UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TESIS DE GRADO

"ANALISIS Y ESTUDIO DE LA APLICABILIDAD DE LA INFORMÁTICA FORENSE EN LOS SISTEMAS DE INFORMACIÓN EN LA POLICIA NACIONAL"

TESIS DE GRADO PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN INFORMATICA Y SISTEMAS COMPUTACIONALES

POSTULANTES:

Pruna Molina Doris Rosario

Tapia Galarza Néstor Rodrigo

LATACUNGA - ECUADOR

2008-2009

AUTORIA

Del contenido de la presente Tesis se responsabiliza en su totalidad los autores:

Egresada Doris Rosario Pruna Molina

C.I. 050240962-6

Egresado Néstor Rodrigo Tapia Galarza

C.I. 050225809-8

Dedicatoria

El fruto de mi trabajo y esfuerzo lo dedico principalmente a mi Madre que con sacrificio, abnegación y amor supo brindarme su apoyo incondicional en todo instante durante este largo recorrido de mi vida, por todos los sabios y buenos consejos que recibí de ella desde niña, por su constancia y cariño que me da a diario me incita a seguir con mis metas.

De manera especial va dedicado a mis Hijas (Nayely Marcela, Romina Estefanía) quienes son es el motivo más grande para salir adelante, y son la fuerza que me inspira para seguir superándome cada día.

A mis hermanas (Janeth, Patricia) por su amistad y cariño sincero, sus conocimientos brindaron un aporte intelectual en el transcurso de mis estudios, siempre estando al pendiente en los momentos que mas las necesitaba.

Doris

Dedicatoria

El fruto de mi trabajo y esfuerzo lo dedico a mis Padres y Hermanos que con sacrificio, y abnegación supieron brindarme su apoyo incondicional en todo instante de mi vida, por todos los buenos consejos que recibí de ellos siempre, por su constancia y cariño sincero he podido seguir cumpliendo mis metas.

Rodrigo

AGRADECIMIENTO

A Dios infinito que hizo posible este trabajo y me brindo la sabiduría necesaria para fortalecer mi mente y espíritu en bien de cumplir lo que me he propuesto.

Un agradecimiento muy especial a mi querida Madre quien me lo ha dado todo, especialmente la oportunidad de seguir una carrera universitaria y poder culminar mi objetivo más anhelado.

A mi esposo (Marcelo) por estar a mi lado apoyándome en todos los momentos que más lo necesito, también debo agradecer a mi tía (Gladys) por su cariño, su bondad y principalmente por su apoyo moral y económico en cada instante difícil y duro de mi vida.

Doris

A mis Padres y hermanos que de una u otra manera colaboraron con un granito de arena para poder cumplir con la realización de este trabajo.

Un agradecimiento eterno a todas las personas muy especiales que han pasado junto a mí, a aquellos amigos que por siempre me brindaron su amistad y confianza, en fin a todas las personas que colaboraron conmigo directa o indirectamente.

Rodrigo

INDICE

INDICE GENERAL

CONTENIDO **Pág.**

CAPITULO II

ANALISIS DE LOS RESULTADOS DE LA INVESTIGACION DE CAMPO

CAPITULO III

PROPUESTA

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

ANEXOS

- ANTEPROYECTO DE TESIS
- FORMATO DE ENCUESTAS AL PERSONAL QUE LABORA EN EL DEPARTAMENTO DE RECURSOS HUMANOS DEL COMANDO DE POLICÍA Nº 13 COTOPAXI
- ESTRUCTURA ORGÁNICA DE LA POLICÍA NACIONAL DEL ECUADOR
- ANÁLISIS FODA DEL DEPARTAMENTO DE PERSONAL DEL COMANDO DE POLICÍA Nº 13 COTOPAXI
- FORMULARIO DE ANALISIS FORENSE

INDICE DE GRAFICOS

GRÁFICO **Pág.**

INDICE DE TABLAS

TABLA **Pág.**

RESUMEN

El propósito de la investigación tiene como objetivo principal el "Análisis y estudio de la aplicabilidad de la informática forense en el sistema de información de la Oficina de Recursos Humanos de la Policía Nacional" ya que actualmente con el adelanto de la tecnología muchas Instituciones han sido victimas de Delitos Informáticos.

El tema de investigación se presenta para dar solución a los problemas de salida de información que existen dentro de esta dependencia, puesto que aún no utilizan una metodología que sea capaz de restringir esta fuga informática.

Para el desarrollo de la Metodología se investigó las necesidades del departamento de Recursos Humanos del Comando de Policía Nº 13 Cotopaxi, a través de las cuales se pudo definir los objetivos propuestos que debe cumplir este análisis, como también las herramientas a utilizarse permitiendo de esta manera elaborar una metodología que emita los resultados esperados ya que se cumplió con los objetivos planteados en el Anteproyecto de Tesis.

Con la realización de las entrevistas al personal del departamento de Recursos Humanos del Comando de Policía Nº 13 Cotopaxi, se determinó que esta dependencia requiere de una Metodología de Informática Forense, para salvaguardar la información que se maneja con el fin de un mejor servicio a esta unidad.

El manejo de esta Metodología dará mayor seguridad a la información que se maneja, evitando que haya fugas o delitos informáticos por lo que el personal de esta Institución podrá llevar sus expedientes o investigaciones de una manera confiada ya que no esta en peligro de ser manipulada o alterada.

INTRODUCCION

El problema que presenta hoy en día El Comando de Policía Nº 13 Cotopaxi, es la falta de una Metodología de Informática Forense para evitar la fuga de importante información que maneja el Departamento de Recursos Humanos de esta unidad de Policía.

Toda institución como lo es El Comando de Policía Nº 13 Cotopaxi, en función de determinados propósitos que se han establecido para las diferentes áreas sustantivas, han sufrido perdida de información de una manera u otra. Una de estas fugas informáticas indudablemente es el uso de información electrónica debido al manejo del Internet.

Para cumplir con todas las actividades normales el departamento de Recursos Humanos del Comando Provincial de Policía Cotopaxi No. 13, ha visto la necesidad de desarrollar una metodología que facilite el ESTUDIO Y ANALISIS DE LA INFORMTICA FORENSE EN EL COMANDO PROVINCIAL DE POLICÍA COTOPAXI No. 13.

A continuación mencionamos los aspectos tratados a lo largo de esta metodología.

El capitulo I, consta el Fundamento Teórico, que incluye: Entorno Generalidades de la Policía Nacional del Ecuador, la Informática Forense, introducción, su importancia, Delitos Informáticos, definición y tipos de los mismos, Redes e Internet.

El capitulo II, Encontramos El Análisis de los resultados de la Investigación de campo, mediante encuestas realizadas al personal policial que labora en la sección administrativa del Comando de Policía Cotopaxi No. 13.

En el capitulo III, tenemos la propuesta de la metodología para el Estudio y Análisis de la informática Forense en el Comando de policía Cotopaxi No. 13, que contiene la introducción, los objetivos con los que se desarrollo la metodología y el impacto que tendrá la misma.

En el capitulo IV, tenemos las conclusiones y recomendaciones a las que a llagado el grupo de investigación con el desarrollo de la metodología.

Por otra parte, consta el glosario de términos y siglas que se constituyen en auxiliar para una mayor comprensión del presente trabajo.

Adicionalmente se presenta las secciones correspondientes a: Bibliografía y Anexos, en el cual consta: el anteproyecto de tesis, el modelo de las encuestas realizadas.

Es necesario mencionar que en cada uno de los capítulos se hallan intrínsecamente presente la información, el trabajo y el esfuerzo por llevar a cabo las cosas de la mejor manera posible, con el único afán de coadyuvar en evitar y controlar el manejo de información en el departamento de Recursos Humanos de la policía nacional acantonada en nuestra ciudad.

Finalmente, se aspira que la siguiente metodológica constituya un verdadero aporte para todas aquellas personas inmersas en el manejo de información el la Policía Nacional.

CAPITULO I

FUNDAMENTO TEORICO

1.1 GENERALIDADES DE LA POLICIA NACIONAL DEL ECUADOR

1.1.1 ANTECEDENTES HISTORICOS.

En efecto en el año de 1822 entramos a formar parte de la Gran Colombia, como Distrito del Sur o Provincia de Quito, en donde ya disponíamos de una nomenclatura de autoridades y empleados para el ejercicio de la función policial, pues con Jefes de Policía, Jueces de Policía, Comisarios, Supervigilantes, Gendarmes y Celadores bajo las dependencia de los Municipios.

Al advenimiento de la República, las funciones policiales y en general la conservación del orden público quedaron en manos de los militares que detentaban el poder en todos los órdenes.

En los primeros años de la República se sostenían los sistemas administrativos implantados por el Libertador Simón Bolívar en la Gran Colombia, en consecuencia, los Municipios conservaban características idénticas a los antiguos cabildos, incluyendo lo relacionado a la intervención policial.

En el año de 1832 el Congreso considerando la necesidad de fijar bases para formar la policía, decreta que los Consejos Municipales, de las Capitales de Departamento elaboren el Reglamento de Policía que regirá en cada uno de ellos, aclarando que la Policía no tendrá ninguna otra intervención que la que le atribuyen las leyes y deberá quedar bajo la responsabilidad de los Consejos Municipales , por lo tanto cesan en sus funciones todos los empleados del ramo y quedan abolidos los nombres de Juez y Jueces de Policía, Supervigilantes, Gendarmes y Celadores, subsistiendo solamente los de Comisarios y Dependientes.

La Asamblea Constituyente de 1843, dicta una nueva ley de Régimen Político y Administrativo, según la cual se centralizaba en el Poder Ejecutivo la mayor parte de las atribuciones que correspondían a los Municipios y se establece que los Ministros de Gobierno y Relaciones Exteriores se encarguen de todo lo que se refiere a la Policía de todos los pueblos. Esto viene a constituir un primer paso para la organización de la Policía como Institución Nacional.

En febrero de 1848, es aprobado por el Ejecutivo el Reglamento expedido por el Municipio de Quito, sentándose bases para una función policial menos localista,

pues comparte responsabilidades con el poder central. Se establece que la Policía de cada cantón estará a cargo de un Jefe de Policía, un Comisario, Celadores y Empleados, el Jefe de Policía será la autoridad máxima y será nombrado por el Ejecutivo. LA Policía deja de ser dependencia administrativa municipal y se constituye una entidad casi independiente con funciones especificas, tales como : las de perseguir a sociedades secretas o sospechosas de cualquier crimen, cuidar que no corran rumores falsos que alarmen a la ciudadanía, los extranjeros que llegaren deberán presentarse con sus pasaportes ante el Jefe de Policía, no deberá permitirse ningún espectáculo, diversión sin licencia de la Policía, prohibición de actos o expresiones contrarios a la religión, a la moral y a las buenas costumbres, entre otras.

A principios de 1965 se produce la anexión definitiva del Ecuador a la Organización Internacional de Policía Internacional INTERPOL.

La Policía Nacional ha venido año a año alcanzando logros cada vez más significativos, gracias al trabajo tesonero y sacrificado de todos sus miembros, lo que ha merecido reconocimiento de los Poderes del Estado, la Prensa y la Ciudadanía, que ven en ella a la Institución noble garantía de la paz y seguridad ciudadana.

1.1.2 MISION DE LA POLICIA NACIONAL DEL ECUADOR

Brindar servicios de seguridad ciudadana, con calidad y ética, en el marco de la legislación vigente, respetando la dignidad humana, para que todos los actores sociales puedan convivir en paz y ejercer con libertad sus derechos.

