UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMATICA

TESIS DE GRADO

SISTEMA EXPERTO PARA EL ANALISIS FORENSE EN DELITOS INFORMATICOS

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMATICA

MENSION: INGENIERIA DE SISTEMAS INFORMÁTICOS

POSTULANTE: FABIOLA CECILIA IBAÑEZ YANA

TUTOR: Lic. EFRAIN SILVA SANCHEZ

REVISOR: MSc. Lic. LUISA VELASQUEZ LOPEZ

La Paz - Bolivia

AGRADECIMIENTOS

A mi DIOS, por haberme dado la gran dicha de disfrutar de esta vida llena de sorpresas, y por haberme brindado la sabiduría necesaria para poder estar donde estoy.

A mi querida mamá, sobre todo por todo su apoyo incondicional desde mis primeros años hasta ahora, sin ella no hubiera podido lograr mis objetivos.

A mi adorada hermana, por el apoyo incondicional que me brinda día a día.

A mi amado esposo, por el apoyo que me brindo desde que nos conocimos hasta ahora.

Quiero darle un agradecimiento muy especial a mi revisora la Msc. Lic. Luisa Velásquez Lopez, por sabios consejos y acertadas observaciones.

Agradecer a mi Tutor el Lic. Efrain Silva Sanchez por su tiempo y dedicación en el seguimiento de mi trabajo.

A todos los que fueron mis docentes, puesto que gracias a sus enseñanzas pude culminar mis estudios.

A todas la parte administrativa de nuestra querida carrera que me colaboraron a lo largo de mis estudios.

También de manera muy especial dar gracias a mis amigas y amigos que conocí en el transcurso de la carrera.

Y por ultimo dar gracias a la Universidad y particularmente a la carrera de Informática por cobijarme en sus aulas por todos estos años.

Dedicatoria:

A mí querida mamá Alcira Yana por su gran ejemplo de superación. Es atí a quien debo toda la persona que soy. Gracias por tu guía y ejemplo durante todos loa años de mi vida. Te quiero.

A mi amado esposo Rainer Gutierrez por ese optimismo que siempre me impulso a seguir adelante, quien con su amor y su ternura me apoyo en todo momento.

A mis queridos hijitos Kevin y Calvin por todas las veces que no pudieron tener a una mamá de tiempo completo, ellos son la luz de mi vida, la fuerza que me impulsa todos los días, este trabajo es de ustedes hijos míos.

RESUMEN

En las últimas décadas el desarrollo tecnológico fue desarrollándose de manera exponencial, del mismo modo existen personas con malas intenciones, las cuales se dedican a manipular los componentes de la computadora, llegando a ser especialistas en cometer delitos informáticos, ya que los mecanismos de control en cuanto a la producción, difusión y acceso a este tipo de material, parecen estar ausentes o al menos, no demuestran la eficiencia y eficacia adecuada, en nuestro medio. Por ello se hizo necesaria la creación de una nueva Ciencia, La Informática Forense. Esta permite a especialistas poder detectar los tipos de delitos cometidos utilizando medios informáticos. Para lograr esto se debe hacer un análisis pericial, el cual debe seguir ciertos pasos para poder obtener los resultados que se esperan. Esta serie de pasos es planteada en un método de análisis forense denominado las 6 R's, que propone la realización de 6 pasos, Reconocimiento, Requisitos, Recolección, Recuperación, Reconstrucción y Resultados.

A partir de esta situación, y haber evidenciado que en nuestro medio, existe escasez de especialistas forenses, el presente trabajo propone desarrollar un Sistema Experto para el Análisis Forense en delitos Informáticos, que coadyuve al perito informático y al estamento policial en la correcta realización del análisis forense en delitos informáticos y así proteger las evidencias del hecho, mediante el uso de silogismos jurídicos, como modelo en la aplicación de la metodología ya mencionada. Se parte de proposiciones como forma de representar la información y lógica de predicados de primer orden para formalizar dicha información sobre un dominio de trabajo y definir reglas que es la forma de almacenar a la base de conocimientos del sistema experto, además de apoyarse en un especialista humano.

Se da a conocer un caso particular de la comisión de un delito catalogado como delito informático, y mediante el prototipo del Sistema Experto, se realizan ciertas preguntas, simulando el conocimiento humano, las cuales permiten coadyuvar al perito informático y al estamento policial en la correcta realización del análisis forense

ÍNDICE

ÍNDICE DE TABLA Y FIGURAS

1 PRESENTACION

1.1 INTRODUCCIÓN

A medida que crece y se diversifica el uso de Infraestructuras Tecnológicas, se incrementan también los riesgos de los equipos de cómputo, dispositivos electrónicos y sistemas informáticos, conectados o no a Internet, esto implica que son vulnerables a ataques o incidentes que ponen en peligro la integridad, disponibilidad, autenticidad de los datos que en ellos se procesa, almacena o transfiere; como también el daño a terceras personas y a dichas infraestructuras es latente.

El desarrollo de las tecnologías de la información y comunicación fue creciendo exponencialmente estos últimos años. Existen personas con malas intenciones, las cuales se dedican a manipular los componentes de la computadora, llegando a ser especialistas en cometer delitos informáticos, ya que los mecanismos de control en cuanto a la producción, difusión y acceso a este tipo de material, parecen estar ausentes o al menos, no demuestran la eficiencia y eficacia adecuada.

Cuando se verifica un delito informático, las personas que trabajan como investigadores, tienen un conocimiento limitado de cómo realizar un análisis informático forense. El tener que analizar las acciones realizadas por los atacantes en los equipos, para conocer y aprender el modo en que estos operan, averiguar el alcance del mismo, y llegado el momento, poder tomar las medidas oportunas para denunciar el ataque a las autoridades competentes, nos conlleva a enfrentarnos a una serie de actividades relacionadas con los hechos criminales.

Es por ello, cuando una persona se enfrenta a estos hechos criminales, se enfrenta en primer lugar, con el sitio donde se realizo el hecho criminal, después con una serie de métodos de análisis pericial para poder determinar el delito y el grado de perjuicio que este conlleva para terceras personas o instituciones.

Esta investigación pretende desarrollar un sistema experto el cual guíe al perito informático, al estamento policial, en la aplicación del método del análisis pericial denominado las 6 R's, para delitos informáticos, que cubra los pasos necesarios desde el aseguramiento de la escena del hecho hasta la presentación de evidencias ante un Tribunal de Justicia, si fuese el caso, o simplemente aprender del incidente.

La policía Boliviana no tiene mucho conocimiento sobre los delitos informáticos, y no saben como actuar frente a estos hechos, de igual manera las personas especializadas en investigar estos delitos, son escasas en nuestro medio.

Los abogados, jueces tienen un conocimiento escaso de lo que es información automatizada, por ende no saben como analizar las evidencias recabadas, por que no cuentan con métodos formales para el proceso de análisis pericial.

Podemos definir la *informática forense* como "*la ciencia de identificar, preservar, analizar y presentar datos almacenados electrónicamente en un medio computacional, datos que son evidencias de un delito informático.*" [Rosales, G, Manual Inf. Forense 2008].

El perito informático, debe ajustarse a ciertas metodologías, frecuentemente apoyadas mediante actas notariales, para que las evidencias electrónicas sirvan como pruebas fehacientes de un posible delito ante eventuales procesos judiciales. Uno de los elementos esenciales, es la correcta incautación de la prueba, que respete los derechos de las partes y no de pie a que se descarte en un tribunal.

1.2 ANTECEDENTES

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, «delitos informáticos», en una encuesta realizada por estudiantes de la Carrera de informática se obtuvo los siguientes resultados: el 86,7% tiene conocimiento de que es un delito informático.

De acuerdo al Código Penal vigente pueden ser victimas de delitos informáticos las personas particulares o personas naturales y personas colectivas o jurídicas tales como empresas, instituciones, municipios, prefecturas, el propio gobierno. http://mar-23.blogspot.com/#uno

Entre 2003 y 2007, la fuerza anticrimen recibió 185 denuncias de manipulación informática y de alteración, acceso y uso indebido de datos en toda Bolivia, pero se desconoce si alguna de ellas fue resuelta. Los datos de la Fuerza Especial de Lucha Contra el Crimen (FELCC) revelan que 177 corresponden a manipulación informática y ocho a alteración, acceso y uso indebido de información. De la primera figura legal, 91 casos hubo en Santa Cruz, 46 en Cochabamba, 30 en La Paz, cuatro en Potosí, tres en

Oruro, dos en Beni y uno en Tarija. Sobre alteración informática, 3 ocurrieron en La Paz, 2 en Cochabamba, 2 en Beni y 1 en Santa Cruz. Entre enero y septiembre de este año hubo 50 denuncias de manipulación electrónica (27 en Santa Cruz, 12 en La Paz, 9 en Cochabamba y 2 en Chuquisaca) y ninguna acerca de alteración.

El 2008, la Fuerza Especial de Lucha Contra el Crimen (FELCC) recibió al menos 50 denuncias de delitos informáticos en el país, de las que sólo 36 fueron investigadas, pero ninguna fue resuelta, por su complejidad y porque sólo hay 2 peritos para atender ese tipo de casos. A ello se suma la falta de fiscales especializados en esa materia para conducir las indagaciones.

Según información disponible, la pornografía infantil alcanzó niveles alarmantes. Uno de los campos es la Internet, donde existen "4.2 millones de sitios que equivale a 12% del total de sitios en la Web, existen 372 millones de páginas dedicadas a este tipo de pornografía, las búsquedas diarias llegan al 25% del total de peticiones en motores de búsqueda, los e-mail pornográficos al día llegan el 8% de su total, el promedio diario de e mail pornográficos / usuario es de 4.5 por usuario de Internet, las descargas mensuales de pornografía en sistemas p2p llega al 35% del total de descargas, el número de sitios Web que ofrecen pornografía ilegal es de 1.000 y los visitantes de sitios Web Pornográficos a nivel mundial llegan a 72 millones al año.

http://www.laprensa.com.bo

El capítulo 11 del Código Penal boliviano, en su artículo 363, tipifica dos tipos de delitos informáticos: uno sobre manipulación informática cuyo fin es obtener un beneficio económico, sancionado con reclusión de uno a cinco años y con multa de 60 a 200 días, y un delito de alteración y uso indebido de datos informáticos cuyo propósito es el apoderamiento o modificación de una base de datos en una computadora o un dispositivo informático (CD-ROM, USB, disquete y otros), que será sancionado con prestación de trabajo hasta un año o multa de hasta 200 días.

http://www.oas.org/juridico/spanish/gapeca_sp_docs_bol1.pdf

Adicionalmente, como parte del estudio realizado por Estudiantes de la carrera de Informática, existen datos del porcentaje de estudiantes que tienen conocimiento de los artículos que regulan los delitos informáticos, y el resultado es que un 33,6% tiene conocimiento de estos artículos que regulan estos tipos de delitos y el 66,7% no conoce.

http://mar-23.blogspot.com/#uno

El Código Penal incorporó estas dos figuras hace diez años, pero entonces el desarrollo de la tecnología de la información no estaba en el nivel actual. En consecuencia los delitos quedaron obsoletos en relación con la evolución agigantada de la informática y la tecnología.

El ex jefe de la División de Delitos Económicos Financieros de la fuerza anticrimen del departamento de La Paz coronel Luís Fernando Remontt tampoco conoció de investigaciones concluidas, pero indicó que en su gestión, entre 2007 y parte de 2008, al menos tres hombres fueron enviados a la cárcel por retener tarjetas de crédito ajenas en cajeros automáticos. El director nacional de la FELCC, coronel Fernando Figueredo, explicó que en 2009 se incrementará el número de investigadores en las divisiones de Delitos Informáticos del país, puesto que cada año sube el índice de este tipo de hechos. Para ello, con la ayuda de la GTZ (Cooperación Técnica Alemana) se capacitará a policías para que resuelvan estas denuncias en las oficinas de la fuerza anticrimen. El Instituto de Investigaciones Forenses (IDIF) organismo dependiente de la fiscalía General de la República, trabaja de la mano con la FELCC en el análisis de pruebas de distintos delitos comunes, a la fecha no tiene expertos para la examinación de delitos informáticos. http://www.ciberjure.com.pe

Existen una variedad de metodologías para el aseguramiento de las pruebas en los delitos informáticos, las cuales en su mayoría fueron puestas en práctica por el FBI. En nuestro medio se carece de metodologías formales para precautelar las pruebas recabadas, además de carecer de personal que pueda poner en práctica cualquier metodología para estas tareas.

1.3 SITUACIÓN PROBLEMÁTICA

Luego de un análisis detallado de cómo las personas que se dedican a realizar investigaciones de hechos criminales, en el momento de hacer la investigación de algún delito informático, además tomando en cuenta todos los aspectos, las causas que lo generan, efectos y soluciones que se plantean para resolver las mismas, las hemos estructurado en la tabla 1.1

Tabla 1.1 Causa - Efecto

	Problema	Causa	Efecto	Solución
1	Cuando se detecta un hecho criminal, la policía, no sabe como actuar en el momento preciso para que las evidencias informáticas del caso no se pierdan por malas o nulas prácticas de levantamiento de evidencias por parte de los peritos informáticos.	Los peritos informáticos no saben como proteger las evidencias, informáticas que existen en el lugar del hecho.	Contaminación de la evidencia de tipo informático, en el lugar del hecho.	Proveer y dar a conocer las prácticas para el levantamiento de pruebas en escenas de crímenes informáticos.
2	Los investigadores no saben que materiales deben utilizar para realizar una adecuada investigación informático-forense.	No conocer una guía metodológica que les indique como y que utilizar para no contaminar las evidencias de tipo informático	Los investigadores pierden tiempo en realizar la investigación de manera informal y sin una guía normalizada para estos procedimientos.	Dar a conocer los estándares internacionales para el manejo y manipuleo de pruebas de tipo informático en el lugar del hecho.

3	Cuando la evidencia es recabada y llevada a las autoridades correspondientes, estas no tienen conocimiento de cómo evitar contaminar la evidencia de tipo informático.	Las autoridades correspondientes no saben como manipular las evidencias recabadas y ver en que magnitud de gravedad pueden afectar a los involucrados.	Contaminación de la evidencia de tipo informático, por malas prácticas manipuleo de evidencia de tipo informático	Implementar los estándares internacionales para el manejo y manipuleo de pruebas de tipo informático por parte de las autoridades correspondientes
4	Las instituciones y personas que son victimas de distintos delitos en el campo informático, no respaldan su información.	Personas e instituciones no tienen la costumbre de respaldar la información	Perdida total o parcial de datos que en determinado momento se pueden considerar como pruebas para aclarar los delitos.	Dar a conocer a las instituciones y personas las buenas prácticas de respaldo de los datos.

Fuente:[Velásquez L, Datos Propios]

1.4 PLANTEAMIENTO DEL PROBLEMA

En consecuencia el problema de investigación es:

¿El sistema experto coadyuvará al perito informático y al estamento policial en el manejo adecuado de las evidencias recolectadas en la escena del hecho?

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

Diseñar un sistema experto que coadyuve al perito informático y al estamento policial en la correcta realización del análisis forense en delitos informáticos y así proteger las evidencias de la escena del hecho.

1.5.2 OBJETIVOS ESPECIFICOS

Para la consecución del objetivo general, los objetivos específicos, que se proponen son:

1. Desarrollar una base de conocimientos utilizando silogismos.
2. Estructurar la base de hechos y la base de reglas, en base a los conocimientos de experiencias recabadas mediante la lógica de proposiciones.
3. Obtener el conocimiento del experto en el ámbito legal y formalizar mediante la lógica de predicados
4. Desarrollar un prototipo utilizando el lenguaje Visual Basic para la interfaz de usuario y el lenguaje prolog para el motor de inferencia.

1.6 HIPOTESIS

HI: El sistema experto provee y da a conocer los pasos que indiquen la correcta utilización del análisis forense en delitos informáticos y así proteger las evidencias de la escena del hecho.

1.7 OBJETO DE ESTUDIO

Este trabajo pretende analizar el método de análisis pericial en delitos informáticos aplicando el método denominado 6R´s.

1.8 JUSTIFICACION

1.8.1 TECNICA

La utilización de sistemas Expertos para la solución de problemas, que comúnmente serian de competencia para persona humanas con un alto grado de experiencia y especialidad en áreas especificas, ayuda, encontrando soluciones próximas a las de los expertos humanos, usando para esto ciertas técnicas de que permiten emular el razonamiento humado. Estas herramienta en particular se pueden dividir en dos: La base de conocimientos que proporciona hechos objetivos y reglas sobre el problema de investigación y una máquina de deducción que proporciona la capacidad de razonamiento que permite al Sistema Experto, extraer conclusiones. El Sistema experto que diseñaremos, colaborará en precautelar la integridad física de la CPU en delitos informáticos, particularmente en Pornografía Infantil, utilizando para esto bases de hechos y bases de conocimientos, apoyándose para las conclusiones en las leyes vigentes dentro nuestro país, relativas a este tema.

1.8.2 CIENTIFICA

Mediante la Lógica de Proposiciones y la Lógica de Predicados, llegaremos a tener un Árbol de de decisiones. Este Árbol de decisiones nos ayudara a obtener una conclusión, utilizando para esto, Algoritmos de estrategia para encontrar soluciones a problemas que satisfacen restricciones, en nuestro caso el éxito o fallo de nuestro árbol.

1.8.3 SOCIAL

La presente investigación ayuda a proteger a las personas que son o fueron victimas de los delitos informáticos, desde el momento en que se realiza la investigación del hecho hasta llegar a una conclusión favorable, ante las autoridades judiciales competentes y evitar perdidas económicas a las instituciones o a terceras personas victimas del delito informático, mediante la prevención de riesgos al precautelar las evidencias, de los componentes informáticos que existen en el lugar del hecho.

1.9 VIABILIDAD

Los delitos informáticos, no están tipificados en toda su magnitud, ya que las leyes contemplan directrices mínimas para los procedimientos y sanciones relacionadas con estos delitos. Es por eso que nuestro sistema experto, se hace viable ante la necesidad

de encontrar herramientas y directrices para llevar adelante casos relacionados en delitos informáticos.

1.10 MÉTODOS Y MEDIOS DE INVESTIGACIÓN CIENTIFICA

En el presente trabajos se utilizan métodos y medios de investigación científica.

Los métodos de investigación son: Observación, Análisis y Síntesis, Inducción, deducción, Abstracción y concreción.

