Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas

Seguridad de la Información del Departamento de Ventas de la Empresa Rualtim S.A.

Trabajo de graduación previo a la obtención del título de Ingeniero de Sistemas

Autores: Andrés Oswaldo Torres Bustamante
Oswaldo Sebastián Zapata Avila

Director: Ing. Diego Condo

Cuenca, Ecuador

2009

DEDICATORIA

Este trabajo, está dedicado con mucho cariño especialmente a mis padres, quienes siempre me ayudaron, me dieron ánimo y voz de aliento para seguir siempre adelante. A mi esposa y mi hijo, que estuvieron siempre a mi lado en las buenas y en las malas, que me brindaron todo su apoyo, porque gracias a su amor he llegado a culminar con éxito esta etapa muy importante en mi vida.

Andrés

A mis padres por el apoyo, comprensión y palabras de aliento a lo largo de mi vida, a mis hermanos y demás familiares que forman parte fundamental de mi vida. A la persona que hoy es el motivo central de esfuerzo y dedicación de mi vida, mi hija Valentina, por el cual cada día me esmero en ser un buen padre y excelente amigo para ella.

Sebastián

AGRADECIMIENTOS

Principalmente agradezco a Dios, por la vida, y haberme guiado hacia la culminación de mi carrera profesional; a la Universidad Del Azuay, a sus docentes que durante los años de estudios supieron brindarme los conocimientos para la realización de este trabajo, en especial al Ing. Diego Condo, director de la presente monografía.

Andrés

A Dios por bendecirme con la vida y permitirme llegar a culminar una etapa importante de mi vida, a mis padres por el sacrificio realizado a lo largo de toda su vida para darme una excelente educación y fomentar principios para que pueda ser una persona de bien, a nuestro director de monografía, el Ing. Diego Condo por los conocimientos y tiempo dedicado para elaborar la presente monografía.

Además agradezco a todos los profesores, compañeros y amigos que me apoyaron durante el transcurso de mi vida universitaria, especialmente aquellos que confiaron en mí en todo momento.

Sebastián

Índice de Contenidos

Índice de Capítulos

CAPITULO I

CAPITULO II

CAPITULO III

Índice de Imágenes

Índice de Fotos

Índice de Gráficos

Indice de Tablas

Índice de Anexos

AUTORÍA

Los autores son los únicos responsables de los conceptos, conclusiones y observaciones emitidos en la presente monografía.

Andrés Torres B.

Sebastián Zapata A.

RESUMEN

Este trabajo tiene como objetivo principal, medir los riesgos y evaluar los controles en el uso de las tecnologías de información, así como el obtener evidencia aplicando un adecuado proceso Informático Forense, el cual será ejecutado en la Empresa Rualtim S.A.

Inmediatamente de evaluar los controles, procesos, riesgos tecnológicos y del análisis de la evidencia obtenida, aplicando la metodología creada para el efecto, se presentará el debido informe que servirá de fundamento para que la Empresa tome decisiones que el caso amerite, conjuntamente se presentará las debidas conclusiones y recomendaciones a partir de la elaboración de la presente monografía.

ABSTRACT

The maín objective of this project ¡s to measure the risks, and evalúate the controls on the use of information technology as well as to obtain evidence by the application of an adequate forensic informatics process; Rualtim S.A.Company will perform this procedure.

Afíer the evaluation of controls, processes, technological risks and the analysis of the obtained evidence, which is acquired by the application of the designed methodology, an inform will be presented; this will be the basis for the company to take the needed decisions according to the specific situation, at the same time conclusions and recommendations will be shown, and they are based on this monograph.

INTRODUCCIÓN

Lo que la presente monografía trata de enfocar, es el análisis de la información en la empresa Rualtim S.A, aplicando previamente la evaluación de riesgos del área más crítica con el manejo de información y que tiene repercusión económica y organizacional de mayor impacto. Además se analizará la información contenida dentro de los recursos informáticos, que intervienen con los eventos expuestos por los directivos de la empresa.

Para poder cumplir con los objetivos de este trabajo, se empleará la metodología especializada para el campo de la Auditoría Informática como de la Informática Forense. El proceso a realizar nos ayudará a obtener evidencia así como descubrir las vulnerabilidades que tiene la empresa al desarrollo normal de sus actividades, por lo que la empresa deberá tener muy en cuenta todo el análisis a desarrollar, para evitar cualquier pérdida económica o de información.

Por lo tanto los resultados obtenidos a través de toda la investigación a realizar, servirán de pauta para que la empresa pueda tomar medidas correctivas o preventivas frente a la información que se presentará al concluir el caso de estudio.

CAPITULO I

CONOCIMIENTO GENERAL DE LA EMPRESA

-

IDENTIFICACIÓN MEDIO DE EVIDENCIA

1.1 Introducción

En el siguiente capitulo detallamos, un breve conocimiento acerca de la empresa Rualtim S.A, conociendo su historia, cuales son los objetivos que persigue la organización así como la situación en la que se encuentra actualmente. Además, la compresión sobre las actividades comerciales y de los procesos que normalmente ocurren dentro de la empresa, nos ayudarán a obtener información substancial para el desarrollo de los siguientes capítulos.

Una vez que se conoció a fondo como la empresa manipula la información a través de sus departamentos, se necesitará identificar los riesgos y vulnerabilidades informáticas, que nos servirán de pauta para establecer ciertas métricas para iniciar el análisis de evidencia, el mismo que se ejecutará en el capítulo III.

1.2 Datos Generales de la Empresa

Razón Social:	Rualtim S.A.
Nombre Comercial:	Sarbelt
Actividad Económica:	Venta al por mayor y menor de teléfonos celulares con sus partes y piezas
Fecha Inicio Actividades:	22 de Agosto del 2006
Gerente General:	Ing. Alex Sarmiento
Establecimiento Matriz:	Azogues
Dirección:	Rivera S/N y Sucre
Teléfono:	2244212
Establecimiento Adicional:	Cuenca
Dirección:	Remigio Crespo 2-160 y Federico Proaño
Teléfono:	2887183

1.2.1 Plan Estratégico

1.2.1.1. Visión

Ser la distribuidora autorizada líder en la prestación de servicios de telefonía celular, reconocida y preferida en el austro ecuatoriano.

1.2.1.2. Misión

Facilitar soluciones de calidad a todos nuestros clientes en todo lo referente a comunicación celular, logrando la preferencia de nuestros usuarios para afianzarnos en el mercado austral con el fin de superar los objetivos y metas propuestas.

1.2.1.3. Objetivos

- Ofrecer todo el portafolio de productos que tiene Porta Celular, para abastecer la demanda insatisfecha fruto de la falta de una empresa líder en nuestra región.
- Afianzar nuestro liderazgo en las provincias de Loja y Azuay, ofreciendo como siempre atención culta, oportuna y personalizada para continuar sumando más clientes satisfechos.

- Captar la mayor cantidad de clientes en los lugares donde se está abriendo la señal de Porta Celular.

- Proporcionar información a los usuarios de otras operadoras sobre los beneficios al ser un cliente de Porta Celular.

- Crear nuevas fuentes de trabajo, con lo cual conseguiremos mejorar la calidad de vida de muchas familias ecuatorianas.

1.3 Historia de la Empresa

- Se estableció en la ciudad de Azogues, provincia del Cañar, aquí se maneja la parte Administrativa de la empresa.
- Amplio conocimiento del negocio de telefonía celular desde el año 2003.
- Distribuidor autorizado de porta desde el año 2006.
- Anteriormente se trabajaba como distribuidor de la operadora Movistar.
- A finales del 2007 se crea una sucursal en la ciudad de Cuenca, desde aquí se maneja toda la parte operacional de la empresa.
- Durante el primer año de operación se mantuvo dentro de las tres mejores distribuidoras a nivel austral.
- Constante crecimiento en ventas de la empresa.