1.1.3 VISION DE LA POLICIA NACIONAL DEL ECUADOR

La Policía Nacional del Ecuador, será una Institución sólida, confiable, efectiva y eficiente, de servicio a la ciudadanía, sustentada sobre principios morales, éticos y jurídicos, dotada de una educación permanente, tecnología moderna, y estructura adecuada; recurso humano calificado y comprometido con los intereses de la comunidad, que contribuya a mejorar los niveles de competitividad para el desarrollo integral del país, a fin de enfrentar con éxito los retos del futuro.

1.1.4 FUNCIONES DE LA POLICIA NACIONAL DEL ECUADOR

- Modernizar y fortalecer la capacidad operativa de las Unidades Policiales para reducir los niveles de inseguridad ciudadana.
- Reestructurar los sistemas operativos policiales, acorde a las demandas ciudadanas e índices delincuenciales.
- Reducir los tiempos de respuesta a los auxilios solicitados por la comunidad.

- Fortalecer la Policía Comunitaria con la participación de las autoridades locales y la comunidad.
- Institucionalizar mecanismos de participación de la comunidad en programas de seguridad ciudadana.
- Incorporar indicadores de gestión a todas las actividades operativas de los servicios policiales.
- Estandarizar la aplicación de los procedimientos policiales, fundamentados en la normatividad vigente y difundirlos a nivel nacional.

1.1.5 ACTIVIDAD DE LA INSTITUCION

- Policía humanizada al servicio de la comunidad.
- Motivación y satisfacción laboral de los miembros para mejorar su desempeño.
- Cambio de actitud y mentalidad para atender las demandas de los actores sociales.
- Formación y capacitación integral.
- Nacionalización de procesos para mejorar la atención al público.
- Gestión institucional sin influencias políticas o religiosas; sin discrimen racial o de género.

1.1.6 SISTEMA ORGANIZACIONAL DE LA POLICIA NACIONAL DEL ECUADOR.

VER ANEXO 2

1.2 INFORMATICA FORENSE

1.2.1 INTRODUCCION

La informática forense está adquiriendo una gran importancia dentro del área de la información electrónica, esto debido al aumento del valor de la información y/o al uso que se le da a ésta, al desarrollo de nuevos espacios donde es usada (por Ej. El Internet), y al extenso uso de computadores por parte de las compañías de negocios tradicionales (por Ej. Transacciones bancarias). Es por esto que cuando se realiza un crimen, muchas veces la información queda almacenada en forma digital. Sin embargo, existe un gran problema, debido a que los computadores guardan la información de forma tal que no puede ser recolectada o usada como prueba utilizando medios comunes, se deben utilizar mecanismos diferentes a los tradicionales. Es de aquí que surge el estudio de la computación forense como una ciencia relativamente nueva.

Resaltando su carácter científico, tiene sus fundamentos en las leyes de la física, de la electricidad y el magnetismo. Es gracias a fenómenos electromagnéticos que la información se puede almacenar, leer e incluso recuperar cuando se creía eliminada.

La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales.

1.2.2 IMPORTANCIA DE LA INFORMÁTICA FORENSE

"High-tech crime is one of the most important priorities of the Department of Justice"

Con esta frase podemos ver cómo poco a poco los crímenes informáticos, su prevención, y procesamiento se vuelven cada vez más importantes. Esto es respaldado por estudios sobre el número de incidentes reportados por las empresas debido a crímenes relacionados con la informática.

1.3 DELITOS INFORMÁTICOS

1.3.1 DEFINICIÓN

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figurar típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún".

1.3.1.1 HACKER:

Es una persona muy interesada en el funcionamiento de sistemas operativos; aquel curioso que simplemente le gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quiénes lo inventaron. La palabra es un término ingles que caracteriza al delincuente silencioso o tecnológico. Ellos son capaces de crear sus propios software para entrar a los sistemas. Toma su actividad como un reto intelectual, no pretende producir daños e incluso se apoya en un código ético:

El acceso a los ordenadores y a cualquier cosa le pueda enseñar como funciona el mundo, debería ser limitado y total. Toda la información deberá ser libre y gratuita.

Desconfía de la autoridad. Promueve la descentralización.
Los Hackers deberán ser juzgados por sus hacks, no por criterios sin sentido como calificaciones académicas, edad, raza, o posición social.

Esta visión de ellos no se ajusta a la realidad, que hay una fina línea entre actuar así y producir un daño o caer en la tentación de robar información. Por no hablar que en numerosas legislaciones, el mero hecho de colocarse en un sistema ya es delito . A pesar de ello hay quiénes opinan que el acceso a sí mismo a un sistema, no puede ser considerado a priori como delito, si no se dan los requisitos, objetivos y subjetivos que configuran los tipos penales correspondientes.

Estos suelen ser verdaderos expertos en el uso de las computadoras y por lo general rechazan hacer un uso delictivo de sus conocimientos, aunque no tienen reparo en intentar acceder a cualquier máquina conectada a la red, o incluso penetrar a una Intranet privada, siempre con el declarado fin de investigar las defensas de estos sistemas, sus lados débiles y "anotarse" el mérito de haber logrado burlar a sus administradores. Muchos de ellos dan a conocer a sus víctimas los "huecos" encontrados

en la seguridad e incluso sugieren cómo corregirlos, otros llegan a publicar sus hallazgos en revistas o páginas Web de poder hacerlo.

La voluntad de divertirse generalmente se traduce por paseos por el sistema haciendo alarde de su intromisión. Es lo que se ha llamado JOY RIDING, O PASEOS DE DIVERSIÓN.

Características De esta clase de hacking: el Hacker es una persona experta en materias informáticas y con edad fluctuante entre los 15 y 25 años de edad es por ello que esta delincuencia se ha denominado "SHORT PANTS CRIMES", es decir, en pantalones cortos, su motivación no es la de causar daños sino de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos.

1.3.1.2 CRACKER:

Personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas. El Pirata informático.
Tiene dos variantes:

El que penetra en un sistema informático y roba información o se produce destrozos en el mismo.

El que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anti-copia.
Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.

1.3.1.3 PHREAKER:

Es el especialista en telefonía(Cracker de teléfono).Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

1.3.1.4 LAMMERS:

Aquellos que aprovechan el conocimiento adquirido y publicado por los expertos. Si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar mas allá. Generalmente, son despreciados por los verdaderos hackers que los miran en menos por su falta de conocimientos y herramientas propias. Muchos de los jóvenes que hoy en

día se entretienen en este asunto forman parte de esta categoría.

1.3.1.5 GURUS:

Son los maestros y enseñan a los futuros Hackers. Normalmente se trata se personas adultas, me refiero a adultas, porque la mayoría de Hackers son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma hay, para enseñar a o sacar de cualquier duda al joven iniciativo al tema. Es como una especie de profesor que tiene a sus espaldas unas cuantas medallitas que lo identifican como el mejor de su serie. El guru no esta activo, pero absorbe conocimientos ya que sigue practicando, pero para conocimientos propios y solo enseña las técnicas más básicas.

1.3.1.6 BUCANEROS:

En realidad se trata de comerciantes. Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago. Por ello, los bucaneros no existen en la Red. Solo se dedican a explotar este tipo de tarjetas para canales de pago que los Hardware Crackers, crean. Suelen ser personas sin ningún tipo de conocimientos ni de electrónica ni de informática, pero si de negocios. El bucanero compra al CopyHacker y revende el producto bajo un nombre comercial. En realidad es un empresario con mucha aficción a ganar dinero rápido y de forma sucia.

1.3.1.6 NEWBIE:

Traducción literal de novato. Es alguien que empieza a partir de una WEB basada en Hacking. Inicial-mente es un novato, no hace nada y aprende lentamente. A veces se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la pagina WEB para seguir las instrucciones de nuevo.

Es el típico tipo, simple y nada peligroso. Está apartado en un rincón y no es considerado.

1.3.1.7 TRASHING:

Esta conducta tiene la particularidad de haber sido considerada recientemente en relación con los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Estas acciones corresponden a una desviación del procedimiento conocido como reingeniería social.

Estas actividades pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada. Esta minuciosa distinción de sujetos según su actuar no son útiles para tipificar el delito pues son sujetos indeterminados, no requieren condición especial; mas vale realizar dicha diferenciación para ubicarnos en el marco en que se desenvuelven y las características de su actuar, favoreciendo con ello el procedimiento penal que se deberá llevar a cabo luego de producirse el delito.

1.3.2 TIPOS DE DELITOS INFORMÁTICOS

1.3.2.1 MANIPULACIÓN DE LOS DATOS DE ENTRADA.

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

1.3.2.2 LA MANIPULACIÓN DE PROGRAMAS.

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

1.3.2.3 MANIPULACIÓN DE LOS DATOS DE SALIDA.

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica de salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

1.3.2.4 FALSIFICACIONES INFORMÁTICAS.

1.3.2.4.1 Como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.

1.3.2.4.2 Como instrumentos. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

1.3.2.5 Daños o modificaciones de programas o datos computarizados.

1.3.2.5.1Sabotaje informático. Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. las técnicas que permiten cometer sabotajes informáticos son:

1.3.2.5.2 Virus. Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

1.3.2.5.3 Gusanos. Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

1.3.2.5.4 Bomba lógica o cronológica. Exige conocimientos ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba.

1.3.2.5.5 Acceso no autorizado a servicios y sistemas informáticos.

Es el acceso no autorizado a sistemas informáticos por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

1.3.2.5.6 Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del

sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

1.4 REDES

1.4.1 DEFINICIONES

Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos y recursos sin importar la localización física de los distintos dispositivos. A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas.

Los ordenadores suelen estar conectados entre sí por cables. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites.

Cada dispositivo activo conectado a la red se denomina *nodo*. Un dispositivo activo es aquel que interviene en la comunicación de forma autónoma, sin estar controlado por otro dispositivo. Por ejemplo, determinadas impresoras son autónomas y pueden dar servicio en una red sin conectarse a un ordenador que las maneje; estas impresoras son nodos de la red.

Dependiendo del territorio que abarca una red se clasifican en:

• **LAN:** Local Area Network. Está constituida por un conjunto de ordenadores independientes interconectados entre sí, pueden comunicarse y compartir recursos. Abarcan una zona no demasiado grande, un edificio o un campus.

• **WAN**: Wide Area Network, comprenden regiones más extensas que las LAN e incluso pueden abarcar varios países.

También un conjunto de redes puede conectarse entre sí dando lugar a una red mayor.

1.4.2 DISPOSITIVOS DE RED

1.4.2.1 UN ROUTER O GATEWAY es un dispositivo conectado en la red que une redes distintas. Por tanto, sus funciones son:

Adaptar la estructura de información de una red a la otra (datagramas con tamaños y estructuras distintas)

- Pasar información de un soporte físico a otro (distintas velocidades y soportes físicos)
- Encaminar información por la ruta óptima
- Reagrupar la información que viene por rutas distintas

1.4.2.2 CONTRAFUEGOS

Un cortafuegos o firewall es un software destinado a garantizar la seguridad en sus comunicaciones vía Internet al bloquear las entradas sin autorización a su computadora y restringir la salida de información.

En otras palabras, un firewall es un mecanismo para proteger redes confiables cuando se conectan a redes no confiables (como Internet), ayuda a prevenir el acceso de intrusos a su computadora, ya sea por medio de Internet o por medio de una red Interna; además de controlar la entrada o salida de datos, no autorizada, a su sistema y bloquear algunos programas troyanos y otras aplicaciones que quieren dañar el sistema.

