-nueva-especializaci%C3%B3n:-la-inform%C3%A1tica-forense.-alberto-david-aira
3. http://www.elhacker.net/InfoForenseWindows.htm
4. http://www.microsoft.com/spain/empresas/legal/forensic.mspx
5. http://www.tudiscovery.com/crimen/ciencia_forense/index.shtml
6. http://homepages.mty.itesm.mx/al617903/ComputerForensics.doc

tópico 1.2

1. http://www.javierpages.com/inforenses/index.php/inforenses?cat=30

tópico 1.3

1. http://www.microsoft.com/spain/empresas/legal/forensic.mspx
2. http://www.e-fense.com/helix/Docs/Jesse_Kornblum.pdf

tópico 1.4

1. http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml
2. http://www.microsoft.com/spain/empresas/legal/forensic.mspx

tópico 1.5

1. http://www.belt.es/expertos/HOME2_experto.asp?id=3989

tópico 1.6

1. http://www.cevejara.net/cevejara/modules.php?name=News&file=article&sid=131
2. http://idicperitos.blogspot.com/

tópico 1.7

1. http://www.e-fense.com/helix/Docs/Forensic%20Examination%20of%20Digital%20Evidence.pdf
2. http://www.e-fense.com/helix/Docs/Jesse_Kornblum.pdf
3. http://science.kennesaw.edu/~rda7838/ISA4350Files/ForensicsCheapProceedings.pdf

4. http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/060.pdf
5. http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf

topico1.8

1. http://www.criminalistaenred.com.ar/Los%20peritos%20en%20la%20reforma.html
2. http://inza.wordpress.com/2007/06/05/evidencias-electronicas-y-peritaje-informatico/
3. http://www.frcu.utn.edu.ar/deptos/depto_3/32JAIIO/sid/SID_13.pdf
4. http://www.yanapti.com/novedades/notas/nota33.htm

tópico 1.9

1. http://www.e-fense.com/helix/Docs/Forensic%20Examination%20of%20Digital%20Evidence.pdf
2. http://www.e-fense.com/helix/Docs/Jesse_Kornblum.pdf
3. http://science.kennesaw.edu/~rda7838/ISA4350Files/ForensicsCheapProceedings.pdf
4. http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/060.pdf

UNIDAD II:

" Escena del crimen"

tópico 2.1

1. http://www.areino.com/forensics-1/
2. http://www.epa.gov/QUALITY/qs-docs/g6-final.pdf
3. http://www.cienciaforense.cl/csi/content/view/39/2/

tópico 2.2

1. http://controltecnologico.blogspot.com/2007/06/practicas-forenses-para-prevenir-los.html
2. http://www.sublimesolutions.com/articulos/articulos_masinfo.php?id=108&secc=articulos
3. http://gecti.uniandes.edu.co/docs/NasTecnologias6.pdf
4. http://www.virusprot.com/Archivos/Eviden-GECTI03.pdf

tópico 2.3

1. http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

Tópico 2.4

1. http://www.cienciaforense.cl/csi/index2.php?option=com_content&do_pdf=1&id=39
2. http://www.elpais.com/articulo/elpcibpor/20060119elpcibpor_1/Tes/informaticos/forenses/hacen/imprescindibles/delitos/guante/blanco

tópico 2.5

1. http://www.alfa-redi.org/rdi-articulo.shtml?x=177
2. http://www.scielo.cl/scielo.php?pid=S0718-00122003000100023&script=sci_arttext

tópico 2.6

1. http://www.delitosinformaticos.com/firmaelectronica/analisis.shtml

UNIDAD III:

"Puntos de pericia"

tópico 3.1

1. http://www.tecnoseguridad.net/anlisis-forense-de-elementos-enviados-a-la-papelera-de-reciclaje/

tópico 3.2

1. http://ruben.cheng-ca.com/es/knowledge/network/trafficmon.htm
2. http://www.trucoswindows.net/tutorial-9-TUTORIAL-TCPView-Pro-Monitoreo-del-trafico-TCP-IP-en-Windows.html
3. http://www.pergaminovirtual.com.ar/revista/cgi-bin/hoy/archivos/00001749.shtml

tópico 3.3

1. http://www.justicewomen.com/handbook/entering_evidence_3_sp.html
2. http://manuelcarballal.blogspot.com/2007/07/metodos-y-tecnicas-de-la-investigacion.html

tópico 3.4

1. http://www.cadenadecustodia.com/
2. http://www.csj.gob.sv/LINEAS%20JURISPRUDENCIALES.nsf/4b925d1337d3ea22062569cb00706b69/64a3b48d2a82688d0625695e007369c6?OpenDocument

UNIDAD IV:

"Análisis forense de la evidencia informática"

tópico 4.1

1. http://www.pymesyautonomos.com/2008/01/03-la-importancia-vital-de-hacer-copias-de-seguridad-de-nuestros-datos
2. http://support.microsoft.com/kb/308422/es

tópico 4.2

1. http://vtroger.blogspot.com/2008/07/anlisis-forense-de-elementos-borrados_14.html
2. http://inza.wordpress.com/2006/11/28/herramientas-de-informatica-forense-para-recuperar-datos-de-disco-duro/
3. http://www.criptored.upm.es/guiateoria/gt_m180b.htm
4. http://vtroger.blogspot.com/2008/01/suite-completa-para-informtica-forense.html

tópico 4.3

1. http://www.ondata.es/recuperar/equipos-forensics.htm
2. http://www.investigacionesinformaticas.com/servicios/forense_adquisiciones/index.htm

tópico 4.4

1. http://bulma.net/body.phtml?nIdNoticia=868
2. http://www.acis.org.co/fileadmin/Conferencias/PresentacionFirmaDigitalACIS.pdf
3. http://www.adobe.com/es/security/digsig.html

tópico 4.5

1. http://sukiweb.net/archivos/2005/08/22/base-de-datos-de-md5-hash/
2. http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/SOF.htm
3. http://www.microsoft.com/latam/technet/productos/windows/default.mspx
4. http://books.google.com.sv/books?hl=es&id=wXzwFPaVku0C&dq=sistemas+operativos&printsec=frontcover&source=web&ots=yzdgtRw3-x&sig=caw6-U_TYXW_FUN2QxM5s-2KjC8&sa=X&oi=book_result&resnum=3&ct=result#PPR10,M1
5. http://comunicacionenconstruccion.wordpress.com/2006/08/16/manipulacion-de-fotos/

tópico 4.6

1. http://bulma.net/body.phtml?nIdNoticia=950
2. http://www.forospyware.com/t167465.html

tópico 4.7

1. http://msdn.microsoft.com/es-es/library/2wawkw1c(VS.80).aspx
2. http://office.microsoft.com/es-es/sharepointtechnology/HA101001473082.aspx

tópico 4.8

1. http://books.google.com.sv/books?id=IUe2bRI8gxUC&pg=PA39&lpg=PA39&dq=informes+periciales&source=web&ots=nDZ3KVhrNd&sig=FuCs49hDo9gyeSgMinNbfbwZXEE&hl=es&sa=X&oi=book_result&resnum=4&ct=result
2. http://www.informespericiales.net/
3. http://www.moebio.uchile.cl/16/bar.htm
4. http://estaticos.elmundo.es/documentos/2007/05/16/informe_pericial_01.pdf

DOCUMENTOS ELECTRÓNICOS

1. **Roles del Perito.** Juan David Gutiérrez; "Informática Forense" (documento pdf), 2006 < http://cicsa.uaslp.mx/ProgrAcadem/FacDerecho/MtraMaGpe/Documentos/exposiciones2007/cap1/teoria%20general%20del%20proceso%20cap%201.doc >; 9/Abril/2008

2. Jim McMillan; "Informática Forense" (documento doc), 2000 < http://www.giac.org/practical/Jim_McMillan_GSEC.doc >;9/Abril/2008

3. Santiago Acurio Del Pino; "Introducción a la informática forense" (documento doc), 2005 < http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf >;10/Abril/2008

4. **Evidencia Digital** Jeimy J. Cano; "Buenas prácticas en la administración de la Evidencia digital" (documento pdf), 2006 <http://gecti.uniandes.edu.co/docs/buenas%20practica%20evidencia%20digital%20jcano.pdf>;15/Abril/2008.

REVISTAS ELECTRÓNICAS

1. **Evidencia Digital** Jeimy José Cano Martínez; "Admisibilidad de la Evidencia Digital: Algunos elementos de revisión y análisis" (documento web), 2003 < http://www.alfa-redi.org/rdi-articulo.shtml?x=1304 >;31/Marzo/2008

E- DEMOSTRACIÓN SOBRE LA UTILIZACIÓN DE HERRAMIENTAS INFORMÁTICO FORENSE

En este apartado se presenta las herramientas utilizadas y la guía de pasos que se llevo a cabo para la demostración de cómo utilizar una de las herramientas planteadas en el apartado F. Herramientas Informáticas. Forenses, la cual fue Hélix.

I. (CASO I) CREACIÓN DE COPIA DE DISPOSITIVOS DE ALMACENAMIENTO MANUALMENTE EN LINUX.

Descripción del caso:

- Se presenta la situación de tener un dispositivo de almacenamiento, en esta categoría pueden ser: discos duros, USB, tarjetas de memoria de distintos dispositivos como cámaras, teléfonos agendas personales, cuadros digitales entre otros. A los cuales se realizara una copia fiel a través de modo consola de Linux.
- De esta forma el investigador podrá hacer distintas copias del archivo que será estudiado para permitirle hacer diversos estudios o compartir la opinión de otros peritos de la misma área.

Objetivos del caso:

- Con este caso se pretende conocer como realizar copias de distintos dispositivos de almacenamiento de información.
- Conocer la estructura de comandos en modo consola de Linux para realizar copias byte por byte de los dispositivos a los cuales se les realizara la copia.

Elementos necesarios para el desarrollo del caso:

- Para esta práctica se utilizara:
  - Dispositivos de almacenamiento de diferentes capacidades para examinar.
  - Disco duro externo para guardar la copia realizada.
  - Computadora Personal o de escritorio con las siguientes características:
    - Memoria RAM 512 Mb
    - Lector de CD.
    - Con o sin disco duro
    - Procesador Celeron de 1.6 GHz
    - Con puertos USB 2.0.
  - Software Helix V1.9 (http://www.e-fense.com/helix/)

Interfaz gráfica del usuario (GUI)

En la **Figura N° 13** se presenta el entorno de Helix en Linux, para poder ver esta pantalla en nuestra computadora es necesario cargar el CD booteable de Helix, esto se hace en un sistema muerto, es decir que la computadora este apagada. En la parte superior izquierda de la pantalla se observan

todos los dispositivos de almacenamiento que están conectados a la computadora, en nuestro caso se observan dos dispositivos USB, uno contiene la copia original(evidencia) y el otro guardara la copia fiel que se hará de la original. En la parte inferior de la pantalla se presenta la barra menú de Helix, de la cual se hará uso para efectuar todas las acciones necesarias para la ejecución de este procedimiento.

Figura N° 13: Entorno de Hélix en Linux.

Desarrollo del caso

Paso 1. Después de familiarizarnos con el entorno de Hélix, para realizar copias o cualquier proyecto con esta herramienta es necesario montar la unidad donde se colocara la copia o se hará el análisis para eso es necesario crear una carpeta en el directorio /mnt.

- **Explicación de Comandos a utilizar:**

[root (mnt)]# Indica el directorio raíz donde se va a trabajar, dentro del directorio mnt se creara una carpeta donde se guardara la copia.

mkdir comando que sirve para crear un nuevo directorio

caso#### nombre del directorio que se creara para guardar la copia que se realizara del dispositivo de almacenamiento original(evidencia).

Ls – l este comando sirve para listar los archivos que contiene el directorio en el que estamos trabajando, al ejecutarlo nos proporcionara el total de archivos contenidos, fecha y hora de creación y los privilegios que se tienen sobre ellos, es este caso: drwxr-xr-x, cuando inicia con

"d" significa que es un directorio, "w" significa que tiene permiso de escritura del archivo, "x" significa que tiene permiso de ejecución del archivo y "r" significa que tiene permiso de lectura del archivo.

A manera de ejemplo se observa en la **Figura N° 14** la instrucción: drwxr-xr-x 2 root root 60 Sep 7 21:54, el primer root que aparece indica que identifica el usuario propietario, el segundo root que aparece indica el nombre de grupo de usuario, 60 que aparece indica los otros usuarios que hay, Sep 7 indica que el archivo se creo el 7 de septiembre a las 9:54pm.

La instrucción completa para crear la copia de un dispositivo de almacenamiento en modo consola de Linux es la siguiente:

[root (mnt)]# mkdir caso####

Para una mejor comprensión de este caso, puede observar en la **Figura N° 14** el entorno consola de Linux donde se desarrolla un ejemplo.

- **Ejemplo:**

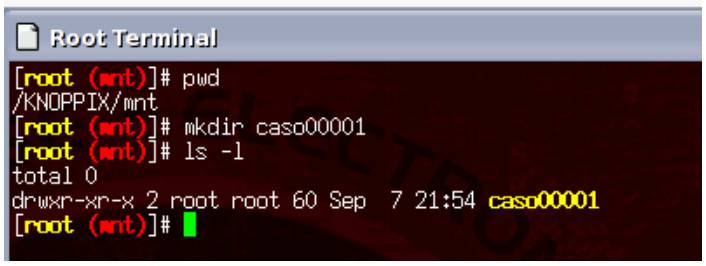


Figura N° 14: Creación de un directorio en Linux utilizando Hélix.

Paso 2. Terminado la creación de una carpeta dentro del directorio "mnt" el siguiente paso es montar la unidad en la cual se transferirá la información, este procedimiento mantiene segura la evidencia porque no se realiza lectura solo copia, es decir no se accede n a los documentos modificando la hora del último acceso.

- **Explicación de Comandos a utilizar:**

[root (mnt)]# Indica en que directorio se esta trabajando y guardando el archivo copiado.

Mount es el comando que permite montar un dispositivo de almacenamiento, en nuestro caso un dispositivo USB.

–t indica el tipo de archivo que se va a cargar

vfat tipo de formato del dispositivo donde se hará la copia.

dev directorio de linux donde se encuentran los dispositivos de almacenamiento.

sda1 dispositivo de almacenamiento montado, en el cual se guardara la copia de la original.

mnt directorio donde son montados los dispositivos de almacenamiento.

caso#### nombre del directorio que se creo y en el cual se guardara la copia hecha.

La instrucción completa para montar el dispositivo USB donde se guardara la copia es la siguiente:

[root (mnt)]# Mount –t vfat /dev/sda1 /mnt/caso####

- Se sugiere que el formato del dispositivo donde se realizara la copia de la evidencia sea "FAT" en especial "FAT32" ya que es el formato recomendado para poder trabajar en un ambiente de tipo Linux.