Foto 1.1.- Distribuidora Rualtim S.A.

1.4 Hechos a revelar durante el periodo a evaluar

La empresa Rualtim S.A desde sus inicios siempre se ha preocupado por mantener un ambiente agradable entre sus departamentos, sin embargo los directivos de la organización han tenido ciertos inconvenientes en el Departamento de Ventas durante los meses de Julio a Noviembre del 2007 dado los siguientes sucesos:

- Durante el mes de Septiembre el cupo de ventas mensuales no fue cubierta por la empresa.
- Luego de que cierto personal de ventas salió de la empresa nuestros clientes empezaron a trabajar con otra distribuidora.
- Se produjo una disputa inusual entre los propios vendedores de la empresa por el cruce de cuentas V.I.P

- Se encontró un documento impreso en el área de ventas que contenía información de los clientes V.I.P, la cual es información confidencial y que es manejaba exclusivamente por el Gerente de Ventas.
- Luego de intentar recobrar la cartera de clientes, se tuvo conocimiento que los clientes fueron visitados y realizaron los contratos con un ex vendedor de la empresa Rualtim S.A.
- Los clientes no tenían conocimiento que las ventas realizadas por este ex vendedor fueron ingresadas en otra distribuidora.
- Los ordenadores se encontraban infestados de virus así como de aplicaciones instaladas sin previa autorización, que comprometen el manejo y disponibilidad de la información en la empresa.
- No se les proporciona mantenimiento ni actualización a los sistemas y recursos informáticos periódicamente.
- No existe un control de acceso a los recursos informáticos de la empresa ni del personal autorizado para ingresar a cada una de los departamentos.

1.5 Diagnostico de la Situación actual de la Empresa

Rualtim S.A, maneja la distribución y venta de los productos/servicios que comercializa la operadora. Por decisión de los directivos la matriz ubicada en la ciudad de Azogues maneja la parte administrativa, mientras que en la ciudad de Cuenca se realiza toda la parte operativa de la empresa.

Como organización se encuentra comprometida con proporcionar un servicio con la más alta calidad, es decir, dando apoyo y servicio a los miles de clientes que conforman la gran red de sub-distribuidores y clientes satisfechos, todo esto basándose en principios que preserva la empresa.

Sin embargo, el mercado en el cual la distribuidora realiza sus operaciones corre demasiados riesgos por el manejo y acceso a la información, debido a la competencia desleal y el aumento de casos en los cuales los vendedores ofrecieron información confidencial de la empresa a otras distribuidoras, causando pérdidas económicas de gran magnitud y consecuentemente disputas internas en la organización.

1.4.1 Organigrama funcional

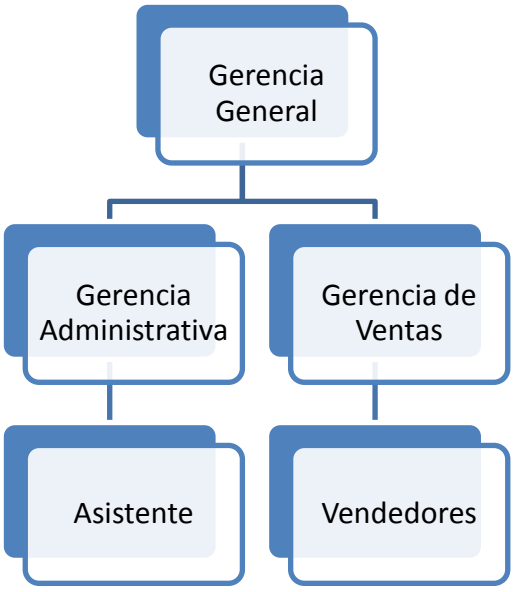


Grafico 1.1. Organigrama de la Empresa

1.4.2 Productos: La Distribuidora comercializa una amplia gama de productos de la compañía PORTA, por lo que sus precios y volumen de ventas estarán en función de la Operadora.

Celulares

- Más de 60 Modelos disponibles
- Servicio Técnico
- Prepago / Postpago

Foto 1.2.- Celular

Amigo Kit

- Banda Ancha
- Celulares
- Base Tip Hogar

Foto 1.3.- Amigo Kit

Cabinas Telefónicas

Foto 1.4.- Cabina Telefónica

Chip

- Prepago / Postpago
- Amigo Chip

Foto 1.5.- Chip

1.6 Identificación de áreas y procesos críticos

Departamento:	Gerencia General
Función:	Garantizar el cumplimiento de las metas de los planes de ventas/distribución mediante la coordinación, planificación y evaluación de los recursos técnicos humanos y administrativos disponibles.
Sistema informático que utiliza:	Ninguno
Tipo de aplicaciones utilizadas para su trabajo:	- Procesador de textos - Hoja electrónica - Editor de presentaciones - Mensajería instantánea - Navegador de Internet

Departamento:	Vendedores
Función:	- Establecer un nexo entre el cliente y la empresa. - Contribuir activamente a la solución de problemas. - Administrar su territorio de ventas. - Alcanzar las metas mensuales puestas por los directivos de la empresa.
Sistema informático que utiliza:	Ninguno
Tipo de aplicaciones utilizadas para su trabajo:	- Procesador de textos - Hoja electrónica - Editor de presentaciones - Mensajería instantánea - Navegador de Internet

Departamento:	Gerencia Administrativa
Función:	Asegurar la administración de las oficinas con los fines de garantizar la adecuada prestación de apoyo logístico requerido por las demás unidades de la empresa.
Sistema informático que utiliza:	PCD
Módulos a los cuales tiene acceso:	- Compras - Ventas - Inventarios
Tipo de aplicaciones utilizadas para su trabajo:	- Procesador de textos - Hoja electrónica - Editor de presentaciones - Mensajería instantánea

Departamento:	Asistente
Función:	Encargado de ingresar al sistema los productos, clientes así como elaborar la respectiva facturación y reportes que se requieran.
Sistema informático que utiliza:	PCD
Módulos a los cuales tiene acceso:	- Compras - Ventas - Inventarios
Tipo de aplicaciones utilizadas para su trabajo:	- Procesador de textos - Hoja electrónica - Mensajería instantánea

Topología de la Red de la Empresa Rualtim S.A.