Todo el tráfico desde dentro hacia fuera y viceversa debe pasar por el firewall. Sólo al tráfico autorizado, definido por las políticas de seguridad, se le permite el paso.

1.4.2.3 UN BRIDGE une dos segmentos lógicos distintos de una misma red física. Dicho de otro modo: divide una red en dos subredes lógicas. El empleo de un bridge aísla el tráfico de información innecesaria entre segmentos, de forma que reduce las colisiones.

1.4.2.4 UN REPEATER amplifica la señal, permite usar longitudes mayores de cable.

1.5. INTERNET

1.5.1 UNA RED DE REDES

Internet es una red mundial de redes de ordenadores, que permite a éstos comunicarse de forma directa y transparente, compartiendo información y servicios a lo largo de la mayor parte del mundo.

Para que dos ordenadores conectados a Internet puedan comunicarse entre sí es necesario que exista un lenguaje en común entre los dos ordenadores. Este lenguaje en común o protocolo es un conjunto de convenciones que determinan cómo se realiza el intercambio de datos entre dos ordenadores o programas.

1.5.2 CLIENTES Y SERVIDORES

El modelo cliente-servidor es uno de los mecanismos habituales para el intercambio de servicios e información en las redes de ordenadores y, en particular en Internet.

Cuando se utiliza un servicio en Internet como visualizar un documento de hipertexto se establece un proceso en el cual entran en juego dos partes:

• **El programa cliente:** el usuario ejecuta en el ordenador local una aplicación que se pone en contacto con el ordenador remoto para solicitar la información deseada.

• **El programa servidor:** es el programa del ordenador remoto que provee la información requerida por el usuario local.

Los términos cliente y servidor se usan también para referirse a los ordenadores en los que se ejecutan esos programas:

• Ordenador cliente: el ordenador que solicita un servicio

• Ordenador servidor: el que responde al pedido

1.5.3 SEGURIDADES DE INTERNET

Intentar comunicar un secreto en un entorno con millones de testigos potenciales como Internet es difícil, y la probabilidad de que alguien escuche una conversación entre dos interlocutores se incrementa conforme lo hace la distancia que las separa. Dado que Internet es verdaderamente global, ningún secreto de valor debería ser comunicado a través de ella sin la ayuda de la criptografía.

En el mundo de los negocios, información como números de tarjetas de crédito, autenticaciones de clientes, correos electrónicos e incluso llamadas telefónicas acaba siendo enrutada a través de Internet. Ya que gran parte de esta información corporativa no debe ser escuchada por terceras personas, la necesidad de seguridad es obvia.

Sin embargo, la Seguridad en Internet no es sólo una preocupación empresarial.

Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de privacidad no desaparece. La privacidad no es sólo confidencialidad, sino que también incluye anonimato. Lo que leemos, las páginas que visitamos, las cosas que compramos y la gente a la que hablamos representan información que a la mayoría de las personas no les gusta dar a conocer. Si las personas se ven obligadas a exponer información que

normalmente desean ocultar por el hecho de conectarse a Internet, probablemente rechazarán todas las actividades relacionadas con la red.

- **Gestión de claves** (incluyendo negociación de claves y su almacenamiento): Antes de que el tráfico sea enviado/recibido, cada router/cortafuegos/servidor (elemento activo de la red) debe ser capaz de verificar la identidad de su interlocutor.
- **Confidencialidad**: La información debe ser manipulada de tal forma que ningún atacante pueda leerla. Este servicio es generalmente prestado gracias al cifrado de la información mediante claves conocidas sólo por los interlocutores.
- **Imposibilidad de repudio**: Ésta es una forma de garantizar que el emisor de un mensaje no podrá posteriormente negar haberlo enviado, mientras que el receptor no podrá negar haberlo recibido.
- **Integridad**: La autenticación valida la integridad del flujo de información garantizando que no ha sido modificado en el tránsito emisor-receptor.
- **Autenticación**: Confirma el origen/destino de la información -corrobora que los interlocutores son quienes dicen ser.
- **Autorización**: La autorización se da normalmente en un contexto de autenticación previa. Se trata un mecanismo que permite que el usuario pueda acceder a servicios o realizar distintas actividades conforme a su identidad.

Dependiendo de qué capa de la pila de protocolos OSI se implemente la seguridad, es posible prestar todos o sólo algunos de los servicios mostrados

anteriormente. En algunos casos tiene sentido proveer algunos de ellos en una capa y otros en otra diferente.

1.5.4 DIRECCIONES IP

Para que dos ordenadores, situados en cualquier parte del mundo, puedan comunicarse entre sí, es necesario que estén identificados de forma conveniente a través de una dirección.

Cada ordenador conectado a Internet tiene una dirección exclusiva y que lo distingue de cualquier otro ordenador del mundo, llamada **dirección IP** o **número IP**.

Dos ordenadores no pueden tener el mismo número IP, pero un ordenador sí puede tener varios números IP(dot quad notation*).*

Las direcciones IP están formadas por cuatro números separados por puntos, cada uno de los cuales puede tomar valores entre 0 y 255. Por ejemplo:
125.64.250.6

Cada vez que se ejecuta una aplicación para utilizar un servicio en Internet, el software de comunicaciones del ordenador local necesita conocer la dirección IP del ordenador remoto con el que se quiere entrar en contacto.

Como memorizar números resulta complicado existe un sistema de identificación por nombres.

1.6 PUERTOS DE ENLACE.

En informática, una puerta de enlace o gateway puede ser:

1. Un dispositivo que traduce un protocolo a otro. En una red traduce paquetes desde un protocolo a otro. Una aplicación que convierte comandos o datos de un formato hacia otro, o de una formato de e-mail a otro, o por ejemplo, un Gateway de VoIP, [1] o Voz sobre IP Gateway, que es un dispositivo de red que ayuda a convertir la voz y llamadas de fax, en tiempo real, entre una red IP y la red telefónica pública conmutada (RTPC).

2. Un dispositivo que actúa como nexo entre dos redes que usan el mismo protocolo, es decir, una puerta de enlace predeterminada.

Una puerta de enlace o gateway es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa o podría decirse una dirección pública. Se podría decir que un gateway, o puerta de enlace, es un

router u ordenador a través del que se enruta la conexión a Internet de un equipo y que conecta dos redes. La dirección IP De un gateway (o puerta de enlace) a menudo se parece a 192.168.1.1 o 192.168.0.1 y utiliza algunos rangos predefinidos, 127.x.x.x, 10.x.x.x, 172.x.x.x, 192.x.x.x, que engloban o se reservan a las redes locales (véase red local). Además se debe notar que necesariamente un equipo que haga de puerta de enlace en una red, debe tener 2 tarjetas de red. Al escribir el número de la puerta de enlace te pide una dirección y una contraseña, que al coincidir se abre una página donde muestra la información del modem, WAN y LAN, que luego se pueden configurar.

La puerta de enlace o más conocida por su nombre en inglés como "Default Gateway", es la ruta por defecto que se le asigna a un equipo y tiene como función enviar cualquier paquete del que no conozca por que interfaz enviarlo y no este definido en las rutas del equipo, enviando el paquete por la ruta por defecto.

1.7 WORLD WIDE WEB

En informática, **World Wide Web** (o la "Web") o **Red Global Mundial** es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet. Con un navegador Web, un usuario visualiza páginas web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.

La Web fue creada alrededor de 1989 por el inglés Tim Berners-Lee y el belga Robert Cailliau mientras trabajaban en el CERN en Ginebra, Suiza, y publicado

en 1992. Desde entonces, Berners-Lee ha jugado un papel activo guiando el desarrollo de estándares Web (como los lenguajes de marcado con los que se crean las páginas Web), y en los últimos años ha abogado por su visión de una Web Semántica.

CAPITULO II

ANALISIS DE LOS RESULTADOS DE LA INVESTIGACION DE CAMPO

2.1 ESTADISTICA DESCRIPTIVA

2.2 METODOLOGIA

Con el propósito de conocer la opinión de los jefes del Comando Nº13 de la Policía Nacional en lo que se refiere a la Informática Forense, se aplicara encuestas, cada una enfocada al grado de conocimientos que ellos tienen.

2.3 PLANES DE LA ENCUESTA

1. Conocer la información del proceso actual de los paquetes que se usa dentro de la Policía.
2. Saber la opinión del Coronel del Comando e identificar el grado de conocimiento que tienen respecto a los principales paquetes informáticos que se utilizan en cada servicio administrativo.
3. Aclarar que al implementar una metodología para mejorar el control de la información de forma que no haya fuga de información importante entre los departamentos que están involucrados para la realización de este análisis.

2.4 DETERMINACION DE LOS REQUERIMIEENTOS DENTRO DE LA POLICÍA NACIONAL.

2.4.1 Estudio de Requerimientos.

Los diferentes departamentos de la Policía Nacional necesitan de una metodología confiable que sea capaz de mantener la seguridad de la información de una forma confidencial, ya que es una Institución que necesita tener mucho cuidado con la información que se maneja.

Se ha podido observar que hasta el momento no habido fuga de información, sin embargo se debe estar alerta ante cualquier peligro de robo de la misma.
En cuanto a los delitos informáticos se desea mantener siempre alerta para lo cual es necesario saber las precauciones que se deben tomar en estos casos.

2.4.2 Requerimientos del Usuario.

- Actualmente la información que aquí se maneja es muy importante por lo que es necesario tener un mayor control de los datos que se manejan en esta Institución.
- Disponer de claves de acceso especiales para cada persona que accede a los diferentes sistemas con los que se trabaja.
- Respaldos de la información que se maneja con la finalidad de que en un caso de daño o pérdida tener un apoyo para el normal funcionamiento de los diferentes departamentos.
- Control en el correo electrónico para que no exista fuga de información.

2.4.2.1 Requerimientos de Información

Para obtener la información necesaria se realizó encuestas a las diferentes autoridades y personal de la institución, teniendo como resultado el análisis de las mismas. A continuación se describen las preguntas de las encuestas realizadas.

2.4.2.2 ENCUESTAS REALIZADAS EN EL COMANDO Nº 13 DE LA POLIÍA NACIONAL

PREGUNTA N· 1:

Es importante para Usted la información que maneja?

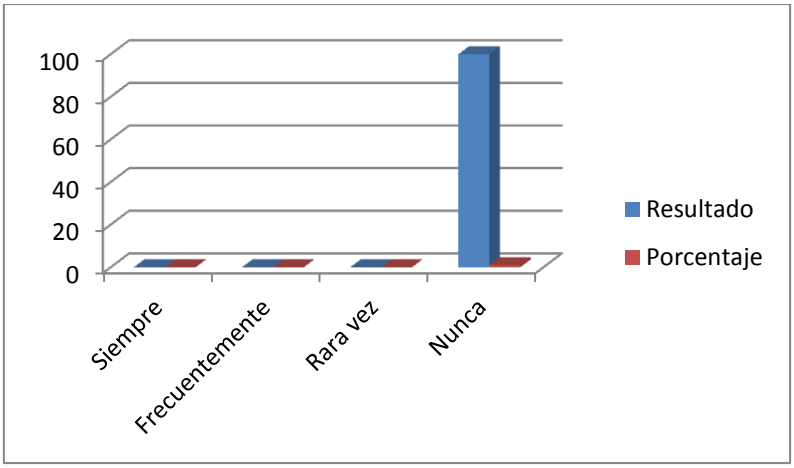
TABLA N· 2.1 IMPORTANCIA DE LA INFORMACIÓN

Alternativa	Resultado	Porcentaje
Si	100	100%
No	0	0%

No responde	0	0%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.1 IMPORTANCIA DE LA INFORMACION



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Con respecto a las funciones que se realizan en el Comando de Policía Cotopaxi No. 13 el 100% del personal que labora en las diferentes dependencias dijo que es importante la información que se utiliza, por lo que se puede concluir que existe una gran responsabilidad en el manejo de la información.