- **Observación:** La observación forma parte del método científico ya que, junto a la experimentación, permite realizar la verificación empírica de los fenómenos. La mayoría de las ciencias utilizan la observación y la experimentación de manera complementaria.
  [http://definicion.de/observacion/-2008]
- **Análisis y Síntesis:** El vocablo análisis puede poseer distintos significados dependiendo de la disciplina en que se aborde, por ejemplo en término de informática e ingeniería se tiene análisis estructural, análisis de sistemas, análisis de conjunto, análisis fundamental, análisis FODA, análisis de entorno y otras. El análisis en términos generales se refiere a la descomposición de un todo en sus distintos elementos, con el fin de estudiar estos de manera separada luego un proceso de síntesis se debe integrar todos estos elementos [Gutiérrez, 2008].

  En esta tesis de grado se pretende observar, describir, examinar y desarrollar un sistema experto el cual ayude al investigador de un delito informático a tener un mejor análisis forense que cubra los pasos necesarios desde el aseguramiento de la escena del delito hasta la presentación de evidencias ante un Tribunal de Justicia, si fuese el caso, o simplemente aprender del incidente. Este sistema experto pretende ser una guía para aquellas personas que se involucran en la investigación de delitos relacionados con la informática, dando a conocer, como colectar y analizar la evidencia digital, que pueda llevar a la correcta investigación del hecho cometido, para que en lo posterior, se pueda prevenir estos delitos y castigar a estas personas que se dedican a realizar estos delitos informáticos.
- **Inductivo y Deductivo:** La inducción se refiere a la generalización de una observación, razonamiento o conocimiento establecido a partir de casos particulares [Genevieve G; 2003]. La deducción es la aplicación de teorías genéricas a situaciones [Carballoso; 2005]. El propósito en este tema es el no perder el conocimiento de experiencia de los humanos, mas al contrario

compilarlos, mejorarlos y ayudarlos para el conocimiento de futuras personas que lo van ha necesitar.

- **Abstracción y Concreción:** La abstracción es un proceso de suma importancia para la comprensión del objeto, mediante ella se detecta la propiedad o relación de las cosas y fenómenos. No se limita a destacar y aislar una propiedad y relación del objeto asequible a los sentidos, si no que se trata de descubrir el nexo esencial oculto e inasequible al conocimiento empírico. Lo concreto es la síntesis de muchos conceptos y por consiguientes de las partes. Las definiciones abstractas conducen a la reproducción de lo concreto por medio del pensamiento. Lo concreto en el pensamiento es el conocimiento más profundo y de mayor contenido esencial. [Gutiérrez, 2008]. Mediante la abstracción podremos comprender la gravedad del delito que se cometió, y mediante la concreción poder determinar que tipo de delito es.

1.11 ALCANCES Y LIMITES

La presente investigación tomara en cuenta los delitos informáticos, en los cuales se debe preservar la seguridad del ordenador, desde el momento en que se realiza la investigación del hecho hasta llegar a una conclusión, ante las autoridades judiciales competentes.

1.12 APORTES

1.12.1 APORTE TEÓRICO

La Lógica de Proposiciones y la Lógica de Predicados, permitirán la obtención de un árbol de de decisiones, el cual nos ayudará a obtener una conclusión, utilizando para esto, Algoritmos de Búsqueda, para encontrar, en nuestro caso el éxito o fallo de las conclusiones de nuestro árbol.

1.12.2 APORTE PRÁCTICO

El aporte práctico está relacionado con el desarrollo del prototipo del sistema experto, que realiza la tarea de un experto colaborando al perito informático y al estamento policial, indicando la correcta realización del análisis forense en delitos informáticos y así proteger las evidencias del hecho.

La implementación del prototipo del sistema experto se realizará utilizando el lenguaje de programación visual Basic con el motor de inferencia prolog.

2 MARCO DE REFERENCIA

El avance de la informática es imparable y debe ser positivo en términos generales, la proliferación de nuevos delitos informáticos, hacen que los delincuentes se aprovechen de éstos recursos; es por eso que la policía, abogados, jueces y todas las personas involucradas en investigaciones de delitos informáticos, se ven en la necesidad de informarse y aprender mas para estar constantemente al día y ser efectivos en la lucha contra el crimen informático. Dentro de toda esta evolución que está dando buenos resultados por la posibilidad de introducir innumerables datos y correlacionarlos, al tiempo que transmitirlos con celeridad, cabe destacar la aplicación, implantación y desarrollo de un sistema experto para poder ayudar a los peritos que trabajan en esta área.

2.1 AMBITO LEGAL

2.1.1 DELITOS INFORMÁTICOS CONOCIDOS POR NACIONES UNIDAS

Los Delitos Informáticos conocidos por Naciones Unidas Son:

Manipulación de computadoras

- Datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos es el más común ya que es fácil de cometer y difícil de descubrir. No es necesario que el infractor sea especialista en informática.
- Programas. El delincuente debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.

- Datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude en los cajeros automáticos.
- Fraude efectuado por manipulación informática. Transacciones financieras repetidas que transfieren montos de una cuenta a otra.

Falsificaciones Informáticas

- Como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.
- Como instrumentos. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

Daños o modificaciones de programas o datos computarizados.

- Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Para ello se utilizan los virus (daño irreversible), gusanos (afectación parcial), bomba lógica o cronológica (destrucción o modificación de datos).
- Acceso no autorizado a sistemas o servicios. Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers), hasta el sabotaje o espionaje informático.
- Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones.
- Reproducción no autorizada de programas informáticos de protección legal. Esto puede entrañar una pérdida económica sustancial para los propietarios legítimos.

Aquí una relación de Casos detectados en Bolivia

- Phishing: Los autores, quienes incluso operan desde otros países ingresan a la página web de alguna entidad financiera en la que escogen a su víctima; la contactan mediante su correo electrónico y le envían un portal falso del banco y bajo pretexto de que la institución está en un proceso de actualización le piden sus datos y el PIN.
- Clonación de tarjetas: La víctima es afectada desde que asiste a un local o un centro comercial donde entrega su tarjeta de crédito para pagar sus compras o consumo, y el delincuente duplica su tarjera en un escáner sofisticado y se dan modos para seguirla y averiguar su clave, con la que después vacían su cuenta.
- Sabotaje informático: Esta modalidad de fraude sucede cuando alguna persona, que puede ser ingeniero en sistemas, informático o conocedor de Internet, de forma

maliciosa obstaculiza, modifica o comete cualquier otra acción que atente contra el normal funcionamiento de un sistema de información personal o de una institución.

- Falsedad y amenazas: La falsificación y suplantación de identidad electrónica todavía no está en la legislación boliviana, pero consiste en que cierta persona averigua la contraseña de un correo electrónico ajeno y una vez que consigue ingresar modifica el contenido de cartas o documentos, o envía mensajes con diferentes fines a destinatarios. La Fuerza Especial de Lucha Contra el Crimen (Felcc) capacitará investigadores con apoyo de la GTZ (1) el próximo año 2009. La GTZ es una empresa federal alemana con sede central en Eschborn, Alemania, y tiene más de 30 años de experiencia en la cooperación internacional para el desarrollo sostenible. Su principal cliente es el Ministerio Federal de Cooperación Económica y Desarrollo BMZ. Además presta servicios a otros Ministerios Federales, gobiernos de otros países, clientes internacionales como la Comisión Europea, las Naciones Unidas, el Banco Mundial y empresas privadas.

http://www.laprensa.com.bo/noticias/07-12-08/index.php

2.1.2 DELITOS INFORMATICOS EN BOLIVIA

Los delitos informáticos en Bolivia son los siguientes:

Manipulación Informática.- Robos, hurtos, estafas, o fraudes cometidos mediante manipulación de los datos de entrada.

Virus Informático.- Programas generalmente destructivos, con la capacidad de ocultarse, auto reproducirse con múltiples copias y capacidad de propagarse en la red o por Internet.

Fraudes Informáticos.- Falsificaciones informáticas que utilizan dispositivos de informática, para producir copias no autorizadas de originales sin autorización del propietario.

Sabotaje Físico / Lógico.- (Daños o modificaciones de programas) Daño leve, mediano o mayor a los dispositivos y unidades lógicas de un sistema informático.

Suplantación Informática.- Falsificaciones informáticas, donde se colocan puntos intermedios disfrazados para burlar controles. Apropiación de identidades electrónicas para obtener beneficios personales.

Interceptación de líneas.- Pinchado de líneas, intercepción lógica o física de las líneas de telecomunicación y redes para analizar el tráfico y filtrar datos.

Modelamiento de delitos.- Utilizar equipos para simular delitos, copiando sistemas e instalaciones para planificar futuros actos delictivos.

Ingeniería reversa.- Proceso inverso al armado de programas, transformándolos a código de máquina, para obtener, vulnerar o romper los códigos, controles de seguridad y protección.

Plagio y piratería.- Violación de los derechos de propiedad intelectual en software, textos, imágenes y demás contenidos propietarios.

Invasión a la privacidad.- Acceso no autorizado a datos personales y su utilización para fines ajenos a los del propietario.

Terrorismo informático.- Acción orientada a causar temor o daño utilizando los medios informáticos, dañándolos, alterándolos o utilizándolos para fines no especificados en su creación.

Pornografía infantil.- Corrupción de menores y divulgación de imágenes y videos de menores.

Spam.- Correo comercial no solicitado.

Phishing.- Suplantación de página Web.

Cuando se imputa a una persona por un delito informático, generalmente el Art.363 bis Manipulación Informática (sólo este tiene pena de cárcel), la imputación incluye además otros delitos con más o menos años de cárcel, por ejemplo abuso de confianza, hurto, uso de instrumento falsificado, estafa agravada, etc. Esto se da porque si bien se pueden manipular los datos de entrada, el proceso o la salida de datos, estos datos en algún momento se reflejan en un papel firmado/rubricado o para causar el daño patrimonial establecido en el Art. 363 bis, alguien deberá recibir el dinero físicamente.

Los delitos informáticos en muchos casos no se castigan por defectos procesales, al igual que otro tipo de delitos, en este punto debemos resaltar la falta de capacitación del Personal que hace prevalecer la Ley (policía y fiscales) en el secuestro de evidencia digital y la preservación de la cadena de custodia de la misma. El Instituto de Investigaciones Forenses, es el que nos ayuda a poder obtener más información de cómo obtener una evidencia clara.

Como consecuencia del desconocimiento de las Nuevas Tecnologías por parte de la mayoría de los Jueces y Fiscales, existe una excesiva dependencia que recae en los "Peritos Informáticos" y esto no solamente se da en Bolivia, por ejemplo en Argentina varios de los expositores en el VII Seminario sobre Delitos en Tecnología, también se manifestaron al respecto. http://www.nobosti.com/spip.php

2.1.3 INSTITUTO DE INVESTIGACIONES FORENSES

En Bolivia se funda el Instituto de Investigaciones Forenses (IDIF), el año 2002. El 10 de Diciembre de 2001, se nombra al primer director nacional del Instituto de Investigaciones Forenses. El Instituto de investigaciones Forenses tiene una visión: Ser un Organismo técnico – científico, independiente, imparcial y altamente especializado en la investigación y comprobación de los delitos, favoreciendo a la transparencia, confianza y efectividad de la administración de justicia. Y un objetivo: Garantizar la confiabilidad del análisis científico y técnico de las evidencias en los delitos perpetrados, de tal manera que contribuya a esclarecer los hechos, modos, autores y circunstancias en que se cometieron, estableciendo la verdad para y dentro del proceso penal. http://www.ciberjure.com.pe

2.1.4 ANALISIS FORENSE

El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par, que se valoran los daños ocasionados. Si los daños han provocado la in operabilidad del sistema, el análisis se denomina análisis postmortem.
http://www.ausejo.net/seguridad/forense.htm

2.1.5 INFORMATICA FORENSE

Según el FBI, la informática forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional ya sea este en el software o en el hardware.
http://comunidad.dragonjar.org/f157/la-informatica-forense

2.1.6 PERITO INFORMATICO

El perito forense es un profesional dotado de conocimientos especializados y reconocidos, a través de sus estudios superiores, que suministra información u opinión fundada a los tribunales de justicia sobre los puntos litigiosos que son materia de su dictamen. Existen dos tipos de peritos, los nombrados judicialmente y los propuestos por una o ambas partes (y luego aceptados por el juez), ambos ejercen la misma influencia en el juicio.

Un perito informático debe extremar las precauciones cuando se le confía una inspección en informática forense. Clonar discos duros, CDs, DVDs, Pen-Drives y en general el clonado de cualquier componente informático es el primer paso para poder trabajar seria y

rigurosamente las evidencias forenses. No debe confundirse la duplicación en el ámbito pericial y forense con falsificaciones o imitaciones más o menos ilegales ni con ningún procedimiento para convertir unos formatos en otros o para descifrar. Las descripciones y transcripciones deben ser idénticas en las buenas duplicaciones realizadas por un perito duplicador experto en duplicaciones. http://www.miguelgallardo.es/perito/informatico/

2.1.7 DELITOS INFORMATICOS CUBIERTOS EN LAS LEYES BOLIVIANAS

En el Capítulo XI del Código Penal Boliviano, en su artículo 363bis y 363ter, tipifica los Delitos Informáticos los cuales son:

Manipulación Informática Art. 363bis: El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de 1 a 5 años y con multa de 60 a 200 días.

Alteración, Acceso y Uso Indebido de Datos Informáticos Art. 363ter.: El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático(CD-ROM, USB, disquete y otros), ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta 200 días. http://www.wipo.int/wipolex/es/

2.1.8 TRIBUNAL DE JUSTICIA

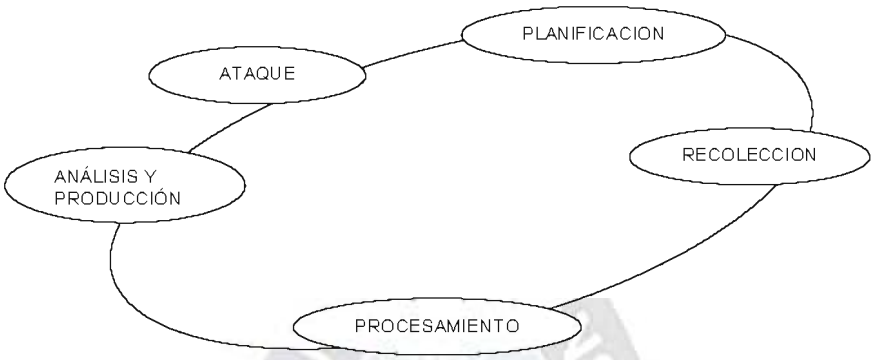
La Corte Suprema de Justicia de Bolivia es el máximo tribunal de justicia ordinaria, contenciosa y contencioso-administrativa de la República de Bolivia. El tribunal de justicia (juzgado o corte) es un órgano público cuya finalidad principal es ejercer la jurisdicción, o sea, resolver litigios con eficacia. Sin perjuicio de cumplir actos de otra índole que las leyes que los organizan les puedan atribuir; estos asuntos son denominados no contenciosos. No debe confundirse el órgano jurisdiccional (el tribunal), con las personas que en calidad de funcionarios sirven en él (jueces y demás personal auxiliar).

http://es.wikipedia.org/wiki/Tribunal_de_justicia

2.1.9 HECHO CRIMINAL

Antes de comenzar con una investigación criminal se debe analizar la secuencia típica de un ataque informático o el uso de un medio electrónico para la comisión de un delito, como se observa en al figura 2.1.

Fig. 2.1 Pasos en un hecho criminal



FUENTE [ROSALES G., MANUAL INFORENSE 2008]

Los pasos mencionados son:

Planificación.- Definir el objetivo.

Recolección.- Reunir información.

Procesamiento.- Procesar la información obtenida.

Análisis y Producción.- Analizar la Información obtenida.

Ataque.- Ejecutar la acción o atacar.

Estos pasos son genéricos, entonces no necesariamente encontraremos pistas en el dispositivo afectado o utilizado, el atacante ha tenido que colectar la información, y bajo el principio de e-leocard a dejado huellas electrónicas que debemos encontrar, cada caso es peculiar según el atacante. Por supuesto, que debemos tomar en cuenta la naturaleza e intelecto del atacante que puede haber utilizado técnicas antiforenses (término utilizado a las propiedades del borrado seguro demostradas en 1996 por el doctor Guttman) en cuyo caso estaremos frente a un atacante o perpetrador del hecho muy sofisticado que si bien minimiza la posibilidad de encontrar rastros también limita en sentido positivo el espectro de posibles atacantes, dado el conocimiento y las técnicas utilizadas.

[ROSALES G., Manual Inforense 2008]

2.2 METODO PARA EL ANALISIS PERICIAL EN DELITOS INFORMÁTICOS

Debido a la complejidad en una investigación de delito electrónico el análisis pericial se lo debe hacer siguiendo una metodología que nos de las pautas de cómo hacer cada tarea y no contaminar la evidencia. Para esto tomaremos la metodología de las 6R's.

Esta complejidad esta dada por la participación de profesionales multidisciplinarios: abogados, profesionales del área de tecnología, policías, etc., los cuales presentan una des uniformidad acentuada en temas de tecnologías de información.

Se considera que la complejidad técnica es solo una parte por cuanto el objetivo de la misma investigación criminal no esta dado por la determinación del modus operandi y el autor, sino por lograr el resarcimiento de los daños sufridos y la sanción de los autores.

Para el análisis pericial se toma como premisa el establecimiento de la relación inequívoca de tres elementos fundamentales de delito o el crimen: Atacante, víctima y escena del hecho. Esta relación se establece mediante las evidencias y pruebas electrónicas además de las tradicionales como las testificales, documentales, etc.