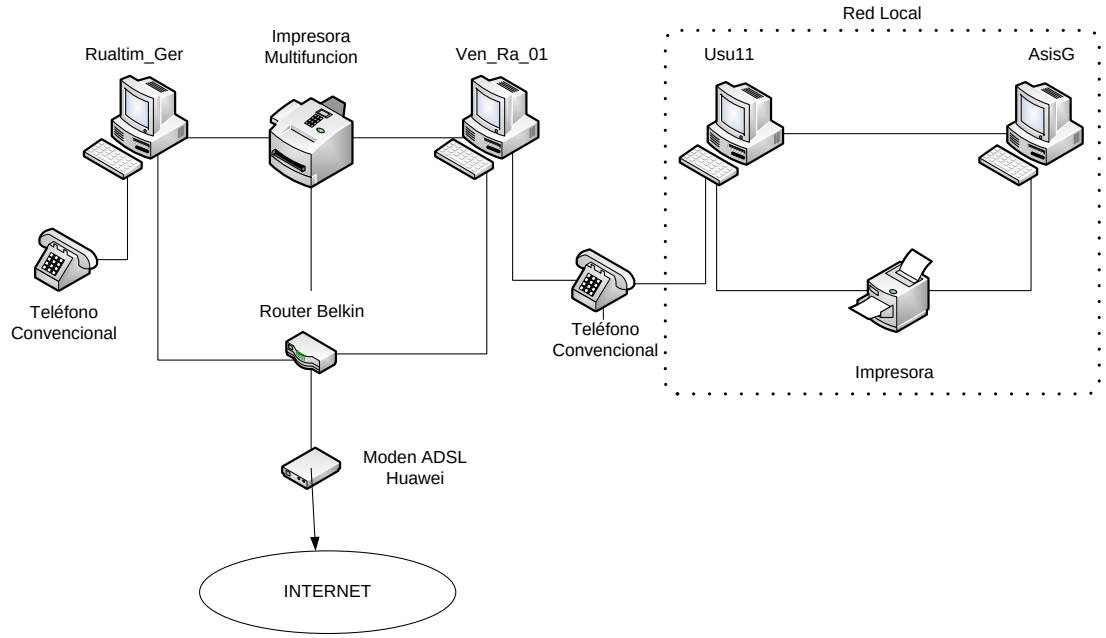


Grafico 1.2. Topología de la Red

Según la organización funcional de la empresa se puede observar que a nivel administrativo se maneja un sistema informático denominado PCD, por medio del cual la empresa gestiona la información concerniente a compras, inventarios y mercaderías.

Por lo descrito anteriormente, se debe conocer el funcionamiento del sistema informático así como de la información que manejan cada una de las áreas de la empresa, para que a continuación se puedan establecer cuáles son las áreas y procesos críticos existentes. A continuación se expondrá el funcionamiento del sistema PCD.

1.6.1 Sistema PCD

La empresa maneja un sistema informático para el área administrativa el cual fue desarrollado en la herramienta FoxPro, este sistema cuenta con los siguientes módulos:

1.6.1.1. Usuarios: A través de este modulo se dan los permisos a las personas encargadas de manejar el sistema, el cual es utilizado principalmente por la gerencia administrativa y su asistente.

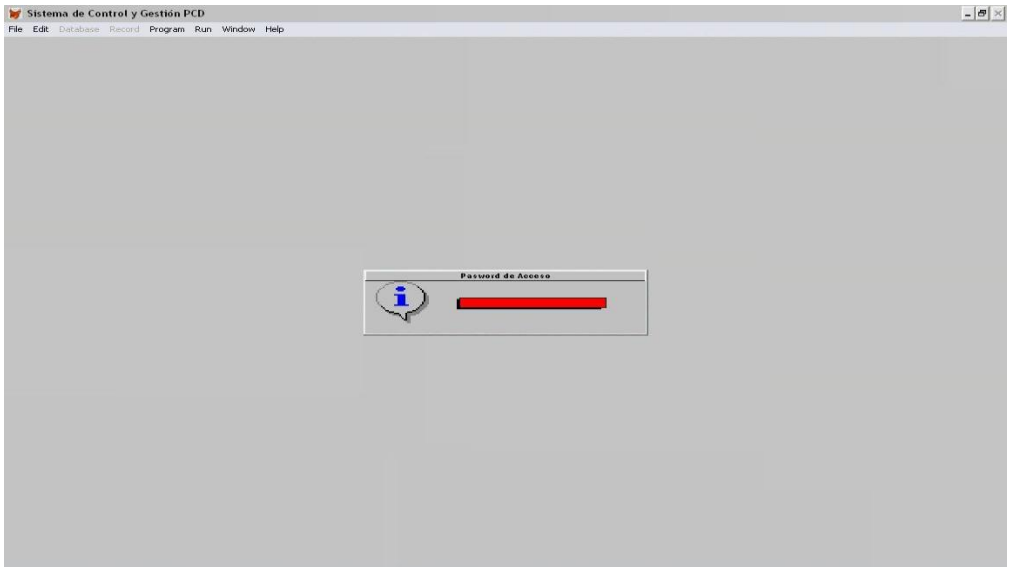


Imagen 1.1.- Ingreso Usuario

1.6.1.2. Compras: A través de este modulo se realiza el ingreso de compras que realiza la empresa.

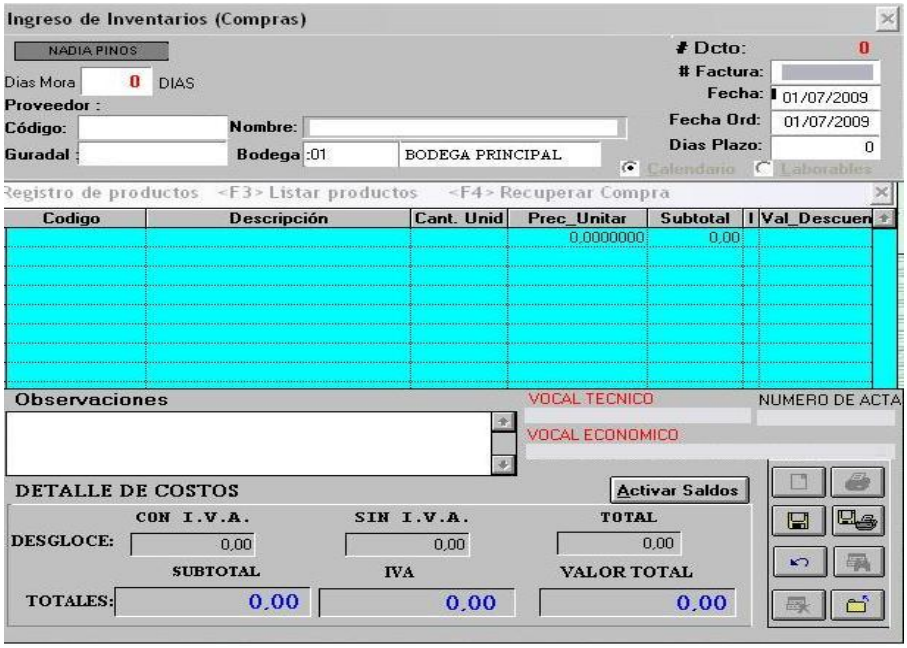


Imagen 1.2.- Ingreso Compras

1.6.1.3. Reporte de Compras: En esta opción el sistema nos proporciona la información sobre las compras realizadas según el tipo de información que se necesite visualizar. El reporte puede ser visualizado en pantalla o ser enviado a impresión.

Imagen 1.3.- Reporte de Compras

1.6.1.4. Productos: En este modulo se realiza el mantenimiento de los productos que maneja la empresa. Se puede realizar una visualización en pantalla o ser enviada a impresión.