PREGUNTA N· 2

Tiene usted conocimiento sobre un delito informático?

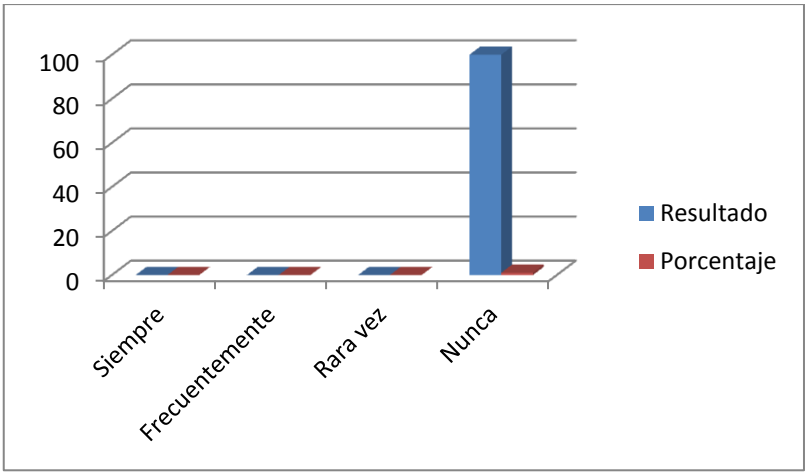
TABLA N· 2.2 CONOCIMIENTO DE UN DELITO INFORMATICO

Alternativa	Resultado	Porcentaje
Si	10	10%
No	60	60%

No responde	30	30%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.2 IMPORTANCIA DE LA INFORMACIÓN



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Con respecto al conocimiento del personal policial administrativo hemos deducido que el 10% tiene conocimiento sobre lo que es el delito informático, el 60% no sabe del tema, mientras que el 30% se abstiene a responder, por lo que se puede concluir que se debe capacitar sobre este tema tan importante como es la fuga de información al personal que labora en esta Institución.

PREGUNTA N· 3

Sabe usted que precauciones tomar para evitar un robo informático?

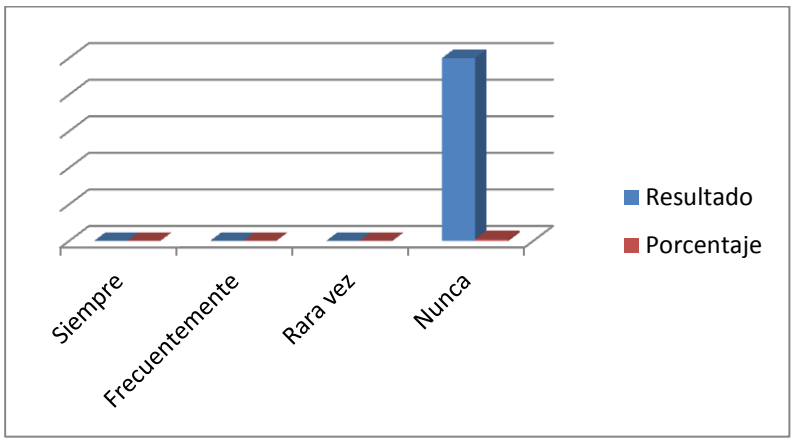
TABLA N· 2.3 SABE COMO EVITAR UN ROBO INFORMÁTICO?

Alternativa	Resultado	Porcentaje
Si	20	20%
No	80	80%

No responde	0	0%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.3 SABE COMO EVITAR UN ROBO INFORMÁTICO?



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Respecto a la encuesta realizada al personal que presta sus servicios en las oficinas del CP-13 hemos deducido que el 20% si sabe como evitar un robo informático, el 80% no sabe del tema, mientras que el 0% no responde, por lo que se puede concluir que la mayoría de los encuestados no tienen idea de lo que podrían hacer para evitar un robo informático.

PREGUNTA N· 4

Conoce usted que ley ampara un delito informático?

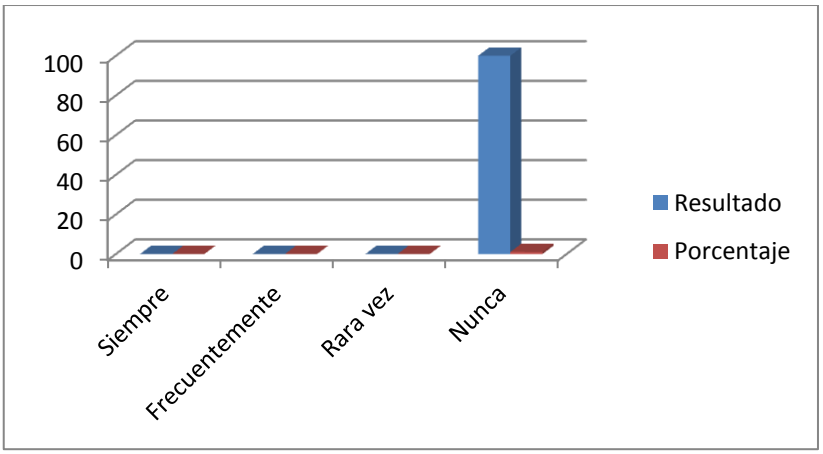
TABLA N· 2.4 CONOCE DE UNA LEY QUE AMPARE UN DELITO INFORMÁTICO?

Alternativa	Resultado	Porcentaje

Si	5	5%
No	90	90%
No responde	5	5%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.4 CONOCE DE UNA LEY QUE AMPARE UN DELITO INFORMÁTICO?



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Respecto a las leyes podemos concluir que casi no tienen conocimiento sobre los artículos que se puede aplicar en caso de un delito informático.

PREGUNTA N· 5

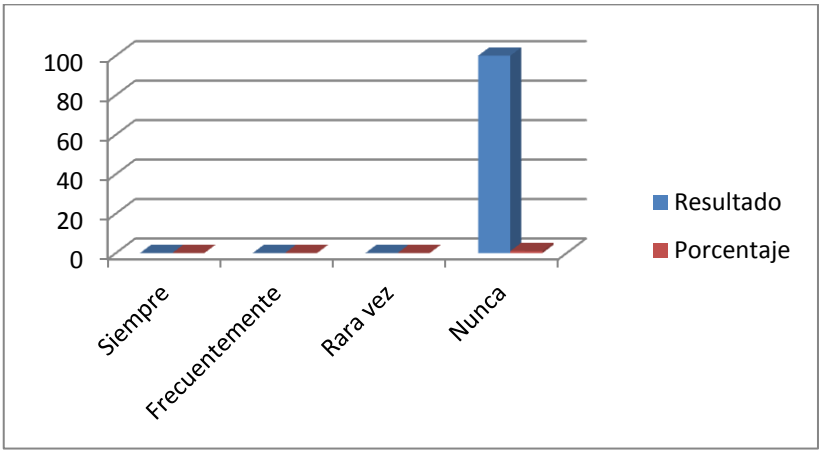
Conoce usted acerca de las firmas electrónicas?

TABLA N· 2.5 CONOCE SOBRE LAS FIRMAS ELECTRONICAS?

Alternativa	Resultado	Porcentaje
Si	0	0%
No	95	95%
No responde	5	5%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.5 CONOCE SOBRE LAS FIRMAS ELECTRONICAS?



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Respecto a las firmas electrónicas no hubo una respuesta positiva ya que es algo nuevo y poco conocido por lo que podemos concluir que no tienen conocimiento sobre lo consultado.

PREGUNTA N· 6

En la función que usted desempeña utiliza usted internet?

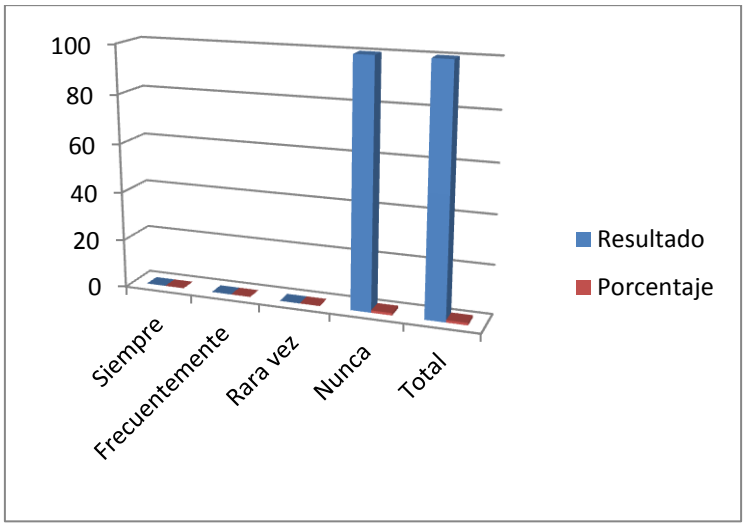
TABLA N· 2.6 UTILIZA USTED INTERNET?

Alternativa	Resultado	Porcentaje

Siempre	95	95%
Frecuentemente	2	2%
Rara vez	2	2%
Nunca	1	1%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.6 UTILIZA USTED INTERNET



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Respecto a esta pregunta en esta Institución el 95% de los encuestados supo manifestar que sí tienen uso del Internet, ya que es muy necesario e indispensable hoy en día , mientras que el 2% dijo que lo usa frecuentemente ya que el trabajo que allí realizan no requiere mucho de Internet, el 2% restante contestó que lo usa rara vez, sólo cuando es necesario mientras que el 1% se limitó a responder, por lo que podemos concluir que el Internet es usado por la mayoría de dependencias del Comando de Policía Nº 13

PREGUNTA N· 7

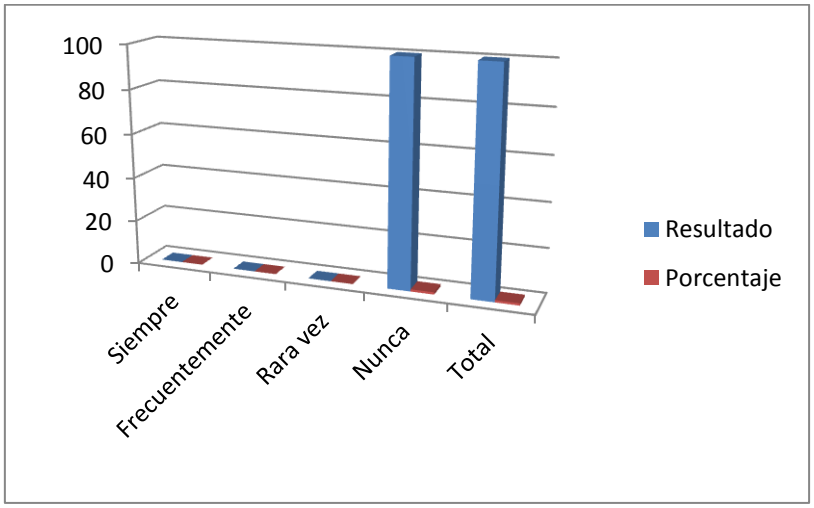
Utiliza usted el correo electrónico?

TABLA N· 2.7 UTILIZA USTED EL CORREO ELECTRÓNICO?