Para la fase de análisis pericial se aplican todos los conceptos y principios de la informática forense. Las fases que se plantean en el método de las 6R's son [ROSALES G., Manual Inforense 2008]:

R1.- Reconocimiento del Delito

R2.- Requisitos Técnicos

R3.- Recolección de Evidencias

R4.- Recuperación de Evidencias

R5.- Reconstrucción del hecho

R6.- Resultados

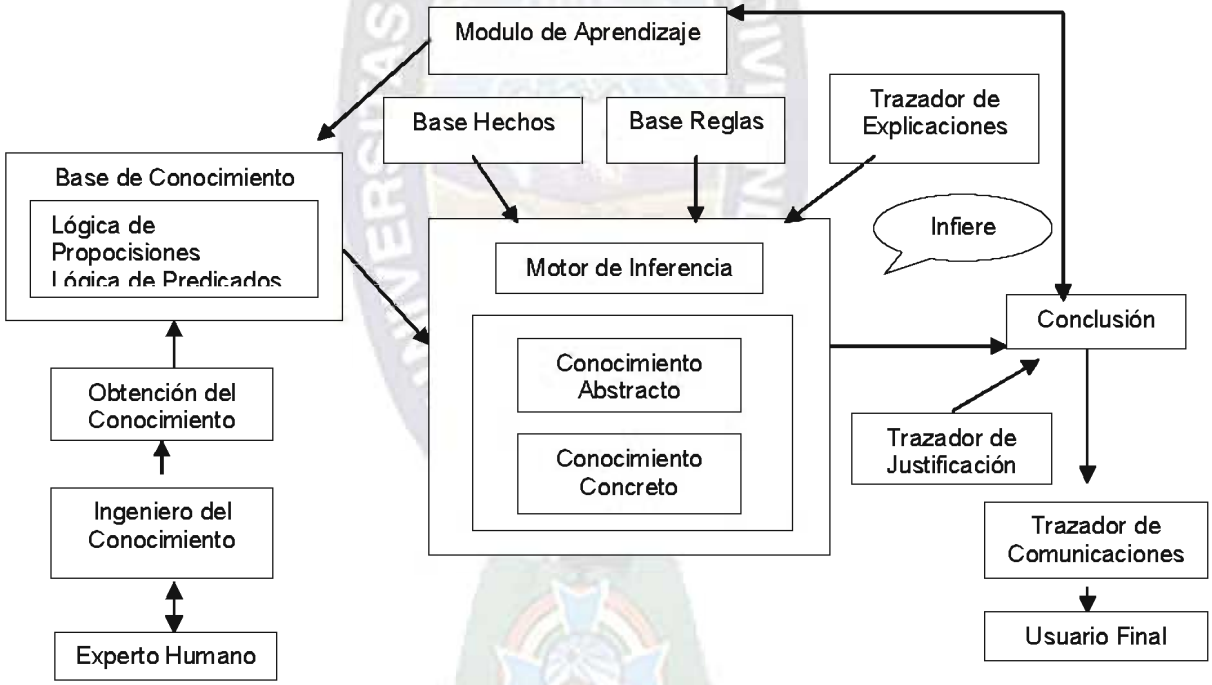
2.3 SISTEMAS EXPERTOS (S.E.)

El Sistemas Expertos es un software que imita el comportamiento de un experto humano en la solución de un problema. Pueden almacenar conocimientos de expertos para un campo determinado y solucionar un problema mediante deducción lógica de conclusiones. También son *SE* aquellos programas que se realizan haciendo explicito el conocimiento en ellos, que tienen información específica de un dominio concreto y que realizan una tarea relativa a este dominio. Programas que manipulan conocimiento codificado para resolver problemas en un dominio especializado en un dominio que generalmente requiere de experiencia humana. [Patterson 90]

Por lo que Un sistema experto puede definirse como un sistema informático (hardware y software) que simula a los expertos humanos en un área de especialización dada. Como tal, un sistema experto debería ser capaz de procesar y memorizar información, aprender y razonar en situaciones deterministas e inciertas, comunicar con los hombres y/u otros sistemas expertos, tomar decisiones apropiadas, y explicar porque se han tomado tales

decisiones. Se puede pensar también en un sistema experto como un consultor que puede suministrar ayuda a (o algunos casos sustituir completamente) los expertos humanos con un grado razonable de fiabilidad. Durante la última década se han desarrollado muy rápidamente numerosas aplicaciones de sistemas expertos a muchos campos. Un Sistema Experto en sí no tiene verdadera Inteligencia Artificial; más bien, es un sistema basado en el conocimiento que, mediante el buen diseño de su base de información y un adecuado motor de inferencias para manipular dichos datos proporciona una manera de determinar resoluciones finales dados ciertos criterios. Los Sistemas Expertos son una herramienta poderosa en el apoyo o guía de los usuarios en los procesos que tienen una secuencia de pasos definida, pero que puede ser configurable, como se observa en la figura 2.2.

Fig. 2.2 Estructura de un Sistema Experto



FUENTE [Msc. L. VELASQUEZ, APUNTES 2007]

Para que un sistema experto aprenda a resolver problemas con un dominio especializado debemos utilizar y analizar la base de conocimientos, la base de reglas, la Lógica de Proposiciones, la lógica de predicados, el silogismo y la base de hechos con el fin de almacenar conocimientos de expertos para un campo determinado y obtener resultados óptimos.

Experto Humano; Los expertos humanos suministran el conocimiento básico en el tema de interés expresado como leguaje natural, y los ingenieros del conocimiento trasladan este conocimiento a un lenguaje, que el sistema experto pueda entender. La colaboración de los expertos humanos, los ingenieros del conocimiento y los usuarios es, quizás, el elemento más importante en el desarrollo de un sistema experto.

Ingeniero del conocimiento; El Ingeniero del Conocimiento trabaja preferentemente en equipo para desarrollar un proyecto. El trabajo que el IC realiza dentro del grupo es: Planificación, Gestión y Control del Proyecto. Interacción con los directivos, expertos y usuarios. Análisis de Viabilidad, Adquisición de Conocimientos y Conceptualización. Ayuda y Asesora en la Formalización del sistema y el Diseño de software. Supervisa la Implementación. Realiza la Validación. Guía y supervisa la Evaluación por parte de los usuarios. Controla el Mantenimiento. Controla y supervisa la documentación del proyecto, del trabajo interno, para los clientes y manual de usuarios. Planificación y control de versiones sucesivas de sistemas. http://www.todoexpertos.com

Obtención del conocimiento; Con el propósito de distinguir la orientación de las corrientes actuales en la obtención del conocimiento, definiremos primero los tipos de éste, que se reducen básicamente a dos: a) conocimiento empírico, y b) conocimiento científico. Se explican a continuación.

- **Conocimiento empírico:** El conocimiento empírico se desprende de la experiencia y a través de los sentidos. Es el conocimiento que le permite al hombre interactuar con su ambiente; es generacional, sin un razonamiento elaborado, ni una crítica al procedimiento de obtención ni a las fuentes de información. Los conceptos empíricos son imprecisos e inciertos, se producen por ideas preconcebidas, tienden a aceptar explicaciones metafísicas y son dogmáticos. Sin embargo, el conocimiento empírico sirve de base al conocimiento científico, al extraerse con método de la realidad.
- **Conocimiento científico:** El conocimiento empírico se convierte en científico al extraerlo de la realidad con métodos y herramientas precisas. Se integra en un sistema de conceptos, teorías y leyes. El conocimiento científico rebasa los hechos empíricos. Puede generalizarse. Puede pronosticarse. El conocimiento científico resiste la confrontación con la realidad, descarta explicaciones metafísicas, y utiliza fuentes de primera mano. Por ejemplo, una enfermera puede notar diferencias entre la profesional y la técnica. Sabe que realizan aparentemente las mismas funciones *(conocimiento empírico*), y aunque pudiera atribuir esto a los estereotipos, no acierta a explicarse las determinantes de la práctica de enfermería, ni a definir las diferencias

que percibe entre una y otra. Sin embargo, al estudiar las determinantes históricas, políticas, culturales, económicas, demográficas, ecológicas, educativas, etc., puede describir, explicar, generalizar y predecir (conocimiento científico) las causas de una práctica profesional en relación con una técnica.

http://www.aibarra.org/investig/tema0.htm

Base De Conocimiento; Una base de conocimientos es un depósito de información creado gracias a una extensa investigación organizada en un árbol de conocimientos completo.

Es la parte del sistema experto que contiene el conocimiento sobre el dominio. Hay que obtener el conocimiento del experto y codificarlo en la base de conocimientos. Una forma clásica de representar el conocimiento en un sistema experto son lar reglas. Una regla es una estructura condicional que relaciona lógicamente la información contenida en la parte del antecedente con otra información contenida en la parte del consecuente. En la Base de conocimiento se halla la base datos y estas están compuestas por lenguajes de predicado, esta es uno de los componentes que contiene el conocimiento del experto o también llamado base de datos, su función es almacenar experiencias, conocimientos, etc. de una determinada área. Existen dos tipos de base de conocimiento: El procedural; Se usa en los lenguajes estructurados como son Pascal, C, Visual Basic etc., y El declarativo; Esta basado en hechos que vienen a ser acciones que se dan dentro del problema se utilizan los lenguajes Prolog y Lisp.

Base De Hechos; Base de hechos (Memoria de trabajo). Contiene los hechos sobre un problema que se han descubierto durante una consulta. Durante una consulta con el sistema experto, el usuario introduce la información del problema actual en la base de hechos. El sistema empareja esta información con el conocimiento disponible en la base de conocimientos para deducir nuevos hechos.

Base De Reglas; En nuestra vida diaria encontramos muchas situaciones complejas gobernadas por: Las reglas deterministas que constituyen la más sencilla de las metodologías utilizadas en sistemas expertos. La base de conocimiento contiene las variables y el conjunto de reglas que definen el problema, y el motor de inferencia obtiene las conclusiones aplicando la lógica clásica a estas reglas. Por regla se entiende una proposición lógica que relaciona dos o más objetos e incluye dos partes, la premisa y la conclusión. Cada una de estas partes consiste en una expresión lógica con una o más afirmaciones objeto-valor conectadas mediante los operadores lógicos y, o, o no. Una regla se escribe normalmente como: “Si premisa, entonces conclusión".

Motor De Inferencia; La estructuración del motor de inferencia esta en base a la base de hechos y la base de reglas. El sistema experto modela el proceso de razonamiento humano con un módulo conocido como el motor de inferencia. Dicho motor de inferencia trabaja con la información contenida en la base de conocimientos y la base de hechos para deducir nuevos hechos. Contrasta los hechos particulares de la base de hechos con el conocimiento contenido en la base de conocimientos para obtener conclusiones acerca del problema. Para las reglas de producción se utilizan los mecanismos de inferencia. Estos mecanismos de inferencia evalúan las reglas y el conocimiento en hechos. Existen dos formas básicas de evaluación de las reglas: Encadenamiento hacia adelante y Encadenamiento hacia atrás.
El encadenamiento hacia adelante se define también como inferencia controlada por los datos o como método "if–added", el encadenamiento hacia atrás se conoce también como inferencia controlada por el objetivo o como método "if-needed".
Su función principal es aplicar el conocimiento abstracto al conocimiento concreto para sacar conclusiones. [Apaza, 2008].

Conocimiento abstracto; Es todo aquel que: El hombre adquiere debido a las diversas necesidades que se le presentan en la vida, por instinto y no por el pensamiento fundamentado, que se aprende sin ciencia y sin leyes, así también es trasmitido por medio de las relaciones con la sociedad, en la escuela de la vida. Todo el conocimiento del Abogado en cuestiones de delitos informáticos, además del conocimiento y experiencias del perito informático, son tomados como conocimiento abstracto.

Conocimiento concreto; Puesto que todo conocimiento concreto incluye unos elementos que siempre tienen que estar presentes para que sea posible, tenemos que poder reconocer estos elementos en todo conocimiento concreto, pero con independencia de lo concreto que conozcamos en él. Es más, la evidencia de estos elementos a priori tiene que ser mayor que la de cualquier otro conocimiento concreto que, en el fondo, se basa en ellos. Así que es preciso hallar alguna forma de conocimiento que nos pone ante los elementos a priori de todo conocimiento objetivo. A ese conocimiento de los elementos a priori, Kant lo llamó *conocimiento puro*. A los argumentos para hallarlo Kant los llamó *conocimiento trascendental*. http://www.kalipedia.com/filosofia/tema/conocimiento-puro.html

Trazador de Explicaciones; Recorrido o camino para satisfacer las condiciones del sistema experto

Trazador de Justificaciones; Recorrido o camino para sustentar, con argumentos convincentes, la realización del sistema experto, en otras palabras, es señalar por que y para que se va a llevar a cabo dicha investigación

Modulo de aprendizaje; Es la unidad base de recursos (contenidos, metodologías y medios) que les sirven a las personas para estudiar una realidad. Se organiza alrededor de un objeto de estudio particular y abarca varios temas o áreas de estudio. El aprendizaje es el proceso a través del cual se adquieren nuevas habilidades, destrezas, conocimientos, conductas o valores como resultado del estudio, la experiencia, la instrucción, el razonamiento y la observación. Este proceso puede ser analizado desde distintas perspectivas, por lo que existen distintas teorías del aprendizaje. El aprendizaje es una de las funciones mentales más importantes en humanos, animales y sistemas artificiales.

Conclusión; es una de las partes fundamentales dentro de los sistemas expertos, porque a diferencia de un sistema de base de datos que obtiene la solución mediante querys, un sistema experto debe inferir (inferencia hacia adelante e inferencia hacia atrás) la solución, para lo cual debe hacer uso de métodos de búsqueda y heurísticas, que le permitan razonar de la misma forma que el experto humano.

Usuario Final; En informática el término usuario final designa a la persona o personas que van a manipular de manera directa un producto de software. Usuario final no es necesariamente sinónimo de cliente o comprador, una compañía puede ser un importante comprador de software, pero el utilizador final puede ser solamente un empleado o grupo de empleados dentro de la compañía, como una secretaria. El concepto clave es la interacción directa con el programa, no la propiedad. En el caso del software de gran distribución, el cliente o comprador es por lo general el mismo que el usuario final.

2.4 LOGICA DE PROPOSICIONES

La lógica es la ciencia que se dedica al cálculo de argumentos; es, como se afirma desde Aristóteles, la teoría del razonamiento. El ideal del que parte es que, si partimos de premisas que son verdaderas, y utilizamos reglas adecuadas para pasar de unos argumentos a otros, la conclusión que extraigamos será indudablemente verdadera. Una forma más sencilla de expresar esto es decir que de la verdad siempre se sigue la verdad.

No ocurre lo mismo con la falsedad; en efecto, si nosotros partimos de unas premisas falsas, puede ocurrir que, independientemente de que el paso de unos argumentos a otros lo hagamos de modo correcto o incorrecto, arribemos a conclusiones que pueden ser bien verdaderas, bien falsas. Una manera más corta de expresar esto es decir que de la falsedad se sigue cualquier cosa.

La lógica desempeña un papel central en muchos campos, y especialmente en matemáticas. La lógica también resulta esencial para construir y probar programas de

computadora. Sin embargo, a veces nuestro razonamiento lógico es diferente y puede dar lugar a errores. Por tanto, es importante identificar las leyes fundamentales de las derivaciones lógicas. Algo básico para las derivaciones lógicas son las proposiciones, que son afirmaciones que pueden ser verdaderas o falsas. Las proposiciones pueden combinarse y manipularse de varias maneras. Estas manipulaciones son el tema del cálculo proposicional. Es importante distinguir entre argumentos que son validos lógicamente y los argumentos que no lo son. Esto quiere decir, se tratara sobre argumentos que cualquier persona razonable podría considerar lógicos. Identificaremos entonces la estructura básica de estos argumentos. Mientras lo hacemos, descubriremos que los argumentos lógicos constan de ciertas proposiciones que no pueden subdividirse. Estas proposiciones atómicas se mantienen unidas mediante conexiones lógicas.

Algunos argumentos lógicos importantes, como ejemplo de un argumento lógicamente valido, considere las siguientes afirmaciones:

1 Todos los delitos informáticos son sancionados

2 La pornografía infantil es un delito informático

3 La pornografía infantil es un delito sancionado

Este argumento lógico tiene tres líneas, y cada línea contiene una afirmación. Las afirmaciones de las líneas 1 y 2 proporcionan las premisas del argumento, y la línea 3 contiene la conclusión que también es una premisa que deriva de las dos primeras. Se puede argumentar contra las premisas y reivindicar que son erróneas. Sin embargo, tan pronto como las premisas sean aceptadas, la conclusión también debe aceptarse, porque se sigue lógicamente de las premisas, y por tanto, el argumento es válido.
http://es.wikipedia.org/wiki/L%C3%B3gica_proposicional

2.5 LOGICA DE PREDICADOS

La lógica de predicados o de primer orden es una generalización de la lógica de proposiciones. Introduciendo nuevos elementos del lenguaje, permite estudiar la estructura interna de los enunciados (sus propiedades, las relaciones entre objetos, etc.). Esta nueva lógica tendría que permitir una descripción más fina de la realidad, pudiendo distinguir los objetos o términos (por ejemplo, los hombres) de sus propiedades o predicados (por ejemplo, la propiedad de ser mortales).

La lógica de predicados (Gottob Frege, 1879) nos permite dar una descripción de la realidad más detallada. Los elementos básicos del alfabeto del la lógica de predicados son: Los símbolos de constantes: se denotan a; b; c;... y representan objetos concretos. Las

constantes son individuos o elementos distinguidos del universo del discurso, que es la colección de objetos sobre los cuales queremos razonar. Las variables: se denotan x; y; z;... y sirven para representar objetos, cuyo dominio hay que especificar. Los símbolos del predicado: se denotan P; Q; R;...La lógica de predicados estudia las frases declarativas con mayor grado de detalle, considerando la estructura interna de las proposiciones, se toman como elementos básicos los objetos y las relaciones entre ellos, es decir se distingue: Que se afirma y de quien se afirma. La lógica de predicados está basada en la idea de las sentencias que realmente expresan relaciones entre objetos, así como también cualidades y atributos de tales objetos. Los objetos pueden ser personas, objetos físicos, o conceptos. Tales cualidades, relaciones o atributos, se denominan predicados. Los objetos se conocen como argumentos o términos del predicado. Al igual que las proposiciones, los predicados tienen un valor de veracidad, pero a diferencia de las preposiciones, su valor de veracidad, depende de sus términos. Es decir, un predicado puede ser verdadero para un conjunto de términos, pero falso para otro. Por ejemplo, el siguiente predicado es verdadero:
Cometen (personas, Delitos)

Los predicados también pueden ser utilizados para asignar una cualidad abstracta a sus términos, o para representar acciones o relaciones de acción entre dos objetos.

2.6 SILOGISMO

Un silogismo es un argumento que consta de tres proposiciones; de ellas, la última se deduce necesariamente de las otras dos. Se trata de una forma de razonamiento deductivo, donde dos de las proposiciones son premisas y la tercera es una conclusión. El silogismo es una argumentación en la que, a partir de un antecedente que compara dos términos con un tercero, permite inferir o deducir un consecuente.

En otras palabras, el modelo de silogismo está formado por tres proposiciones que incluyen un término medio (que es común a las dos premisas y se elimina en la conclusión) y dos extremos. Por ejemplo:

"Todos los delitos informáticos son sancionados".

"La pornografía infantil es un delito informático".

"La pornografía infantil es un delito sancionado".

Hay que tener en cuenta que un silogismo no siempre arrojará conclusiones verdaderas, más allá de que siga una forma válida de razonamiento. Cabe destacar que los silogismos suponen que, de dos premisas negativas, nunca puede obtenerse una

conclusión. Por otra parte, de dos premisas afirmativas, no puede obtenerse una conclusión negativa.