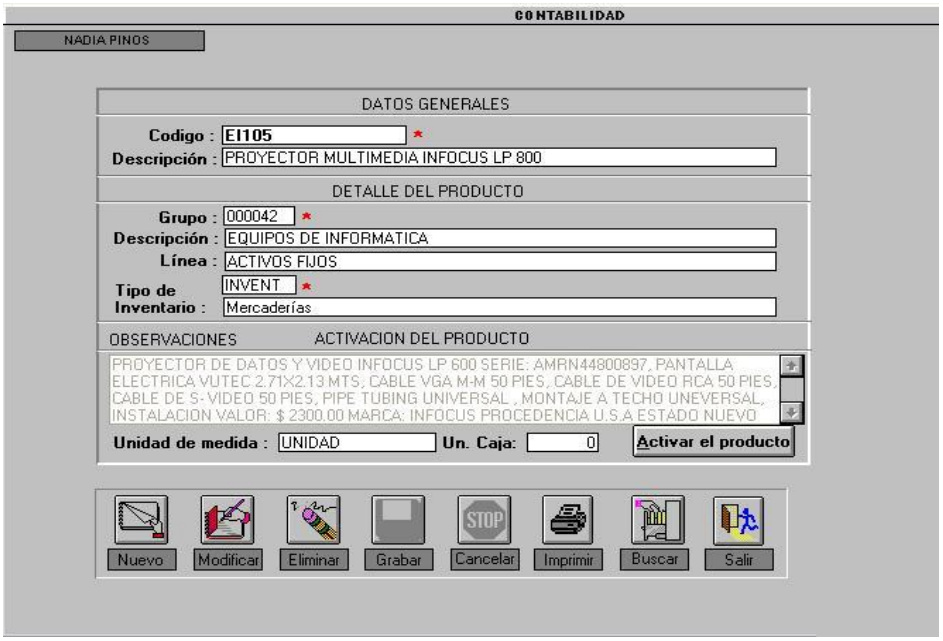


Imagen 1.4.- Mantenimiento de Productos

1.6.1.5. Ventas: Este modulo realiza toda la operación sobre la venta de cada uno de los productos que tiene la empresa.

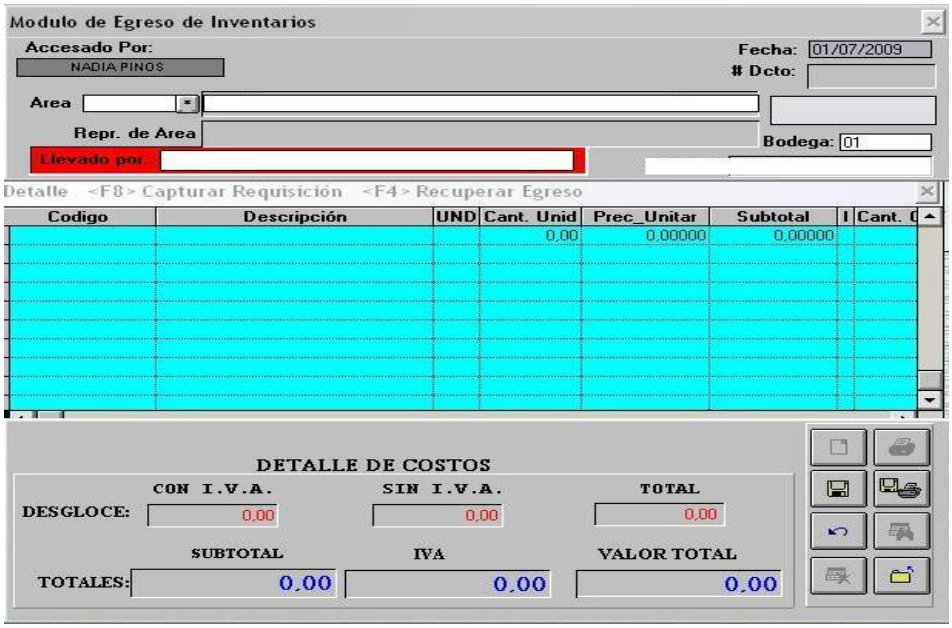


Imagen 1.5.- Modulo de Ventas

1.6.1.6. Clientes: A través de esta pantalla se reporta la información de los clientes que realizaron alguna compra. El reporte puede ser visualizado en pantalla o ser enviado a impresión.

Imagen 1.6.- Modulo de Clientes

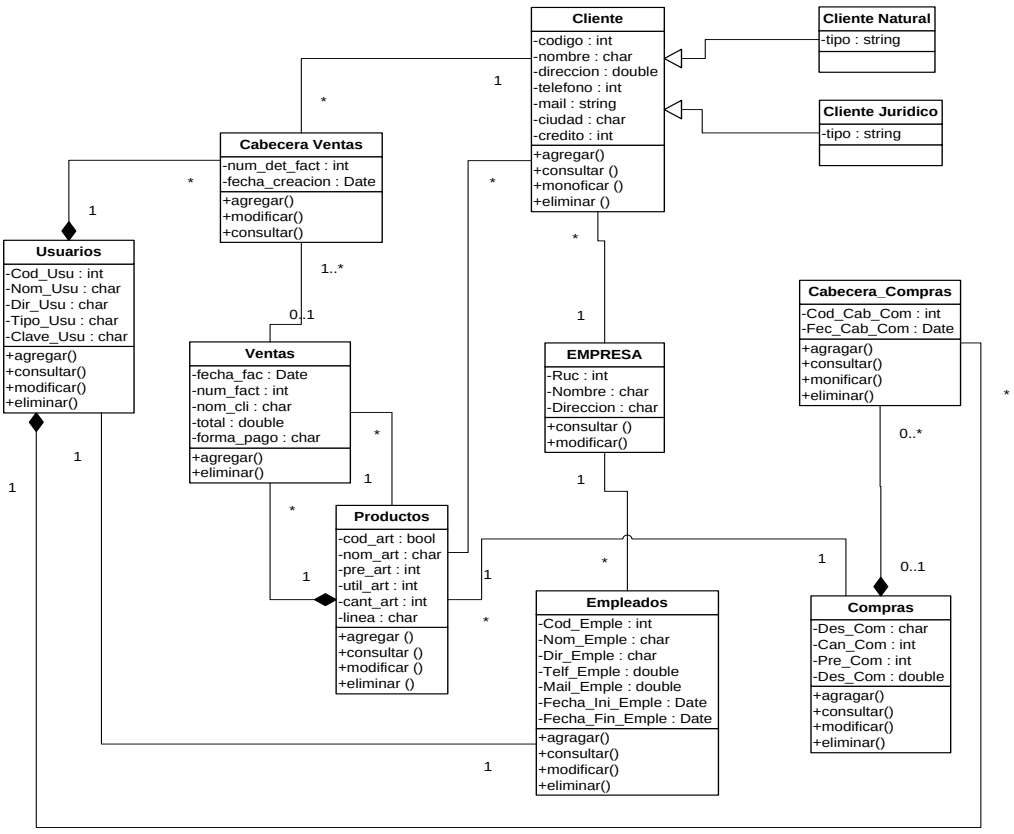


Grafico1.3.- Diagrama de Clases

1.7. Evaluación De Riesgos Y Transacciones

Una vez que se conoció el funcionamiento del sistema PCD, la organización funcional de la empresa y la información que es manipulada por cada área, se procedió a realizar la fase II y III de la Auditoria Informática, por medio de la cual obtuvimos los siguientes resultados:

CALIFICACION DE IMPACTO

Valor	Impacto	Descripcion en terminos economicos
5	Leve	Pequeño daño economico
10	Moderado	Daños entre 500 y 4000 dolares
20	Grave	Daños entre 4001 y 9999 dolares
40	Catastrófico	Mas de 10000 dolares

Áreas	Impacto
Gerencia General	Moderado
Gerencia Administrativa	Considerable
Ventas	Alta

Con los resultados obtenidos a través de la evaluación de riesgos en los departamentos de la empresa Rualtim S.A, se puede concluir que el impacto económico y técnico por la perdida o fuga de información en el departamento de Ventas es muy alto.