Alternativa	Resultado	Porcentaje
Siempre	95	95%
Frecuentemente	2	2%
Rara vez	3	3%
Nunca	0	0%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.7 UTILIZA USTED CORREO ELECTRÓNICO?



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Respecto al uso de correo electrónico el 95% tiene una cuenta personal, ya que supieron manifestar que es muy necesario tener un e-mail para poder comunicarse, mientras que el 2% usa el correo electrónico frecuentemente, el 3% lo usa rara vez por lo que podemos concluir que el Correo Electrónico es muy usado en esta Institución.

PREGUNTA N· 8

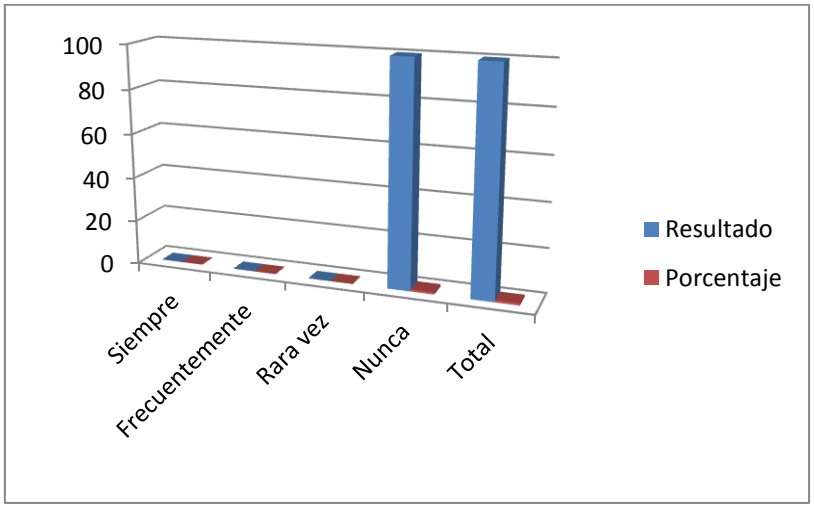
Ha sufrido alguna vez un robo de información?

TABLA N· 2.8 HA SUFRIDO ROBO DE INFORMACIÓN?

Alternativa	Resultado	Porcentaje
Siempre	0	0%
Frecuentemente	0	0%
Rara vez	1	1%
Nunca	99	99%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.8 HA SUFRIDO ROBO DE INFORMACIÓN?



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Respecto al robo de información solo el 1% de las personas que laboran en esta institución supo manifestar que alguna vez si han sufrido una fuga de información, mientras que el 99% restante dijo que nunca han sufrido un robo de información o que por lo menos no se han dado cuenta, por lo que podemos concluir que no están muy al tanto de lo que es en realidad un robo de información y cuando se los han realizado.

PREGUNTA N· 9

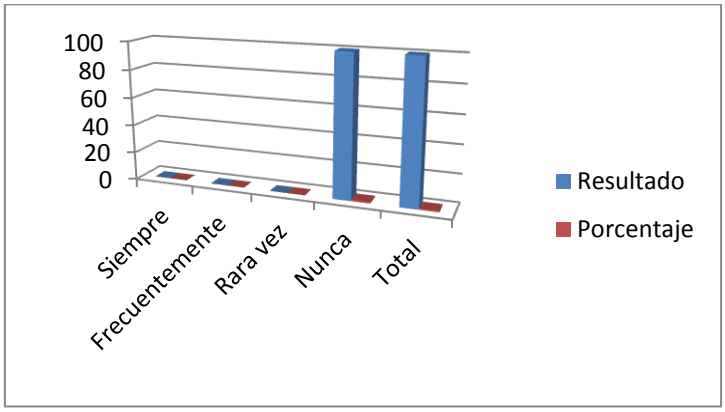
Utiliza claves de acceso para ingresar a la información que usted manipula?

TABLA N· 2.9 USA CLAVES DE ACCESO?

Alternativa	Resultado	Porcentaje
Siempre	50	50%
Frecuentemente	20	20%
Rara vez	10	10%
Nunca	20	20%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.9 USA CLAVES DE ACCESO?



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Con respecto al manejo de claves de acceso para el ingreso al sistema o a la base de datos que manejan solo el 50% del personal manifestaron que si tienen claves de acceso, mientras que el 20% dijo que solo frecuentemente cuando el sistema lo requiere, el 10% supo manifestar que rara vez lo usa, mientras que el 20 % restante dijo que nunca usan una clave de acceso, por lo que podemos concluir que no todo el personal que maneja la parte administrativa tiene claves de seguridad para manejar su información.

PREGUNTA N· 10

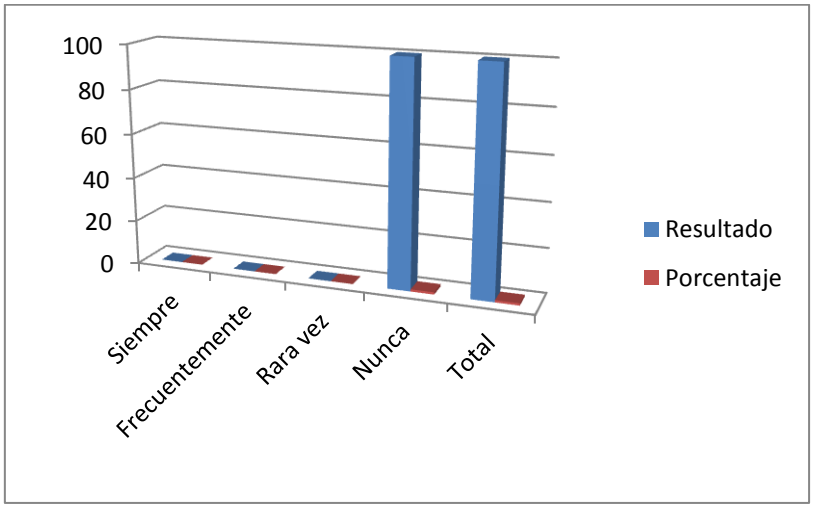
Ha tenido alguna charla o conferencia sobre las leyes que defienden este tipo delito?

TABLA N· 2.10 HA RECIBIDO CHARLAS Y CONFERENCIAS SOBRE LEYES QUE DEFIENDEN ESTE DELITO?

Alternativa	Resultado	Porcentaje
Siempre	0	0%
Frecuentemente	0	0%
Rara vez	0	0%
Nunca	100	100%
Total	100	100%

FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

GRAFICO N· 2.10 HA RECIBIDO CHARLAS Y CONFERENCIAS SOBRE LEYES QUE DEFIENDEN ESTE DELITO?



FUENTE: ELABORADO POR EL GRUPO DE INVESTIGACIÓN

Análisis:

Sobre las leyes que defienden los delitos informáticos el 100% supieron manifestar que no saben cuales son las leyes que amparan a este gran problema ya que nunca han recibido una charla o conferencia que los ha participes de este tipo de estatutos.

CAPITULO III

PROPUESTA

3.1 TEMA: "ANALISIS Y ESTUDIO DE LA INFORMATICA FORENSE EN LA POLICIA NACIONAL**"**

3.2 INTRODUCCION

El análisis forense de un sistema involucra primeramente la recopilación de información dispersa en todo el sistema y posteriormente un análisis de la misma; mientras más completa y precisa resulte dicha información, más real será el análisis realizado. La adecuada conservación de la información del sistema original cumple un rol fundamental en la investigación, de modo que el procesamiento de la misma debería llevarse a cabo sobre una copia de los datos del sistema original.

El disponer de una copia exacta de todo el sistema es el objetivo ideal de la recopilación, pero esto es en sí imposible dado que en el proceso de recolección otros usuarios o programas pueden disparar cambios en el sistema, destruyendo parte de la evidencia. Por este motivo las técnicas forenses tradicionales se han centrado en apagar los sistemas y realizar un análisis sobre la información que persista: logs de programas, tiempos de acceso, contenidos de archivos, etc. Esto facilita la captura de la información y el establecimiento de una línea de tiempo irrefutable.

Respetar este orden aumenta las probabilidades de salvar los datos más efímeros (en caso de que sean los que nos interesan). Con respecto a esto debemos

mencionar que no es posible registrar todos los cambios que ocurren en procesos o archivos en tiempo real, pues al tomar datos de un sector se modifican en otro.

Otro aspecto fundamental a la hora de realizar un análisis es determinar la confiabilidad de la información.

La destrucción de la información dentro de un sistema es algo complicado; por ejemplo, la información contenido en un archivo borrado persiste hasta que sea sobrescrita por uno nuevo. En sistemas de archivos con un clustering eficiente los datos pueden persistir por años, aunque más no sea parcialmente. A medida que aumenta el grado de abstracción de las capas del sistema, encontramos más información remanente, aunque su significado está más oculto, es más ambiguo.

Haciendo una analogía con el mundo real pueden clasificarse los procesos que ocurren en un ordenador en dos grupos. Por un lado identificamos procesos de tipo *arqueológico*, que son el resultado de la acción directa de un ser humano sobre la computadora; por ejemplo, el contenido de archivos, registros de acceso, registros de tráfico de red. Por otro lado, al hacer referencia a los procesos *geológicos* nos referimos a los procesos autónomos del sistema, aquellos sobre los que los humanos no tiene control alguno, como la asignación y el reciclado de bloques de memoria, la asignación de ID para archivos o procesos. Los procesos de tipo geológico destruyen las evidencias arqueológicas que quedan en el sistema, es decir, los procesos autónomos sobrescriben los datos que pueden haber quedado almacenados por el accionar de una persona.

3.3 OBJETIVOS

3.3.1 OBJETIVO GENERAL

- Aplicar una metodología de Informática Forense en el sistema de control de personal del Comando de Policía Nº 13 Cotopaxi.

3.3.2 OBJETIVOS ESPECIFICOS

- Determinar normas para que los procesos de consulta puedan ofrecer un servicio de calidad al personal policial y a la ciudadanía.
- Dar una mejor administración a los archivos y documentos existentes en la policía nacional para evitar la pérdida de la información.
- Desarrollar una metodología que facilite el control de la información únicamente para el personal que la maneja, con la finalidad de que no haya un delito informático.

3.4 JUSTIFICACION

La Policía Nacional al no contar con políticas de seguridad adecuadas para el manejo de la información, esta se ve vulnerable a accesos ilícitos por personas no autorizadas; inconscientemente así la Institución a permitido el desarrollo de actividades como la libre manipulación de la documentación digitalizada, acciones que necesariamente están relacionados directamente con la informática forense, así pues se puede decir que estos archivos contienen datos y estadísticas

relacionadas con todo el país, con la cual puede ser usada para procesar una variedad de crímenes, incluyendo un homicidio, fraude financiero, tráfico y venta de drogas, evasión de impuestos y pornografía infantil.

La importancia de investigar este problema radica especialmente en realizar controles en el robo de procesos informáticos, evitando todo tipo de duplicidad de información, proporcionando una herramienta para el procesamiento, traslado y control de la información de la Policía Nacional.