2.6.1 SILOGISMO JURÍDICO

El silogismo jurídico está integrado por una premisa mayor, que es la norma jurídica, y por una premisa menor, que son los hechos, y por último la conclusión. Cabe señalar que el fondo del asunto está determinado por las Leyes de Codigo Penal Boliviano. Y el procedimiento está reglamentado por los artículos 363bis y 363 ter. Por lo que se refiere el Capítulo XI, las Sanciones se basan en el incumplimiento al las reglas y normas. Acción; se llama acción el medio de hacer valer ante las autoridades los derechos establecidos en el reglamento. Excepción; Son las defensas que puede emplear el demandado para impedir el curso de la acción o para destruirla. Proceso; Es la solución heterocompositiva, es decir, la solución imparcial, a cargo del Juez.

¿Qué es el Silogismo Jurídico?

Es lograr una relación coherente entre el aspecto formal y la norma; es decir adecuar unos hechos a la descripción abstracta que hay en la norma por lo tanto este tipo de razonamiento servirá efectivamente para garantizar la solidez en la argumentación que el abogado o cualquier operador del derecho presente para sustentar su posición, sin perder de vista que lo que se evalúa es la corrección de la conclusión a partir de la estructura lógica de sus premisas de base.

¿Cuáles son los tipos de Silogismo Jurídico?

Silogismo Aristotélico (Aristóteles) y Silogismo Concretivo (Miró Quesada)

¿Cómo esta compuesto?

El Silogismo se compone de dos premisas y una conclusión derivada de aquéllas. Se dice que la conclusión es válida si las premisas lo son, pero desde un punto de vista formal. No importa aquí la corrección o verdad material de las premisas, sino simplemente que la conclusión se derive de ellas. Las premisas de la inferencia del silogismo jurídico requieren, una vez determinadas, la verificación de su estructura lógica. Así, surge la necesidad de analizar si la estructura de la premisa mayor de carácter normativo se ajusta a la forma supuesto-consecuencia; y si de otro lado la premisa menor corresponde efectivamente a un caso especial del supuesto de hecho general contenido en la premisa mayor, en la norma vigente.

A es siempre mayor que B.

X es A.

……

Luego X es mayor que B.

Una de las premisas y la conclusión son procesos de conexión simples.

Realizada dicha constatación y si encontramos para ambos casos respuestas afirmativas, llegaremos a una conclusión que será lógicamente válida, es decir que responderá positivamente a un análisis de coherencia lógica al ser consecuencia de la subsunción de ambas premisas.

Ahora bien, desde el horizonte de la cuestión planteada, el silogismo jurídico es una expresión sistémica, que ubica al juez (Constitucional) en un plano deductivo y argumental, en donde dentro de una estructura cerrada, la premisa mayor, le es dada por la norma por aplicar al caso, mientras la premisa menor es dada por el hecho relevante y la conclusión por la aplicación al caso sub-examine.

Ejemplos de silogismo jurídico:

Los ejemplos pueden ser de variada índole, en el caso de la pena de muerte, las premisas son tangibles, ya que:

La premisa mayor sería: la Constitución prohíbe la pena de muerte;

La premisa menor seria: la ley señala e indicó la pena de muerte para ciertos delitos,

La conclusión sería: esa ley es inconstitucional.

García Maynez nos dice que silogismo jurídico es el razonamiento de aplicación de los preceptos del derecho. Esta compuesta por una premisa mayor, que esta constituida por la norma genérica, la menor por el juicio que declara realizado el supuesto de aquella, y la conclusión por el que imputa a los sujetos implicados, en el caso, las consecuencias de derecho.

Ejemplos1:

Premisa mayor: Al que sin el permiso correspondiente porte un arma del uso exclusivo del ejército, Armada o Fuerza Aérea, se le sancionará con prisión de tres meses a un año y de uno a diez días de multa. (Art. 83 del CPF).

Premisa menor: Juan Pérez porta un arma R 15.

Conclusión: Deben aplicarse a Juan Pérez de tres meses a un año de prisión y multa de uno a diez días de salario.

Ejemplos2:

Premisa mayor: Al que inundare en todo o en parte un camino público o echare sobre él las aguas de modo que causen daño, se le impondrán de uno a cinco años de prisión y de cien a diez mil días multa. (Art. 167 del CPF)

Premisa menor: Juan Pérez provocó la inundación del camino a Pueblo Escondido. Conclusión: A Juan Pérez le serán impuestos de uno a cinco años de prisión y una multa de cien a diez mil días.

Ejemplos3:

Premisa mayor: Se aplicará prisión hasta de dos años y privación de derechos civiles hasta por seis años a quien cometa adulterio en el domicilio conyugal o con escándalo. (Art. 273 del CPF).

Premisa menor: Juan Pérez es encontrado cometiendo adulterio en su casa. Conclusión: Juan Pérez estará en prisión por un plazo no mayor a dos años y podría perder sus derechos civiles hasta por seis años.

La idea de un perfecto silogismo judicial, es que permita la perfecta verificación de los hechos es una ilusión metafísica, ya que las condiciones del uso del término verdadero, como los criterios de aceptación de la verdad en todo proceso inclusive el de constitucionalidad, exigen inequívocamente decisiones dotadas de márgenes más o menos amplios de discrecionalidad.

Por consiguiente no es extraño reconocer que en la actividad judicial, especialmente en la Corte Constitucional existen espacios específicos de poder imposibles de extirpar para permitir su reducción y control; estos espacios son el poder de denotación (de interpretación o de verificación jurídica), el poder comprobación probatoria (verificación fáctica), el poder de connotación (comprensión equitativa), y el poder de disposición (valoración ético política).

Por muy perfeccionado que esté un sistema la verificación jurídica de los presupuestos constitucionales de una ley, nunca podrán ser absolutamente ciertas y objetivas, ya que la interpretación de la ley, no es solamente una actividad recognoscitiva, sino que es el fruto de una escogencia práctica respecto de hipótesis alternativas.

http://silogismo-juridico.html

2.7 INFERENCIA LÓGICA

Primero presentamos los tipos de inferencia, la inferencia válida en computación y matemáticas y al final una serie de reglas que se utilizan para la inferencia deductiva. La inferencia es la forma en la que obtenemos conclusiones en base a datos y declaraciones establecidas. Un argumento, por ejemplo es una inferencia, donde las premisas son los datos o expresiones conocidas y de ellas se desprende una conclusión. Una inferencia puede ser: Inductiva, deductiva.

Inductiva. (De lo particular a lo general) Aquí por ejemplo si durante la primera semana el maestro llega 10 minutos tarde, podemos concluir que todo el semestre va a llegar tarde. Esta conclusión no necesariamente es válida porque puede ser que el maestro algún día llegue temprano. En general una inferencia inductiva es la que se desprende de una o varias observaciones y en general no podemos estar seguros de que será verdadero lo que concluimos. En este caso podemos mencionar el ejemplo el mentiroso: Un joven le dice a un amigo, tu todos los días dices mentiras, y él contesta, no es cierto, ayer en todo el día no dije una sola mentira. Resumiendo, la inferencia inductiva es la ley general que se obtiene de la observación de uno o más casos y no se puede asegurar que la conclusión sea verdadera en general.

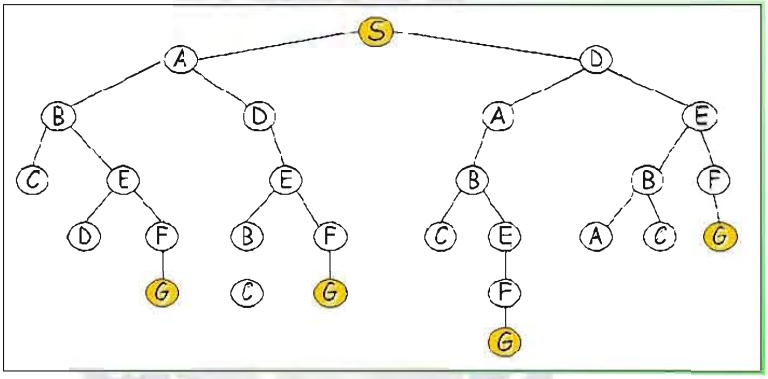
Deductiva (de lo general a lo particular) Cuando se conoce una ley general y se aplica a un caso particular, por ejemplo se sabe que siempre que llueve hay nubes, concluimos que el día de hoy que está lloviendo hay nubes. También se conoce como inferencia deductiva cuando tenemos un caso que analiza todos los posibles resultados y de acuerdo a las premisas sólo hay una posible situación, en este caso decimos que la situación única es la conclusión. Es este caso estamos seguros de que si las premisas son verdaderas entonces la conclusión también lo es. En este caso se encuentran MPP: Modus Ponendo Ponens y MTT: Modus Tollendo Tollens que de acuerdo a la tabla de verdad de la condicional son dos formas de establecer una inferencia válida. La inferencia deductiva es la única aceptada como válida. http://Callirgos_Razonamiento.htm

2.8 ÁRBOLES DE DECISIÓN

Un árbol de decisión es un modelo de predicción utilizado en el ámbito de la inteligencia artificial. Dada una base de datos se construyen diagramas de construcciones lógicas, muy similares a los sistemas de predicción basados en reglas, que sirven para representar y categorizar una serie de condiciones que ocurren de forma sucesiva, para la resolución de un problema. Un árbol de decisión tiene unas entradas las cuales pueden ser un objeto o una situación descrita por medio de un conjunto de atributos y a partir de esto devuelve una respuesta la cual en últimas es una decisión que es tomada a partir de las entradas. Los valores que pueden tomar las entradas y las salidas pueden ser valores discretos o continuos. Se utilizan más los valores discretos por simplicidad, cuando se utilizan valores discretos en las funciones de una aplicación se denomina clasificación y cuando se utilizan los continuos se denomina regresión. Un árbol de decisión lleva a cabo un test a medida que este se recorre hacia las hojas para alcanzar así una decisión. El árbol de

decisión suele contener nodos internos, nodos de probabilidad, nodos hojas y arcos. Un nodo interno contiene un test sobre algún valor de una de las propiedades. Un nodo de probabilidad indica que debe ocurrir un evento aleatorio de acuerdo a la naturaleza del problema, este tipo de nodos es redondo, los demás son cuadrados. Un nodo hoja representa el valor que devolverá el árbol de decisión y finalmente las ramas brindan los posibles caminos que se tienen de acuerdo a la decisión tomada, donde se posesiona en el nodo S cuyo objetivo es llegar al nodo G como se muestra en la [Fig. 2.2].

Fig. 2.2 Representación de un árbol



2.8.1 ENCADENAMIENTO HACIA ADELANTE

El motor de inferencia parte de los hechos para llegar a los resultados, es decir, no selecciona más que reglas que verifiquen las condiciones de la parte izquierda (fase de detección-filtrado). Se aplica, entonces, la fase de elección (resolución de conflictos) sobre este conjunto de reglas, para determinar la regla a utilizar posteriormente. La aplicación de esta regla entraña en general una actualización de la base de hechos (fase de ejecución). Este proceso se repite hasta que no existen más reglas aplicables o se haya alcanzado el objetivo. La eficacia del motor de inferencia reside en la pertinencia de la decisión tomada (regla elegida) durante la fase de elección. La regla elegida condiciona la rapidez con la que el sistema llegará a la solución, lo cual determinará la eficacia del motor de inferencia. Sin embargo, esta forma de razonamiento posee diversos inconvenientes:

- El sistema activa todas las reglas aplicables incluso aunque algunas no ofrezcan ningún interés.
- La base de hechos debe contener el suficiente número de hechos iniciales para que el sistema pueda llegar a una solución.
- Los usuarios deben, pues, suministrar al SE todas las informaciones que poseen, incluso aunque algunas sean inútiles.

- En caso de rechazo, un solo hecho podría permitir llegar al objetivo, pero el usuario no está informado, puesto que el proceso no es interactivo.
- Este método corre el riesgo de caer en la explosión combinatoria si el número de reglas y de hechos es importante, y sobre todo si el objetivo a alcanzar no es conocido, pues es necesario, entonces, aplicar todas las reglas aplicables para deducir todo lo que se puede deducir. Tantos más cuantos muchos motores de inferencia que razonan con encadenamiento hacia delante trabajan con búsqueda en amplitud (aplicación de todas las reglas aplicables en un momento dado).

2.8.2 ENCADENAMIENTO HACIA ATRAS

El sistema parte del objetivo (o de una hipótesis de objetivo) y trata de volver a los hechos para demostrarlos. Las reglas seleccionadas son las de la parte derecha (consecuente, que corresponden al objetivo investigado). Las condiciones desconocidas (parte izquierda de las reglas) subsisten mientras que existan sub objetivos que demostrar. Este proceso se repite hasta que todos los sub objetivos se hayan demostrado, o se alcance el objetivo final o hasta que no exista la posibilidad de seleccionar más reglas. En este caso, el sistema puede solicitar del usuario la resolución de uno o varios sub-objetivos (cuestiones, test) y el proceso comienza de nuevo. El rechazo ocurre cuando el sistema no puede seleccionar reglas, ni plantear cuestiones al usuario (reglas insuficientes o incoherentes o cuando el usuario no puede responder a las preguntas del SE). La estrategia empleada es muy simple, puesto que consiste en utilizar la primera regla aplicable, en su orden de numeración, para intentar, a continuación, verificar uno tras otro los sub-objetivos producidos (exploración con búsqueda en profundidad). La exploración puede detenerse:

- Cuando el objetivo inicial se demuestra
- Cuando se han explorado sin éxito todas las posibilidades

El sistema puede, entonces, consultar al usuario sobre los sub objetivos no resueltos.

El razonamiento hacia atrás tiene algunas ventajas:

- El sistema plantea cuestiones únicamente cuando es necesario y después de haber explorado todas las posibilidades.
- El árbol de búsqueda es, normalmente, más pequeño que en el caso de encadenamiento hacia delante.
- El proceso es interactivo

Uno de los riesgos del encadenamiento hacia atrás es el de meterse en un bucle: para demostrar A hay que demostrar B, para demostrar B hay que demostrar A.

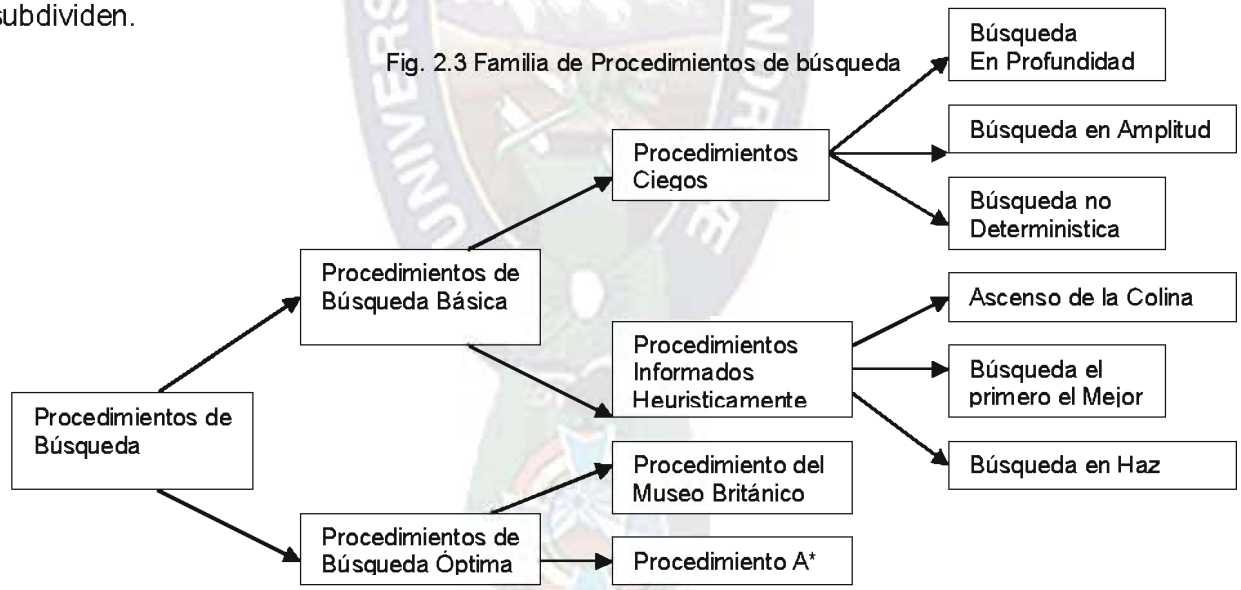
Hay un tercer tipo de encadenamiento denominado encadenamiento mixto, en donde el motor de inferencia puede igualmente utilizar alternativamente los encadenamientos hacia adelante y hacia atrás y examinar en cada ciclo si estos dos razonamientos confluyen. Esto permite realizar la mitad del camino y pararse en el medio o punto de conjunción. En la práctica, este tipo de razonamiento varía de un motor de inferencia a otro y no existe aún una idea claramente definida y admitida por todos. Por el contrario, el objetivo de este encadenamiento es tratar de paliar los inconvenientes de los dos precedentes manteniendo sus ventajas. Sin embargo, su implantación parecer tener algunas dificultades.

2.9 REDES Y BÚSQUEDA

En este caso mencionaremos algunos métodos de búsqueda aplicados a las redes (grafos y árboles) dentro del Área de la Inteligencia Artificial. La familia de procedimientos de búsquedas es bastante amplia, sin embargo a continuación se verá parte de esta familia de procedimientos gráficamente, en forma de árbol, la asociación de estas búsquedas.

Como se ve en la figura 2.3 los procedimientos de búsquedas aplicados para redes se dividen en procedimientos básicos y procedimientos óptimos, y a su vez estos se subdividen.

Fig. 2.3 Familia de Procedimientos de búsqueda



FUENTE [SOTO C., S.E. DE DIAGNOSTICO 2005]

2.9.1 BUSQUEDA BASICA

Procedimientos Ciegos

Los algoritmos de los procedimientos de profundidad, amplitud y no determinístico consiste en ir registrando en una lista los estados a los que se va llegando en la búsqueda, se termina el algoritmo cuando se obtiene el estado meta o la lista queda vacía, si se ha

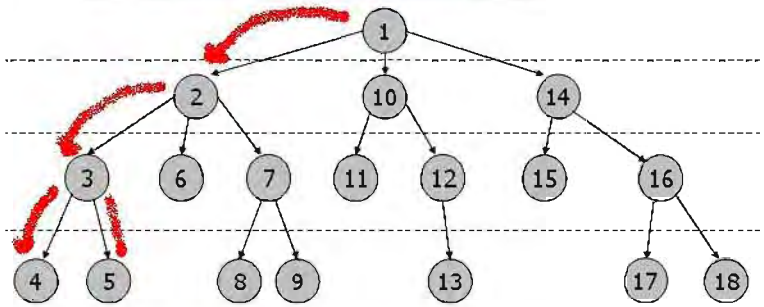
obtenido el estado meta la solución será la lista (los estados que en ella se encuentran), si la lista está vacía quiere decir que la búsqueda fue un fracaso ya que no halló la solución.

Se les denomina métodos ciegos porque siempre se evaluará el primer estado que se encuentra en la lista, sin saber si este es el mejor o peor.