En la **Figura N° 15,** se muestra un ejemplo para el montaje del dispositivo de almacenamiento en donde se guardara la copia.

- **Ejemplo:**

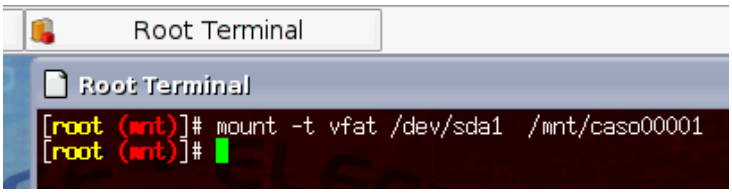


Figura N° 15: Montaje de la unidad donde se transferirá la información.

Paso 3. Finalizado el montaje de la unidad donde se pondrá la evidencia el siguiente paso es realizar la copia del dispositivo que contiene la evidencia, es necesario recordar que los pasos mencionados anteriormente son necesarios para realizar las siguientes prácticas.

Para realizar la copia, como se muestra en la **Figura N° 16** es necesario colocar un nombre a la copia que se realiza.

- **Explicación de Comandos a utilizar:**

[root (mnt)]# Indica el directorio en el que se esta trabajando.

dd comando que permite la creación de imágenes de archivos

if= Indica el origen de la evidencia o el dispositivo

dev directorio de linux donde se encuentran los dispositivos de almacenamiento.

sdb dispositivo de almacenamiento original(evidencia)

of = Indica el destino, o el dispositivo en el cual se guardara.

mnt directorio donde son montados los dispositivos de almacenamiento.

caso#### nombre del directorio que se creó y en el cual se guardara la copia hecha.

nombre_de_la_imagen.img nombre del archivo copiado, es decir la imagen del archivo, este archivo tiene extensión .img

Para la creación de una imagen del archivo(copia) idéntica debe colocar en el modo consola de Linux la siguiente instrucción:

[root (mnt)]# dd if=/dev/sdb of =/mnt/caso####/nombre_de_la_imagen.img bs=8192

- Se recomienda utilizar un cache de 8192 que este se define con el comando de "bs" existe otra capacidad de cache.

Se presenta en la **Figura N° 16** esta instrucción con un ejemplo en el cual la copia creada tiene como nombre PRcaso00001.img

- **Ejemplo:**

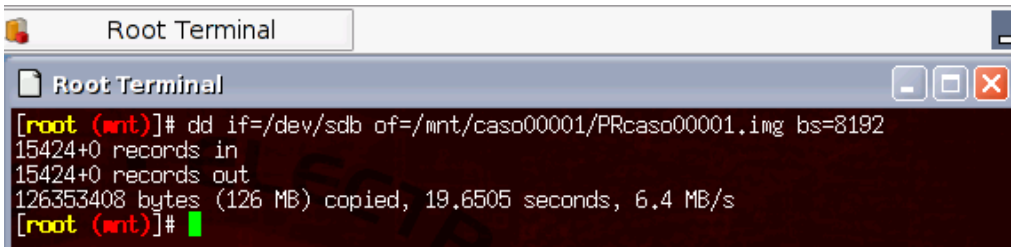


Figura N° 16: Creación de la imagen del dispositivo analizado.

Paso 4. Después de realizar la copia es necesaria la verificación del archivo recién creado, esto se hace de la siguiente manera:

- **Explicación de Comandos a utilizar:**

[root (mnt)]# dir muestra el contenido del directorio mnt

[root (mnt)]# cd /caso#### accesamos al directorio caso#### donde se almaceno la copia de la evidencia.

[root (caso####)] dir muestra el contenido del directorio caso#### para verificar si se encuentra la copia que se creo.

[root (caso####)] ls –l lista los archivos que contiene el directorio caso#### con su fecha y hora de creación.

Para ver el desarrollo de este paso de forma práctica, observe la **Figura N° 17** en la cual se verifica si realmente se encuentra el archivo imagen que se creo de la evidencia.

➢ **Ejemplo:**

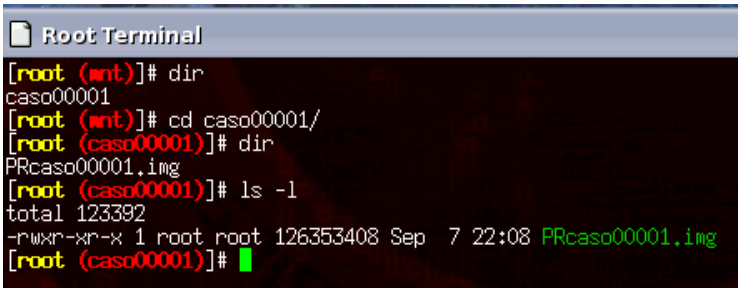


Figura N° 17: Verificación de la existencia de la imagen creada

Se desarrollo este caso para dispositivos de almacenamiento de diferentes capacidades, mostrando el tiempo aproximado de duración que se obtuvo para cada uno de ellos en la **Tabla Nº 37.**

DISPOSITIVO	CAPACIDAD	DURACION[121]
USB	128 MB	8 min
USB	256 MB	16 min
USB	512 MB	32 min
USB	1 GB	64 min
HD	80 GB	5120 min = 85 horas

Tabla Nº 37: Tiempo de duración aproximado para crear la copia de los dispositivos de almacenamiento (imagen)

Para ver con mas detalle el manejo de herramientas ver CD apartado DEMOSTRACION DE HERRAMIENAS INFORMATICAS.

[121] Este tiempo puede variar dependiendo de las prestaciones de la computadora, las pruebas se hicieron con un equipo con 512MB en RAM además de un procesador de Pentium IV 3.0 GHz.

CONCLUSIONES

CONCLUSIONES

I. EN BASE A OBJETIVOS DEL PROYECTO

1. Los parámetros necesarios para llevar a cabo la investigación científica, exploratoria, descriptiva y experimental son: la formulación del problema, el análisis del problema y el enunciado del problema y para obtener el conocimiento que muestran las bases firmes del problema propuesto se describen las herramientas de recolección de datos y su interpretación estadística.
2. El tipo de muestreo que se utilizo para determinar la población y muestra es el *muestreo estratificado* ya que permite identificar las subpoblaciones que están involucradas en la aplicación de la Informática Forense en El Salvador.
3. Para la realización de la investigación fue necesario tener claro cual era la población que estaba involucrada en la aplicación de informática forense y el esclarecimiento de delitos informáticos las cuales son: la Fiscalía General de la República, Procuraduría General de la República, Centros Judiciales y Policía Nacional Civil, de esta forma se establecieron las poblaciones y muestras de las cuales se obtuvo información que ayudo a comprobar la hipótesis de la investigación.
4. La elaboración de los instrumentos de recolección de datos se realizo considerando criterios como validez y confiabilidad, la utilización de una pre-encuesta permitió disminuir los errores que tenían las herramientas y de esta forma se refino el diseño de dichos instrumentos, permitiendo que las preguntas fueran claras y entendibles para las poblaciones encuestadas.
5. La elaboración de los instrumentos de recolección de datos, favoreció de manera oportuna el poder recolectar la información pertinente para el estudio y análisis sobre la informática forense en el salvador y poder decir como esta relacionada ésta especialidad de la rama de informática en esclarecer delitos para los cuales se ha hecho uso de tecnología de información y perjudicar así a terceros, conociendo estos delitos como delitos informáticos.
6. La tabulación y análisis de los datos obtenidos en la investigación de campo, ha facilitado observar y determinar así el rumbo que actualmente lleva nuestro país en el área de informática forense y así contrarrestar los delitos informáticos que se comenten, siendo esta una forma nueva de dañar a la población por parte de los delincuentes y éstos conociendo que las instituciones con las funciones de proteger y guardar la seguridad no están en la capacidad de hacerles frente, siguen llevando a cabo sus delitos sin ningún castigo.
7. El tipo de hipótesis que se utilizo para el desarrollo del proyecto fue la *hipótesis descriptiva* debido a que permite describir la situación actual de las variables que intervienen en el estudio y las relaciones que se dan entre éstas.
8. Luego del análisis de datos obtenidos a través de los instrumentos de medición se realizo la prueba estadística de chi cuadrado para comprobar la información con respecto a las hipótesis planteadas en la investigación, determinando así el cumplimiento de la hipótesis en la cual se baso la investigación.

9. Al rechazar la hipótesis nula de nuestro trabajo de investigación, esto ha dado un elemento nuevo para poder hacer frente a los delitos informáticos que se realizan en nuestro país, esto es la aplicación de la informática forense siendo ésta una rama de la informática, ayudando a esclarecer de manera clara y oportuna como se realizó el delitos y aun a determinar quien o quienes fueron los autores de esos delitos.
10. Utilizar indicadores es fundamental para los proyectos de desarrollo, esto no debe hacer perder de vista su finalidad, la cual es contribuir al mejoramiento de la calidad de vida y bienestar de la población. Es decir, que la construcción de indicadores sociales no constituye un fin en sí mismo, sino que son instrumentos para solucionar problemas sociales.
11. Un elemento importante que aporta esta investigación es el conjunto de indicadores que permitirán monitorear los cambios que vaya teniendo la aplicación de la informática forense, estos servirán una vez obtenido los resultados poder tomar decisiones para mantener o mejor los cambios y determinar cuál es el desarrollo de esta ciencia en nuestro país en un momento determinado.
12. De las poblaciones de esta investigación, se presenta con propiedad que de todas las encuestadas la que poseen una mayor dificultad para realizar tareas de investigación en casos de delitos informáticos es la fiscalía general de la república, por no tener personal disponible con capacidad para llevar una investigación de este tipo de delitos.
13. Existe una serie de metodologías que se utilizan en la informática forense, estas son aplicadas según el marco legal de los países en los cuales se apliquen, en el salvador estas no son aplicadas debido a la falta de conocimiento de su uso y a la ausencia de leyes que amparen su aplicación.
14. La aplicación de la informática forense en los diferentes estratos de la población salvadoreña, viene a ser una solución a los problemas que actualmente enfrenta en el área de delitos informáticos, sin embargo este concepto es parcialmente aceptado y esto hace que la informática forense en el salvador esté en sus inicios.

II. EN BASE A LA INVESTIGACIÓN DE CAMPO

1. El conocimiento de informática forense por parte de las entidades involucradas en el esclarecimiento de delitos informáticos es relativamente bajo, es decir, teórico; lo que indica que en el país se está iniciando esta especialidad. Por la razón de que esta temática es nueva, tanto para jueces, abogados y fiscales estos tienen desconfianza de la utilización de esta especialidad como herramienta para el análisis de evidencias digitales porque no poseen bases solidas sobre ella.
2. Los jueces conocen sobre delitos informáticos e informática forense, pero existe una desconfianza en las metodologías o procesos realizados por los peritos informáticos al analizar la evidencia digital recolectada, utilizando la informática forense para dichas actividades. Además consideran que la cadena de custodia es un elemento importante que debe ser respetada por los integrantes de la Policía Nacional Civil.

3. Los jueces afirman que la evidencia digital es confiable, lo cual es beneficioso para un proceso judicial ya que son ellos los que tienen la función de aceptar o desestimar las pruebas presentadas en el juicio, fomentando así la necesidad de la creación de métodos, uso de estándares, investigación de herramientas informáticas forenses y el uso de dichas evidencias digitales para mostrar o recrear sucesos que puedan ayudar al esclarecimiento de delitos informáticos.

4. Existen dos elementos que influyen en la confiabilidad de la evidencia digital presentada durante un juicio, el romper la cadena de custodia y la contaminación de la evidencia, provocando que la confiabilidad se vea disminuida generando dudas por las partes involucradas en el juicio.

5. La incredulidad ante la validez y confiabilidad de la evidencia digital en un juicio se debe a que se considera una prueba fácil de manipular y en la cual, a juicio de los abogados y jueces, no se puede detectar a simple vista si ha sido contaminada o no por algún perito u otra persona, generando la invalidez de ésta para ser presentada en un juicio.

6. Recrear la escena es un punto importante que debe de fortalecerse para aumentar la confiabilidad de la informática forense, ya que las demostraciones de cómo sucede un evento es un elemento fundamental para lograr convencer al juez de cómo ha sucedido un delito al mismo tiempo permite sentar bases para resolver casos similares.

7. En nuestro país no existe ninguna ley especifica que ampare el uso de la informática forense como herramienta para el análisis de le evidencia digital, ni la tipificación de la mayoría de los delitos informáticos que existen actualmente.

8. El uso de las nuevas tecnologías, el bajo costo de éstas y la disponibilidad de la información a través de internet de cómo cometer delitos informáticos, ha permitido que se lleven a cabo nuevo tipo de delitos informáticos, por lo cual debe de existir un marco legal que pueda regule la nueva forma de proceder de los delincuentes en nuestro país.

9. Dentro de las poblaciones definidas en nuestro estudio esta contemplada la Policía Nacional Civil, de la cual no se obtuvo información por medio de las encuestas, sino únicamente la descripción de los procedimientos que ellos realizan durante las investigaciones de delitos informáticos.

10. Se obtuvo la información de que los peritos nacionales que se han capacitado en informática forense en el país, ha sido porque son elementos que laboran dentro de la Policía Nacional Civil ya que las organizaciones a través de las cuales se han impartido estas capacitaciones han sido por medio de la ILEA y de la ANSP brindándoles seminarios, capacitaciones a los investigadores forenses así como también proporcionando esta información a los peritos encargados del análisis de la evidencia digital. Siendo este un aspecto negativo, ya que fuera de éstas instituciones, no se cuenta con ninguna otra organización que brinde este conocimiento para peritos, evitando el desarrollo de la informática forense dentro del país.

11. Se desconocen las herramientas informáticas forenses que utiliza la Policía Nacional Civil para el esclarecimiento de delitos informáticos porque dicha información es considerada confidencial por la institución.

12. La falta de conocimiento, metodologías adecuadas a un caso en particular y técnicas por parte de peritos informáticos para la realización del análisis a la evidencia digital embalada, afecta el resultado del análisis realizado y por ende la validez en la evidencia presentada como prueba de un delito.

13. La utilización de estándares para la aplicación de la informática forense beneficia al perito en la utilización de la misma como un recurso serio, confiable y valido para realizar el análisis de evidencia digital y la presentación del resultado final.

14. El beneficio de tener un mayor conocimiento y experiencia en informática forense, por parte de los peritos, es que les permitirá una correcta elección de las metodologías, técnicas y herramientas que se emplean para el esclarecimiento de delitos informáticos, permitiendo así resolver un caso en el menor tiempo posible y con los mejores resultados.

15. Las universidades encuestadas no cuentan actualmente con una asignatura en su pensum curricular relacionada a la informática forense, debido a que no se posee suficiente conocimiento de esta ciencia por parte de los docentes de las carreras de ingeniería y licenciatura de sistemas, además de no contar con el recurso tecnológico requerido.