Al realizar la matriz de riesgos sobre los procesos en el departamento de ventas se obtuvo el siguiente resultado (Anexo 2):

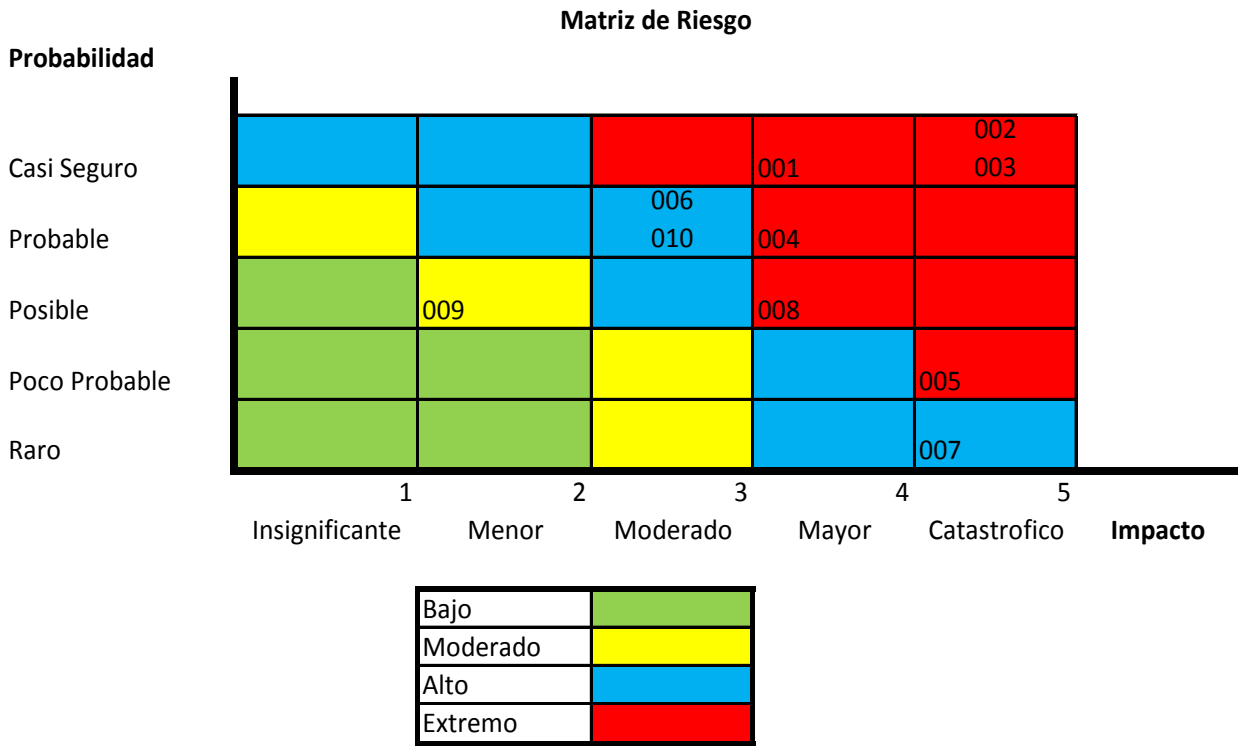


Grafico 1.4.- Matriz de riesgos

Riesgos existentes en el departamento de Ventas

1) Modificación de los archivos del sistema operativo
2) Instalación de programas espía, keylogger, virus, etc
3) Acceso remoto al ordenador
4) Eliminación de información personal de los vendedores
5) Robo del ordenador del departamento
6) Interrupción del sistema operativo
7) Robo de recursos por terceras personas
8) Alteración de información confidencial
9) Falla en el servicio de la red
10) Manejo inadecuado del ordenador

De acuerdo al grafico 1.4 se puede observar que existen muchos riesgos en el departamento de Ventas de la empresa Rualtim S.A, lo cual abre la puerta para que se cometan fraudes y delitos informáticos. Por lo tanto, los incidentes reportados por los directivos de la empresa más los riesgos existentes en el departamento permitirán

que a través del análisis forense se puedan obtener resultados confiables, para que la empresa tome las medidas adecuadas que el caso amerite.

1.8.Identificación y delimitación del tipo de evidencia.

1.8.1 Ámbito del análisis

Debemos destacar que una vez realizado la evaluación de riesgos a través de la Auditoria Informática, el resultado obtenido nos sirve de pauta para tener un conocimiento más amplio sobre el problema que se tratará en los capítulos posteriores. Ya que se estableció que el Departamento de Ventas tiene un impacto demasiado alto con el manejo de la información tanto a nivel departamental como informático, el análisis se enfocará a recopilar evidencia en los recursos informáticos que este departamento manipule, el cual será desarrollado en el Capitulo III de la presente monografía.

1.8.2 Equipo que será analizado

Para poder obtener información fidedigna sobre los recursos informáticos que intervendrán en el análisis forense, se procedió a verificar físicamente los ordenadores existentes en el Departamento de Ventas, además de la revisión de la topología de red de la empresa como la constatación de algún documento que respalde que el ordenador pertenece a este departamento (anexo). Por lo cual se obtuvo como resultado que el computador ven_ra_ 01(Grafico 1.3), será sujeto al análisis forense el cual lo denominaremos de aquí en adelante computador 01, el mismo que presenta las siguientes características:

Marca:	Hp Compaq
Modelo:	Dc5700 Minitower
Serie:	MXJ8160116
Procesador:	Intel Core Duo 2.20Ghz
Capacidad de almacenamiento en disco:	80 Gb
Serie Disco Duro:	9QZ48080

Capacidad de memoria RAM:	2Gb
Sistema Operativo Instalado:	Windows Xp Profesional SP3

Foto 1.6 Ordenador 01 Departamento de Ventas

1.8.3 Información que será analizada

Una vez que se realizó la evaluación de las áreas y procesos críticos más la información suministrada por los directivos de la empresa, podemos determinar que el proceso a ejecutar en el ordenador 01 se fundamentará en la búsqueda de evidencia que contenga información referente a Clientes, Cartera, Ventas, Reportes y Renovaciones, ya que esta información tiene una relación directa con los hechos pasados y que tuvo un impacto económico como organizacional de gran dimensión.

1.9 Conclusión

Luego de haber finalizado este capítulo, se pudo conocer el funcionamiento general de la empresa Rualtim S.A, lo cual aportará información fundamental para el desarrollo de los capítulos siguientes. Uno de los aspectos básicos para el desarrollo de este capítulo, fue realizar un análisis de riesgos sobre las áreas y procesos que maneja la empresa, lo cual permitió revelar las vulnerabilidades existentes en el departamento de Ventas ayudando a complementar la información sobre los hechos

revelados por los directivos de la Empresa, para así poder realizar los procesos pertinentes enmarcados en los parámetros establecidos para las áreas de aplicación.

CAPITULO II

MARCO TEORICO CONCEPTUAL

INFORMATICA FORENSE

2.1. Introducción

La Auditoría Informática y la Informática Forense actualmente tienen un gran campo de acción en la Información que manejan las empresas, debido a la proliferación de redes y sistemas informáticos los cuales incrementaron los riesgos a los que está expuesta la información y que la seguridad se vea afectada directamente para que se lleve a cabo un delito o fraude informático.

De ahí se crea la necesidad de poder mantener la integridad y confidencialidad de la información que soportan los sistemas informáticos en las empresas, para ello, el marco teórico descrito en este capítulo que será aplicada a las áreas de estudio, facilitaran la tarea para poder realizar el desarrollo de los capítulos posteriores.

Cabe señalar que la metodología descrita en el capítulo II es de trascendental importancia, para poder obtener los resultados esperados por las empresas cuando se haya violentado las condiciones básicas de seguridad o exista un indicio sobre el cometimiento de un delito o fraude informático.

2.2. Definición de Informática Forense

2.2.1. Concepto

Informática Forense.- Según el FBI, *"la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional."* [1]

La Informática Forense tiene que ser llevada a cabo bajo un procedimiento que maneje una estandarización sobre las acciones a realizar, ya que este será el camino eficaz para encontrar y presentar los acontecimientos informáticos dentro de una investigación, ya sea esta de carácter penal o civil.

[1] Michael G. Noblett www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

De ahí la aparición de la Informática Forense como una disciplina auxiliar de la justicia actual, que ayuda a enfrentar los desafíos y técnicas de los intrusos informáticos, así como aportar las bases legales a través de la evidencia digital que se revelará en el debido proceso legal.