- **La búsqueda en profundidad** es buena siempre y cuando las trayectorias parciales improductivas no sean muy largas, ésta búsqueda se introduce en el árbol de búsqueda extendiendo una trayectoria parcial a la vez.

Se comienza en el vértice inicial (vértice con índice 1) y se marca como vértice activo, a diferencia con la BEP ahora se visitan en orden creciente de índice todos los vecinos del vértice activo antes de pasar al siguiente. Hasta que todos los vértices hayan sido visitados, en cada paso se van visitando en orden creciente de índice todos los vecinos del vértice activo, como se muestra en la figura 2.4.

Fig. 2.4 Representación del recorrido en profundidad



Cuando se han visitado todos los vecinos del vértice activo, se toma como nuevo vértice activo el primer vértice X visitado después del actual vértice activo en el desarrollo del algoritmo.

Sea G = (V, A) un grafo conexo, V' = V un conjunto de vértices, A' un vector de arcos inicialmente vacío y P un vector auxiliar inicialmente vacío:

1. Se introduce el vértice inicial en P y se elimina del conjunto.
2. Mientras V' no sea vacío repetir los puntos 3 y 4. En otro caso parar.
3. Se toma el primer elemento de P como vértice activo.
4. Si el vértice activo tiene algún vértice adyacente que se encuentre en V':

Se toma el de menor índice.

Se inserta en P como último elemento.

Se elimina de V'.

Se inserta en A' el arco que le une con el vértice activo.

- **La búsqueda en amplitud** se comienza en el vértice inicial (vértice con índice 1) y se marca como vértice activo, a diferencia con la BEP ahora se visitan en orden creciente de índice todos los vecinos del vértice activo antes de pasar al siguiente. Hasta que todos los vértices hayan sido visitados, en cada paso se van visitando en orden creciente de índice todos los vecinos del vértice activo.

Cuando se han visitado todos los vecinos del vértice activo, se toma como nuevo vértice activo el primer vértice *X* visitado después del actual vértice activo en el desarrollo del algoritmo.

Sea G = (V, A) un grafo conexo, V' = V un conjunto de vértices, A' un vector de arcos inicialmente vacío y P un vector auxiliar inicialmente vacío:

1. Se introduce el vértice inicial en P y se elimina del conjunto.
2. Mientras V' no sea vacío repetir los puntos 3 y 4. En otro caso parar.
3. Se toma el primer elemento de P como vértice activo.
4. Si el vértice activo tiene algún vértice adyacente que se encuentre en V':

   Se toma el de menor índice.

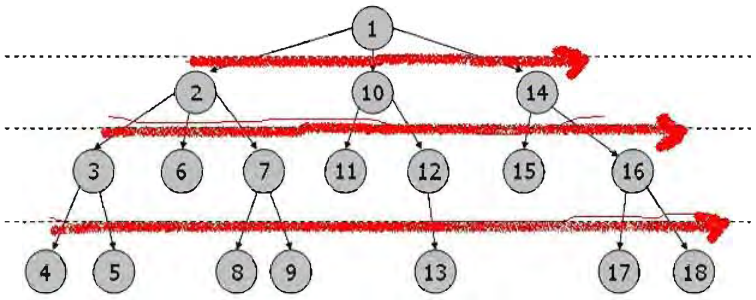
   Se inserta en P como último elemento.

   Se elimina de V'.

   Se inserta en A' el arco que le une con el vértice activo.

Si el vértice activo no tiene adyacentes se elimina de P, como se muestra en la [Fig. 2.5]

Fig. 2.5 Representación del recorrido en Amplitud



- **La búsqueda no determinista** es eficaz cuando no se tiene la certeza de cual búsqueda, en profundidad o en amplitud, puede ser la mejor. Se mueve al azar en el árbol de búsqueda; toma una trayectoria parcial y la extiende al azar.

Procedimientos Informados Heurísticamente

Estos métodos usan una información adicional para establecer un criterio de selección del nodo o estado a procesar. Este conocimiento podría no ser correcto, sin

embargo es una herramienta de gran valor en la búsqueda. A este conocimiento que no tiene garantía de ser correcto se le llama conocimiento heurístico. A una búsqueda utilizando conocimiento heurístico se le llama heurística.

El objetivo (n) es una función lógica que es cierta cuando n es el nodo objetivo y falso en todos los demás casos. El valor inferido del coste desde un nodo n del gráfico, que corresponde a un estado dado, hasta el objetivo se denomina la función objetivo o función de mérito f(n).

• **La búsqueda ascensión a la colina** el procedimiento es semejante a la búsqueda en profundidad con la diferencia que los nodos sucesores son ordenados según el valor de la función mérito antes de adicionarse a la lista. Esto es, el nodo a ser procesado corresponde al "mejor" nodo sucesor según la función de mérito.

Este método es eficaz cuando se tiene una medida natural de la distancia de cada lugar a la meta, y existe la posibilidad de que una buena trayectoria se encuentre entre las trayectorias parciales que parecen ser buenas en cada punto alternativo.

• **La búsqueda en haz** esta búsqueda es parecida a la búsqueda en amplitud en cuanto a que avanza nivel por nivel. Sin embargo, a diferencia de ésta, la búsqueda en haz se mueve hacia abajo sólo a través de los mejores (w) nodos de cada nivel; los otros nodos se ignoran. En consecuencia, el número de nodos explorados se mantiene manejable, aun cuando haya gran cantidad de ramificaciones y la búsqueda sea profunda. Siempre que se usa la búsqueda en haz, sólo existen (w) nodos en consideración a cualquier profundidad, y no el inmenso número exponencial de nodos con los que tiene que tratar siempre que utiliza la búsqueda en amplitud.

La búsqueda en haz es buena cuando se tiene una medida natural de la distancia a la meta, y es probable que una buena trayectoria se encuentre entre las trayectorias parciales que parecen ser buenas en todos los niveles. La búsqueda en haz extiende un número fijo de trayectorias parciales en paralelo y elimina el resto.

• **Búsqueda Primero el Mejor** es probable que las trayectorias encontradas por la búsqueda primero el mejor sean más cortas que las halladas con otros métodos, ya que la búsqueda primero el mejor siempre avanza desde el nodo que parece estar más cercano al nodo meta. Tenga presente, sin embargo, que es probable no es lo mismo que con certeza.

Para poder realizar la búsqueda en primer lugar del mejor lo más eficientemente posible, se debe realizar la inferencia del coste del objetivo de la manera más exacta posible. Es decir, debe realizarse una inferencia que esté lo más cerca posible del coste

verdadero utilizando conocimiento sobre el problema. Este método puede mejorar si se utiliza acotación para evitar generar los hijos con costes mayores al valor buscado.

Estos procedimientos al igual que los métodos ciegos son adecuados para resolver problemas de localización. Evidentemente los métodos que usan información adicional son más robustos. Entre tanto estos métodos no son eficientes para resolver problemas del tipo de optimización.

2.9.2 BUSQUEDA ÓPTIMA

Procedimiento Del Museo Británico

Un procedimiento para encontrar la trayectoria más corta en una red consiste en encontrar todas las trayectorias posibles y seleccionar la mejor de ellas. Este laborioso procedimiento se conoce, como procedimiento del Museo Británico. Si se desea encontrar todas las trayectorias posibles, tanto la búsqueda en amplitud como la búsqueda en profundidad funcionando con una modificación: la búsqueda continúa hasta que se hallen todas las soluciones. Si la amplitud y la profundidad del árbol son pequeñas, no hay problema. Por desgracia, el tamaño de los árboles de búsqueda suelen ser grandes y cualquier procedimiento para hallar todas las trayectorias posibles se vuelve en extremo fastidioso. Afortunadamente, existen estrategias que permiten encontrar trayectorias óptimas sin tener que encontrar primero todas las trayectorias posibles.

Búsqueda De Ramificación Y Cota

El esquema de ramificación y cota siempre se mantiene al tanto de todas las trayectorias parciales que compiten para su consideración posterior. La más corta de ellas se extiende un nivel, creándose tantas trayectorias parciales nuevas como ramas existan. En seguida, se consideran estas nuevas trayectorias junto con las anteriores restantes: de nuevo, se extiende la más corta. Este proceso se repite hasta llegar a la meta a través de una trayectoria. Dado que la trayectoria más corta es la que siempre se escoge para su extensión, la trayectoria que primero encuentra la meta es probable que sea la óptima.

Para convertir lo probable en cierto, se tiene que extender todas las trayectorias parciales hasta que tengan una longitud igual o mayor que la trayectoria completa más corta. La razón es que el último paso para alcanzar la meta puede ser lo suficientemente largo para hacer que la supuesta solución resulte más larga que una o más trayectorias parciales. Puede ser que sólo un paso pequeño extienda una de las trayectorias parciales al punto de solución. Para asegurarse de que esto no suceda, en lugar de terminar al encontrar una trayectoria, termine cuando la trayectoria parcial más corta tenga una longitud mayor

que la trayectoria completa más corta. Este método es el más eficiente de los métodos de búsqueda. Las variaciones respecto a los métodos anteriores son el criterio de selección del nodo a procesar, esto es del nodo a ramificar y la acotación de las ramas o sub árboles que presente peor solución. La segunda variante hace que el método sea más robusto que los otros métodos de búsqueda. El criterio de selección del estado a procesar puede ser:

- Primero el mejor: La secuencia de estados que presenta "mejor" (mayor o menor) valor para la función de mérito entre las listas en COLA
- LIFO: ultimo nodo que ingreso en COLA.

La última secuencia de estados que ingreso en COLA.

- FIFO: primer nodo que ingreso en COLA.

La primera secuencia de estados que ingreso en COLA.

Otros procedimientos

Existen muchas formas de buscar trayectorias óptimas, cada una tiene sus ventajas:

- El procedimiento del Museo Británico es bueno sólo cuando el árbol de búsqueda es pequeño.
- La búsqueda de ramificación y poda con conjetura es eficaz cuando existe una buena estimación de límite inferior de la distancia que resta hacia la meta.
- El procedimiento A* es eficaz cuando la búsqueda de ramificación y cota con conjetura y la programación dinámica son buenas.

2.10 PROTOTIPO

En el desarrollo de Sistemas Expertos se nos plantean dos importantes riesgos:

i) No existen implementaciones similares que puedan servir de orientación al encargado del desarrollo en casi la totalidad de los casos.

ii) En muchos puntos, los requisitos necesarios están esbozados con muy poca precisión.

El diseño y la especificación requieren una temprana determinación de la interfaz del software y de la funcionalidad de los componentes. Durante el desarrollo, resulta apropiado empezar con implementaciones tipo test para encontrar el camino hacia una solución definitiva y para hacerlas coincidir con las necesidades del usuario.

Un método efectivo es la implementación de un prototipo de Sistema Experto que permita llevar a cabo las funciones más importantes de éste, aunque con un esfuerzo de desarrollo considerablemente inferior al de una implementación convencional. Este proceder se define bajo el nombre de 'Rapid Prototyping'. Para Sistemas Expertos, el 'Rapid

Prototyping' es el procedimiento más adecuado, pues posibilita una rápida reacción a los deseos en constante cambio tanto por parte de los expertos como parte del usuario.

3 PROCESO DE INVESTIGACION

3.1 OBSERVACION

En la etapa de observación se detectaron falencias y vacíos en la investigación criminal, con respecto a la protección de la escena del hecho en delitos informáticos. La principal razón de esta situación, es la insuficiencia de personal especializado en peritaje informático. En el país se cuenta con dos especialistas en el área, uno de ellos es el Ing. Guido Rosales Uriona, principal representante de la empresa Yanapti, dedicada al área de seguridad en sistemas.

Otra situación que se debe tomar en cuenta es la contaminación de la escena del hecho, esta se puede dar en forma física o en forma virtual. La contaminación física se pude dar, a consecuencia de la mala manipulación de los componentes informáticos, y la contaminación virtual a través de conexiones inalámbricas que siguen funcionando después del hecho.

Para verificar un delito informático las personas que trabajan como investigadores, tienen un conocimiento limitado de cómo realizar un análisis informático forense.

El tener que analizar las acciones realizadas por los atacantes en los equipos, para conocer y aprender el modo en que estos operan, averiguar el alcance del mismo y, llegado el momento, poder tomar las medidas oportunas para denunciar el ataque a las autoridades competentes, se hace difícil, por no tener las herramientas adecuadas. Lo cual nos conlleva a enfrentarnos a una serie de actividades relacionadas con los hechos criminales, es por ello, que cuando una persona se encuentra con este tipo de situaciones, se enfrenta en primer lugar, con el sitio donde se realizo el hecho criminal, después con una serie de métodos de análisis pericial para llegar a determinar el delito y el grado de perjuicio que este conlleva para terceras personas o instituciones.

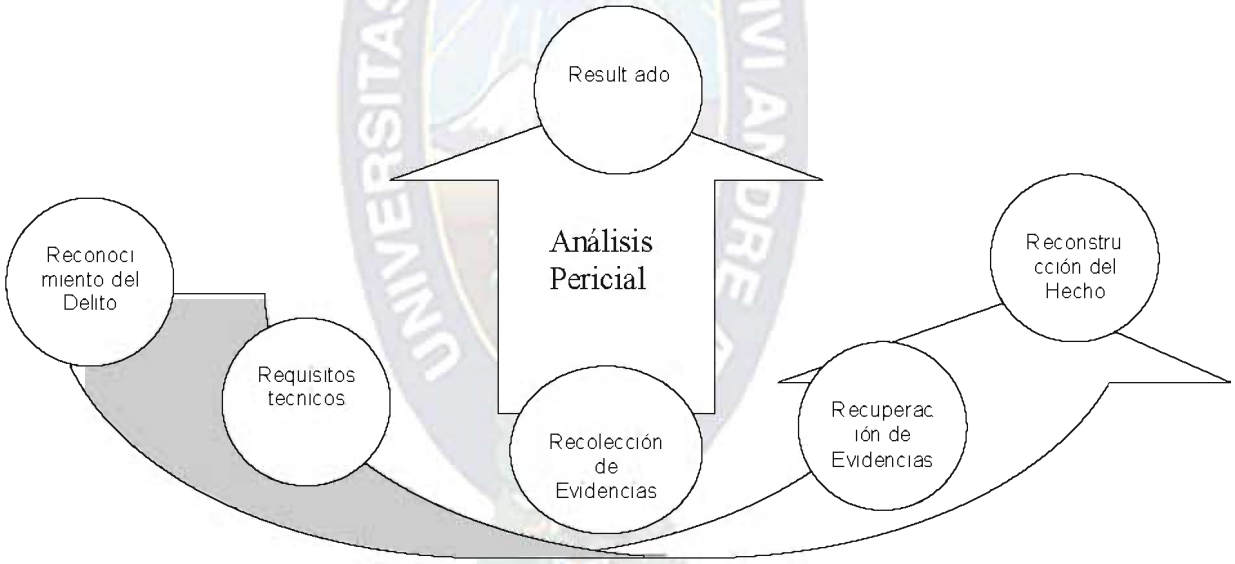
3.2 ANÁLISIS Y SÍNTESIS

Después de haber señalado la etapa de observación, de la investigación criminal se evidencia que para un análisis pericial se tiene que tomar en cuenta el método de las 6R´s mencionado en el capitulo 2 de la presente investigación.

Para el análisis pericial se toma como premisa el establecimiento de la relación inequívoca de tres elementos fundamentales de delito o el crimen: Atacante, víctima y escena del hecho. Esta relación se establece mediante las evidencias y pruebas electrónicas además de las tradicionales como las testificales, documentales, etc.

Para el análisis pericial se aplican todos los conceptos y principios de la Informática Forense. El método de análisis pericial que se plantea, es detallado en la figura 3.1.

Fig. 3.1 Método de análisis pericial



R1.- Reconocimiento del Delito.- Se entiende que ante la detección de un hecho delictivo o alguna conducta contraria a lo establecido, muchas veces sentimos el impulso de castigar al responsable. En este punto el objetivo es analizar si podemos hacerlo o si existe el marco normativo, legal para iniciar un proceso de investigación criminal. Cuando se hace la etapa de reconocimiento, se debe evaluar la pericia forense de una manera similar a los proyectos, correspondiendo la etapa al análisis de pre-factibilidad donde de una manera general se determina si existe o no el delito y si este puede ser investigado, juzgado, probado y castigado.

R2.- Requisitos Tecnicos.- Esta etapa se caracteriza por la evaluación que debe hacerse entre nuestra situación real contra las leyes, reglamentos, estándares internacionales y recomendaciones para la administración de los recursos tecnológicos. Si bien el principal recurso a evaluar es la fuente de la evidencia digital y específicamente las mismas evidencias buscando que satisfaga los parámetros de la seguridad: disponibilidad, confidencialidad, integridad, autenticidad y no repudio, es también importante analizar el nivel de madurez que tenemos implementado.

R3.- Recolección de Evidencias.- En el análisis pericial la etapa de relevamiento se diferencia de la realizada en la escena del hecho por cuanto las fuentes de información se extienden a dispositivos y medios que no necesariamente estaban presentes físicamente en la escena del hecho. En este punto se puede ampliar la investigación a medios de respaldo, documentación, procedimientos, manuales, guías y todo medio que contenga información en diferentes formatos. Incluso permite utilizar métodos de investigación experimental como, cuestionarios, entrevistas, observación y otros con la finalidad de identificar evidencias relacionadas, pertinentes, auténticas y fiables, es por esta razón que es necesario crear un S.E. para poder analizar la recolección de evidencias en la escena del hecho.

R4.- Recuperación de Evidencias.- Mucha de la evidencia obtenida o identificada no estará en formato fácilmente legible: en los medios de almacenamiento magnético, existen datos aparentemente borrados sobre la superficie. Estos datos deben ser recuperados mediante procedimientos especiales. Se debe también aplicar especial cuidado en la recuperación de archivos borrados tomando en cuenta que el borrado por sistema operativo generalmente ocurre marcando el primer carácter con un código especial, marcando su correspondiente cluster en la FAT como no usado lo mismo que en la MFT, pero lo más importante, la información no es borrada físicamente. La información puede ser recuperada usando herramientas especiales o editando la información en formato hexadecimal.

Es importante definir el objetivo de la recuperación, generalmente se puede obtener archivos completos e íntegros, no solamente datos segmentados. Si el atacante no ha utilizado herramientas de borrado seguro sobrescribiendo por n veces los bits, la recuperación de archivos borrados es un proceso que devuelve importante información en la investigación forense. También es importante considerar el formato de grabación del sistema operativo que generalmente es incremental y no tiende a sobrescribir hasta que el disco este lleno.