Desde que la Internet y las nuevas tecnologías de información y comunicación vinieron a formar parte de la vida cotidiana del hombre, la comunicación entre estos a sido mas fluida basada en la utilización de recursos informáticos y tecnológicos; lastimosamente este tipo de herramientas en su gran mayoría proporcionan al individuo total libertad en su utilización misma que en algunos casos es desviada a ocasionar perjuicios a mediana y gran escala dentro de los principales activos de una empresa y/o institución entre los cuales se destaca la información que manejan dentro de ellas, por lo que es necesario crearse reglas para mantener la seguridad y el control tanto de la información como de los usuarios que la manipulan En este momento es cuando la informática forense entra a la sociedad, y se ha visto en la necesidad de implantar en la Policía Nacional, pues es una institución que guarda información muy importante de ahí nace la viabilidad de esta propuesta se basa en que la informática forense es una disciplina en la seguridad computacional, que se enfoca en encontrar evidencia digital después de que un incidente ha ocurrido. Por lo que esta investigación se

enfoca principalmente a generar una metodología de control interno que nos permita conocer que paso con la información y quien la manipulo.

La informática forense trabaja conjuntamente con estándares de evidencia para que esta pueda ser aceptada en una corte. Es importante que estas investigaciones sean tecnológicas-legales en vez de que sean solamente tecnológicas o solamente legales ya que de esta manera se hace más eficiente la investigación.

Con el presente trabajo se aporta científico y tecnológico a esta Institución para que en el futuro no sea victima de un robo de información y pueda tener un medio rápido, preciso y confiable, que se convierta en método para realizar el seguimiento y control de los proyectos que aquí se emprendan.

3.5 IMPACTO

El tema propuesto por el grupo de investigación constituye una ayuda importante para la prevención y control de cualquier delito informático.

Sin embargo el impacto más importante del estudio y análisis de la informática forense es que nos apoyará como una herramienta para poder evitar o determinar a un intruso en el sistema de control de personal del Departamento Recursos Humanos del Comando de Policía Nº 13 Cotopaxi.

En una perspectiva de corto a mediano plazo el estudio y análisis de la Informática Forense nos ayudará a resolver los mayores problemas que actualmente nos asechan como son:

– No existe un estándar para la recuperación de Evidencias Digitales.

– Las actuaciones no se realizan con suficiente rapidez.

Sin embargo el Estudio y análisis de la informática forense tendrá un impacto directo en los trabajos que se realizan en este departamento, como son:

Actualización de datos (personal, familiar y calificaciones) de todo el personal que labora en esa unidad.

Acciones dañinas llevadas a cabo por empleados, ex empleados o personal externo.

Sólo en aquellos casos en los que realmente merece la pena la inversión de dinero, se realizan investigaciones forenses de intrusiones: su costo puede ser muy elevado, pueden no conducir a nada concluyente, las conclusiones pueden no permitir capturar al atacante o que este no esté al alcance.

3.6 DESCRIPCION DEL AREA

El Departamento involucrado en la realización del estudio y análisis de la Informática Forense en la Policía Nacional es el departamento de Recursos Humanos (P-1, Personal), el mismo que cumple a cabalidad las funciones encomendadas para la mejor marcha de la institución.

3.6.1 ORGANISMOS QUE CONSTITUYEN EL DEPARTAMENTO DE RECURSOS HUMANOS – (P-1, Personal) – DEL COMANDO DE POLICIA No. 13 COTOPAXI.

En esta oficina laboran los siguientes organismos:

Jefe del Departamento de Recursos Humanos o (P-1, Personal):

Sr. Mayor de Policía Víctor Hugo Tapia, que tiene bajo su cargo la responsabilidad de determinar medios de control sobre el personal que labora en esta noble institución.

Secretarias

Sras. Cabo Primero Elsa Núñez, Cabo Segundo Mónica Álvarez y Srta. Policía Fernanda Landeta.

Las mismas que se dedican a actualizar la Base de Datos en el sistema de cada uno de los miembros de esta unidad.

Este sistema es realizado en Fox, la Base de Datos se encuentra en el servidor, mismo que se encuentra en la Dirección General de Personal de la Comandancia General de Policía en la ciudad de Quito.

3.6.2 ANALISIS FODA DEL DEPARTAMENTO DE PERSONAL DEL COMANDO DE POLICÍA No 13 DE COTOPAXI

Este análisis nos permitirá conocer todos los puntos a favor que tiene este departamento para cumplir sus funciones en beneficio del personal que labora en esta unidad de policía, entre estas podemos citar:

VER ANEXO No 3

3.7 SITUACION ACTUAL

Este Departamento tiene bajo su responsabilidad trabajar y cumplir directamente con el personal de esta Institución llevando en orden la base de datos y actualizándola según sea conveniente.

3.7.1 INFRAESTRUCTURA Y SERVICIOS.

a) INFRAESTRUCTURA

La infraestructura del Departamento de Personal del Comando de Policía No 13 de Cotopaxi cuenta con el mobiliario necesario, este organismo no es lo suficientemente amplio puesto que todos los trámites que realizan los miembros se los lleva a cabo en la misma oficina, pero esto no ha sido un problema para el desenvolvimiento de las labores.

Actualmente no se ha hecho ninguna adquisición de equipos de cómputo pues los que poseen tienen vida útil satisfactoria, debido a que esta oficina no requiere de tecnología de punta.

Como herramientas de Software que este departamento posee con sus respectivas licencias que están a disposición para el estudio, desarrollo y factibilidad del proyecto son:

SOFTWARE

CANTIDAD	CARACTERISTICAS
4 PC	Sistema Operativo: Windows XP. Servidor de Base de Datos: SQL Server 2000 Lenguaje de Programación: Visual Fox 8.0 Microsoft Office 2007

HARDWARE

CANTIDAD	CARACTERISTICAS
Servidor	
3 PC Pentium IV	Disco duro 120 GB o más Memoria Ram 512 MB o más Velocidad 2,8 GHz o más Procesador Compaq Prolances 150 Tarjetas de red – video – cd-rom – dv-drw
1 1	Hub. Swisht
2 Impresora	Lexmark 5160, HP

b) SERVICIOS

El Servicio que presta este Departamento de Recursos Humanos es de actualizar el listado del personal policial en los diferentes servicios que se encuentran , así como también la ubicación actual, es decir los diferentes

destacamentos o puestos en que se encuentran actualmente brindando su servicio.

3.8 ESTUDIO DE FACTIBILIDAD

Un punto importante en el análisis del proyecto informático es el estudio de la Viabilidad y dentro de este es el análisis de Costo-Beneficio que representa una valoración de la justificación económica del proyecto.

Para la evaluación del costo-beneficio de un proyecto existen varias técnicas de estimación, para el presente utilizaremos el Modelo de costos Constructivo (COCOMO), que es un conjunto de modelos que se utilizan para estimar el esfuerzo y el tiempo de duración del proyecto.

El modelo de costos COCOMO tiene tres grados de profundidad, pero para nuestro análisis utilizaremos el Modelo 2 ó COCOMO intermedio ya que lo podemos adaptar de mejor manera a nuestro proyecto de investigación.

3.8.1 Factibilidad Técnica

Con el análisis desarrollado en el Hardware y Software en la Oficina de Departamento de Recursos Humanos del Comando Provincial de Policía Cotopaxi No. 13, llegamos a la conclusión que si es factible realizar nuestro proyecto de investigación por motivo que nos brindan todas las facilidades tanto como accesibilidad a la información requerida.

3.8.2 Factibilidad Económica

En esta parte de la determinación de recursos. Los recursos básicos a considerar son el tiempo propio y del equipo de sistemas, el costo de hacer un estudio de una metodología completa, el costo estimado de inversión.

La aplicación de nuestra metodología propuesta servirá para abaratar los costos de seguimiento de un delito o pérdida de información causada por diversas circunstancias

- **Costos Directos**

Son todos los suministros que se van a utilizar como por ejemplo: Flash Memorias, CD´s, fotocopias, cartuchos de tinta para la impresora, también se pueden nombrar dentro de Otros Gastos las horas de Internet y otras necesidades que se hayan tenido.

- **Costos Indirectos**

Se han tomado en cuenta las diferentes fases a seguir para la realización del proyecto, considerando un costo de mínimo por día para el desarrollador de la metodología, aunque no se descarta inconvenientes, aunque económicamente puede darse el 95% de factibilidad para el desarrollo del proyecto dentro del Comando de Policía No 13 Cotopaxi.

- **Costo Operativo**

Para obtener el valor estimado del costo operativo se ha considerado el tiempo aproximado en el que se desarrollará el proyecto.

El personal que se requiere para el desarrollo del proyecto se personifica en los autores del presente trabajo convirtiéndose en un ahorro para el Comando de Policía No 13 Cotopaxi, esto da como consecuencia el 100% de operar.

- **Costo de Inversión**

Para obtener este costo se ha estimado los requerimientos de hardware, software y costo de capacitación del usuario. En cuanto al hardware y software se refiere a lo que se necesitará para el funcionamiento de este Estudio y Análisis de Informática Forense, cabe aclarar que el Comando

de Policía No 13 de Cotopaxi actualmente cuenta con este equipo. El Comando de Policía No 13 de Cotopaxi posee las licencias del Software mencionado anteriormente, el Hardware con que cuenta el departamento involucrado para la realización de este proyecto se acoplan a las necesidades requeridas, la capacitación de los usuarios también será hecho por el investigador del trabajo por consecuencia se lo califica el 100%.

- **Costo beneficio**

Hacemos referencia el beneficio que tendrá este Departamento con la implementación de nuestro proyecto de análisis dentro del Comando de Policía No 13 Cotopaxi.

3.8.2.1 CONCLUSIONES DE LA FACTIBILIDAD ECONOMICA

Después de haber analizado los costos y beneficios de nuestro proyecto propuesto se puede observar que es económicamente factible por todos los beneficios que representa.

3.8.3 FACTIBILIDAD OPERATIVA

El sistema con el que trabaja este Departamento de Recursos Humanos (P-1, Personal) brinda muchas ventajas de operación como la facilidad de manipulación de información dentro de la base de datos, facilita también el ahorro de tiempo, facilidad de acceso a los datos de cada miembro de la institución que presta su servicio en esta provincia, actualización de datos de manera rápida y confiable, con todo esto el Comando de Policía No. 13 Cotopaxi se pone en un nivel de riesgo de fuga de información muy alto, pues los miembros que trabajan en este departamento no son profesionales en sistemas y al realizar este Estudio y Análisis de Informática Forense no hay temor a que se produzca un delito informático, ya que por medio de la aplicación de estas herramientas de Informática Forense ellos también están en la capacidad de evitarlo.

3.9 HERRAMIENTAS PARA EL ANÁLISIS FORENSE DIGITAL

Para el estudio y análisis forense del sistema nos centraremos en la utilización de herramientas del sistema operativo o las propias del ToolKit que investigamos como parte de nuestro plan de tesis. Por lo que hemos realizado la investigación de forma manual. Pero hemos comprobado que una de las dificultades que encontramos el grupo de investigación a la hora de analizar determinadas evidencias digitales es que los atacantes emplean cada vez herramientas más sigilosas y perfeccionadas para realizar sus delitos informáticos. Por lo tanto no estará de más disponer de un conjunto de herramientas específicas para el análisis de evidencias que nos ayudaran a completar de forma más eficiente nuestra investigación.

Dejando a parte el software comercial, en el que podremos encontrar herramientas específicas como EnCase de la empresa Guidance Software, considerado un estándar en el análisis forense de sistemas, nos centraremos en herramientas de código abierto (Open Source).

A continuación se detalla un cuadro de las herramientas más usadas en Informática Forense.