2.2.2. Términos Importantes

2.2.2.1. Evidencia digital

La evidencia digital constituye un medio que permite obtener información almacenada digitalmente sobre la vinculación de una persona de forma fraudulenta en un sistema informático, en la mayoría de casos esta evidencia se utilizará en un futuro para esclarecer un caso.[2]

2.2.2.2. Cadena de custodia

Esta expresión es un término legal que se refiere a la capacidad de garantizar la identidad e integridad de un espécimen o evidencia desde su obtención, durante su análisis y hasta el final del proceso.[3]

2.2.2.3. Perito

Persona idónea y/o profesional dotada de conocimientos y habilidades especializadas, que suministra información u opinión fundada sobre los puntos de su ámbito científico.[4]

2.2.2.4. Evidencia

Certeza clara, manifiesta y tan perceptible, que nadie puede racionalmente dudar de ella. Toda prueba obtenida conforme a la Ley.[5]

[2] Pedro Miguel Lollett
[3] Alfredo Reino
[4] Pedro Miguel Lollett
[5] Pedro Miguel Lollett

2.2.2.5. Forense

Perteneciente o relativo al Foro, a la Justicia. Añádase por antonomasia a las ciencias que estudian las Evidencias para procesos judiciales.[6]

2.2.2.6. Auditoria Forense

Se define inicialmente a la auditoría forense como una auditoría especializada en descubrir, divulgar y atestar sobre fraudes y delitos en el desarrollo de las funciones públicas y privadas.[7]

2.2.2.7. Prueba Pericial

La prueba pericial es el medio por el cual personas ajenas a las partes, que poseen conocimientos especiales en alguna ciencia, arte o profesión y que han sido precisamente designadas en un proceso determinado, perciben, verifican hechos y los ponen en conocimiento del juez, y dan su opinión fundada sobre la interpretación y apreciación de los mismos. [8]

2.2.2.8. Peritaje Informático Forense

Proceso de Identificación, Adquisición, Preservación, Análisis y Presentación de Evidencia Digital, de acuerdo a Procedimientos Técnico-Legales preestablecidos, como apoyo a la Administración de Justicia en la resolución de un caso Legal.[9]

2.2.2.9. Imagen de Evidencia

Copia del Medio de evidencia utilizada para realizar el Análisis Forense, por clonación o método seguro.[10]

---

[6] Pedro Miguel Lollett
[7] Pedro Miguel Lollett
[8] Pedro Miguel Lollett
[9] Pedro Miguel Lollett
[10] Pedro Miguel Lollett

2.2.2.10. Escena del Crimen

Es el espacio físico o virtual donde se cometió un delito y sus consecuencias, el que debe ser aislado para evitar la contaminación de la Evidencia antes de su correcta preservación.[11]

2.2.3. Principios y Metodología

En una primera instancia dentro del análisis forense se tendrá que responder a una serie de cuestiones referente a los motivos, métodos y culpabilidad que abarca un ataque informático, a continuación enumeraremos una serie de preguntas comunes que rodean un delito informático:

- ¿Cómo se infiltraron?
- ¿Qué obtuvieron?
- ¿Cuáles fueron los medios utilizados?
- ¿Cuánto tiempo han estado?
- ¿Cómo prevenimos una recurrencia?
- ¿Quiénes están involucrados?

2.2.3.1. Evitar la modificación de las evidencias

Se debe tener mucha cautela para manejar los medios que serán utilizados en el procedimiento forense informático, tratando de manejar una copia idéntica de la evidencia obtenida, de tal manera que si ocurriera algún error se pueda recuperar la evidencia original.

2.2.3.2. Asegurar la evidencia

Se requiere la custodia de cada uno de los elementos que intervienen en el caso y que se encuentran a cargo del perito, se debe documentar cada uno de los eventos efectuados con la evidencia, desde el momento en que fue entregada hasta el

[11] Pedro Miguel Lollett

momento que deja de ser custodiada, tratando de no dejar escapar ningún evento que tenga relevancia a futuro.

2.2.3.3. Proceder sistemáticamente

La persona encargada de realizar la investigación tiene que actuar con demasiada cautela con cada uno de los procesos que se realizarán, utilizando una metodología como las herramientas adecuadas al caso, una vez finalizado el proceso se tendrá que presentar los debidos resultados para que cualquier persona externa pueda validar en cualquier momento los mismos.

2.3. Etapas de la Informática Forense

El proceso de investigación de la informática forense consta básicamente de 4 etapas principales, las cuales proporcionan un manejo adecuado de la evidencia en cada una de las fases, a continuación se muestra una figura de las etapas a seguir:

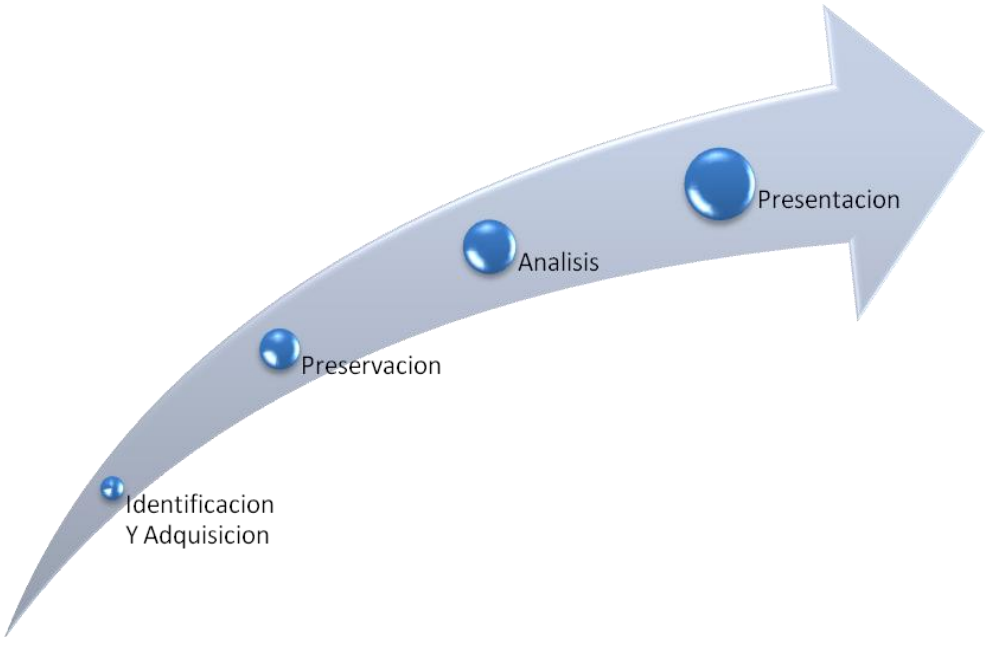


Grafico 2.1.- Etapas de la Informática Forense

Durante el proceso de estudio a realizar emplearemos estas etapas, sin embargo puede existir una etapa adicional dependiendo del caso de estudio, todo esto obedecerá a las técnicas especializadas que se utilicen. En cualquiera de estas etapas

la metodología empleada deberá ser estricta, prestando mucha atención a la documentación que tiene que ser detallada con cada uno de los eventos vinculados al caso en cuestión.

Para cumplir con el análisis forense, la metodología utiliza ciertas directrices que permite confirmar cada etapa realizada, para que en cualquier instancia esta pueda ser ratificada por un tercero, tratando que cada una de las pruebas recopiladas no puedan ser cuestionadas ante un Tribunal de Justicia o sus respectivas autoridades.

2.3.1. Identificación Y Adquisición

En primera instancia se identificará cada uno de los instrumentos que pueden ser considerados como evidencia para su posterior adquisición, el ámbito de trabajo puede ser muy amplio debido a la complejidad de estudio como al extenso tipo de información de los sistemas computacionales a indagar.