16. La fiscalía no cuenta con un departamento destinado a tratar los delitos informáticos, dentro de las investigaciones se logro contactar a la única fiscal encargada de llevar investigaciones sobre este tipo de delitos; por consecuencia los casos por delitos informáticos son asignados a fiscales que carecen de los conocimientos necesarios en esta área, dando como resultado la impunidad de este tipo de delitos.

17. A nivel internacional se está fomentando el estudio y la práctica de la informática forense, dándole la oportunidad a peritos informáticos internacionales de contar con las bases teóricas y prácticas necesarias que requiere esta materia, lo cual tiene como resultado un mejor desempeño y aplicación de la misma en los casos donde sea requerida su utilización en esos países.

18. El beneficio de conocer que herramientas son las utilizadas por los peritos en el ámbito internacional, es para estudiar cuales de estas herramientas se pueden utilizar también en nuestro entorno, además de conocer cual es el propósito que cada una de ellas tiene por sus bondades, que análisis que se puede realizar con cada una de ellas a la evidencia digital dependiendo lo que se desea obtener, cuales son los requisitos de hardware/ software y el costo de cada una de ellas.

RECOMENDACIONES

RECOMENDACIONES

1. Las instituciones encargadas de investigar y esclarecer los delitos informáticos deben de capacitar al personal brindándoles conocimiento sobre informática forense, ya que la aplicación de esta especialidad sirve como herramienta para la persecución y procesamiento judicial de los delincuentes.
2. Familiarizar a las unidades policiales con respecto a informática forense porque son las que tienen contacto en primer lugar con las evidencias encontradas en la escena del crimen, por lo que son estos los encargados de guardar la cadena de custodia para evitar que la evidencia sea contaminada.
3. Creación en la Fiscalía General de la República de una unidad dedicada a las investigaciones de delitos informáticos que esté debidamente equipada con tecnología y recurso humano capacitado en informática forense.
4. Capacitaciones continúa sobre informática forense a los jueces porque ellos son los encargados de admitir o no las evidencias presentadas en un juicio y tomar una decisión para dar el veredicto final.
5. Existencia de instituciones certificadoras de informática forense para que cualquier profesional en informática pueda capacitarse en esta área y obtener este tipo de conocimiento.
6. Que la Policía Nacional Civil, realice un estudio de Costo-Beneficio para determinar que opción le conviene más a la institución desde el punto de vista de recursos económico, el traer al país a los expertos informáticos forenses internacionales o el mandar a capacitar fuera del país a sus elementos.
7. Se debe instruir a peritos nacionales en el manejo de herramientas informático forense que utilizan a nivel internacionales otros peritos a la hora de realizar sus peritajes para facilitar la labor de los peritos a nivel nacional y brindar resultados confiables y valederos en un juicio, ya que como resultado de la investigación que se realizo, los peritos internacionales manifestaron que Encase y Hélix son las herramientas que ellos ocupan con mayor frecuencia para la realización del análisis a la evidencia digital.
8. Se recomienda la creación de un directorio que contenga tanto a los ingenieros informáticos como a los peritos informáticos con que cuenta el país para conocer a quienes se pueden abocar la sociedad en general si se desea la opinión de un experto en materia informática forense y poder contar con esta población para la realización de un posterior estudio.
9. Se recomienda comunicar a la población en general a donde tienen que acudir para ir a denunciar delitos de tipo informáticos.
10. Promover talleres que aborden temas relacionados a informática forense en universidades o instituciones de educación superior y hacer partícipe a profesionales responsables del esclarecimiento de delitos informáticos.
11. Se deben fortalecer los conocimientos de tratamiento y manipulación de la evidencia digital a los profesionales que ejercen como peritos informáticos mediante capacitaciones de este tipo para evitar en procesos judiciales cometer errores que puedan ocasionar la libertad del imputado responsable del delito.

12. La educación de los abogados se debe fortalecer en el ámbito de 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.

13. Los elementos primordiales con los cuales se recomienda contar si se desea instalar un laboratorio de informática forense como apoyo a una cátedra dirigida a ingenieros informáticos desde el punto de vista de los expertos en el tema son:

- Contar con un juego de herramientas forenses informáticas.
- Se debe contar con el hardware requerido para soportar estas herramientas y software especializados en el análisis de evidencia digital
- Clonadoras de discos duros para hacer copias fieles de éstos y trabajar con éstas para el posterior análisis y no con los discos originales, preservando así una de las reglas generales de la informática forense.
- Discos duros externos para mayor facilidad de realizar copiar de la evidencia relevante.

14. El beneficio de conocer que elementos comprometen la integridad de la evidencia digital es que se pueden buscar formas de fortalecer a los investigadores forenses para disminuir la posibilidad de generar dudas de la evidencia que analizan, estudian e interpretan.

REFERENCIA BIBLIOGRÁFICA

REFERENCIA BIBLIOGRÁFICA

I. LIBROS

1. Órgano Legislativo de El Salvador; CODIGO PROCESAL PENAL El Salvador Estado: VIGENTE; Imprenta Nacional, El Salvador, 1997.
2. Mohay G.; COMPUTER AND INTRUSION FORENSICS; Artech House, Londres Inglaterra, 2003.
3. Rojas Soriano Raúl; Guía para realizar investigaciones sociales; Editorial P y V, 30° Edición, México, 1998.
4. KENDALL & KENDALL; ANALISIS Y DISEÑO DE SISTEMAS; Prentice Hall Hispanoamérica S.A., 4ta edición, México, 1991.
5. Mejía Salvador I.; Guía para la elaboración de trabajos de investigación, monografías o tesis; Imprenta de la Universidad de El Salvador, 5ª edición; El Salvador, 2006.
6. E. V. Krick; Introducción a la ingeniería y al deseno en la ingeniería; Limusa, México, 2005.
7. Fuentes de Galeano Josefina; ¿Cómo entender y aplicar el método de investigación científica?; Imprenta de la Universidad de El Salvador, 2da Edición, El Salvador, 2006.
8. Dr. Acurio Del Pino Santiago; Introducción a la informática Forense, Imprenta Nacional del Ecuador, Ecuador, 1999.
9. Ander-Egg, Ezequiel; Técnicas de Investigación Social, Editora Gráficas Díaz, S.L., 1era edición, Alicante, España, 1990.
10. García, Carlos Ernesto; Gerencia Informática; Informatik S.A. de C.V., 4ta edición, San Salvador, El Salvador, 2007.
11. Dr. Aguirre Jorge Ramió; Libro Electrónico de Seguridad Informática, Universidad Politécnica de Madrid, 6ta Edición v4.1, España, 2006.
12. Fowler Newton, Enrique; El muestreo estadístico aplicado a la auditoria, Ediciones Macchi, 1era edición, Argentina, 1972.
13. Winograd, Manuel. Fernández, R. Norberto. Farrow, Andrew; "Herramientas para la toma de decisiones en América Latina y el Caribe"; Programa de las naciones Unidas, México, 1997.
14. Programa de las Naciones Unidas para El Desarrollo; "Indicadores sobre violencia en El Salvador"; Talleres Gráficos UCA, 1ª edición, El Salvador, 2002.
15. Hernández Sampieri, Roberto y otros, "Metodología de la investigación" McGraw Hill. Interamericana, DF. México, 1998.
16. Fowler Newton, Enrique; "El muestreo estadístico aplicado a la auditoria", Ediciones Macchi, 1era edición, Argentina, 1972.

17. Salvador I. Mejía;" Guía para la elaboración de trabajos de investigación monográfico o tesis", Imprenta Universitaria, 5ª edición, Cuidada Universitaria, 2006.

18. Josefina Pérez Fuentes de Galeano, Irma Yolanda González de Landos;"Como entender y aplicar el método de investigación científica", Imprenta Criterio, 2ª edición, 2006.

II. PÁGINAS WEB

CONTENIDO DEL TRABAJO

1. Roger Carhuatocto*;"*Codes of practices for digital forensics"; (document WEB), 2003 <http://cp4df.sourceforge.net/>; 10/Marzo/2008

2. Elena Pérez Gómez *;"*Centro para empresas y profesionales"; (documento WEB), 2006 <http://www.microsoft.com/spain/empresas/legal/forensic.mspx>; 10/Marzo/2008

3. Nexos Software S.A. *;"*Computación Forense"; (documento WEB), 2006 <http://www.nexos-software.com.co/Articulo_17.htm>;10/Marzo/2008

4. Alarcón Luis Alfredo; "La prueba pericial" ; (documento WEB), 2006 <http://www.monografias.com/trabajos34/prueba-pericial/prueba-pericial.shtml>; 12/Marzo/2008.

5. Osvaldo Horacio Rapetti*; "*A las puertas de una Nueva Especialización: La informática Forense"; (documento WEB), 2007 <http://www.forensic-es.org/contenido/07/10/las-puertas-de-una-nueva-especializaci%C3%B3n:-la-inform%C3%A1tica-forense.-alberto-david-aira>;15/Marzo/2008

6. Raymod J. Orta Martínez*; "*Informática Forense como medio de pruebas"; (documento WEB), 2008 <http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml>; 16/Marzo/2008

7. Colín Sánchez*; "*Concepto de Perito"; (documento WEB), 2007 < http://www.cevejara.net/cevejara/modules.php?name=News&file=article&sid=131 > ; 16/Marzo/2008

8. Juan Cristóbal Cobo*; "*Hipótesis de investigación"; (documento WEB), 2005 <http://200.76.166.4/~cristobal/estudio_archivos/page0035.htm>;25/Marzo/2008

9. Darío Cutin*; "*La tasa de piratería de software para computadora"; (documento WEB), 2007 < http://w3.bsa.org/latinamerica-spanish/press/newsreleases/2007-global-piracy-study.cfm >;28/Marzo/2008

10. BSA*; "*Fourth Annual BSA and IDC Global Software Piracy Study"; (document WEB), 2007 < http://w3.bsa.org/globalstudy/ >;28/Marzo/2008

11. Juan Martos*; "*El Perito informático, ese gran desconocido"; (documento WEB), 2006 < http://www.recoverylabs.com/prensa/2006/10_06_peritaje.htm>;28/Marzo/2008

12. Javier García Menéndez*; "*Clasificación de La información" (documento WEB), 2005< http://www.uniovi.es/FILE/clasificacion.html >;30/Marzo/2008

13. Management Sciences for Health; "Manual de administración de planificación" (documento WEB), 2008< http://erc.msh.org/FPMH_spanish/chp7/p5.html >;30/Marzo/2008

14. Pita Fernández; "Determinación de tamaño muestral (documento WEB), 1996< http://www.fisterra.com/mbe/investiga/9muestras/9muestras.asp >;1/Abril/2008

15. Pita Fernández; "Determinación del tamaño muestral (documento WEB), 1996< http://www.fisterra.com/mbe/investiga/9muestras/9muestras.asp >;1/Abril/2008

16. UNAM; "B. Determinación del universo, población y muestra (documento WEB), 1996< http://www.tuobra.unam.mx/publicadas/010926133228-B_DETERM.html >;1/Abril/2008

17. Juan Carlos Oliva; "Tipo de Estudio o Tipo de Investigación" (documento WEB), 1995< http://www.mistareas.com.ve/Tipo-de-estudio-tipo-de-investigacion.htm >;2/Abril/2008

18. Caiceo y Mardones; "Descripción de tipos de investigación" (documento WEB), 2003< http://www.profesiones.cl/papers/lee.php?id=9 >;2/Abril/2008

19. Van Dalen y William J. Meyer; "La investigación Experimental" (documento WEB), 2006< http://noemagico.blogia.com/2006/092201-la-investigacion-experimental.php >;4/Abril/2008

20. Ronal Aylmer; "Principios básicos del diseño de experimentos" (documento WEB), 2006< http://www.udc.es/dep/mate/estadistica2/cap2.html >;4/Abril/2008

21. Julio Cabrero García; "Metodología de la investigación" (documento WEB), 1991< http://perso.wanadoo.es/aniorte_nic/apunt_metod_investigac4_5.htm#Experimental >;4/Abril/2008

22. Tevni Grajales G.; "Población y selección de La muestra" (documento PDF), 2000< http://tgrajales.net/investpobmuestra.pdf >;7/Abril/2008

23. Núñez de Arco J. ; "¿Qué es el instituto de investigaciones forenses (idif)?" (Página WEB), <http://www.fiscalia.gov.bo/idif/hojas/quees.htm>;10/Abril/2008

24. Autoridad de desperdicios sólidos ADS Estado libre asociado de Puerto Rico: "información general de desperdicios electrónicos o "e-waste", (Página Web), <http://www.ads.gobierno.pr/secciones/reciclaje/equipos_electronicos.htm>; 20/Abril/2008.

25. Grupo de Bajío; "¿Cuánta energía cuesta tener un equipo de cómputo encendido?" (Página Web), <http://www.glib.org.mx/article.php?story=20030506235650189&mode=print>,20/ Abril/2008.

26. Red Peruana contra la pornografía infantil; "En el Salvador piden medidas efectivas contra la Explotación Sexual Infantil", (Página Web), <http://nopornoinfantil.blogspot.com/2007/11/en-el-salvador-piden-medidas-efectivas.html>; 21/Abril/2008.

27. Virusprot; "Panorama Actual de la Seguridad Informática y los Virus", (Página Web), 2001; <http://www.virusprot.com/Opiniones2002.html>, 21/Abril/2008.

28. Cano Jeimy J. M.Sc.; "CASEY: Preparación Forense de Redes R.E.D.A.R"; (Documento PPT), 2000; Universidad de los Andes, Colombia, <http://www.acis.org.co/memorias/JornadasSeguridad/IIJNSI/forense.ppt>, 21/Abril/2008.

29. .Procuraduría General de La Republica de El Salvador; "Memórias Laborales"; (pagina web), 2008, <http://www.pgr.gob.sv/MLabores.htm> ; 1/Julio/2008.

30. Programa de las Naciones Unidas para el Desarrollo; "Segundo Informe sobre Desarrollo Humano en Centroamérica y Panamá"; (documento web), 2003, <http://www.estadonacion.or.cr/Region2003/Paginas/ponencias/Adm_Justicia_ELS.pdf>; 3/Julio/2008.

31. Alfredo Ascanio PBWIKI; "Tamaño de la Muestra"; (pagina web); 2008; >http://e-askain2007.pbwiki.com/Tama%C3%B1o%20de%20la%20muestra>; 3/Julio/2008.

32. Procuraduría General de la República de El Salvador; "Informe de Labores", 2007; < http://www.pgr.gob.sv/Documentos/MEMORIA%20DE%20LABORES/InformeDeLaboresPGR_Junio2006-Mayo2007.pdf>, 3/Julio/2008

33. Policía Nacional Civil de El Salvador; "Subdirección de Investigación", 2008; < http://www.pnc.gob.sv/conocenos/sub_inv.htm>, 6/Julio/2008.