TABLAS 3.1 HERRAMIENTAS PRINCIPALES PARA INFORMATICA FORENSE

The Forensic ToolKit	Afind	Hfind	sfind	The Sleuth Kit y Autopsy

Este ToolKit le permitirá recopilar información sobre el ataque, y se compone de una serie aplicaciones en línea de comandos.	Realiza búsqueda de archivos por su tiempo de acceso, sin modificar la información de acceso al mismo.	Busca archivos ocultos en el Sistema Operativo.	Busca flujos de datos ocultos en el disco duro, éstos son distintos de los archivos ocultos y no aparecerán con herramientas normales del sistema operativo.	Puede analizar archivos de datos de evidencias generadas con utilidades de disco. Incluye funciones como registro de casos separados e investigaciones múltiples.

FUENTE: GRUPO DE INVESTIGACIÓN.

3.9.1 ANÁLISIS DE LA HERRAMIENTA THE FORENSIC TOOLKIT- FTK

Esta es una colección de herramientas forenses, es para plataformas Windows, que fueron creadas por un equipo de Foundstone. Este ToolKit nos permitirá recopilar información sobre el ataque a los archivos más importantes que aquí se manejan, y se compone de una serie de aplicaciones en línea de comandos que nos permitirán generar diversos

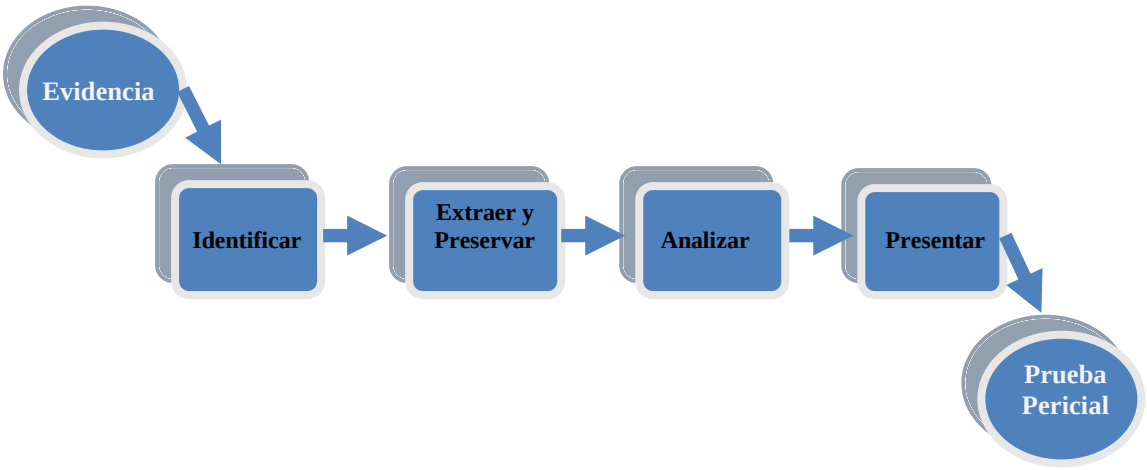
informes y estadísticas del sistema de archivos. Para poder utilizarlos deberemos disponer de un intérprete de comandos como cmd.exe.

Forensic Toolkit de Access Data (FTk) ofrece a los encargados del Departamento de Recursos Humanos del Comando de Policía No13 de Cotopaxi controlar la fuga de información y la capacidad de realizar exámenes forenses informatizados completos y exhaustivos, la herramienta FTK posee funciones eficaces de filtro y búsqueda de archivos. Los filtros personalizables de FTK permiten buscar en miles de archivos para encontrar rápidamente la prueba que se necesita. FTK ha sido reconocida como la mejor herramienta forense para realizar análisis forenses, por este motivo hemos querido aplicar a nuestro trabajo de investigación.

La herramienta FTK nos permite navegar rápidamente por las imágenes adquiridas y nos permitirá también generar registros de auditoría e informes del caso, es compatible con Pasword de seguridad.

3.10 METODOLOGIA

FASES PARA LA REALIZACIÓN DEL ANÁLISIS FORENSE



FUENTE: GRUPO DE INVESTIGACIÓN.

A) Identificación de la evidencia digital.

El primer paso es **identificar** qué computadoras de la Institución Policial pueden contener evidencia, reconociendo la frágil naturaleza de los datos digitales, para lo cual nos plantearemos las siguientes preguntas.

¿Qué tipo de información esta disponible?
¿Cómo la podemos "llevar" de forma segura?
¿Qué puede formar parte de la evidencia?

Es el proceso de conocer los datos, dónde están localizados y cómo están almacenados.
zar una primera distinción entre evidencias volátiles (evidencias que desaparecen pronto debido a falta de alimentación eléctrica, corte de conexiones telemáticas, etc.) y no volátiles (evidencias que perduran aún a falta de alimentación eléctrica, etc.).

El obtener las evidencias volátiles es fundamental en la Policía Nacional y estas evidencias mencionadas anteriormente se pueden observar en el siguiente cuadro.

TABLA: 3.2 OBTENCIÓN DE EVIDENCIAS.

VOLATILES (SIN REINICIAR EL EQUIPO)	VOLATILES (EQUIPO REINICIADO)	REDES
1. Registros y cache del procesador 2. Tabla de procesos 3. Estadísticas del kernel y módulos 4. Memoria RAM 5. Ficheros temporales del sistema 6. Estado de la red 7. Ficheros abiertos	1. Sistemas de ficheros montados 2. Sistemas de ficheros virtuales (/proc)	1. Tarjetas de red de ordenadores. 2. Routers. 3. Hubs. 4. Switch. 5. Modems.

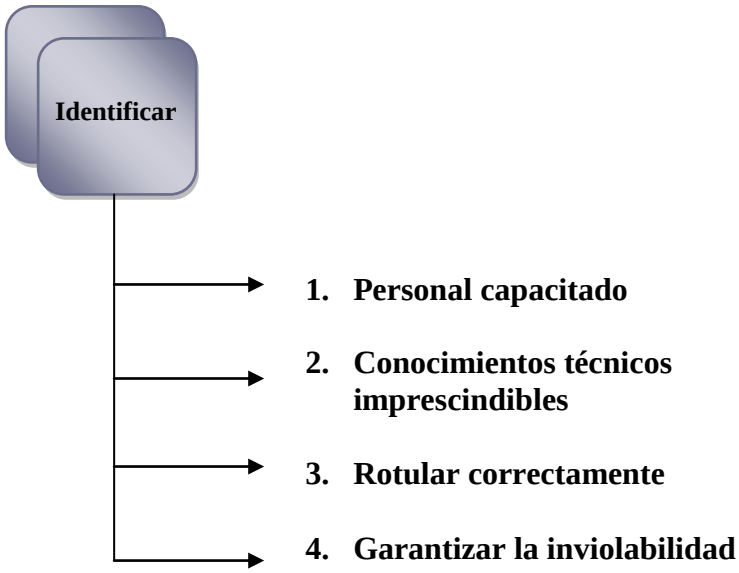
FUENTE: GRUPO DE INVESTIGACIÓN.

Donde obtener evidencias:

1. Monitor, teclado y ratón (solo necesario en ciertos casos).
2. Dongles (Mochilas) (dispositivos que se conectan en el puerto paralelo del ordenador y verifican que el programa es original y no es copia).
3. Cámaras de fotos digitales y cámaras de vídeo digitales.
4. Discos duros, disquetes, CDs, DVDs. Normalmente en estos dispositivos es donde más información encontraremos. La evidencia digital estará contenida en los sistemas de ficheros de cada uno de estos dispositivos.
5. Impresoras

De estos dos últimos dispositivos periféricos es difícil encontrar evidencias una vez apagados, pero pueden ser necesarios para analizar otro tipo de evidencias, como huellas digitales.

Elementos para la identificación de la Evidencia Digital



FUENTE: GRUPO DE INVESTIGACIÓN.

B) PRESERVACIÓN DE LA EVIDENCIA DIGITAL.

La segunda gran tarea es **preservar** la evidencia contra daños accidentales o intencionales, usualmente esto se realiza efectuando una copia o imagen espejada exacta del medio analizado.

Una verdadera imagen espejada es una copia sector a sector de la unidad original investigada.

Para lo cual se ha tomado en cuenta lo siguiente:

- Se debe tratar de no realizar ningún cambio sobre la misma.
- Se deben registrar y justificar todos los cambios.
- Realizar un by-pass del sistema operativo y crear por “fuera” un backup de toda la evidencia.

- Las copias duplicadas deben ser escritas en otro disco rígido o CD-ROM.
- Se debe realizar una documentación de todo el proceso de la generación de imágenes.
- Se deben autenticar todos los archivos e imágenes utilizadas con hashes MD5 o SHA1.

Orden de volatilidad

Se debe preservar la evidencia más volátil al principio:

- Registros, caches, memoria de periféricos.
- Memoria (kernel, física)
- Estado de las conexiones de red.
- Procesos que se están ejecutando.
- Discos rígidos.
- Diskettes.
- CD-ROMs, impresiones.

Esta es la fase más importante y crítica de la metodología, puesto que una vez que se halla comprobado el delito informático. Para ello es necesario poseer evidencias digitales preservadas de tal forma que no haya duda alguna de su verosimilitud y siempre de acuerdo a las leyes vigentes. Este proceso de preservación se debe realizar tan pronto como sea posible.

Recordemos que las primeras evidencias que hay que obtener son las volátiles, que al guardarlas en ficheros se convertirán en evidencias no volátiles.

Los pasos para preservar la evidencia se detalla a continuación en la siguiente tabla.

TABLA: 3.3 PRESERVACIÓN DE EVIDENCIAS.

EXTRACCIÓN	EMBALAJE	TRANSPORTE
1. Si el dispositivo del cual queremos una copia esta encendido. 2. Toda evidencia digital guardada en dispositivos de almacenamiento debe ser copiada en software que no alteren su evidencia. 3. Formas para crear duplicados a nivel de bit de los discos de almacenamiento de información. 4. Retención de tiempos y fechas. 5. Preservar datos de dispositivos de mano como PDAs, PocketPCs, etc. 6. Generar los procesos de checksum criptográfico de la copia y del original.	1. Empaquetar los dispositivos que contiene las evidencias. 2. Identificador único 3. Nombre de la persona y organización (fuerza de la policía, 4. Responsable de la recolección y empaquetado del material. 5. Breve descripción del material 6. Localización desde donde y a quien fue incautado. 7. Día y hora de la incautación. 8. Los dispositivos magnéticos u ópticos deben ser introducidos en unas cajas con material protector. 9. Documentación en papel (como manuales y libros) en bolsas de plásticos para protegerlos de daños. 10. Toda persona involucrada en un examen forense debería tomar las precauciones necesarias	1. Transportar los dispositivos que contiene las evidencias. 2. Toda evidencia debe ser transportada a un lugar seguro y cerrado. 3. La cadena de custodia se debe mantener meticulosamente durante el transporte. 4. Si el paquete debe ser enviado mediante correo postal, hay que asegurarse de usar un método que permita el seguimiento del mismo.

FUENTE: GRUPO DE INVESTIGACIÓN.

Elementos para la preservación de la evidencia digital

FUENTE: GRUPO DE INVESTIGACIÓN.

C) ANÁLISIS DE LA EVIDENCIA DIGITAL.

El concepto de evidencia digital se forma (normalmente) por el contenido de los ficheros (datos) y la información sobre los ficheros (metadatos). Basándose en estas evidencias el investigador debe intentar contestar a las siguientes preguntas en la fase de análisis:

1. ¿Quién?

Reunir la información sobre el/los individuo/s involucrados.

2. ¿Qué?

Determinar la naturaleza exacta de los eventos ocurridos.

3. ¿Cuándo?