2.3.1.1 Cómo proceder en el lugar de los hechos

Como primera medida, lo que se debe tener en cuenta es no alterar o perder ninguna de las evidencias, ya sean estas digitales o físicas en el lugar de los hechos, a fin de poder relacionar las mismas entre sí o en su caso poder hacerlo con el probable responsable, como por ejemplo:

- Tomar los objetos con guantes de hule.
- Por ningún motivo se debería jalar o cortar cables que pudieran representar conexiones de equipos, periféricos o conexiones de entrada o salida de datos.
- Aislar todo dispositivo móvil como teléfonos celulares o dispositivos tipo PDA.
- Controlar el abastecimiento de luz para los equipos.
- Ordenar a la persona que se encuentra en el equipo que suspenda de manera inmediata lo que está haciendo y tratar de tener control de las actividades que realiza hasta que se encuentre separado del equipo y los periféricos.
- Se debe proceder a tomar fotografías del estado, posición de los equipos, sus puertos y demás características sobre los recursos informáticos.

2.3.1.1.1. Información Volátil

Es información que se pierde al momento de desconectar un equipo computacional o al corte de alimentación inadecuada por una tercera persona.

2.3.2.1.2. Información no Volátil

Podemos conseguirla en los dispositivos de almacenamiento como discos duros, USB, Cd, etc. En la práctica este tipo de información resulta más fácil manejarla, preservarla y analizarla.

2.3.1.2. Dispositivos Computacionales para obtención de Evidencia

- Monitor, teclado y ratón (utilizada en casos donde estos dispositivos tengan una relación directa con el infractor y pueda ser utilizada como evidencia)
- Cámara de fotos/video digital
- Cintas de backups
- Tarjetas PCMCIA
- Discos duro, disquete, CD, DVD
- Impresora/escáner/fotocopiadora
- Teléfonos móviles, organizadores de mano (PDA, PocketPC, etc.)
- Tarjetas de red, router, switch, hub, modem
- Redes/Tarjetas inalámbricas
- Puntos de accesos
- Memory Stick/Cards, lector de tarjetas
- Localizador de vehículos y personas
- Contestadoras, fax

Uno de los aspectos críticos referente a la identificación de evidencia digital, es el uso de una adecuada rotulación y el detalle de los elementos informáticos intervenidos. Esto es fundamental para el debido procedimiento judicial, ya que la evidencia digital tendrá el mismo valor probatorio que lo que tiene una prueba en una

escena de un crimen. Debido a esto, si no se toman ciertas precauciones así como el de contar con un laboratorio utilizando la tecnología necesaria, impedirá o retrasará la realización de la investigación.

Para finalizar esta etapa recordemos que la adquisición de la evidencia no debe ir en contra de las leyes que rigen en nuestro país sobre el ámbito informático, por lo cual tenemos que conocer la normativa legal sobre cada uno de los procedimientos a realizar.

2.3.2. Preservación

Esta fase de la investigación se encarga de proteger cada uno de los objetos que tengan valor probatorio, las cuales deben ser completas y verificables. A lo largo del proceso forense esta fase intervendrá en cada instancia, ya que interactúa con las otras fases de la investigación.

Una vez establecida la cadena de custodia se tendrá que preservar cada uno de los aspectos técnicos relativos a la integridad de la evidencia original, evitando la alteración de la información. Aquí se crea la necesidad sobre la utilización de software que permita realizar copias de la evidencia original, la cual nos faculte realizar una imagen a nivel de bit-stream y no una simple copia de archivos, puesto que aquí se pierde información que puede llegar a ser evidencia potencial.

2.3.2.1. Pasos para preservar la evidencia digital

a) Si el dispositivo del cual tenemos que hacer copia de su sistema de almacenamiento está encendido, extraerlo siempre que sea posible y ponerlo en una estación de trabajo para la adquisición de datos.

b) Si existe evidencia digital dentro de los dispositivos de almacenamiento de un computador, esta debe ser copiada utilizando software que maneje procedimientos que de ninguna manera alteren la evidencia y que sean válidos ante un tribunal de justicia en el proceso legal.

c) Conservación sobre el tiempo y fecha de los sistemas.

d) Preservar información de dispositivos móviles y de mano a través de herramientas informáticas, que nos permiten duplicar la información que se está ejecutando así como la contenida en los dispositivos móviles y de mano.

e) Generar los procesos de checksum criptográfico de la copia y del original, este proceso significa generar un hash, valor único para un determinado conjunto de bytes de la evidencia.

f) Documentar detalladamente quien preservó la evidencia, cuáles fueron los medios utilizados, donde la preservo, cuando y porque, así se responsabiliza a cada una de las personas que se encuentran a cargo de la investigación.

g) Empaquetar los dispositivos detalladamente:

h) Los dispositivos magnéticos, ópticos u otros dispositivos que expongan placas, deberán ser en primera instancia colocados en bolsas antiestáticas y después ponerlas en una caja respectiva u otro material protector.

i) Toda la documentación como manuales y libros la colocamos en bolsas de plástico para protegerlos de daños externos.

j) La persona que se encuentre realizando un análisis forense deberá tomar las precauciones necesarias para preservar las evidencias.

k) Transporte de los dispositivos a un lugar seguro y cerrado. La cadena de custodia se debe mantener meticulosamente durante todo el transporte.

2.3.3. Análisis Forense

La fase de análisis tiene como objetivo investigar todos aquellos datos que fueron recopilados y preservados en las etapas anteriores para darles un valor probativo en la investigación, permitiendo que la información obtenida contribuya hacia la reconstrucción del incidente. Sin embargo, la tarea de reconstrucción de sucesos no tiene una metodología precisa, por lo tanto realizamos un razonamiento sobre el cual se trata de involucrar sistemáticamente cada una de las evidencias disponibles sobre las cuales trabajaremos, sin descuidar que el manejo de la evidencia debe ser prudente para que no pierda su confiabilidad.

Ahora tendremos que buscar la vinculación existente entre cada una de las evidencias recopiladas, se realizarán hipótesis acerca de cómo se creó esa evidencia y se confirmará o se anulará la hipótesis llevando a cabo las respectivas pruebas. Esto nos servirá para reconstruir el proceso de ataque realizado tratando de aproximarse lo más posible a la realidad, pero el investigador forense no siempre puede estar totalmente seguro sobre cada uno de los eventos que ocurrieron durante el delito o fraude informático, puesto que disponemos de una cierta cantidad de información recopilada. A pesar de esta situación, el perito presentará las debidas explicaciones posibles basadas únicamente en la información obtenida de la evidencia.

Los datos que se analizarán pueden ser documentos creados, modificados o eliminados por usuarios no autorizados, ficheros borrados del sistema, registro de acceso indebido a las conexiones de red, ficheros ocultos que ejecutan acciones para guardar información del usuario, registro de comandos ejecutados, procesos en ejecución, archivos personales, etc. La mayor parte de estos datos, sobre todo la información que fue eliminada, deberá ser analizada con las respectivas herramientas de software diseñadas con esta finalidad.

Al analizar la evidencia el perito tiene la tarea de intentar responder las siguientes preguntas:

- ✓ **¿Quién?** Recopilar toda la información sobre cada una de las personas que se encuentran implicadas en el delito informático.

- ✓ **¿Cuándo?** Identificar en que instancia se realizaron los sucesos.
- ✓ **¿Qué?** Establecer hasta qué punto el atacante comprometió el sistema o que información fue robada.
- ✓ **¿Cómo?** Aquí tendremos que revelar cada herramienta que fue utilizada para cometer el delito, la experiencia es un factor primordial para obtener los resultados esperados, para lo cual el personal deberá estar altamente capacito para efectuar esta tarea.