34. Policía Nacional Civil de El Salvador; "División Investigación Criminal", (Página Web), 2008; <http://www.pnc.gob.sv/conocenos/dic.htm>, 6/Julio/2008.

35. Policía Nacional Civil de El Salvador; "División Policía Técnica Científica", (Página Web),2008; <http://www.pnc.gob.sv/conocenos/dptc.htm>, 6/Julio/2008.

36. Policía Nacional Civil de El Salvador; "División OCN INTERPOL", (Página Web),2008; <http://www.pnc.gob.sv/conocenos/interpol.htm>, 6/Julio/2008.

37. "Desarrollo y uso de Indicadores Ambientales para la planificación y toma de decisiones". (Página Web), 2002 <http://habitat.aq.upm.es/bpal/onu/bp757.html>; 14/Julio/2008.

38. "Sistema de Indicadores Sociales de Venezuela", (Página Web),2005 <http://www.sisov.mpd.gov.ve/glosario/index.html>; 14/Julio/2008.

39. *Ortegón, Pacheco y Prieto;* Metodología del marco lógico para la planificación, el seguimiento y la evaluación de proyectos y programas, (Documento Web), 2005. < http://www.eclac.cl/publicaciones/xml/9/22239/manual42.pdf > ; 18/ Julio/2008.

40. Corte Suprema de Justicia, "Distribución de tribunales por departamento", (Página Web),2008, <http://www.csj.gob.sv/TRIBUNALES/tribunal_01.html>; 01/Junio/2008.

41. El Diario de Hoy, "FGR usa sólo8%de prueba científica en procesos penales", (Documento Web), 2008, < http://www.elsalvador.com/mwedh/pdf/20080406/EDH20080406NAC016P.pdf >, 16/abril/2008.

42. El Diario de Hoy, "Policía busca adquisición demás equipo con partida de fideicomiso", (Documento Web), 2008, <http://www.elsalvador.com/mwedh/pdf/20080406/EDH20080406NAC017P.pdf >, 16/abril/2008.

43. Pértegas Díaz, S., Pita Fernández, S., "Determinación del tamaño muestral para calcular la
significación del coeficiente de correlación lineal", (Página Web), 2008, < http://www.fisterra.com/mbe/investiga/pearson/pearson.asp#TABLA%201>, 1/Junio/2008.

44. Instituto Nacional de Tecnología Agropecuaria de Argentina INTA, "Programa nacional de apoyo al desarrollo de los territorios", (documento web), 2008, <http://www.inta.gov.ar/ies/docs/otrosdoc/indicadores_prognac_territorios.pdf>, 25/Julio/2008.

45. Julia García Salinero;" Prueba de Chi cuadrado y Análisis de la varianza"; documento web,2005. http://www.nureinvestigacion.es/FICHEROS_ADMINISTRADOR/F_METODOLOGICA/pdf_FORMET_20.pdf ; 3/agosto/2008

46. Juan Francisco Monge Ivars, Ángel A. Juan Pérez;" Estadística no paramétrica: prueba chi-cuadrado"; documento web, 2005. http://www.uoc.edu/in3/emath/docs/Chi_cuadrado.pdf; 3/agosto/2008.

47. Salvador Pita Fernández, Sonia Pértega Díaz;" Asociación de variables cualitativas: test de Chi-cuadrado"; documento web, 2004. http://www.fisterra.com/mbe/investiga/chi/chi.asp ; 4/agosto/2008.

48. GIAC, "Forensic Examination Report Examination of a USB Hard Drive", documento web, 2004, http://www.giac.org/certified_professionals/practicals/gcfa/206.php, 24/ agosto/2008.

49. Brian Carrier, "The Sleuth Kit Informer", Sitio web, 2004, http://www.sleuthkit.org/informer/sleuthkit-informer-17.html, 24/ agosto/2008.

50. Daniel Fernández Bleda, "Informática Forense, teoría y practica", Documento web, 2004, http://www.isecauditors.com/downloads/present/hm2k4.pdf, 24/ agosto/2008.

51. Estefania Cantero, "Informática Forense", Documento web, 2007, http://www.felaban.com/memorias_congreso_clade2007/info_forense.pdf, 24/agosto/2008.

52. Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática "Buenas practicas de la administración de la evidencia digital", Sitio Web, 2006, http://74.125.45.104/search?q=cache:KrIALnitrLYJ:gecti.uniandes.edu.co/docs/buenas%2520practica%2520evidencia%2520digital%2520jcano.pdf+HB171:2003&hl=es&ct=clnk&cd=1&gl=sv, 24/agosto/2008.

53. Julio C. Ardita, "Experiencias en análisis forenses informáticos", Documento web, 2006, http://www.utpl.edu.ec/seguridad/images/seguridad/Tendencias_SolucionesInformaticas/experienciasanalisisforense.pdf, 24/agosto/2008.

54. "autopsy forensic browser";documento web, 2003. http://www.sleuthkit.org/autopsy/desc.php; 28/agosto/2008

55. "Algoritmo MD5"; documento web, 2008. http://es.wikipedia.org/wiki/Algoritmo_MD5; 6/agosto/2008

56. e-fense;"Helix, Incident Response & Computer Forensics Live CD". Sitio web, 2005. http://www.e-fense.com/helix/ ;29/agosto/2008

57. Guidance software;"análisis forense informático"; documento web, 2004. http://www.ondata.es/recuperar/encase-detailed1.htm; 29/agosto/2008

58. "Forensic and Incident Response Environment"; document web, 2002. http://biatchux.dmzs.com/; 30/agosto/2008

59. Javier Fernández; "herramientas de seguridad en Gebian"; documento web, 2003. http://www.linux-cd.com.ar/manuales/debian-seguridad/ch-sec-tools.es.html; 31/agosto/2008.

60. "The Coroner's Toolkit "; documento web, 1999. http://www.porcupine.org/forensics/tct.html;30/agosto/2008.

61. Web tutoriales;"servidores SSH"; documento web, 2004. http://www.webtutoriales.com/recursos-gratis/servidor-ssh.html; 31/agosto/2008.

62. Guidance software , "La norma en análisis forense informático", Documento web, 2008, http://helling.files.wordpress.com/2008/01/encaseforensicv6spanish.pdf, 31/ agosto/2008.

63. X-ways Software Technology AG;" WinHex: Software para informática forense y recuperación de archivos"; document web, 2008. http://www.x-ways.net/winhex/index-e.html; 31/agosto/2008.

64. Storm Night;" Knoppix, Linux en CD"; document web, 2003. http://www.maestrosdelweb.com/editorial/knoppix/ ;31/agosto/2008.

65. Autores;"S-T-D 01"; document web, 2004. http://www.knoppix-std.org/index.html; 31/agosto/2008.

66. autores;"S-T-D 01"; document web, 2004. http://www.knoppix-std.org/tools.html; 31/agosto/2008.

67. autores;"Ethereal";documento web, 2008. http://es.wikipedia.org/wiki/Wireshark; 31/agosto/2008.

68. Guidance software; "Encase Forensic";Documento web, 2008. http://www.guidancesoftware.com/es/products/ef_index.asp; 31/agosto/2008.

69. Guidance software, "Requisitos del sistema para Encase Forensic", Sitio Web, 2007, http://www.guidancesoftware.com/es/products/ef_requirements.asp, 31/ agosto/2008.

70. Estefania Cantero, "Informática Forense", Documento web, 2007, http://www.felaban.com/memorias_congreso_clade2007/info_forense.pdf, 31/agosto/2008.

71. Hélix, "Formato de cadena de custodia", Documento web, 2006, http://www.e-fense.com/helix/Docs/coc.pdf, 31/ agosto/2008.

72. RECOVERY LABS, "Informe pericial", Sitio Web, 2008, http://www.delitosinformaticos.info/peritaje_informatico/informe_pericial.html, 31/agosto/2008.

73. Equipos de investigación de incidentes y delitos informáticos," Seminario Informática Forense I EIIDI" Sitio Web, 2007, http://www.eiidi.com/index.php?option=com_content&task=view&id=17&Itemid=34, 2/ Septiembre/2008.

74. Brezinski & Killalea, "RFC 3227 Traducción al español", Sitio Web, 2002, http://www.normes-internet.com/normes.php?rfc=rfc3227&lang=es, 2/Septiembre/2008.

75. Comisión de reglamento técnico y comerciales,"EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información"; documento web, 2007, http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf, 24/septiembre/2008.

76. Lorenzo, G. "Diccionario Informático"; Sitio Web; <http://www.lorenzoservidor.com.ar/info01/diccio-p-r.htm#r>; 23/ Septiembre/2008.

77. ADSL Todo; "Diccionario informático"; 2007; Sitio Web; <http://www.adsltodo.com/diccionario-informatico/>; 23/ Septiembre/2008.

78. Canales, José Ignacio; "Diccionario Básico de Informática"; Sitio Web; <http://europcs.info/ftp/cursos/diccionario/diccionario.htm#R>; 23/Septiembre/2008.

TÉRMINOS INCLUIDOS EN EL GLOSARIO

1. **Herramientas de la información forense.**

Asociación Bancaria.;"La informática forense y La banca" (documento PDF), 2003< http://www.asobancaria.com/upload/docs/docPag1993_1.pdf>; 25/Marzo/2008

2. **Definición de delitos informáticos.**

Organización de las Naciones Unidas;"Definición de Delito Informático" (documento web), 2008< http://www.alegsa.com.ar/Dic/delito%20informatico.php>; 26/Marzo/2008.

Christian Hess Araya; "Delitos Informáticos" (documento PDF), 2003 <http://www.hess-cr.com/secciones/dere-info/charla-delitos.zip >;27/Marzo/2008

3. **Definición de pragmático:**

Diccionario en línea; "Definición de pragmático" (documento web), < http://espanol.geocities.com/andy_n_ve/pala.html >;28/Marzo/2008

4. **Definición de Tecnologías de Información:**
Universidad Autónoma Gabriel René Moreno*; "*Definición de Tecnologías de Información" (documento web), 2008 < http://virtual.sociologiauagrm.org/mod/glossary/view.php?id=81&mode=&hook=ALL&sortkey=&sortorder=&fullsearch=0&page=55&MoodleSession=798deb5f8a08d06ab1985b6fcbecdf74 >;28/Marzo/2008

5. **Definición de Cadena de Custodia:**
Fiscalía General de La Nación Colombia*; "*Cadena de custodia en el sistema acusatorio" (documento web), 2005 < http://www.fiscalia.gov.co/pag/divulga/Semanario/sem17.htm >; 1/Abril/2008

6. **Definición de Actividad Cognoscitiva:**
Psicología de La educación para padres y profesionales *; "*Definición de Actividad Cognoscitiva" (documento web), 2005 < http://www.psicopedagogia.com/definicion/actividad%20cognoscitiva >;4/Abril/2008

7. **Definición de Litigio:**
Ascencio Romero Ángel*; "*Definición de Litigio" (documento web), 2003 < http://cicsa.uaslp.mx/ProgrAcadem/FacDerecho/MtraMaGpe/Documentos/exposiciones2007/cap1/teoria%20general%20del%20proceso%20cap%201.doc >; 4/Abril/2008

III. DOCUMENTOS ELECTRÓNICOS

1. Juan David Gutiérrez; "Informática Forense" (documento pdf), 2006 < http://cicsa.uaslp.mx/ProgrAcadem/FacDerecho/MtraMaGpe/Documentos/exposiciones2007/cap1/teoria%20general%20del%20proceso%20cap%201.doc >; 9/Abril/2008

2. Jim McMillan; "Informática Forense" (documento doc), 2000 < http://www.giac.org/practical/Jim_McMillan_GSEC.doc >;9/Abril/2008

3. Santiago Acurio Del Pino; "Introducción a la informática forense" (documento doc), 2005 < http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/Acurio.pdf >;10/Abril/2008

4. Tevni Grajales Guerra; "Formulación de Hipótesis" (documento pdf), 2000 < http://tgrajales.net/investhipot.pdf>; 14/Abril/2008

5. BSA; "2006 Global Software Piracy Study" (documento pdf), 2007 < http://w3.bsa.org/globalstudy//upload/2007-Losses-Global.pdf >;14/Abril/2008

6. Jeimy J. Cano; "Buenas prácticas en la administración de la Evidencia digital" (documento pdf), 2006 <http://gecti.uniandes.edu.co/docs/buenas%20practica%20evidencia%20digital
a. %20jcano.pdf>;15/Abril/2008.

7. Banco Hipotecario; "Ley de impuestos sobre la renta" (documento pdf), <http://www.bancohipotecario.com.sv/Red_Hipotecario/Asesor_Legal/Ley_de_impuesto_sobre_la_renta_de_El_Salvador.pdf>, 20/Abril/2008.

IV. REVISTAS ELECTRÓNICAS

2. Jeimy José Cano Martínez; "Admisibilidad de la Evidencia Digital: Algunos elementos de revisión y análisis" (documento web), 2003 < http://www.alfa-redi.org/rdi-articulo.shtml?x=1304 >;31/Marzo/2008

V. REFERENCIA DE FUENTES PERSONALES

1. Lic. Boris Solórzano. Profesión: Abogado. Objetivo de la entrevista: conocer el marco legal de informática forense en El Salvador. Fecha: San Salvador, 28 de Febrero de 2008.

2. Ing. Gustavo D. Presman[122]. Profesión: Perito Informático. Objetivo de la entrevista: Asesoría sobre el peritaje informático en Argentina. Fecha: 4 de Marzo de 2008. Y Asesoría sobre el temarios impartidos en informática forense para profesionales en Derecho. Fecha: 24 de agosto de 2008.

3. Lic. Alicia Alvarenga Conde. Profesión: Licenciada en Ciencias de la Computación. Objetivo de la entrevista: conocer su punto de vista sobre la informática forense, ya que ella asesoró un trabajo de graduación bibliográfico en una Universidad privada del país sobre ese tema. Fecha: San Salvador, 11 de Marzo de 2008.

4. Ing. Edson Montoya. Profesión: Ingeniero de Sistema Informáticos. Objetivo de la entrevista: conocer su punto de vista sobre la informática forense ya que ha participado como perito informático en procesos judiciales. Fecha: San Salvador, 22 de Marzo de 2008.

5. Lic. Johanna Álvarez. Profesión: Abogada. Objetivo de la entrevista: interpretación de los artículos contemplados en el código penal acerca de los peritos en El Salvador. Fecha: San Salvador, 27 de Marzo de 2008.

VI. TESIS

1- Martínez Díaz, Ana Iris, "Indicadores Ambientales para una Clasificación Municipal. Departamento de Chalatenango", Universidad de El Salvador, El Salvador, 2004.