Reconstruir la secuencia temporal de los hechos.

4. ¿Cómo?

Descubrir que herramientas se han usado para cometer el delito.

La evidencia almacenada debe ser analizada para extraer la información relevante y recrear la cadena de eventos sucedidos. El análisis requiere un conocimiento profundo de lo que se está buscando y como obtenerlo.

Hay que asegurarse que la persona que analiza la evidencia está totalmente calificada para ello.

Cualquier elemento enviado para su análisis forense debería ser en primer lugar revisado para comprobar la integridad del paquete antes de empezar dicho análisis.

Cualquier deficiencia en el paquete se debe documentar. Es importante que el cliente especifique que información es prioritaria de modo que si no se puede lograr una recuperación completa (en caso que el cliente desee dicha recuperación), la recuperación se concentre sobre lo más importante.

Analizar las evidencias digitales va a depender del tipo de dato a analizar, del tipo de sistema en el cual se clasifique el dispositivo comprometido (ordenadores, etc.).

Existen cuatros categorías de datos que se detallan en la siguiente tabla:

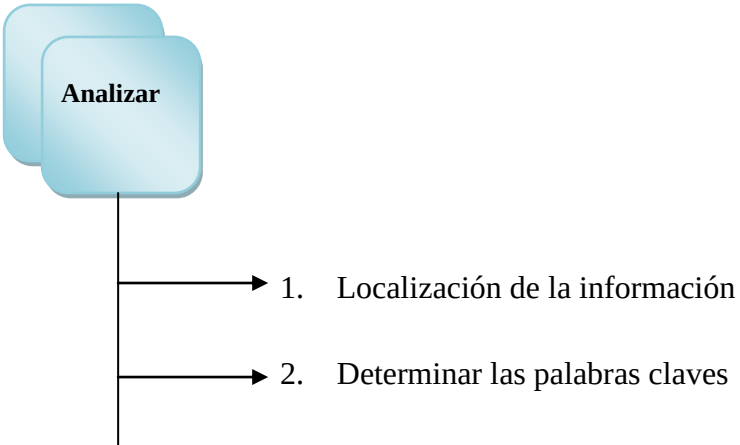
TABLA: 3.4 CATEGORÍAS DE DATOS

DATOS ACCESIBLES	**ELEMENTOS EN FUNCIÓN DEL SISTEMA**	**REDES**	**SISTEMAS EMBEBIDOS**	**OTROS DISPOSITIVOS**
*Son los datos más comunes. *Que haya una gran	*Sistemas informáticos *Sistemas Windows *Registro del sistema	*Información proporcionada por la tarjeta de red	*Su recolección de datos es igual que la de un disco duro	*Debido a la exclusividad de cada uno de ellos

cantidad de información a analizar *Que estén cifrados, por ejemplo office. *Datos que han sido eliminados (si no han sido sobreescritos se pueden volver a recuperar). *Datos en "ambient data", este tipo de datos necesita software especial para poder ser recuperados. *Datos en estenografía (proceso por el cual se puede ocultar datos dentro ficheros)	*Contenido de Sistema de Fichero *Papelera de reciclaje *Ficheros de acceso directo * Evidencias volátiles. *Mensajes de correo electrónico. *Ficheros de impresión. *Logs del sistema operativo. *Documentos de texto *Hojas de cálculo *Ficheros gráficos	*Tabla de direcciones IP asignadas por el servidor * Cache de ARP (Protocolo de Resolución de Direcciones). *Logs del firewall. *Memoria del firewall. * Logs de servidores (Web, FTP, de correo electrónico). * Mensajes de correo electrónico almacenados en el servidor.	*CIS (Card Information System) Area oculta que contiene información del fabricante. * MBR (Master Boot Record) En las tarjetas este sector esta presente por razones de compatibilidad y raramente se usará como arranque de un disco duro *Sector de arranque. Se usa junto al MBR para establecer la geometría del dispositivo.	*Hay que conseguir la documentación propia del dispositivo (a través del fabricante, Internet, etc.) para saber donde puede almacenar evidencias. Podemos hacer la siguiente clasificación: *Sistemas de oficina *Teléfonos fijos. *Fax. *Fotocopiadoras

FUENTE: GRUPO DE INVESTIGACIÓN

Elementos para el análisis de la evidencia



FUENTE: GRUPO DE INVESTIGACIÓN.

D) PRESENTACION Y REPORTES

Basándonos en las fases anteriores, en toda la documentación disponible del caso y basándose también en la cadena de custodia, la presentación y/o sustentación del informe pericial es la fase de comunicar el significado de la evidencia digital, los hechos, sus conclusiones y justificar el procedimiento empleado.

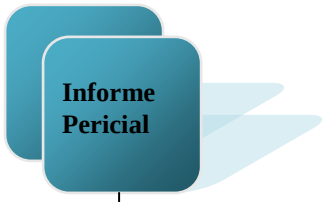
El propósito de la presentación de los informes es proporcionar al lector toda la información relevante de las evidencias de forma clara, concisa, estructurada y sin ambigüedad para hacer la tarea de asimilación de la información tan fácil como sea posible.

La forma de presentación es muy importante y debe ser entendible por personas no conocedoras del tema en discusión.

Es decisivo presentar las evidencias en un formato sencillo de entender, acompañado de explicaciones que eviten la terminología técnica.

La investigación debe presentar evidencias informáticas de una manera lógica, precisa y persuasiva. Esto requiere que las acciones del experto forense puedan ser reconstruidas paso a paso con fechas, horas, cuadros y gráficos (el uso de programas como Excel, Word, PowerPoint, etc. puede ser de gran ayuda en este punto).

Es importante que el investigador sepa sustentar correctamente cada tarea realizada en su investigación.



1. Autenticación del material informático
2. Descripción detallada de todas las fuentes de información utilizadas
3. Pasos realizados durante la investigación
4. Nombre de la herramienta forense y versión
5. Contestación de cada uno de los puntos de la pericia, indicando cualquier observación o impedimento en la búsqueda de evidencia

FUENTE: GRUPO DE INVESTIGACIÓN

Análisis Forense en el Sistema de la Dirección General de Personal de la Policía Nacional del Comando Cotopaxi No. 13; En la primera parte, discutimos los preparativos y cómo se debe preparar un entorno informático para realizar un análisis forense eficiente. Ahora nos adentramos en el ámbito de la intrusión y del entendimiento de los pasos

del hacker a nivel de redes de sistema. Veremos utilidades y técnicas útiles en este trabajo de investigación.

Como vimos en la primera parte, debemos descubrir la intrusión (aunque aún no hay las herramientas o los medios utilizados para llevarla a cabo) y comenzar a descubrir las "huellas dactilares" (digitales). También debemos localizar el inicio de la intrusión, para tener una idea global del alcance de ésta.

Nuestros objetivos son bastante simples. Queremos determinar la magnitud del Delito Informático realizado por el atacante sobre la red, el método de entrada y quién es físicamente el atacante (si es posible).

Sería realmente útil disponer de personal calificado en todas las empresas capaces de analizar registros de aplicaciones, acceso de usuarios y en general, auditar la seguridad de una forma proactiva. Desafortunadamente, la situación real es bastante diferente a esto y muy pocas empresas tienen a su disposición detectores de intrusos (IDS – Intrusión Detection Systems), firewalls monitorizados, autentificación fuerte (las contraseñas son cosa del pasado) y sistemas de auditoria y registro de eventos completos. El problema es aún mayor en entornos grandes, donde debido a la gran cantidad de datos que se procesan, es prácticamente imposible realizar un análisis casi en tiempo real. Por eso, cuando un incidente ocurre, necesitamos de una herramienta y una

metodología para investigar el estado de la red y poder tomar decisiones o recomendaciones inteligentes.

Es recomendable usar un ordenador portátil con los sistemas operativos Windows 2000 (y el Kit de Recursos de Windows 2000) y Linux para realizar las pruebas pertinentes. También es necesario cargar ambos sistemas con una variedad de utilidades de análisis esenciales.

Estas son sólo algunas de las utilidades disponibles y representan las esenciales para analizar una red, aunque, por supuesto, sus preferencias pueden ser otras.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Con el estudio y análisis realizado se ha podido observar que las empresas que manejan información han aprendido que para asegurar la integridad, privacidad de información no se debe ahorrar en sistemas de seguridad, planes de contingencia. Los administradores sin previa experiencia de análisis forense no deben precipitarse a la hora de restablecer el servidor parcheándolo rápidamente para que esté operativo lo antes posible, ya que solo un análisis forense exhaustivo puede determinar el alcance del incidente y responder a todas las preguntas que surgen tras sufrir un ataque.

- Se ha logrado optimizar el archivo de documentos, teniendo la información en una base de datos documental y evitando la perdida de los mismos.

- Se culminó con el desarrollo de la investigación proponiendo una metodología que ayudará al Departamento de Recursos Humanos del Comando de Policía Nº 13 Cotopaxi a precautelar la información que se maneja con la finalidad de evitar delitos informáticos y a la vez saber qué medidas se deben tomar.

4.2 RECOMENDACIONES

- Al realizar un análisis de informática forense es necesario tomar notas de lo que se hace con el disco duro, y a que hora, almacenándolo en una ubicación segura como por ejemplo una caja fuerte. Es recomendable que siempre que se trabaje

con el medio original esté acompañado por un especialista, para que conste a los efectos legales y el testimonio pueda ser confirmado por alguien con un nivel de conocimientos similar.

- Es importante todos los hechos pertinentes al caso durante la preparación, recuperación y análisis de las pruebas sobre un ataque sean anotados para poder desarrollar un informe detallado de incidencia que se debe preparar una vez terminado el análisis. Este documento deberá servir como una prueba del incidente o compromiso. Siempre que se realiza cualquier apunte al cuaderno, el asistente debe tener completo conocimiento y entendimiento de lo que ha sido apuntado.

- Es necesario que se implante una cultura informática en los departamentos de esta Institución para que este proyecto sea aprovechado en su plenitud y se pueda hacer mejor uso y manejo de los programas informáticos.

- Se debe tener cuidado con las claves de usuario ya que el mal uso de ellos pueden causar fugas de información.

- Se debe designar al personal que va a estar involucrado directamente con el sistema para que haya buen manejo de la información y no exista ningún delito informático.

BIBLIOGRAFÍA

BASICA

- ARANDA, Alcides; Planificación Estratégica Educativa 2000.

- BOOCH, Grady; Análisis y Diseño Orientado a Objetos con aplicaciones1996
- GONZALEZ, José; Manuales Técnicos 1992.
- JAMES A SENN; Análisis y Diseño de Sistemas de Información, Mc Graw-Hill, Interamericana de España.
- Power Soft ; Power Designer Data Architect User´s Guide.
- REINO, Luís; Proyector de Investigación para Tesis de Grado 2000.

CITADA

- http://laconsigna.files.wordpress.com/2008/05/informatica-forense.pdf
- http://www.monografías.com/trabajos14/sqlserver/sqlserver.shtml
- http://www.maestros delweb.com/editorial/sql2kinstal/
- http://usuarios.lycos.es/cursosgbd/Ud5htm

VIRTUAL

- http://www.BondingwhitUserSecurityinNotes.com
- http://www.DominioAdministrador6.help
- http://www.LaWebdelProgramador.com
- http://www.mit.edu/people/mkgray/net/web-growth-sumary.html
- http://www.netcraft.com/survey/
- http://www.sin.items.mx/servicioseducativos/manuallotus/contenio-maulhtm.