R5.- Reconstrucción del hecho.- La evidencia recolectada y recuperada no siempre es íntegra. Parte del análisis pericial, es unir todas las partes para construir los supuestos hechos ocurridos. En esta etapa de reconstrucción, el perito trabaja bajo diferentes hipótesis que deberán ser corroboradas y demostradas por las evidencias encontradas. Es en esta etapa que se plantean opciones de Modus Operandi.

En este punto es muy útil aplicar conceptos de Inter criminis para poder seguir las posibles etapas que el atacante ha podido seguir para perpetrar el delito.

R6.- Resultados del trabajo.- El resultado de un trabajo pericial es presentado en formato de dictamen, el mismo que de manera general incluye los siguientes puntos:

i) Introducción.- comprende la designación oficial por parte del fiscal o juez acompañado en anexo el acta de juramento.

ii) Puntos de Pericia (Objetivos).- Aquellos definidos por la instancia legal correspondiente.

iii) Dictamen (Conclusiones).- Conclusiones en función a los puntos de pericia definidos.

iv) Detalle de la Pericia.- Informe técnico en extenso y abundante detalle donde se explique todos los pasos seguidos, análisis de contexto, herramientas utilizadas, documentación analizada, medios revisados, personas entrevistadas, métodos aplicados, sustento técnico y todo aquello que permita opinar sobre el trabajo realizado.

3.3 DEDUCCION

3.3.1 RAZONAMIENTO MEDIATO

Para comprender mejor el presente trabajo y poder obtener conclusiones generales, partiremos por el Razonamiento Mediato de dos casos particulares sobre delitos informáticos cubiertos en las leyes Bolivianas, en sus artículos 363bis y 363ter, que tipifica los Delitos Informáticos.

Razonamiento Mediato para el caso:"Comisión de un delito Informático".

Utilizando como base a la metodología de las 6 R´s, tenemos: Pedro manipula o transfiere datos informáticos ocasionando perjuicio a Juan y es encontrado con material informático que puede usarse como evidencia. La mala manipulación o transferencia de datos informáticos ocasiona perjuicio a terceros conduciendo resultados incorrectos.

R1 Reconocimiento del Delito: Ante la detección de un hecho delictivo, se hace la etapa de reconocimiento y evaluar la pericia forense, para determinar si existe o no el delito y luego ser investigado, probado, juzgado y castigado.

R2 Requisitos Técnicos: Se debe evaluar la situación real contra las leyes para evaluar particularmente la evidencia digital, buscando satisfacer los parámetros de la seguridad: disponibilidad, confidencialidad, integridad, autenticidad.

R3 Recolección de Evidencias: Las fuentes de información se extienden para ampliar la investigación a medios de respaldo, documentación, procedimientos, manuales, guías y todo medio que contenga información en diferentes formatos.

R4 Recuperación de Evidencias: Las evidencias obtenidas e identificadas estarán en formato difícilmente legibles, en medios de almacenamiento magnéticos, existen datos aparentemente borrados, datos que deben ser recuperados mediante procedimientos y herramientas especiales o editando la información en formato hexadecimal.

R5 Reconstrucción del hecho: La evidencia recolectada y recuperada es siempre parte del análisis pericial, es unir todas las partes para construir los supuestos hechos ocurridos, y así determinar el modus operandi del atacante.

R6.- Resultados del trabajo: El resultado de un trabajo pericial es presentado en formato de dictamen, el mismo comprende la designación oficial por parte del fiscal o juez y aquellos definidos por la instancia legal correspondiente, y el dictamen en función a los puntos de pericia definidos, para dar el Informe técnico en extenso y abundante detalle donde se explique todos los pasos seguidos, análisis de contexto, herramientas utilizadas, documentación analizada, medios revisados, personas entrevistadas, métodos aplicados, sustento técnico y todo aquello que permita opinar sobre el trabajo realizado.

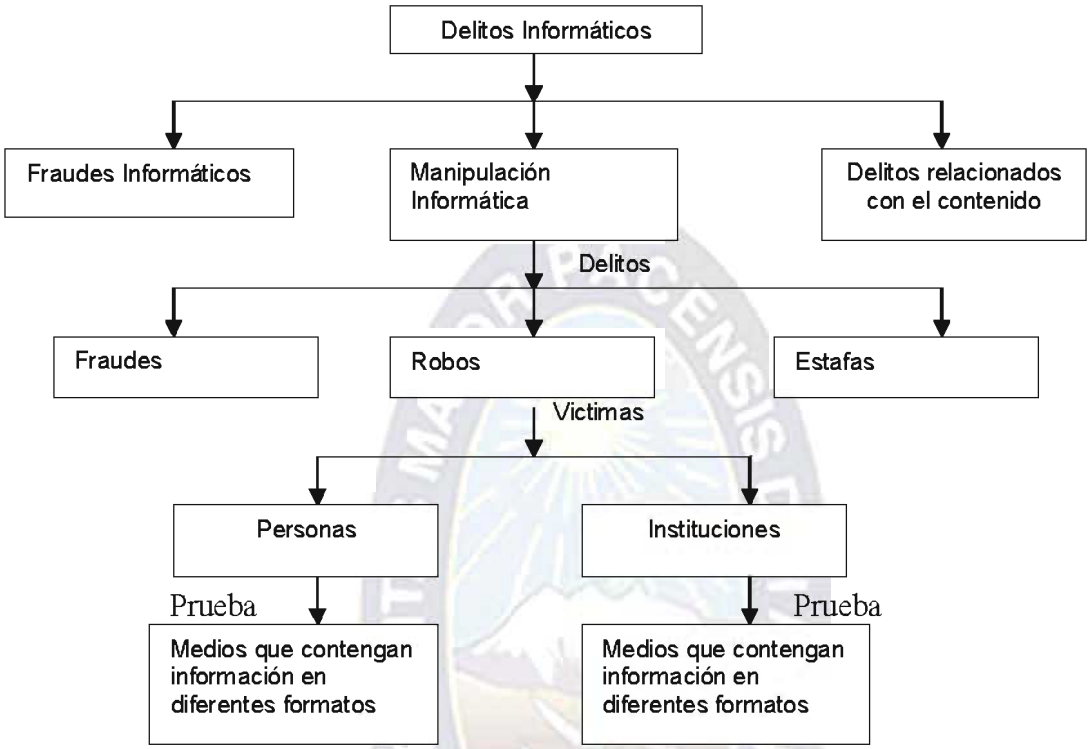
Representación Mediante Árboles De Decisión

Los árboles de decisión resultan totalmente expresivos en la representación del lenguaje propositivo. La deducción mediante árboles de decisión es a la vez una de las modalidades más sencillas y mejores del algoritmo de aprendizaje utilizando un encadenamiento hacia atrás, ya que está orientado hacia el objetivo. Constituye un adecuado medio para el aprendizaje sobre la instauración de procesos judiciales.

Un árbol de decisión es un modelo de predicción el cual tiene unas entradas las cuales pueden ser un objeto o una situación descrita por medio de un conjunto de atributos y a partir de esto devuelve una respuesta la cual en últimas es una decisión que es tomada a partir de las entradas. Al aplicar este modelo de predicción a nuestra deducción, permitirá,

que este proceso resulte sencillo, ya que el estudio que se esta realizando se amolda a la estructura que presenta un árbol de decisión, tal cual se observa en la figura 3.2.

Fig. 3.2 Representación de la Deducción mediante árboles de dedición.



Adquisición De La Información

Para almacenar el conocimiento sobre procesos judiciales y registrar algunas conclusiones intermedias a continuación realizamos la representación de esa información mediante proposiciones para luego efectuar una inferencia deductiva mediante silogismos jurídicos.

ALGUIEN DENUNCIA: victima (personas, empresas,……..)

ALGUIEN ES ACUSADO: persona (delincuente)

Representamos los argumentos empleados con respecto a procesos judiciales mediante Lógica Proposicional y Lógica de Predicados de primer orden para la representación de la información:

Una vez obtenida las proposiciones, la forma clásica de representar el conocimiento en un sistema experto son las reglas. Una regla es una estructura condicional que relaciona lógicamente la información: Definiendo el Dominio de trabajo que se lo realiza a continuación:

Proposiciones (principio razón suficiente)

1: La manipulación informática es un delito Informático sancionado.

2: Los virus informáticos, son delitos Informáticos sancionados.

3: El fraude informático es un delito Informático sancionado.

4: El sabotaje informático es un delito Informático sancionado.

5: La suplantación informática es un delito Informático sancionado.

6: La intercepción de líneas es un delito Informático sancionado.

7: La ingeniería reversa es un delito Informático sancionado.

8: Accesos secretos ilícitos son delitos Informáticos sancionados.

9: El plagio y la piratería son delitos Informáticos sancionados.

10: El terrorismo informático es un delito Informático sancionado.

11: Si se manipulan datos informáticos de entrada se puede cometer el delito de robo.

12: Si se manipulan datos informáticos de entrada se puede cometer el delito de hurto.

13: Si se manipulan datos informáticos de entrada se puede cometer el delito de estafa.

14: Si se manipulan datos informáticos de entrada se puede cometer el delito de fraude.

15: Si se produce copias no autorizados es una falsificación informática.

16. Se utiliza dispositivos electrónicos para realizar copias de seguridad.

17: Existe información digital que es propenso a copias.

18: Un atacante comete delito de tipo informático.

19: Un delito es un robo de información.

20: Un delito es un hurto de informaciones.

21: El atacante tiene relación con su victima.

22: La victima tiene relación con la escena del crimen en el momento en que se cometió el delito.

23: La escena del crimen tiene relación con el atacante en el momento en que se cometió el delito.

24: En la escena del hecho hay evidencias electrónicas.

25: En la escena del hecho hay pruebas electrónicas.

26: Las evidencias electrónicas tienen relación con la victima del delito.

27: Algunas personas manipulan procesamientos de datos informáticos.

28: Algunas personas transfieren datos informáticos en perjuicio de terceros.

29: Algunas personas se apoderan de datos almacenos en una computadora ocasionando perjuicio al titular de la información.

30: Algunas personas se apoderan de datos almacenos en un CD-Rom ocasionando perjuicio al titular de la información.
31: Algunas personas se apoderan de datos almacenos en un USB ocasionando perjuicio al titular de la información.
32 Algunas personas se apoderan de datos almacenos en un disquete ocasionando perjuicio al titular de la información.
33: Algunas personas acceden a datos almacenos en una computadora ocasionando perjuicio al titular de la información.
34: Algunas personas acceden a datos almacenos en un CD-Rom ocasionando perjuicio al titular de la información.
35: Algunas personas acceden a datos almacenos en un USB ocasionando perjuicio al titular de la información.
36: Algunas personas acceden a datos almacenos en un disquete ocasionando perjuicio al titular de la información.
37: El perito informático detecta un hecho delictivo informático.
38: El perito informático evalúa la evidencia digital encontrada en la escena del hecho.
39: El perito informático extiende la investigación.
40: El perito informático obtiene evidencias en formato magnético de la escena del hecho.
41: El perito informático recolecta evidencias incompletas encontradas en la escena del hecho.
42: El perito informático evalúa la evidencia digital obtenidas de la escena del hecho.
43: El perito informático obtiene un resultado de la investigación

Base De Conocimientos

Para almacenar la anterior información, una forma clásica de representar el conocimiento en un sistema experto son las reglas. Una regla es una estructura condicional que relaciona lógicamente la información: Definiendo el Dominio de trabajo, para el primer caso se lo realiza a continuación:

P: es un perito informático
X: es cualquier persona
Y: es cualquier delito cometido por el imputado o delincuente, estipulado en el código penal Boliviano.
E: es cualquier evidencia digital que involucre al imputado o delincuente.
Z: es una victima (persona, institución).

Definición de los Predicados

Manipula_Datos_Informaticos(X,Z), (x) manipula datos informáticos (z) ocasionando perjuicios

Transfiere_Datos_Informaticos(X,Z), (x) transfiere datos informáticos (z) ocasionando perjuicios

Ocasiona_Perjuicios (X,Z), (x) ocasionando perjuicios a (z)

Inicia_proceso(X), a (x) se le inicia un proceso judicial.

Comete _ Delito(X,Z), (x) comete un delito (y) que motiva un proceso judicial.

Realiza_Reconocimiento (P), (p) realiza el reconocimiento de la escena del hecho.

Evalùa_Perica_Forence(P), (p) es el que evalúa la pericia forense.

Prueba _acusadora (E), (e) es una prueba que acusa al imputado o delincuente.

Evalúa (P, E), el (p) evalúa (e)

fuente_de_información (E,P), (e) es una fuente de información importante para el perito

medio_de_respaldo (E,P), la (e) es un medio de respaldo para (p)

medio_de_almacenamiento (E), (e) es un medio de almacenamiento de información

incompleta (E), la (e) encontrada en la escena del hecho no esta completa

une_partes (P, E), el (p) une partes de (e) encontradas en la escena del hecho

trabajo_pericial (P), el (p) realiza un trabajo pericial para determinar el delito

tiene_designación_oficial (P), el (p) tiene una designación oficial para realizar el trabajo de investigación de delito.

posee_un_informe_extenso (P, E), el (p) posee un informe extenso de (E) encontradas en la escena del hecho.

herramienta_especial (H), la (h) es una herramienta especial para el perito informático.

Base De Hechos

Contiene los hechos sobre un problema, en este caso señalamos el caso particular:

"Caso Comisión de un delito Informático". Pedro manipula o transfiere datos informáticos ocasionando perjuicio a Juan y es encontrado con material informático que puede usarse como evidencia. La manipulación o transferencia de datos informáticos ocasionando perjuicio a terceros y conduce a un resultado incorrecto.

Por tanto se tiene los siguientes hechos de un conflicto sobre el 1er caso particular mencionado.

X1 manipula o transfiere datos informáticos ocasionando perjuicio a X2 y es encontrado con material informático que puede usarse como evidencia.

Comete _ Delito(X1)
Manipula_Datos_Informaticos(X1),
Transfiere_Datos_Informaticos(X1),
Ocasiona_Perjuicios (X1, X2)
Material_Informatico(Evidencia)

Motor De Inferencia

Emular el proceso de razonamiento del experto humano o especialista, con la información contenida en la base de conocimientos, la base de hechos para deducir nuevos hechos, mediante el uso de un SILOGISMO JURIDICO:

P1: El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, se le iniciara un proceso judicial

P2: X1 manipula o transfiere datos informáticos ocasionando perjuicio a X2 y es encontrado con material informático que puede usarse como evidencia.

∴ C: Debe instaurarse a X1 un proceso judicial, por manipular o transferir datos informáticos

Formalizando utilizando lógica de predicados de primer orden:

$$\frac{\forall(x);[Manipula\_Datos\_Informatics(X) \Rightarrow Inicia\_Proceso(X)] \quad Manipula\_Datos\_Informatics(t)}{\therefore Instaura\_Proceso\_Judicial(t)}$$

Razonamiento Mediato para el caso: "Pornografía Infantil".

Utilizando como base a la metodología de las 6 R´s, tenemos: Pedro manipula o transfiere imágenes pornográficas de Ana, ocasionando perjuicio a la menor y es encontrado con material pornográfico que puede usarse como evidencia.

R1 Reconocimiento del Delito: En el año 2005, la INTERPOL de Bolivia recibió la primera denuncia que involucró al país en pornografía infantil en la red Internet. En razón a la denuncia recibida por INTERPOL- Bolivia, de su similar Wesbaden de Alemania, que hace referencia a la comisión del delito de pornografía infantil a través del Internet.

R2 Requisitos Técnicos.- Por intermedio de un IP (Protocolo para la comunicación en una red a través de paquetes conmutados, es principalmente usado en Internet), servicio WIFI con fecha de instalación desde el 8 de agosto de 2004. Con esta información,

funcionarios de la FELCC, División Trata y Tráfico de Personas procedieron al Allanamiento de un Inmueble de la Ciudad de La Paz, en el momento del acto se detuvo una persona, quien fue arrestada. El hecho mencionado se encuentra tipificado como Pornografía Infantil, previsto y sancionado en el Art.281 Cuarter del Código Penal, modificado por Ley 3325 de 18 de enero de 2006.

R3.- Recolección de Evidencias.- La mencionada persona después fue arrestada después de haber tardado 20 minutos en abrir la puerta de la habitación, donde se encontraba en el interior del mencionado inmueble, tiempo suficiente en el que pudo borrar o hacer desaparecer las evidencias o datos Informáticos, importante para la averiguación de la verdad para la investigación del caso. El policía Investigador de la FELCC, señala que el file de video fue diseminado a través de la pagina de Internet eDonkey2000, esta información digital contiene imágenes de menores de edad sometidos a actos sexuales que fueron difundidas posiblemente en vivo. Se tomaron fotografías del inmueble donde se encuentra instalada la línea WIFI, que da referencia del equipamiento sofisticado con el que cuenta, Cámaras Filmadoras, Cintas de Video, CDs, Cámara Digital. También se encontraron Numerosas cintas de video en formato VHS y CDs con material pornográfico, Revistas y otros documentos que dan cuenta de la personalidad y gustos del aprendido, además se encontraron, Videos con imágenes pornográficas en vivo, que involucran a menores de edad. El aprendido señala que forma parte de la comunidad EMULE, utilizando el Software del mismo nombre, el mismo permite que todos los usuarios tengan acceso a la información del disco duro donde se encuentra instalado el mencionado programa, y por ende el aprendido, también tiene acceso a todos los discos duros de los demás usuarios, situación que da la probabilidad de que los usuarios de este programa son coautores del delito en cuestión.

R4.- Recuperación de Evidencias.- Las evidencias recavadas al momento de la detención del sujeto: Cámaras Filmadoras, Cintas de Video, CDs, Cámara Digital, VHS y CDs con material pornográfico. Además tomar en cuenta que el aprendido señaló que forma parte de la comunidad EMULE, utilizando el Software del mismo nombre.

R5.- Reconstrucción del hecho.- Mucha de la evidencia recabada se encontraba con innumerables errores y daños que probablemente fueron causados de manera deliberada, además debemos tomar en cuenta el tiempo que el presunto delincuente tuvo para poder contaminar estas evidencias, hecho que nos lleva a determinar la recontracción de esa evidencia dañada.