2- Molina Fuentes, Claudia Carolina, "Diseño de un sistema de control para las áreas administrativas de los gobiernos municipales", Universidad de El Salvador, El Salvador, 2008.

[122] Cabe mencionar que la entrevista realizada al Ing. Presman se llevo a cabo vía correo electrónico debido a que su lugar de residencia en Argentina.

GLOSARIO DE TÉRMINOS

GLOSARIO DE TÉRMINOS

A

Actividad Cognoscitiva: Es un proceso a través del cual el sujeto capta los aspectos de la realidad, a través de los órganos sensoriales con el propósito de comprender la realidad.

AES: (Advanced Encryption Standard). Esquema de cifrado por bloques, que fue adoptado como estándar de cifrado por el gobierno estadounidense. AES es uno de los algoritmos más utilizados en criptografía simétrica.

ANSP: Academia Nacional de Seguridad Pública: Ente encargado de forjar y capacitar las unidades policiales de El Salvador

Archivos sospechosos: archivos que están sujetos a análisis forense, los cuales probablemente tengan información sobre la investigación que se este realizando.

B

Backdoors: del inglés "puerta trasera", programa que permite acceder de forma remota a los sistemas infectados y obtener el control de los mismos.

Balística: Es la rama de la Criminalística que se encarga del estudio de las armas de fuego, de los fenómenos en el momento del disparo, de los casquillos percutidos, de los proyectiles disparados, de la trayectoria de estos últimos y de los efectos que producen.

BSA: La *Business Software Alliance* es una organización no lucrativa que representa a los fabricantes de software propietario ante los consumidores y que combate la copia y el uso no autorizado de software en empresas o instituciones.

C

Cadena de Custodia: es la aplicación de una serie de normas tendientes a asegurar, colocar y proteger cada elemento material probatorio para evitar su destrucción, suplantación o contaminación, lo que podría implicar serios tropiezos en la investigación de una conducta punible.

Comienza, la cadena de custodia, cuando el servidor público en actuación de indagación o investigación policial coloca y rotula el elemento material probatorio y evidencia física (huellas, rastros, manchas, residuos, armas, instrumentos, dinero, documentos, grabaciones en audio y video, etc.). Tal procedimiento inicia en el sitio donde se descubren, recauden o encuentren elementos materiales probatorios y finaliza por orden de autoridad competente.

CEO: (Chief Executive Officer): Gerente General.

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.

CRC: Código de Redundancia Cíclica. Método de control de errores en datos. Indice

D

Delitos de Cuello Blanco: Son todos aquellos delitos cometidos por funcionarios, políticos y empresarios con un poder económico que todo corrompe, evadiendo impuestos, explotando a los trabajadores de todos los niveles económicos, protegidos por todas las autoridades.

DD: Data Definición, (definición de archivo), permite realizar copias exactas de bloques de memoria.

E

Embalar: Colocar convenientemente dentro de cajas, cubiertas o cualquier otro envoltorio los objetos que han de transportarse

Encuadre: Es la porción de realidad captada por el objetivo.

Escena del crimen: lugar donde se perpetro el hecho delictivo de carácter informático, por ejemplo una habitación de un hotel, un Ciber, etc.

Espacio unallocated: espacio muerto no utilizable ni por el sistema operativo ni por otros programas.

Esteganografía: es una disciplina que trata sobre técnicas que permiten la ocultación de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

Evidencia Digital: abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor.

Evidencia Volátil: evidencia almacenada en memoria RAM y que se pierde al apagar la computadora.

Exploits: códigos que explotan vulnerabilidades en el software, utilizado por atacantes y por el malware para infectar sistemas de forma automática.

F

Firmas digitales: en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

H

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. Los valores hash también se utilizan en las firmas digitales. Dado que se pueden utilizar

valores hash pequeños para representar cantidades de datos de mayor tamaño, sólo es necesario firmar el hash de un mensaje, en lugar de todos los datos del mismo.

HPA: Detecting Host Protected Areas (HPA) in Linux, "The Sleuth Kit Informer Issue #17". Noviembre 15 de 2004.

I

IDS: "Sistema de detección de intrusiones", es un sistema de seguridad que detecta inapropiado o malicioso actividad en un equipo o red. Un sistema de detección de intrusos (IDS) se utiliza para determinar si una computadora o servidor de red ha experimentado una intrusión no autorizada. Un IDS funciona como un sistema de alarma. Si se detecta una posible intrusión, el sistema IDS enviar una alerta o advertencia que un símbolo del administrador para llevar a cabo una investigación más a fondo que podría incluir informática forense y el enjuiciamiento.

ILEA: International Law Enforcement Academies: Institución perteneciente a Estados Unidos de América cuyo objetivo es dar soporte a instituciones policiales fortaleciendo y mejorando sus actividades contra el crimen.

Indulto: Significa perdón, causa de extinción de la responsabilidad penal que supone el perdón de la pena.

Inferencia: es una evaluación que realiza la mente entre conceptos que, al interactuar, muestran sus propiedades de forma discreta, necesitando utilizar la abstracción para lograr entender las unidades que componen el problema, creando un punto axiomático o circunstancial, que nos permitirá trazar una línea lógica de causa-efecto, entre los diferentes puntos inferidos en la resolución del problema.

ISP: proveedor de servicio de internet.

L

Línea de tiempo: cronología de las actividades realizadas durante un proceso forense por medio de la aplicación de metodologías de informática forense.

Litigio: El litigio es un conflicto de intereses, donde existe la pretensión por una parte y la resistencia por otra. Para que un conflicto sea verdaderamente un litigio, es necesario que una de las partes exija que la otra sacrifique sus intereses al de ella, y la segunda oponga resistencia a la pretensión del primero.

M

Mbox: Término genérico para una familia de formatos de fichero que se usan para almacenar conjuntos de correos electrónicos. Todos los mensajes en un buzón mailbox están concatenados en un único fichero.

MD5: En criptografía, MD5 (acrónimo de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

Md5sum: cálculo del código que identifica cada una de las particiones del disco duro a partir de su contenido de forma única.

Medio Electrónico: entiéndase por medio electrónico todos los dispositivos como Computadoras, celulares, agendas electrónicos, dispositivos de almacenamiento, tarjetas inteligentes, entre otros.

Metadatos: son definidos como datos sobre los datos. Son como las etiquetas de un producto, nos brinda información relativa a este como, el peso fecha de caducidad, etc.

N

Netcat: Programa para uso de los administradores de redes.

NIST: es el Nacional Institute of Standards and Technology, una unidad de los EE.UU. Departamento de Comercio. Anteriormente conocida como la Oficina Nacional de Normas, NIST promueve y mantiene las normas de medición. También tiene programas activos para alentar y ayudar a la industria y la ciencia para desarrollar y utilizar estas normas.

P

Pendrive: tipo de dispositivo USB de almacenamiento.

Perpetran: Realización de un hecho, sinónimo de llevar a cabo o realizar una acción.

Pragmático: El contexto debe entenderse como situación, practica o persona practica.

Print Spooler: (cola de impresión) Cuando se imprime un documento, el formato de salida se almacena en el disco, y la cola de impresión alimenta la impresión de imágenes a la impresora en el fondo más lenta en velocidades de impresión.

Post-Mortem: Después de la muerte.

R

RAID: utiliza múltiples discos como si se tratara de una unidad lógica sola. El sistema operativo y el usuario ven un solo disco, pero en realidad la información es almacenada en todos los discos.

RFC Request for Comments: la traducción en español es: *Solicitud para comentario.* La cual es una serie de documentos, iniciada en 1969, en los cuales se describen conjuntos de protocolos y estándares de Internet, estándares propuestos de temas relacionados y ,generalmente, las ideas en proceso de aceptación son documentados y publicados, ordenándolos por medio de una numeración y son referencias oficiales ya establecidas.

ReiserFS: es un sistema de ficheros B*-tree que tiene un gran rendimiento y que sobrepasa con creces a ext2 y ext3 cuando se trata de trabajar con ficheros pequeños (archivos menores de 4KB), en ocasiones diez o quince veces mejor. ReiserFS es extremadamente escalable y soporta transaccionalidad. ReiserFS es sólido y estable para su uso en escenarios genéricos así como en casos extremos cuando es necesario trabajar por ejemplo con grandes sistemas de ficheros, manejar ficheros muy grandes o directorios conteniendo miles y miles de ficheros.

S

Safeback: se utiliza para crear imagen-espejo (flujo de bits) archivos de copia de seguridad de discos duros o para hacer un espejo-imagen ejemplar de toda una unidad de disco duro o partición. SafeBack archivos de imagen pueden detectar los intentos de alterar la reproducción. Además es un estándar de la industria auto-autenticación de la herramienta informática forense que se utiliza para crear copias de seguridad de las pruebas de grado de unidades de disco duro.

Secuestro del equipo: se refiere al levantamiento que hacen los agentes policiales de la evidencia encontrada en el lugar donde se cometió el delito, por ejemplo: dispositivos de almacenamiento, computadoras, etc.

Serología Forense: La determinación del tipo y características de la sangre, pruebas de sangre, examen de las tinciones de sangre y la preparación del testimonio en un juicio, son la principal función de un serólogo forense, quien analiza el semen, saliva, y otros líquidos corporales -que pueden o no- estar vinculados con análisis de ADN.

Servlet: son pequeños programas escritos en Java que se ejecutan en el contexto de un navegador web

Sistema muerto: se maneja este termino al equipo informático cuando este esta apagado y se va ha realizar el análisis forense en ese estado.

Sistema vivo: es cuando se analiza el equipo informático en estado encendido, es decir si en la escena del crimen se encuentran computadoras encendidas, debe de proceder a analizarse para que la información pueda extraerse exactamente.

Slackspace:(holgura el espacio) es el espacio entre el final de un archivo y el final del disco, también llamado "archivo de holgura", que se produce naturalmente porque los datos rara vez se fijan para llenar los lugares de almacenamiento exactamente, y el residual de datos se producen cuando un archivo más pequeño que está escrito en la misma categoría, tiene una mayor capacidad de los archivos anteriores. En informática forense, holgura el espacio es examinado porque puede contener datos significativos.

T

Tablet PC: es una computadora entre portátil y un PDA, en el que se puede escribir a través de una pantalla táctil.

Tecnología de Información: Término general que se refiere al conocimiento y uso de computadoras y sistemas de comunicación electrónicos en organizaciones

V

VMware: virtualiza todos los dispositivos dentro del entorno virtual, incluyendo el adaptador de video, el adaptador de red, y los adaptadores de disco duro.

ANEXOS

ANEXOS

ANEXO #1: CARTA ESCUELA DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA DE SISTEMAS INFORMATICOS

Ciudad universitaria, 4 de Abril de 2008

Ing. Rubén Asencio
Coordinador de trabajos de Graduación
Escuela de Ingeniería de Sistemas Informáticos
Facultad de Ingeniería y Arquitectura
Presente

Estimado Ing. Asencio:

1) Por este medio me permito hacer de su conocimiento que la Escuela de Ingeniería de Sistemas Informáticos, está interesada en el desarrollo del trabajo de graduación titulado "ESTUDIO Y ANALISIS SOBRE LA INFORMATICA FORENSE EN EL SALVADOR" el cual será dirigido por el docente director Ing. Julio Alberto Portillo.

   Entiendo que el trabajo será desarrollado por los siguientes bachilleres:

   Ramiro Alexander Belloso Urbina
   Mirna Noemy Mancía Rivera
   Oscar José Moran Bautista
   Guadalupe Beatriz Olmedo Portillo

2) Considero que los resultados de dicho trabajo de graduación pueden ser de alta trascendencia para el desarrollo del campo forense en el país; por lo que estaré pendiente de los mismos para propiciar su oportuna divulgación.

Atentamente,

"HACIA LA LIBERTAD POR LA CULTURA"

ESCUELA DE INGENIERIA DE SISTEMAS INFORMATICOS DIRECCION

Ing. Carlos Ernesto García García
Director de la Escuela de Ingeniería de Sistemas Informáticos

FINAL 25 AV. NTE., CIUDAD UNIVERSITARIA, SAN SALVADOR, EL SALVADOR, C.A.
APARTADO POSTAL 740 TEL.:(503) 235-7035 FAX:(503) 225-2506
e-mail: eisi@ing1.ues.edu.sv

ANEXO #2: REPORTAJE SOBRE LA FISCALÍA Y EL USO DE PRUEBAS CIENTÍFICAS.

16

NACIONAL EL DIARIO DE HOY
Domingo 6 de abril de 2008 nacional@elsalvador.com

Ante tribunales de justicia

FGR usa sólo 8% de prueba científica en procesos penales

FOTO EDH/ARCHIVO

LA FALTA DE PERSONAL es una de las grandes limitantes que tiene el laboratorio científico para entregar los resultados de las pruebas.

» Policía Técnica Científica aduce que tiene 14 mil casos y que el tiempo no les alcanza

FOTO EDH/LUIS VILLALTA

LA FALTA DE TECNOLOGÍA fue una de las principales limitantes que tuvo la Policía durante muchos años. Se pretende mejorar esta situación con los fondos del fideicomiso.

Jaime López

La prueba científica es un elemento irrefutable para lograr la condena o absolución de una persona procesada penalmente ante un tribunal de justicia, siempre y cuando ésta no haya sido contaminada o falseada en la cadena de custodia, la cual se establece mediante procedimientos y protocolos estandarizados por la legislación salvadoreña.

Sin embargo, esta valiosa herramienta es poco utilizada por la Fiscalía General de la República para fundamentar sus casos. Estiman que su uso es de un 8% de la totalidad de los delitos cometidos en el país y que son ventilados en los tribunales, afirmó el juez Sexto de Instrucción de San Salvador, Roberto Arévalo Ortuño.

Los juzgadores han percibido que en los últimos años hay un ligero interés por la prueba científica en los diferentes procesos judiciales que se entablan.

"Hemos tenido casos donde la prueba científica ha tenido una contundencia enorme porque puede ser que no haya ningún testigo, pero si tienen este tipo de argumentos la Fiscalía gana el caso aplastantemente o más que ganar el caso, se llega a la verdad real de los hechos", manifestó el juez.

No es fácil para la defensa, en esos casos, desvirtuar la prueba científica, cuando evidencias como huellas dactilares, fluidos, sangre y cabellos, entre otros, encontrados en la escena del delito, corresponden al implicado y a nadie más, esto debido a que las pruebas de Ácido Desoxirribonucleico (ADN) son únicas.

Pero la prueba por sí sola no es determinante para ser utilizada en un proceso judicial, ya que para que ésta sea fulminante en contra de un acusado, debe cumplir con estándares legales.

La contaminación de una evidencia puede darse en diferentes momentos del proceso, desde su recolección en la escena del crimen, ya sea por falta de conocimiento e inexperiencia de los agentes policiales al custodiar la zona o delimitar hasta dónde llega la escena, o manipulación inadecuada de las mismas.