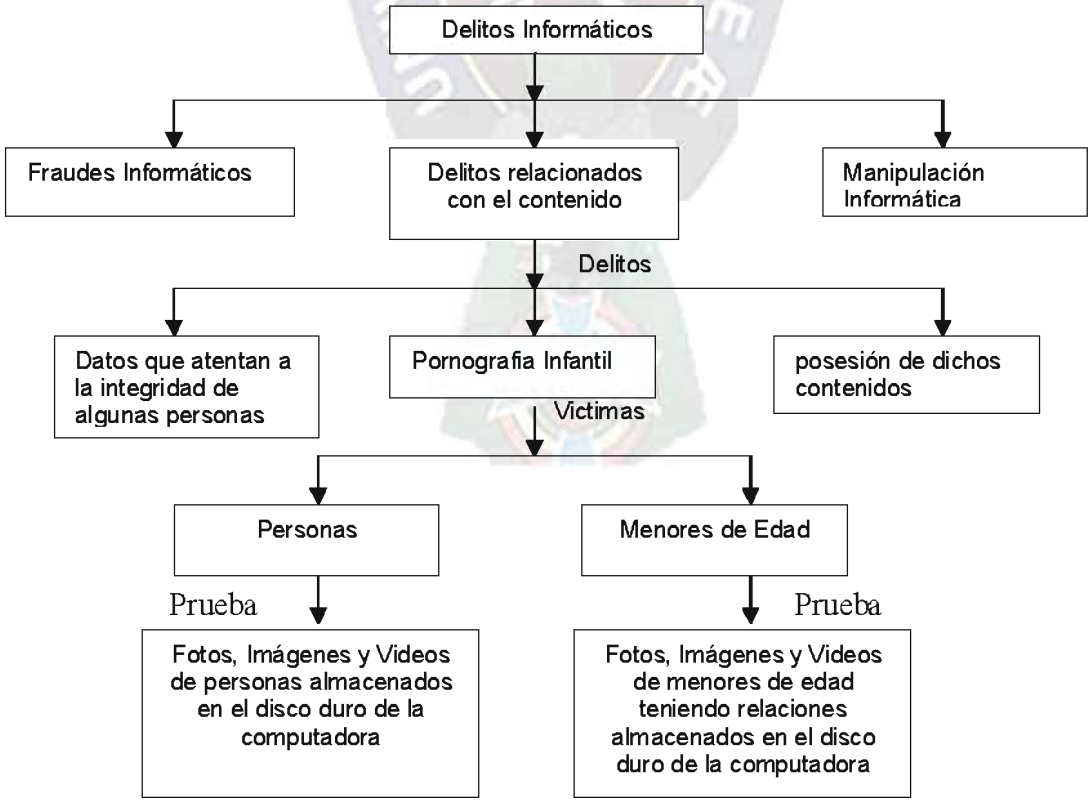
R6.- Resultados del trabajo.- Finalmente luego de un largo periodo de investigación con un juicio de por medio, se declaro al acusado como inocente del delito de pornografía infantil, al no encontrar las suficientes pruebas en su contra, ya q la evidencia recabada, no fue tratada con el debido cuidado y siguiendo los lineamientos para el tratado de esta.

Representación mediante árboles de decisión

Los árboles de decisión resultan totalmente expresivos en la representación del lenguaje propositivo. La deducción mediante árboles de decisión es a la vez una de las modalidades más sencillas y mejores del algoritmo de aprendizaje utilizando un encadenamiento hacia atrás, ya que está orientado hacia el objetivo. Constituye un adecuado medio para el aprendizaje sobre la instauración de procesos judiciales.

Un árbol de decisión es un modelo de predicción el cual tiene unas entradas las cuales pueden ser un objeto o una situación descrita por medio de un conjunto de atributos y a partir de esto devuelve una respuesta la cual en últimas es una decisión que es tomada a partir de las entradas. Al aplicar este modelo de predicción a nuestra deducción, permitirá, que este proceso resulte sencillo, ya que el estudio que se esta realizando se amolda a la estructura que presenta un árbol de decisión, tal cual se observa en la figura 3.3.

Fig. 3.3 Representación de la Deducción mediante árboles de dedición.



Adquisición De La Información

Para almacenar el conocimiento sobre procesos judiciales y registrar algunas conclusiones intermedias a continuación realizamos la representación de esa información mediante proposiciones para luego efectuar una inferencia deductiva mediante silogismos jurídicos.

ALGUIEN DENUNCIA: victima (niños, niñas, adolescentes.....)
ALGUIEN ES ACUSADO: persona (delincuente)

Representamos los argumentos empleados con respecto a procesos judiciales mediante Lógica Proposicional y Lógica de Predicados de primer orden para la representación de la información:

Una vez obtenida las proposiciones, la forma clásica de representar el conocimiento en un sistema experto son las reglas. Una regla es una estructura condicional que relaciona lógicamente la información: Definiendo el Dominio de trabajo que se lo realiza a continuación:

Proposiciones (principio razón suficiente)

1: La manipulación informática es un delito Informático sancionado.
2: El atacante tiene relación con su victima.
3: La victima tiene relación con la escena del crimen en el momento en que se cometió el delito.
4: La escena del crimen tiene relación con el atacante en el momento en que se cometió el delito.
5: En la escena del hecho hay evidencias electrónicas.
6: En la escena del hecho hay pruebas electrónicas.
7: Las evidencias electrónicas tienen relación con la victima del delito.
8: Algunas personas manipulan procesamientos de datos informáticos.
9: Algunas personas acceden a datos almacenos en una computadora ocasionando perjuicio al titular de la información.
10: Algunas personas acceden a datos almacenos en un CD-Rom ocasionando perjuicio al titular de la información.
11: Algunas personas acceden a datos almacenos en un USB ocasionando perjuicio al titular de la información.

12: Algunas personas acceden a datos almacenos en un disquete ocasionando perjuicio al titular de la información.

13: El perito informático detecta un hecho delictivo informático.

14: El perito informático evalúa la evidencia digital encontrada en la escena del hecho.

15: El perito informático extiende la investigación.

16: El perito informático obtiene evidencias en formato magnético de la escena del hecho.

17: El perito informático recolecta evidencias incompletas encontradas en la escena del hecho.

18: El perito informático evalúa la evidencia digital obtenidas de la escena del hecho.

19: El perito informático obtiene un resultado de la investigación

20: La pornografía infantil es un delito Informático sancionado.

21: Si hay actos contra la moral de menores de edad es considerado delito de pornografía infantil.

22: Si los actos contra la moral a menores de edad es difundido vía Web es considerado pornografía infantil.

23: Todas las victimas de pornografía infantil tienen que iniciar un proceso de investigación criminal para sancionar al pedofilo.

24: Si los actos contra la moral a menores de edad es difundido vía Web es considerado pornografía infantil.

25: Si los actos contra la moral a menores de edad es difundido mediante cualquier instrumento digital (CDs, Flash, etc.) es considerado pornografía infantil.

26: Algunos pedofilos son personas con malas intensiones que manipulan los Componentes de las computadoras.

27: El marco normativo Legal sirve para sancionar a los pedofilos.

Base De Conocimientos

Para almacenar la anterior información, una forma clásica de representar el conocimiento en un sistema experto son las reglas. Una regla es una estructura condicional que relaciona lógicamente la información: Definiendo el Dominio de trabajo, para el segundo caso se lo realiza a continuación:

P: es un perito informático

X: es cualquier persona considerado pedofilo, al cual le gusta los niños.

Y: es delito de pornografía infantil

E: es cualquier evidencia digital que involucre al imputado o delincuente.

Z: es menor de edad (niño, niña, adolescente,..), cuando tiene menos de 18 años de edad.

Definición de los Predicados

Delito _ Informático (Y), (y) es una delito informático establecido en el código penal Boliviano.

Sancionado (Y), (y) es sancionado por el código penal Boliviano

Inicia _ proceso(X), a (x) se le inicia un proceso judicial

Victima (Z), (z) es una victima del pedofilo

Gusta(X,Z), a (x) le gusta (z)

Manipula_Imagenes_Pornograficas(X,Z), (x) manipula imágenes pornográficas (z) ocasionando perjuicios

Transfiere_Imagenes_Pornograficas(X,Z), (x)transfiere imágenes pornográficas(z) ocasionando perjuicios

Ocasiona _ perjuicios (X,Z), (x) ocasionando perjuicios a (z)

Inicia _ proceso(X), a (x) se le inicia un proceso judicial.

Comete _ Delito(X, Z), (x) comete el delito (z) que motiva un proceso judicial.

Comete _ Delito(X, Y), (x) comete el delito (y) que motiva un proceso judicial.

Realiza_Reconocimiento (P), (p) realiza el reconocimiento de la escena del hecho.

Evalùa_Perica_Forense (P), (p) es el que evalúa la pericia forense.

Prueba _acusadora (E), (e) es una prueba que acusa al imputado o delincuente.

Evalúa (P, E), el (p) evalúa (e)

fuente_de_información (E,P), (e) es una fuente de información importante para el perito

medio_de_respaldo (E,P), la (e) es un medio de respaldo para (p)

medio_de_almacenamiento (E), (e) es un medio de almacenamiento de información

incompleta (E), la (e) encontrada en la escena del hecho no esta completa

une_partes (P, E), el (p) une partes de (e) encontradas en la escena del hecho

trabajo_pericial (P), el (p) realiza un trabajo pericial para determinar el delito

tiene_designación_oficial (P), el (p) tiene una designación oficial para realizar el trabajo de investigación de delito.

posee_un_informe_extenso (P, E), el (p) posee un informe extenso de (E) encontradas en la escena del hecho.

herramienta_especial (H), la (h) es una herramienta especial para el perito informático.

Base De Hechos

Contiene los hechos sobre un problema, en este caso señalamos el caso particular:

"Caso Pornografía Infantil" Pedro manipula o transfiere imágenes pornográficas de Ana, ocasionando perjuicio a la menor y es encontrado con material pornográfico que puede usarse como evidencia.

Por tanto se tiene los siguientes hechos de un conflicto sobre el 2do caso particular mencionado.

X1 manipula o transfiere imágenes pornográficas ocasionando perjuicio a X2 y es encontrado con material pornográfico que puede usarse como evidencia.

Comete _ Delito(X1)
Manipula_Datos_Informaticos(X1),
Transfiere_Datos_Informaticos(X1),
Ocasiona_Perjuicios (X1,X2)
Material_Pornpografico(Evidencia)

Motor De Inferencia

Emular el proceso de razonamiento del experto humano o especialista, con la información contenida en la base de conocimientos, la base de hechos para deducir nuevos hechos, mediante el uso de un SILOGISMO JURIDICO:

P1: El que con la intención de obtener un beneficio indebido para sí o un tercero, publique videos de pornografía infantil, ocasionando daño a los menores, se le iniciara un proceso judicial

P2: X1 manipula o transfiere imágenes pornográficas ocasionando perjuicio a X2 y es encontrado con material pornográfico que puede usarse como evidencia.

∴ C: Debe instaurarse a X1 un proceso judicial, por manipular o transferir imágenes pornográficas.

Formalizando utilizando lógica de predicados de primer orden:

$$\frac{\forall(x);[Manipula\_Imagenes\_Pornograficas(X) \Rightarrow Inicia\_Proceso(X)] \quad Manipula\_Imagenes\_Pornograficas(t)}{\therefore Instaura\_Proceso\_Judicial(t)}$$

3.4 ANALISIS DE DATOS Y RESULTADOS

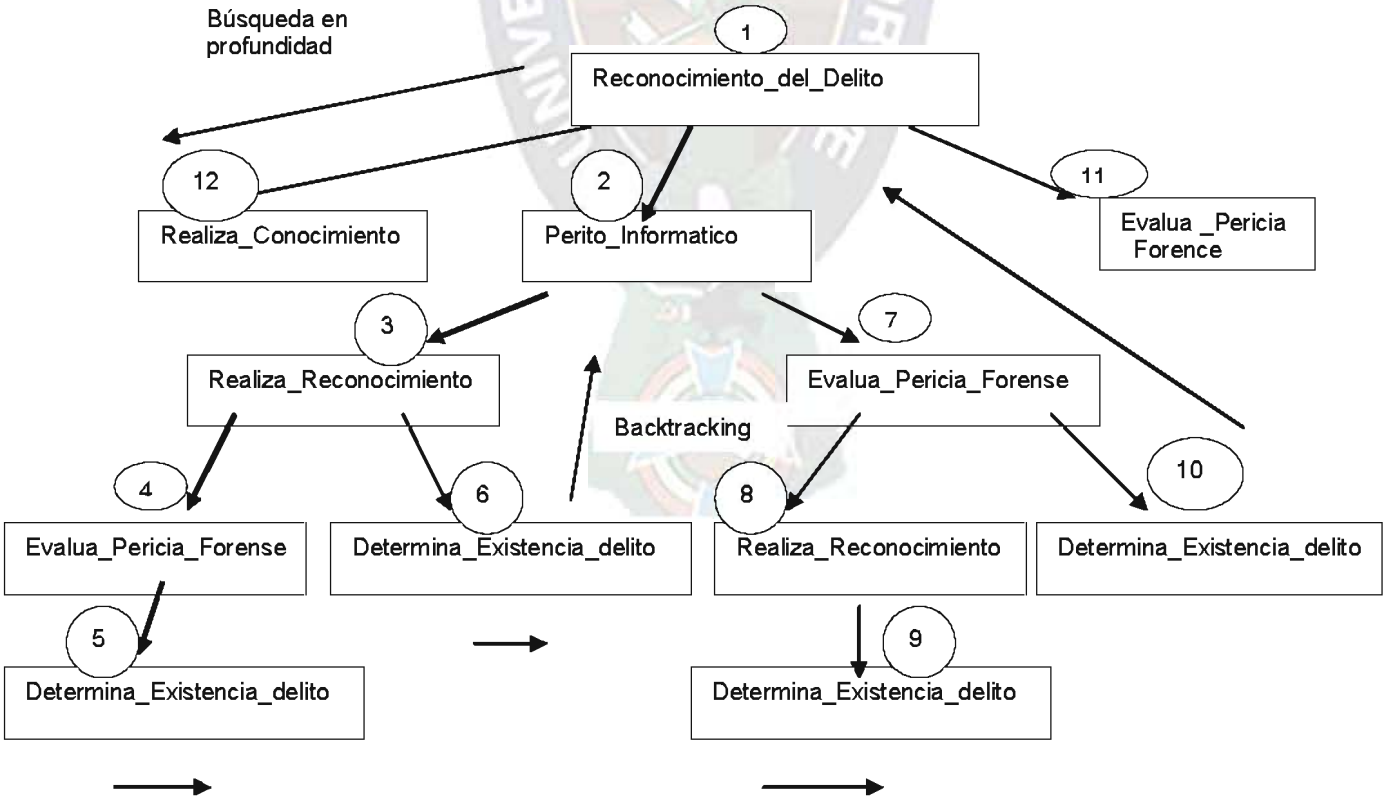
En esta parte del trabajo exponemos el análisis de datos y resultados mediante la representación de árboles de decisión de los dos casos anteriormente expuestos.

La estructura de un árbol de decisión se basa en la base de hechos que es la información introducida por el estudiante, la base de reglas que son las reglas obtenidas de la base de conocimiento y el trazador de explicaciones que es el modulo que proporciona una explicación al estudiante de por qué está haciendo una pregunta y como ha llegado a la conclusión.

La conclusión es la parte fundamental del sistema experto porque este debe inferir, para lo cual se debe hacer uso de métodos de búsqueda, en el presente trabajo se utilizan los métodos de búsqueda en profundidad, amplitud y el de retroceso.

De acuerdo a la Figura 3.4 primero se realiza una búsqueda en profundidad hasta que ya no tenga hechos, entonces luego se utiliza la búsqueda en amplitud para realizar las consultas, una vez concluida para retomar a la regla anterior para seguir con las consultas se utiliza el retroceso. Por lo que se podría decir que se está utilizando un encadenamiento hacia atrás.

Fig. 3.4 Árbol de Búsqueda Binaria para la etapa de Reconocimiento del delito (R1)



Búsqueda en Amplitud

3.4.1 ALGORITMO DE ENCADENAMIENTO HACIA ATRAS

```
Encadenamiento_hacia_atras(hecho:raiz)
   /devuelve valor true o false
    Raíz = hecho
    Regla = raíz
    If para cada hecho de la regla actual que no ha sido analizado
          Se invoca a profundidad(hecho)
          Se invoca a encadenamiento_hacia_atras (raiz)
          Return (true)
End
Profundidad(hecho)
    Se inserta en la cola el hecho
    Regla = hecho
    If para cada hecho no analizado de la regla
          Se invoca a profundidad(hecho)
    Else
          Se invoca a amplitud(regla)
          Se invoca a backtraking(cola)
End
Amplitud(regla)
    Para cada hecho de la regla
    Si este hecho no está analizado entonces
          Se analiza /pregunta/consulta
          Se obtiene hecho_objetivo
          Se almacena en la Base_de_Hechos(hechos_objetivo)
End
Backtraking(cola)
    Se extrae de la cola el último elemento almacenado
    Este elemento será el nuevo hecho
    Se invoca a profundidad(hecho)
End
```

3.5 PROTOTIPO

El prototipo es útil para la interacción entre un sistema experto y un usuario, esta interacción se realiza en un lenguaje natural, y sigue el patrón de la conversación entre seres humanos. Para conducir este proceso de manera aceptable para el usuario es especialmente importante el diseño de interfaz de usuario. Un requerimiento básico de la interfaz es la habilidad de hacer preguntas. Para obtener información fiable del usuario, tenemos que poner especial cuidado en el diseño de las preguntas. Esto puede requerir diseñar el interfaz usando menús o gráficos. A continuación mostramos las pantallas básicas del prototipo del sistema experto:

1.- Pantalla principal del prototipo; Es la primera interfaz entre el sistema experto y el usuario en el cual se le da una breve introducción explicándole de que se trata el sistema experto y a la vez darle la bienvenida y se le invita a ingresar al sistema, como se muestra en la [Fig. 3.5].

Fig. 3.5 Pantalla principal del prototipo

2.- Reconocimiento del Delito (R1).- En esta pantalla observamos que cuando se hace la etapa de reconocimiento, se debe evaluar la pericia forense realizándole algunas preguntas al usuario como se muestra en las figuras: [Fig. 3.6], [Fig. 3.7], [Fig. 3.8].

Fig. 3.6 Reconocimiento del Delito (R 1)

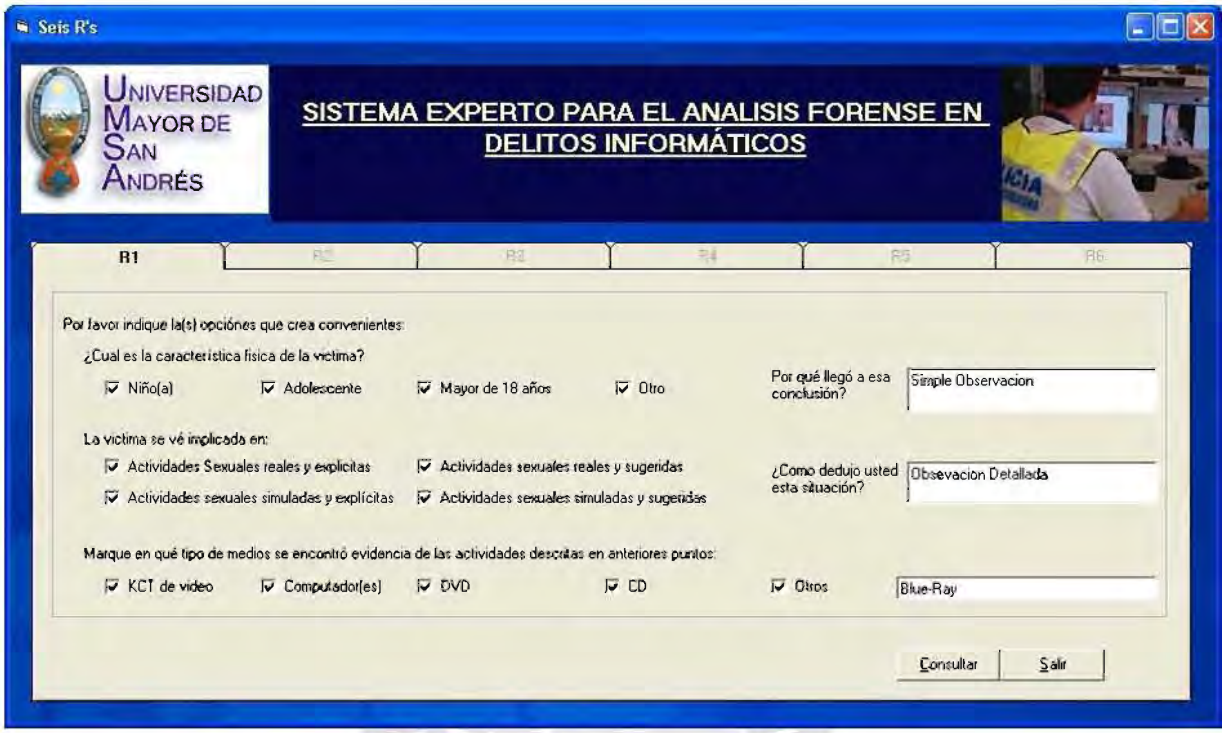


Fig. 3.7 Reconocimiento del Delito (R 1)

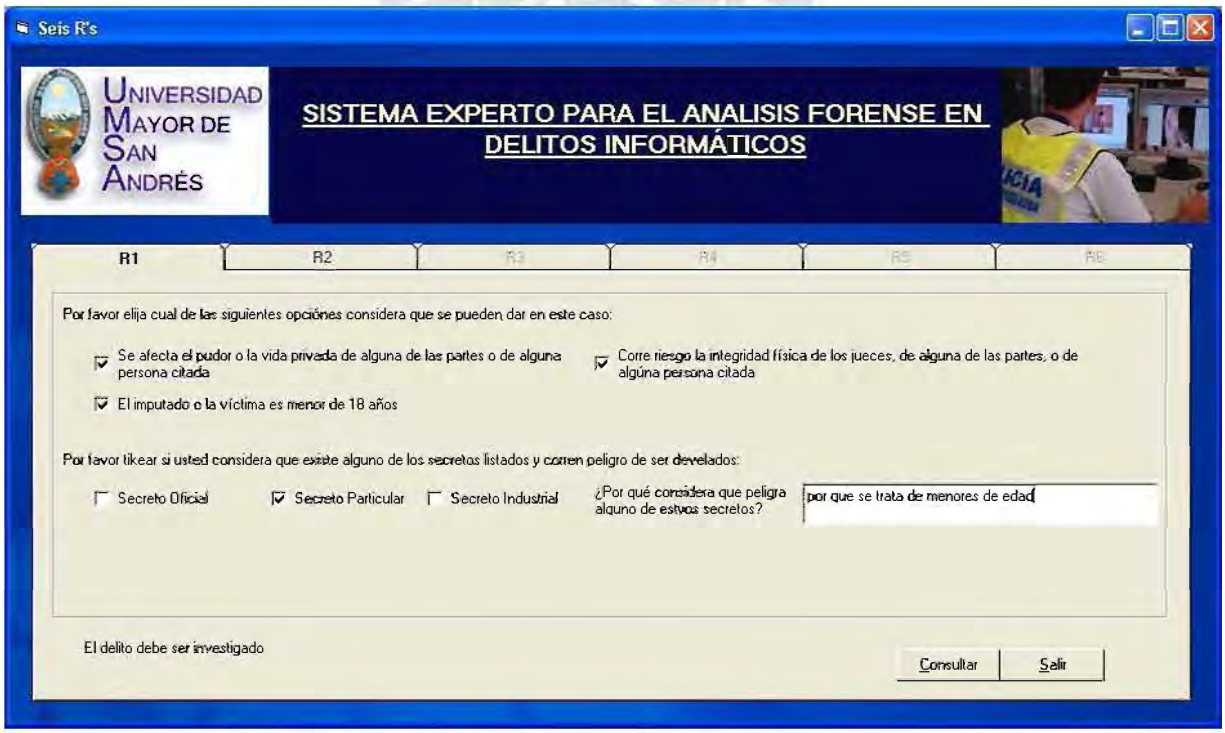
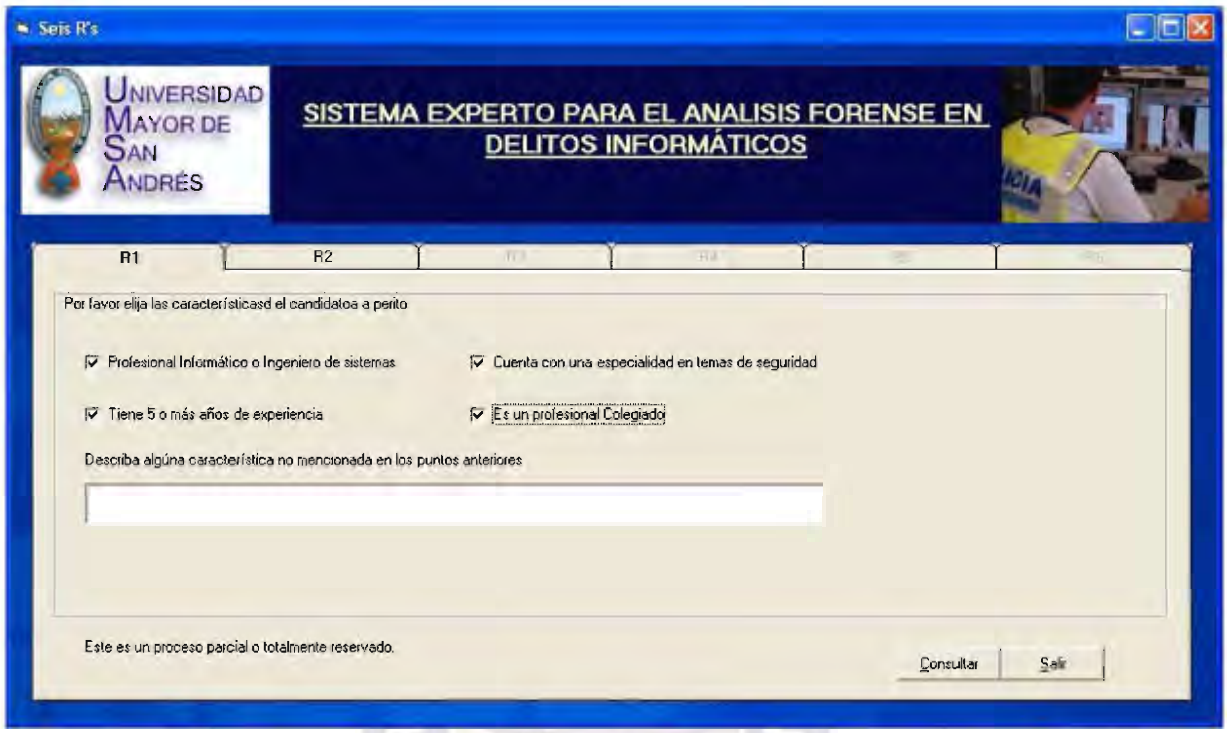


Fig. 3.8 Reconocimiento del Delito (R 1)



3.- Requisitos Técnicos R2; En estas pantallas observamos que esta etapa se caracteriza por la evaluación que debe hacerse. Si bien el principal recurso a evaluar es la fuente de la evidencia digital y específicamente las mismas evidencias buscando que satisfaga los parámetros de la seguridad: disponibilidad, confidencialidad, integridad, autenticidad y no repudio, es también importante analizar el nivel de madurez que tenemos implementado. Se debe evaluar la pericia forense realizándole algunas preguntas al usuario como se muestra en las figuras: [Fig. 3.9], [Fig. 3.10], [Fig. 3.11].

Fig. 3.9 Requisitos Técnicos (R 2)

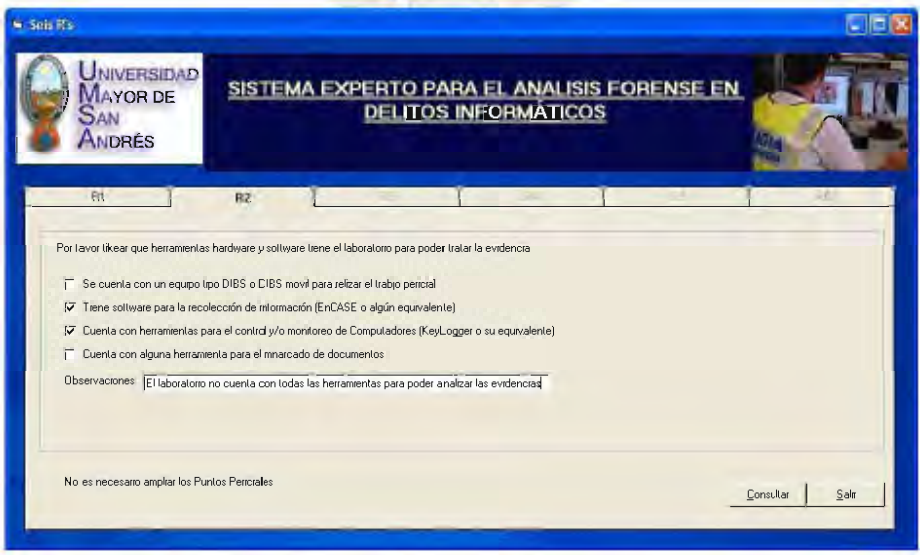


Fig. 3.10 Requisitos Técnicos (R 2)

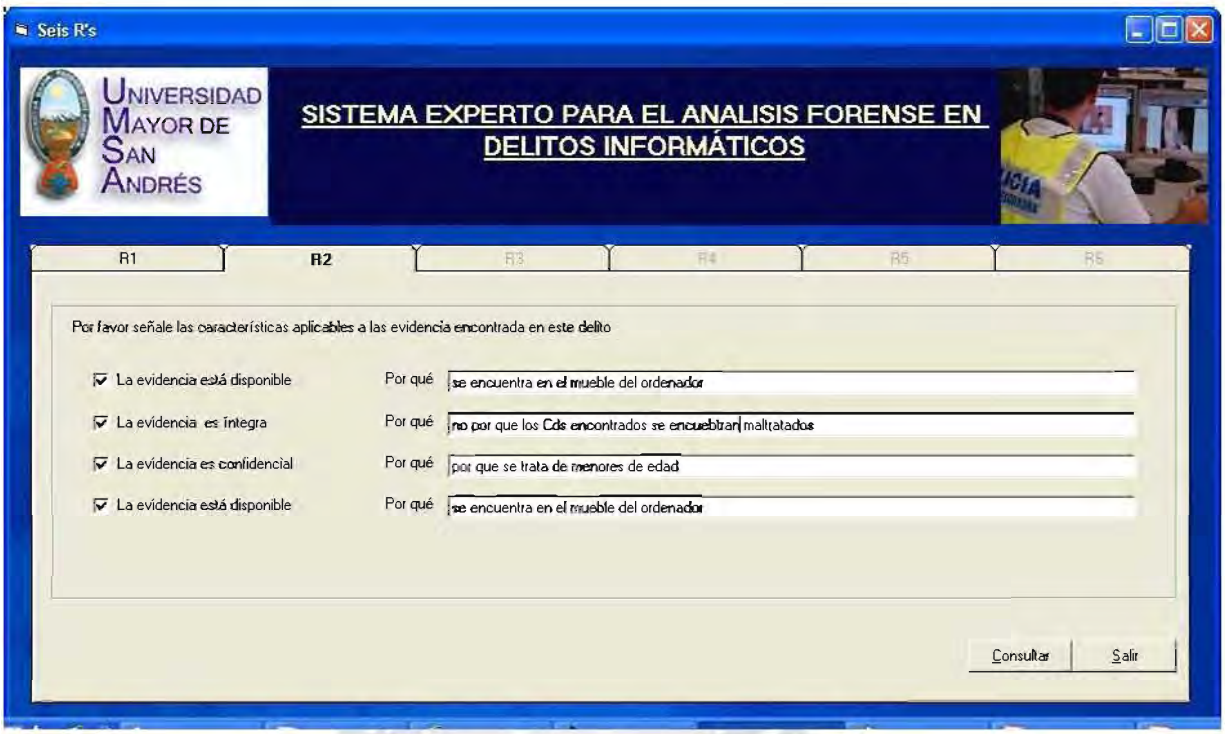
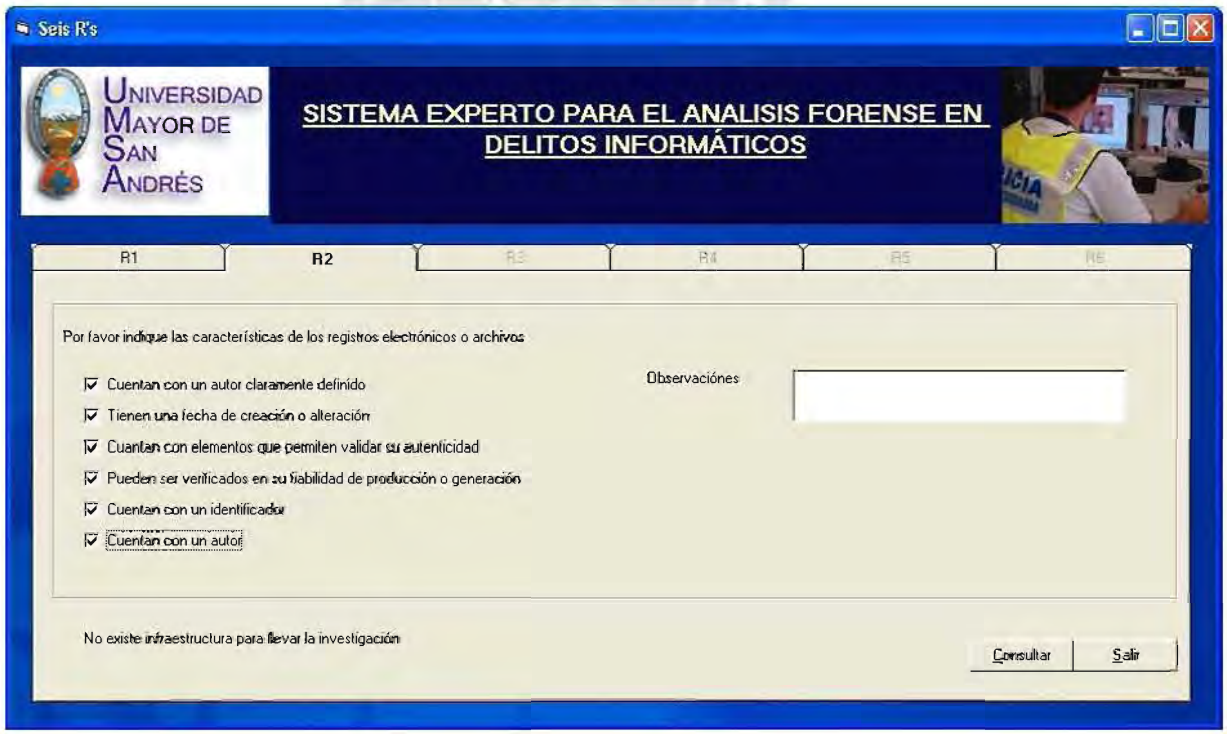


Fig. 3.11 Requisitos Técnicos (R 2)



4 DISCUSION

4.1 CONCLUSIONES

Se ha presentado en este trabajo el diseño de un sistema experto y la implementación del prototipo que coadyuve al perito informático y al estamento policial en la correcta realización del análisis forense en delitos informáticos y así proteger las evidencias del hecho, a través de programación lógica ya que el conocimiento está definido por reglas lógicas mediante la utilización de silogismos jurídicos.

El sistema experto provee y da a conocer los pasos que indiquen la correcta realización del análisis forense en delitos informáticos y así proteger las evidencias del hecho.

La inferencia deductiva mediante silogismos jurídicos para la búsqueda de una posible conclusión de la pericia de un delito informático, tiene una gran utilidad en el aprendizaje del sistema experto.

Se dispone del prototipo para asesorar y colaborar al perito informático, al estamento policial en una determinada situación problemática que sean involucradas para la instauración de un proceso judicial.

La aplicación del lenguaje Visual Basic conjuntamente con prolog, permitieron el desarrollo del prototipo del sistema experto para el análisis forense en delitos informáticos, permitiendo realizar las consultas y dudas al perito informático y al estamento policial de una manera sencilla y práctica, para la ejecución correcta del método de análisis pericial denominado las 6R's.

5 PARTE FINAL

5.1 REFERENCIA BIBLIOGRAFICA

- Grassmann W., 1997, Matematica Discreta y Logica, 1ra Ed., Editorial Prentice Hall, Barcelona, España.
- Giarratano J., 1998, Sistemas Expertos principios y programación, 3ra Ed., Editorial PWS, Estados Unidos.
- García, R., 2004, Ingeniería de Sistemas Expertos, 1ra. Ed., Nueva Librería, Buenos Aires.
- Sampieri, H., 2006, Metodología de la Investigación, 4ta. Ed., Mc Graw Hill, Iztapalapa, México.
- Zegarra, J.V., 2006, 4 Formas de Elaborar una Tesis y Proyectos de Grado, Editorial Juventud, La paz.
- Castillo, E., Gutiérrez, J.M., y Hadi, A.S., 2006, Sistemas Expertos y Modelos de Redes Probabilísticas.
- Choque, J., 2008, Tesis: Sistema Experto Legal de Apoyo a la Solución de Conflictos Laborales.
- Rosales, G, 2008, Manual Informática Forense, 1ra Ed., Yanapti, Bolivia
- <http//:www.laprensa.com.bo/noticias>, [15: 10:0 7pm, lunes, 8 de Diciembre de 2008].
- <http//: www.seas.esEnlaces patrocinados/Silogismo Jurídico>, [10:07:20 am, lunes, 12 de Abril de 2010].
- <http//: www.oas.org/juridico/spanish >, [13:07:20 pm, lunes, 7 de junio de 2010].