"Por ejemplo es posible determinar que el dinero decomisado a una persona ha estado mezclado con droga, a través del equipo técnico especializado de laboratorio (el ION Scan)", afirmó Arévalo Ortuño.

En ese tipo de hechos, la tecnología es de suma importancia porque puede procesar la prueba en menos tiempo y con un 100% de efectividad.

A pesar de su vital importancia, procesar la prueba científica tiene un alto costo, tecnológicamente hablando.

La obtención de maquinaria de detección como el IBIS (para balística), el AFIS (para huellas digitales), el ION Scan (para droga) tiene un alto costo para el Estado y está supeditada a la realidad de adquisición de cada país, lo que en algunos casos impide a las autoridades acceder a tecnología moderna con alta precisión.

Aunado a esta deficiencia, paralelamente está el auge de delincuencia de estos países que saturan los escasos recursos técnicos disponibles.

En los últimos dos años, en El Salvador han ocurrido 3,928 homicidios en 2006 y 3,476 en 2007 que deben investigarse, al igual que otros delitos.

Esta situación atañe a la Fiscalía General de la República, obligada constitucionalmente a dirigir la investigación del delito. No obstante, llegar a la verdad o esclarecer un hecho no es responsabilidad única de un sólo ente del Estado, sino de todo un sistema, que si no trabaja coordinadamente y al mismo ritmo, los resultados nunca serán los esperados.

Basado en esa premisa, la Fiscalía se queja de no tener en su poder los informes y peritajes de la Policía Técnica Científica, en el periodo requerido por ley. Ante esa dificultad, muchos sospechosos son puestos en libertad a las 72 horas y estos hechos vienen a engrosar las listas de la impunidad.

"No siempre tenemos una respuesta rápida del laboratorio en los casos que se investigan, debido a la mora histórica", aseveró la fiscal de la unidad de Vida, Patricia Lara.

A 15 años de la creación de la Policía Nacional Civil (PNC) en El Salvador, los equipos de laborato-

EL DIARIO DE HOY NACIONAL
Domingo 6 de abril de 2008 nacional@elsalvador.com

DEFICIENCIAS

La Policía Técnica Científica experimenta dificultades para investigar delitos cibernéticos como fraudes y robos de datos, que se cometen a través de la Internet. Tampoco cuenta con especialista en sonido para análisis de grabaciones, no posee tecnología para el análisis de ADN.

200 personas

Es la cantidad que labora en el laboratorio técnico científico de la Policía, entre técnicos y peritos en áreas como fisicoquímico, serología y farmacia.

LABORATORIO. Investigadores técnicos utilizan el IBIS para determinar con qué arma se cometió determinado delito.

"Entre un 80 y un 85 por ciento de los homicidios sustentados con prueba científica en los tribunales han sido ganados"

PATRICIA LARA
Fiscal de la Unidad de Vida

EQUIPAN DELEGACIONES

Las 21 delegaciones del país y los dos laboratorios regionales en Santa Ana y San Miguel serán fortalecidos con mejor equipo de fichaje e inspecciones oculares. Invertirán 90 mil dólares para cambiar las cámaras fotográficas porque la mayoría está dañada.

54 juicios

Esa fue la cantidad de vistas públicas por homicidio ganadas por la Fiscalía, donde la prueba científica fue determinante.

Policía busca adquisición de más equipo con partida de fideicomiso

El Diario deHoy

Gracias a los recursos del fideicomiso, la División de la Policía Técnica Científica ha comenzado el proceso de modernización de sus laboratorios, mediante la adquisición de una lista de aparatos sofisticados como el sistema automatizado de identificación de huellas dactilares, sistema integrado de identificación balística, equipo para grafología y análisis físico químico para restauración de señas, seriales y pinturas, entre otros.

Equipos como el sistema automatizado de identificación balística (IBIS) ya fue adquirido por la corporación mediante una inversión de 1.7 millones de dólares. "El equipo ha demostrado su nobleza porque hemos investigado armas que registran más de 30 homicidios, todo su historial y ha permitido la captura de implicados", afirmó el subcomisionado Julio César Santana Vela.

Al IBIS se ha sumado el sistema de video espectro comparador DSC 5000, a un costo de 158 mil dólares, el cual permite identificar alteraciones de visas en pasaporte, billetes y papel moneda falsa, manuscritos y sellos alterados, cuyos resultados no solo son apreciados en pantalla de un computador sino impresa, a fin de ofrecerlas como prueba en un tribunal. Dentro de las nuevas adquisiciones también hay siete microscopios de luz polarizada, necesarios para evaluar evidencias serológicas (análisis de sangre y fluidos), para casos de homicidios, violaciones y otro tipo de agresiones, valorados cada uno en 23 mil dólares.

Para fortalecer la lucha contra el narcotráfico en el país y analizar la pureza de todo tipo de droga, la corporación adquirió un aparato valorado en 65 mil dólares. Con el nuevo equipamiento, el laboratorio técnico científico de la Policía, será el mejor de Centroamérica y Colombia, aseguró Santana Vela.

ADQUISICIONES PENDIENTES

En los próximos meses la corporación policial obtendrá un microscopio electrónico valorado en 400 mil dólares y un sistema automatizado de identificación de huellas dactilares (AFIS por sus siglas en inglés), valorado en un millón 900 mil dólares.

Cuentan con una partida de 500 mil dólares para la ampliación del edificio del laboratorio en la colonia San Francisco, al poniente de la capital, lo que le permitirá separar la parte administrativa de la técnica y operativa del laboratorio. El terreno donde está instalado el laboratorio es propiedad de la PNC.

LOS REGIONALES

Los laboratorios regionales situados en San Miguel y Santa Ana estarán en la capacidad de desarrollar y procesar evidencias en equipo de balística, grafotecnia, inspecciones oculares, dactiloscópicas y restauración de señas y seriales.

15 armas

de fuego diarias son las enviadas al laboratorio científico de la Policía para verificar si con ellas se han cometido delitos.

LABORATORIO CENTRAL

En los regionales no se podrán realizar análisis de sustancias psicotrópicas (drogas), toxicología, poligrafía, revelado fotográfico y la evaluación de microevidencias. Ese servicio sólo será brindado por el laboratorio central situado en la colonia San Francisco, en la capital.

"Los investigadores, fiscales y recolectores de evidencia deben ser personas críticas y analíticas"

JULIO CÉSAR SANTANA VELA
Jefe de la Policía Técnica Científica

"Con prueba científica la Fiscalía gana un caso de forma aplastante y más que eso, llega a la verdad real"

ROBERTO ANTONIO ARÉVALO
Juez Sexto de Instrucción

rio técnico científico, heredado de los anteriores cuerpos de seguridad, ya cumplieron su vida útil, están obsoletos y no responden a la ola de delincuencia y complejidad de los delitos actuales.

MODERNIZACIÓN

Para satisfacer esa inmanejable demanda, la PNC ha recibido un refuerzo de siete millones de dólares este año, suma con la que ya licitó todo el equipo técnico necesario.

Con esos fondos, el laboratorio ya sustituyó más del 15 por ciento de su equipo y calculan que al finalizar 2008, la Policía Técnica Científica estará totalmente reforzada.

Según el jefe de dicha división, subcomisionado Julio César Santana Vela, a diferencia del pasado, ahora por ley todos los casos de violencia y delincuencia que ocurren en el territorio nacional, deben ser investigados técnica y científicamente por la Policía, lo que incrementa su labor.

Los 420 homicidios menos que de 2007, según el subcomisionado Santana Vela, fue un respiro importante para la labor de los peritos de la Policía.

Pero aún así, sólo el año pasado, la referida División llevó, a sus laboratorios, las pruebas y evidencias de 14 mil casos, lo que demandó practicar más de 52 mil indagaciones, sobre todo por homicidios, lesiones, robos, hurtos, violaciones, narcotráfico, falsificación de moneda y otros documentos.

Santana Vela afirmó que existen hechos donde ni si quiera han tenido ni 24 horas para procesar la evidencia e interpretar los resultados. Según la fiscal Lara, en los últimos casos han luchado por llevar la prueba científica con la testimonial aún mismo paso.

Sin embargo, es consciente de que la segunda es más vulnerable, y siempre está anidada a un interés de una de las partes "ya sea por sentimiento de venganza, se puede mentir por amor u otro interés de tipo económico".

ANEXO #3: INFORME PROPORCIONADO POR LA DEFENSORÍA DEL CONSUMIDOR SOBRE DENUNCIAS DE DELITOS.

Defensoría del consumidor
La Razón... ¡A quien la tiene!

DEFENSORIA DEL CONSUMIDOR
OFICINA SSF

DENUNCIAS RECIBIDOS POR MOTIVO

Desde: 01-Ene-07 ***Hasta:*** 31-Dic-07

Tipo nombre_proveedor Caso no	*Nombre consumidor*	*motivo*	*Fecha presentacion*	*Monto Reclamado*
Motivo Denuncia:	**CLONACION DE TARJETAS**			3
DENUNCIA				3
TARJETA DE CREDITO				3
BANCO PROMERICA S.A				1
21278	ANTONIO RAFAEL MENDEZ MILIA	CLONACION DE TARJETAS	13/12/2007	$810.00
CREDOMATIC DE EL SALVADOR, S. A. DE C.V.				1
16419	SILVIA MARLENE MONTES OCHOA	CLONACION DE TARJETAS	15/02/2007	$234.92
TARJETAS DE ORO, S. A. DE C. V.				1
20678	FLOR DE MARÍA ALVARENGA DE RI	CLONACION DE TARJETAS	22/11/2007	$1,828.97

Total Casos: 3

DEFENSORIA DEL CONSUMIDOR
OFICINA SSF

DENUNCIAS RECIBIDOS POR MOTIVO

Desde: 01-Ene-08 ***Hasta:*** 11-Abr-08

Tipo nombre_proveedor Caso no	Nombre consumidor	motivo	Fecha presentacion	Monto Reclamado	
Motivo Denuncia:	CLONACION DE TARJETAS				1
DENUNCIA					1
TARJETA DE CREDITO					1
BANCO HSBC SALVADOREÑO S.A.					1
23839	WALTER RICARDO TORRES MUÑOZ	CLONACION DE TARJETAS	13/03/2008	$0.00	

Total Casos: 1

ANEXO #4: DISTRIBUCIÓN DE TRIBUNALES EN SAN SALVADOR

En San Salvador se encuentran 17 juzgados de instrucción, 10 de los cuales se encuentra en el Centro Judicial Isidro Menéndez y los 7 restantes se encuentra en el municipio de Soyapango.

TRIBUNALES de EL SALVADOR
CORTE SUPREMA DE JUSTICIA

DISTRIBUCIÓN DE TRIBUNALES POR DEPARTAMENTO
TOTAL DE TRIBUNALES: 549

DISTRIBUCION DE TRIBUNALES POR DEPARTAMENTO

JUZGADOS DE PRIMERA INSTANCIA 36%															
MATERIA	SAN SALVADOR	SANTA ANA	SAN MIGUEL	SAN MIGUEL	USULUTÁN	SONSONATE	LA UNIÓN	LA PAZ	CUSCATLÁN	CUSCATLÁN	AHUACHAPÁN	MORAZÁN	SAN VICENTE	CABAÑAS	TOTAL
SENTENCIA	6	2	2	1	1	1	1	1	1	1	1	1	1	1	21
INSTRUCCIÓN	17	5	4	3	2	2	3	3	-	2	2	1	2	-	46
VIG. PENIT. Y EJEC. PENAS	2	2	2	1	1	-	-	-	-	1	-	-	1	-	10
CIVIL	9	5	2	2	1	1	2	1	-	1	1	-	1	-	26
MERCANTIL	5	-	-	-	-	-	-	-	-	-	-	-	-	-	5
FAMILIA	7	2	2	1	1	1	1	1	1	1	1	1	1	1	22
MENORES	5	2	1	2	1	1	1	1	1	1	1	1	1	1	20
LABORAL	5	1	1	1	-	1	-	-	-	-	-	-	-	-	9
INQUILINATO	2	-	-	-	-	-	-	-	-	-	-	-	-	-	2
MILITAR	1	-	-	-	-	-	-	-	-	-	-	-	-	-	1
MENOR CUANTIA	2	-	-	-	-	-	-	-	-	-	-	-	-	-	2
EJEC. MEDIDAS	2	1	1	-	-	-	-	-	-	-	-	-	1	-	5
MIXTOS	1	-	2	2	4	3	-	1	3	1	1	2	1	2	23
TRANSITO	4	1	2	1	-	1	-	-	-	-	-	-	-	-	9
Totales	**68**	**21**	**19**	**14**	**11**	**11**	**8**	**8**	**6**	**8**	**7**	**6**	**9**	**5**	**201**

Número de juzgados de instrucción que se encuentran en San Salvador.

Fuente: Corte Suprema de Justicia de El Salvador

TRIBUNALES de EL SALVADOR
CORTE SUPREMA DE JUSTICIA

DEPTO. DE SAN SALVADOR

PRIMERA PARTE	SEGUNDA PARTE
CENTRO PENAL INTEGRADO	TRIBUNALES, JUZGADOS, OFICINAS JURÍDICAS Y OFICINAS ADMINISTRATIVAS QUE SE ENCUENTRAN AFUERA DE LAS INSTALACIONES DEL CENTRO JUDICIAL "DR. ISIDRO MENÉNDEZ"

CENTRO PENAL INTEGRADO
PRIMERA PARTE

TRIBUNAL Y TITULAR (ES)	DIRECCIÓN
JUZGADO 1º DE INSTRUCCIÓN Lic. Levis Italmir Orellana Campos Lic. José Rodolfo Meléndez González (Secretaría)	Edificio "A 2 - 1º Nivel"
JUZGADO 2º DE INSTRUCCIÓN Lic. Edelmira Violeta Flores Orellana Lic. Douglas René Padilla (Secretaría)	Edificio "A 2 - 1º Nivel"
JUZGADO 3º DE INSTRUCCIÓN Lic. Alba Estela Zelaya Chévez Lic. Luz Leticia Elena Flores (Secretaría)	Edificio "A 2 - 1º Nivel"
JUZGADO 4º DE INSTRUCCIÓN Lic. Aristarco Chavarría Flores Lic. Ligia Carolina Funes (Secretaría)	Edificio "A 2 - 1º Nivel"
JUZGADO 5º DE INSTRUCCIÓN Lic. Edward Sydney Blanco Lic. Patricia Anabel Miranda Roque (Secretaría)	Edificio "A 1 - 1º Nivel"
JUZGADO 6º DE INSTRUCCIÓN Lic. Roberto Antonio Arévalo Ortuño Lic. Oscar William Fernández Morán (Secretaría)	Edificio "A 1 - 1º Nivel"
JUZGADO 7º DE INSTRUCCIÓN Dr. Miguel Ángel García Arguello Lic. Carlos Manuel Cañadas (Secretaría)	Edificio "A 1 - 1º Nivel"
JUZGADO 8º DE INSTRUCCIÓN Lic. Gloria de La Paz Lizama Funes Lic. Aída Hortensia Villatoro Hernández (Secretaría)	Edificio "A 1 - 1º Nivel"
JUZGADO 9º DE INSTRUCCIÓN Lic. Patricia Cruz de Chavarría Lic. Luís Abercio Mejía Vásquez (Secretaría)	Edificio "A 2 - 2º Nivel"
JUZGADO 10º DE INSTRUCCIÓN Lic. Carlos Ernesto Calderón Lic. William Steve Larios Romero (Secretaría)	Edificio "A 2 - 2º Nivel"

Juzgados y Titulares que se encuentran en el centro judicial Isidro Menéndez.

Fuente: Corte Suprema de Justicia de El Salvador

TRIBUNALES de EL SALVADOR
CORTE SUPREMA DE JUSTICIA

MUNICIPIO DE SOYAPANGO
DEPTO. DE SAN SALVADOR

TRIBUNAL Y TITULAR (ES)	DIRECCIÓN
Juzgado 1º de Instrucción Soyapango Licda. Marta Lydia Peraza Guerra	6ª Av. Nte. Res. Las Arboledas, No. 2,
Juzgado 2º de Instrucción Soyapango Licda. Ethel Jacqueline Orellana Moreira	Urb. Arboleda, Pje. 3 Block F No. 28,
Juzgado 3º de Instrucción Delgado Licda. Lesvia Alvarenga Barahona	Col. Acolhuatan, Pol. 3 No. 13, Ciudad
Juzgado 4 º de Instrucción Marcos Lic. Ernesto Vladimir López Cruz	1ª Calle Ote. Col. El Milagro No. 56, San
Juzgado 5 º de Instrucción Mejicanos Lic. Gilberto Ramírez Melara	Col. España, Calle PP. Jesús Yañez No. 21,
Juzgado 6 º de Instrucción Lic. Rigoberto Chicas	
Juzgado 7 º de Instrucción Ilopango Licda. Sandra Carolina Méndez	3ª Calle Ote. No. 11, Bº El Centro,

Juzgados y Titulares que se encuentran en el municipio de Soyapango

Fuente: Corte Suprema de Justicia de El Salvador

ANEXO #5: TABLA ÁREAS BAJO LA CURVA NORMAL TIPIFICADA DE 0 A Z[123] PARA DETERMINAR EL NIVEL DE CONFIANZA Y EL COEFICIENTE DE CONFIABILIDAD[124].

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[125]	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[126]	0.4854	0.4857

[123] Tomado del Libro: "El Muestreo estadístico aplicado a la auditoria". Ver *apartado Referencia Bibliográfica – I:Libros literal 12* para su mayor comprensión.

[124] Fuente: Ver apartado Referencias Bibliográficas- I:Libros: numeral 16.

[125] Nivel de confianza 95%, Z = 1.96 (0.4750x2 = 0.95)

[126] Nivel de confianza 97%, Z = 2.17 (0.4850x2 = 0.97)

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: TABLA DE LOS VALORES DEL ERROR MUESTRAL DEPENDIENDO DEL NIVEL DE CONFIANZA ELEGIDO

º	e	Prueba bilateral	Prueba unilateral
80 %	0,200	1,282	0,842
85 %	0,150	1,440	1,036
90 %	0,100	1,645	1,282
95 %	**0,050**	1,960	1,645
97,5 %	0,025	2,240	1,960
99 %	0,010	2,576	2,326

Valores de error muestral[127] "e" utilizados con mayor frecuencia en el cálculo del tamaño muestral en función del nivel de confianza elegida para el estudio.

[127] Fuente: Ver apartado Referencias Bibliográficas- II: Paginas Web: numeral 43.

ANEXO #7: "CARTA ENTREGADA POLICIA NACION CIVIL"

2 0 ABR. 2008

POLICIA NACIONAL CIVIL
DIVISION POLICIA TECNICA Y CIENTIFICA

San Salvador, 25 de abril de 2008

Of. No. 0512DPTC/2008

Ing. Carlos Ernesto García García
Director de la Escuela de Ingeniería
de Sistemas Informáticos, Universidad
de El Salvador, Facultad de Ingeniería y Arquitectura
Presente

30 APR 2008

Estimada Ingeniero García:

Atentamente y con atención a su nota de fecha 06 de abril/2008, en donde solicita que 4 alumnos de la Facultad de Ingeniería y Arquitectura de esa Universidad puedan desarrollar un trabajo de graduación sobre ***"Estudio y Análisis sobre la Informática Forense en El Salvador"*** *en esta División, atentamente le informo, que por el momento no es factible autorizar a dichos alumnos, ya que la información que solicitan son demasiado sensibles y confidenciales, por tal motivo no podremos contribuir a lo peticionado.*

Sin otro particular, me suscribo,

Muy atentamente

POLICIA NACIONAL CIVIL DIVISION POLICIA TECNICA Y CIENTIFICA JEFATURA EL SALVADOR, C.A.

DIOS UNION LIBERTAD

Subcom. Julio César Santana Vela
Jefe División Policía Técnica y Científica, PNC

Avenida Las Buganvillas, No. 17-7, Colonia San Francisco, San Salvador, PBX: 2529-2400, Fax: 2298-9843
E-mail: dptc@pnc.gob.sv

ANEXO #8: "CARTA ENTREGADA POR LA DIC"

POLICIA NACIONAL CIVIL
SUBDIRECCION DE INVESTIGACIONES
DIVISION DE INVESTIGACION CRIMINAL

San Salvador 7 de julio de 2008

JEFATURA/DIC/08 OF. No. 322-09

Señor
Ing. Carlos Ernesto García García
Director de la Escuela de Ingeniería de
Sistemas Informáticos
Presente.

De la manera más atenta me permito saludarle, augurándole éxitos en su importante gestión, ocasión que aprovecho para referirme a su solicitud fecha 04 de los corrientes, al respecto hago de su conocimiento que las Divisiones de INTERPOL y Policía Técnica y Científica de esta corporación policial, son los que realizan informática forense. Por lo que recomiendo sea a esas Divisiones a quienes les haga llegar lo requerido.

Dios Unión Libertad

POLICIA NACIONAL CIVIL DIVISION DE INVESTIGACION CRIMINAL JEFATURA EL SALVADOR

Subcmdo. Luis Gerard Dennery Martínez
Jefe División de Investigación Criminal

*FGDM*Lorena*

ANEXO #9: "DELITOS INFORMÁTICOS PROPORCIONADOS POR LA DIVISIÓN DE INTERPOL Y NOTICIAS PUBLICA EN EL PERIÓDICO EL DIARIO DE HOY"

Delitos informáticos

No.	DELITO	FECHA
1	distribución de pornografía infantil	15/06/2005
2	distribución de pornografía infantil	07/03/2006
3	distribución de pornografía infantil	20/03/2006
4	distribución de pornografía infantil	31/03/2006
5	amenazas	06/06/2006
6	distribución de pornografía infantil	17/07/2006
7	hacking	01/08/2006
8	distribución de pornografía infantil	12/09/2006
9	extorsión	10/10/2006
10	distribución de pornografía infantil	13/10/2006
11	distribución de pornografía infantil	19/10/2006
12	distribución de pornografía infantil	21/10/2006
13	amenazas	25/10/2006
14	amenazas	07/11/2006
15	distribución de pornografía infantil	13/11/2006
16	amenazas	20/11/2006
17	amenazas	18/12/2006
18	amenazas	18/12/2006
19	estafa electrónica	20/12/2006
20	estafa electrónica	04/01/2007
21	amenazas	11/01/2007
22	amenazas	26/03/2007
23	amenazas	13/04/2007
24	amenazas	26/04/2007
25	amenazas	09/05/2007
26	distribución de pornografía infantil	03/07/2007

No.	DELITO	FECHA
27	distribución de pornografía infantil	23/08/2007
28	amenazas	28/08/2007
29	amenazas	19/09/2007
30	amenazas	01/10/2007
31	difamación	03/11/2007
32	amenazas	14/11/2007
33	distribución de pornografía infantil	15/11/2007
34	distribución de pornografía infantil	05/12/2007

Delitos informáticos tratados en la División de INTERPOL, comprendidos en el periodo de Junio de 2005 a Diciembre de 2007.

Noticias de delitos informáticos publicadas en el periodo "El Diario de Hoy"

FECHA	ENLACE	DELITO
Domingo, 24 de Junio de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1483393	Fraude con tarjetas de crédito
Jueves, 26 de Julio de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1585626	Fraudes informáticos
Sábado, 18 de Agosto de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1640164	Fraude con tarjetas de crédito
Viernes, 31 de Agosto de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1670794	Falsificación de documentos personales
Martes, 23 de Octubre de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1784185	Fraude con tarjetas de crédito
Sábado, 17 de Noviembre de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1842735	Debilidad contra delitos. FGR
Martes, 11 de Diciembre de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1899872	piratería
Viernes, 14 de Diciembre de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1908259	Clonación de tarjetas
Viernes, 14 de Diciembre de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1908308	Delitos informáticos
Sábado, 15 de Diciembre de 2007	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6329&idArt=1908124	Clonación de tarjetas, robo, estafas
Lunes, 4 de Febrero de 2008	http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=6358&idArt=2044950	Clonación de tarjetas

ANEXO #10: MODELOS DE ENCUESTAS

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA DE SISTEMAS INFORMÁTICOS

Dirigida a: Fiscales

Objetivo: Conocer su opinión sobre la aplicación de la informática forense, el tratamiento de la evidencia digital y el esclarecimiento de delitos informáticos.

Aclaración: Toda la información proporcionada será de gran utilidad para nuestra investigación y se mantendrá en total confidencialidad, únicamente servirán para fines académicos.

Indicaciones:
A continuación se presentan algunas preguntas a las cuales le solicitamos marcar con una **X** la respuesta que usted considere conveniente.

1. ¿Conoce sobre informática forense?

   Si ☐ No ☐

   Si su respuesta es Si. Marque la casilla que mejor represente su conocimiento.

   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

2. ¿De qué manera obtuvo el conocimiento sobre informática forense?

   Libros ☐
   Internet ☐
   Capacitaciones ☐
   Revistas especializadas ☐
   Otros ☐
   _____

3. ¿Según su experiencia y conocimiento la Fiscalía considera la evidencia digital confiable para la resolución de casos de delitos informáticos?

   Si ☐ No ☐

   Si su respuesta es **Si**. Marque la casilla que mejor represente la confiabilidad de la evidencia.

   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

4. ¿Ha recibido capacitaciones relacionadas con el manejo de evidencia digital?

   Si ☐ No ☐

   Si su respuesta es SI, ¿Donde la recibió?

   _____
   _____

5. ¿Qué tipo de delitos informáticos son los que se tratan con mayor frecuencia en la Fiscalía General de la República?

   Pornografía infantil ☐
   Piratería ☐
   Fraude comercial ☐
   Clonación de tarjetas de crédito ☐
   Robo de información confidencial ☐
   Financiamiento del crimen ☐
   Otros ☐

   _____
   _____
   _____

6. ¿Qué factores pueden hacer que una evidencia sea inválida como prueba para la resolución de un caso?

   Romper la cadena de custodia ☐
   Poca validez en la recreación de escena ☐
   Otros ☐

   _____
   _____

7. ¿Considera Usted que existen vacíos en las leyes penales salvadoreñas que impiden el desarrollo y esclarecimiento de un caso de delito informático?

   Si □ No □
   ¿Por qué?
   _____
   _____
   Si su respuesta es NO, pase a la pregunta número nueve.

8. ¿Cree necesario realizar reformas al código penal en relación a los delitos informáticos?

   Si □ No □
   ¿Por qué?
   _____
   _____

9. ¿Considera importante que existan leyes que amparen la aplicación de la informática forense en el país?

   Si □ No □
   ¿Por qué?
   _____
   _____

   Observaciones

Gracias por su valiosa colaboración.

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA DE SISTEMAS INFORMÁTICOS

Dirigida a: Abogados.

Objetivo: Conocer su opinión sobre el tema y aplicación de la informática forense en nuestro país para el esclarecimiento de delitos informáticos. Con los resultados obtenidos se espera abonar a la investigación con el título: Estudio y análisis sobre la informática forense en El Salvador.

Aclaración: Toda la información proporcionada será de gran utilidad para nuestra investigación y se mantendrá en total confidencialidad, únicamente servirán para fines académicos.

Indicaciones: A continuación se presentan algunas preguntas a las cuales le solicitamos marcar con una **X** la respuesta que usted considere conveniente. Además al final se presenta un apartado para observaciones en el que puede plasmar sus opiniones o cometarios sobre tópicos no abordados en esta encuesta.

1. ¿Ha escuchado el término de informática forense[128]?
   Si ☐ No ☐

   Si su respuesta es **Si.** Marque la casilla que mejor represente su conocimiento y pase a la pregunta **N°2**, de lo contrario pase a la pregunta **N°3**.
   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

2. ¿Por qué medio ha escuchado de informática forense?
   Libros ☐
   Internet ☐
   Capacitaciones ☐
   Revistas especializadas ☐
   Policía ☐
   Casos judiciales ☐
   Otros ☐
   Especifique:
   _____
   _____
   _____
   _____

[128] **Definición de Informática forense**: Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional para esclarecer como se ha cometido un delito informático.

3. ¿Ha escuchado hablar sobre evidencia digital o prueba científica?

Si ☐ No ☐

Si su respuesta es **Si,** pase a la pregunta **N°4**, de lo contrario pase a la pregunta **N°5**.

4. Según su experiencia y conocimiento. ¿Considera a la evidencia digital o prueba científica confiable y válida para el esclarecimiento y resolución de casos por delitos informáticos?

   Si ☐ No ☐

   Si su respuesta es **Sí**. Marque la casilla que mejor represente su confiabilidad y validez en la evidencia digital.

   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

5. ¿Qué factores considera que hacen inválida la confiabilidad y la validez de la evidencia digital en un juicio?

   Romper la cadena de custodia ☐
   Contaminar la evidencia ☐
   Poca validez en la recreación de escena ☐
   Otros ☐
   Especifique:
   _____
   _____
   _____
   _____
   _____

6. Según su experiencia y conocimiento. ¿Qué tipo de delitos informáticos ocurren con mayor frecuencia en el país?

   Pornografía infantil ☐
   Piratería ☐
   Fraude comercial ☐
   Clonación de tarjetas de crédito ☐
   Usurpación de identidad ☐
   Robo de información confidencial ☐
   Financiamiento del crimen ☐
   Otros ☐
   Especifique:
   _____
   _____
   _____
   _____

7. ¿Considera que existen vacíos en las leyes salvadoreñas que impiden el esclarecimiento de un caso por delitos informáticos?
   Si ☐ No ☐
   ¿Por qué?
   _____
   _____

8. ¿Cree necesario realizar reformas al código penal para que contemple artículos relacionados con delitos informáticos?
   Si ☐ No ☐
   ¿Porque?
   _____
   _____
   _____

9. ¿Conoce si se están realizando reformas en el código para enfrentar casos por delitos informáticos?
   Si ☐ No ☐

OBSERVACIONES:

Gracias por su valiosa colaboración y el tiempo prestado.

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA DE SISTEMAS INFORMÁTICOS

Dirigida a: Jueces.

Objetivo: Conocer su opinión sobre el tema y aplicación de la informática forense en nuestro país para el esclarecimiento de delitos informáticos. Con los resultados obtenidos se espera abonar a la investigación con el título: Estudio y análisis sobre la informática forense en El Salvador.

Aclaración: Toda la información proporcionada será de gran utilidad para nuestra investigación y se

Indicaciones: A continuación se presentan algunas preguntas a las cuales le solicitamos marcar con una **X** la respuesta que usted considere conveniente. Además al final se presenta un apartado para observaciones en el que puede plasmar sus opiniones o cometarios sobre tópicos no abordados en esta encuesta.

1. ¿Ha escuchado el término de informática forense[129]?
   Si ☐ No ☐

   Si su respuesta es **Si.** Marque la casilla que mejor represente su conocimiento y pase a la pregunta **N°2**, de lo contrario pase a la pregunta **N°3**.
   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

2. ¿Por qué medio ha escuchado de informática forense?
   Libros ☐
   Internet ☐
   Capacitaciones ☐
   Revistas especializadas ☐
   Policía ☐
   Casos judiciales ☐
   Otros ☐
   Especifique:
   _____
   _____
   _____
   _____

[129] **Definición de Informática forense**: Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional para esclarecer como se ha cometido un delito informático.

3. ¿Ha escuchado hablar sobre evidencia digital o prueba científica?

Si ☐ No ☐

Si su respuesta es **Si,** pase a la pregunta **N°4**, de lo contrario pase a la pregunta **N°5**.

4. Según su experiencia y conocimiento. ¿Considera a la evidencia digital o prueba científica confiable y válida para el esclarecimiento y resolución de casos por delitos informáticos?

   Si ☐ No ☐

   Si su respuesta es **Sí**. Marque la casilla que mejor represente su confiabilidad y validez en la evidencia digital.

   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

5. ¿Qué factores considera que hacen inválida la confiabilidad y la validez de la evidencia digital en un juicio?

   Romper la cadena de custodia ☐
   Contaminar la evidencia ☐
   Poca validez en la recreación de escena ☐
   Otros ☐
   Especifique:
   _____
   ____
   _____
   _____
   _____

6. Según su experiencia y conocimiento. ¿Qué tipo de delitos informáticos ocurren con mayor frecuencia en el país?

   Pornografía infantil ☐
   Piratería ☐
   Fraude comercial ☐
   Clonación de tarjetas de crédito ☐
   Usurpación de identidad ☐
   Robo de información confidencial ☐
   Financiamiento del crimen ☐
   Otros ☐
   Especifique:
   _____
   _____
   _____
   _____

7. ¿Considera que existen vacíos en las leyes salvadoreñas que impiden el esclarecimiento de un caso por delitos informáticos?

   Si ☐ No ☐

   ¿Porque?

   _____
   _____

8. ¿Cree necesario realizar reformas al código penal para que contemple artículos relacionados con delitos informáticos?
   Si ☐ No ☐

¿Por qué?

_____
_____
_____

9. ¿Conoce si se están realizando reformas en el código para enfrentar casos por delitos informáticos?
   Si ☐ No ☐

OBSERVACIONES:

Gracias por su valiosa colaboración y el tiempo prestado.

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA DE SISTEMAS INFORMÁTICOS

Dirigida a: Peritos informáticos internacionales.

Objetivo: Conocer su opinión sobre la informática forense, con los resultados obtenidos se espera abonar al trabajo de graduación con el título: Estudio y análisis sobre la informática forense en El Salvador.
Aclaración: Toda la información proporcionada será de gran utilidad para nuestra investigación y se mantendrá en total confidencialidad, únicamente servirán para fines académicos.

Indicaciones:
A continuación se presentan preguntas a las cuales le solicitamos marcar con una **X** la respuesta que usted considere conveniente y de su respuesta en aquellas en las cuales se le pide su opinión. Además al final se presenta un apartado para observaciones para que pueda plasmar sus opiniones o comentarios sobre tópicos no abordados en esta encuesta.

1. ¿Ha escuchado el término de informática forense[130]?
   Si ☐ No ☐

   Si su respuesta es **Si.** Marque la casilla que mejor represente su conocimiento y pase a la pregunta **N°2**, de lo contrario pase a la pregunta **N°3**.
   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

2. ¿Dónde obtuvo sus conocimientos sobre Informática forense? En esta pregunta puede elegir más de una opción si así lo amerita su experiencia.
   - Dentro de su país ☐
     Especifique el nombre de su país:

   - Fuera de su país ☐
     Lugar donde se capacito:

   - De forma Autodidacta ☐
   - Otros ☐

   Especifique:

[130] **Definición de Informática forense**: Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional para esclarecer como se ha cometido un delito informático.

3. Según su experiencia y conocimiento, ¿Que campos son necesarios que un perito informático conozca?

Base de datos ☐
Redes ☐
Software ☐
Hardware ☐
Leyes ☐
Recuperación de archivos ☐
Criptografía ☐
Otros ☐
Especifique:

4. ¿Mencione cuales herramientas informáticas ha utilizado con mayor frecuencia en la aplicación de la informática forense?

5. ¿Conoce si existen estándares para la recolección y tratamiento de la evidencia digital?

Si ☐ No ☐

Mencione algunos:

6. ¿Conoce si existen estándares para la aplicación de la informática forense?
   Si ☐ No ☐
   Mencione algunos:

7. ¿Conoce instituciones certificadoras en informática forense a nivel nacional o internacional?
   Si ☐ No ☐
   Si su respuesta es Si.
   ¿Cuáles son?

8. De los temas expuestos en las capacitaciones recibidas. ¿Cuál o cuáles temas considera los más interesantes?

9. ¿Ha enfrentado algún caso que no se pudo resolver?
   Si ☐ No ☐
   Si su respuesta es **Si**, ¿cuáles de los siguientes factores considera que impidieron su resolución?
   Tecnología ☐
   Metodología ☐
   Conocimientos ☐
   Otros ☐
   Especifique:

10. Por su experiencia y conocimiento. ¿Qué equipo informático y software tendría que tener un laboratorio especializado en informática forense si se deseara crear dentro de las universidades como recurso practico en apoyo a una cátedra sobre este tema?

OBSERVACIONES

Gracias por su valiosa colaboración y el tiempo prestado.

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA DE SISTEMAS INFORMÁTICOS

Dirigida a: Peritos informáticos nacionales.

Objetivo: Conocer su opinión sobre la aplicación de la informática forense en nuestro país y el esclarecimiento de delitos informáticos, con los resultados obtenidos se espera abonar a la investigación con el título: Estudio y análisis sobre la informática forense en El Salvador.

Aclaración: Toda la información proporcionada será de gran utilidad para nuestra investigación y se mantendrá en total confidencialidad, únicamente servirán para fines académicos.

Indicaciones:
A continuación se presentan preguntas a las cuales le solicitamos marcar con una **X** la respuesta que usted considere conveniente y contestes aquellas en las cuales se le pide su opinión. –Además al final se presenta un apartado para observaciones para que pueda plasmar sus opiniones o comentarios sobre tópicos no abordados en esta encuesta.

1. ¿Ha escuchado el término de informática forense[131]?
   Si ☐ No ☐

Si su respuesta es **Si.** Marque la casilla que mejor represente su conocimiento y pase a la pregunta **N°2**, de lo contrario pase a la pregunta **N°3**.
0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

2. ¿Dónde obtuvo sus conocimientos sobre Informática forense? En esta pregunta puede elegir más de una opción si así lo amerita su experiencia.
   - Dentro del país ☐
     Lugar donde se capacito:
     _____
   - Fuera del país ☐
     Lugar donde se capacito:
     _____
   - De forma Autodidacta ☐
   - Otros ☐
     Especifique:
     _____
     _____
     _____

[131] **Definición de Informática forense**: Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional para esclarecer como se ha cometido un delito informático.

3. ¿Cómo cree que esta la informática forense en El Salvador con respecto a su aplicación? Marque la casilla que mejor represente su opinión.
   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

4. ¿Cómo cree que esta la informática forense en El Salvador con respecto a su aceptación por parte del órgano judicial? Marque la casilla que mejor represente su opinión.
   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

5. ¿Cómo cree que esta la informática forense en El Salvador con respecto a su aceptación por parte de la Fiscalía General de la República? Marque la casilla que mejor represente su opinión.
   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐

6. Según su experiencia y conocimiento, ¿Que campos son necesarios que un perito informático conozca para la aplicación de la informática forense?
   Base de datos ☐
   Redes ☐
   Software ☐
   Hardware ☐
   Leyes ☐
   Recuperación de archivos ☐
   Criptografía ☐
   Otros ☐
   Especifique:
   _____
   _____
   _____

7. ¿Qué elementos considera que serian necesarios reforzar para que exista un mayor crecimiento la informática forense en El Salvador?
   Judicial ☐
   Legislativo ☐
   Educación superior ☐
   Otros ☐
   Especifique:
   _____
   _____
   _____

8. En base a su experiencia y conocimiento ¿En qué casos de delitos informáticos a participado con mayor frecuencia?
   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 ☐
   Especifique:
   _____
   _____
   _____

9. ¿Mencione cuales herramientas informáticas que ha utilizado con mayor frecuencia en la aplicación de la informática forense?
   _____
   _____
   _____
   _____
   ____

10. ¿Conoce si existen estándares para la recolección y tratamiento de la evidencia digital?
Si ☐ No ☐
Mencione algunos:
_____
_____
_____ _____
_____

11. ¿Conoce si existen estándares para la aplicación de la informática forense?
    Si ☐ No ☐
    Mencione algunos:

    _____
    _____
    _____
    _____

12. ¿Conoce si existen instituciones certificadoras de informática forense en El Salvador?
    Si ☐ No ☐
    Si su respuesta es Si.
¿Cuáles son?
_____
_____
_____

13. En promedio, ¿Cada cuanto tiempo recibe capacitaciones sobre informática forense?
    Menos de 6 meses ☐ 6 meses ☐ 1 año ☐ 2 años ☐ Más de 2 años ☐

14. De los temas expuestos en las capacitaciones recibidas. ¿Cuál o cuáles temas considera los más importantes?

    _____
    _____
    _____
    _____

15. ¿Dónde recibió la/las capacitaciones?
    Dentro del país ☐
    Especifique el lugar:

    _____
    _____
    _____

    Fuera del país ☐
    Especifique el lugar:

    _____
    _____
    _____

16. ¿Ha enfrentado algún caso que no se pudo resolver?
    Si ☐ No ☐
    Si su respuesta es **Si**, ¿cuáles de los siguientes factores considera que impidieron su resolución?
    Tecnología ☐
    Metodología ☐
    Conocimientos ☐
    Otros ☐

    _____
    _____
    _____

17. Por su experiencia y conocimiento. ¿Qué equipo informático y software tendría que tener un laboratorio especializado en informática forense si se deseara crear dentro de las universidades como recurso practico en apoyo a una cátedra sobre este tema?

    _____
    _____
    _____

OBSERVACIONES

Gracias por su valiosa colaboración y el tiempo prestado.

UNIVERSIDAD DE EL SALVADOR
FACULTAD DE INGENIERIA Y ARQUITECTURA
ESCUELA DE INGENIERIA DE SISTEMAS INFORMÁTICOS

Dirigida a: Catedráticos que imparten la carrera de Informática

Objetivo: Conocer su opinión sobre la aplicación de la informática forense en nuestro país, con los resultados obtenidos se espera abonar a la investigación con el titulo: Estudio y análisis sobre la informática forense[132] en El Salvador.

Aclaración: Toda la información proporcionada será de gran utilidad para nuestra investigación y se mantendrá en total confidencialidad, únicamente servirán para fines académicos.

Indicaciones: A continuación se presentan algunas preguntas a las cuales le solicitamos marcar con una **X** la respuesta que usted considere conveniente. Además al final se presenta un apartado para observaciones para que pueda plasmar sus opiniones o cometarios sobre tópicos no abordados en esta encuesta.

1. ¿Conoce sobre informática forense?
   Si ☐ No ☐
   Si su respuesta es Si. Marque la casilla que mejor represente su conocimiento.
   0-25% ☐ 26%-50% ☐ 51%-75% ☐ 76%-100% ☐
   Si su respuesta es **Si** continúe al numeral 2, Si su respuesta es **No** diríjase al numeral 3.

2. ¿De que manera obtuvo el conocimiento sobre informática forense?
   Libros ☐
   Internet ☐
   Capacitaciones ☐
   Revistas especializadas ☐
   Otros ☐
   _____

3. ¿En la facultad donde es impartida la carrera de ingeniería de sistemas o licenciatura en sistemas, tiene alguna asignatura que brinde conocimientos sobre informática forense?
   Si ☐ No ☐

[132] **Definición de Informática Forense:** Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional para esclarecer como se ha cometido un delito informático.

4. ¿Considera necesario la creación de una asignatura especializada sobre informática forense?
   Si □ No □
   ¿Porqué?_____
   _____
   _____

OBSERVACIONES:

Gracias por su valiosa colaboración y el tiempo prestado.

ANEXO #11: ORÍGENES DE DATOS OBTENIDOS, PARA LA COMPROBACIÓN DE HIPÓTESIS

Variable independiente "Aplicación de la informática forense"

Pregunta: 1- ¿Ha escuchado el término de informática forense?

Jueces		Abogados		Fiscalía		Peritos		Total	
Si	10	Si	58	Si	1	Si	3	Si	72
No	0	No	38	No	0	No	0	No	38
								Total	110

Variable dependiente "Esclarecimiento de delitos informáticos"

Pregunta: 4- Según su experiencia y conocimiento. ¿Considera la evidencia digital o prueba científica confiable y válida para el esclarecimiento y resolución de casos por delitos informáticos?

Jueces		Abogados		Fiscalía		Total	
Si	10	Si	67	Si	1	Si	78
No	0	No	9	No	0	No	9
		Total	76			Total	87

Aclaración:

En la muestra de abogados se ha tomado en cuenta a 76, siendo estos los que conocen sobre evidencia digital, dato que puede verse en la pregunta 3 de la encuesta dirigida a abogados.

ANEXO #12: TABLA DE DISTRIBUCIÓN DE 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