2.3.3.1. Categorías del análisis forense

2.3.3.1.1. Datos lógicamente accesibles

Son los datos más comunes y las dificultades que podemos encontrar en estos son:

- ✓ Que exista una gran cantidad de información a analizar.
- ✓ Que estén cifrados.
- ✓ Que estén corruptos o que tengan trampa.

2.3.3.1.2. Datos que han sido eliminados

Son todos los datos que han sido eliminados en toda la vida de los diferentes medios de almacenamiento como son: Discos Duros, Memory Stick, Memory Cards, etc.

2.3.3.1.3. Datos en "ambient data"

Es el espacio no asignado, ficheros de swap/page file, espacio entre sectores, espacio entre particiones, datastreams alternativos. Este tipo de datos necesita software especial para poder ser recuperado.

2.3.3.1.4. Datos en estenografía

Es el proceso por el cual se puede ocultar datos dentro ficheros. Se debe utilizar técnicas estenográficas para buscar información oculta en los sistemas.

2.3.3.2. Elementos a analizar en función del tipo de sistema

2.3.3.2.1. Sistemas informáticos

a) Sistema Windows

- ✓ El registro del sistema permite tener la información sobre todas las configuraciones que se realizan en el ordenador así como ciertas opciones del sistema que se encuentran en ejecución.
- ✓ Archivos y carpetas del sistema de archivos cifrados.
- ✓ Tabla de asignación de ficheros.
- ✓ Podemos examinar la papelera de reciclaje.
- ✓ Servicio de directorio dentro de una red distribuida de computadoras.
- ✓ El visor de sucesos contiene información sobre las aplicaciones, seguridad y sistema del ordenador, nos facilita el acceso a todos los registros.

b) Sistemas Unix/Linux

- ✓ Ficheros SUID/SGID
- ✓ Historial de la Shell
- ✓ Listado descriptores de ficheros.

Además de analizar las evidencias localizadas en los sistemas anteriores se deberá buscar en otros lugares tales como:

- ✓ Los mensajes de correo electrónico que pueden estar almacenados dentro de aplicaciones como Outlook, incredimail, evolution, etc.
- ✓ Cache de los browsers
- ✓ Ficheros/Historiales/Favoritos de los browsers.
- ✓ Log del sistema operativo/aplicaciones.
- ✓ Historial de clientes chat.
- ✓ Documentos de texto, hojas de cálculo.
- ✓ Ficheros gráficos.

2.3.3.2.2. Redes

- Tabla de direcciones IP determinada por el DHCP.

- La cache de ARP que es una tabla que por lo general contiene las direcciones IP.
- Log/Memoria del Sistema de detección de intrusos.
- Log/Memoria del firewall.
- Mensajes de correo electrónico almacenados en el servidor.
- Log de modem/router/servidor.

2.3.3.2.3. Redes inalámbricas

- Información proporcionada por las tarjetas inalámbricas de red.
- Log de modem inalámbrico.
- Puntos de acceso.

2.3.3.2.4. Dispositivos móviles

- Teléfonos móviles, Organizadores de mano
- Ficheros con información almacenada en la tarjeta SIM del móvil.
- Información contenida dentro del chip de memoria Flash.
- Mensajes de texto almacenados dentro del teléfono.
- Grabaciones de audio, video o imágenes almacenadas.

2.3.3.2.5. Sistemas embebidos

- Memory sticks y memory cards (Smarts Card y Compact Flash)

2.3.4. Presentación Judicial

Reporte Final

Este elemento es tan importante como los anteriores, pues una inadecuada presentación de los resultados puede llevar a falsas expectativas o interpretación de los hechos que ponga en entredicho la idoneidad del investigador. Por tanto, la claridad, el uso de un lenguaje amable y sin tecnicismos, una redacción impecable

sin juicios de valor y una ilustración pedagógica de los hechos y los resultados, son elementos críticos a la hora de defender un informe en las investigaciones. Generalmente existen dos tipos de informes, los técnicos con los detalles de la inspección realizada y el ejecutivo para la gerencia y sus dependencias, se debe tener en cuenta las siguientes observaciones:

- ✓ Es necesario documentar las acciones realizadas de manera exhaustiva.
- ✓ Se debe mencionar cual es el software y numero de versión que se uso para el análisis y cual para la recolección.
- ✓ Que métodos se usaron para recolectar y analizar los datos del dispositivo y el por qué se prosiguió de tal o cual forma.
- ✓ El proceder de las acciones del investigador durante el caso debe regirse por la toma de la mejor decisión. Esta decisión debe fundamentarse en su conocimiento, habilidad, las circunstancias del incidente y su papel de neutralidad en la investigación.
- ✓ El reporte final debe estar redactado con base en las anotaciones que se hicieron a lo largo del proceso investigativo y debe ser detallado de forma extensa pero conservando la objetividad en cuanto a lo que es relevante para la investigación.

No debemos olvidar que los reportes realizados deberán ser concretos, ilustrativos y consistentes con los hechos y resultados obtenidos, todo esto con la finalidad de corroborar que la información recopilada desde un inicio de la investigación hasta que finalizó, fue manejada de forma correcta, dando información significativa para las personas u organizaciones que lo demanden.

2.4. Fases de la Auditoria Informática[12]

2.4.1. Fase I: Conocimientos del Sistema

- ➢ Aspectos Legales y Políticas Internas.
  - Sobre estos elementos está construido el sistema de control y por lo tanto constituyen el marco de referencia para su evaluación.

[12] www.mitecnologico.com/Main/FasesAuditoriaInformatica

- Características del Sistema Operativo.
  - Organigrama del área que participa en el sistema
  - Manual de funciones de las personas que participan en los procesos del sistema
  - Informes de auditoría realizadas anteriormente
- Características de la aplicación de computadora
  - Manual técnico de la aplicación del sistema
  - Funcionarios (usuarios) autorizados para administrar la aplicación
  - Equipos utilizados en la aplicación de computadora
  - Seguridad de la aplicación (claves de acceso)
  - Procedimientos para generación y almacenamiento de los archivos de la aplicación.

2.4.2. Fase II: Análisis de transacciones y recursos

- Definición de las transacciones.
  - Dependiendo del tamaño del sistema, las transacciones se dividen en procesos y estos en subprocesos. La importancia de las transacciones deberá ser asignada con los administradores.
- Análisis de las transacciones
  - Establecer el flujo de los documentos
  - En esta etapa se hace uso de los flujo gramas ya que facilita la visualización del funcionamiento y recorrido de los procesos.
- Análisis de los recursos
  - Identificar y codificar los recursos que participan en el sistema.
- Relación entre transacciones y recursos

2.4.3. Fase III: Análisis de riesgos y amenazas

- Identificación de riesgos
  - Daños físicos o destrucción de los recursos
  - Pérdida por fraude o desfalco
  - Extravío de documentos fuente, archivos o informes
  - Robo de dispositivos o medios de almacenamiento

- Interrupción de las operaciones del negocio
- Pérdida de integridad de los datos
- Ineficiencia de operaciones
- Errores

➢ Identificación de las amenazas
- Amenazas sobre los equipos:
- Amenazas sobre documentos fuente
- Amenazas sobre programas de aplicaciones

➢ Relación entre recursos/amenazas/riesgos
- La relación entre estos elementos deberá establecerse a partir de la observación de los recursos en su ambiente real de funcionamiento.

2.4.4. Fase IV: Análisis de controles

➢ Codificación de controles
- Los controles se aplican a los diferentes grupos utilizadores de recursos, luego la identificación de los controles deben contener una codificación la cual identifique el grupo al cual pertenece el recurso protegido. 4.2.Relación entre recursos/amenazas/riesgos
- La relación con los controles debe establecerse para cada tema (Rec/Amz/Rie) identificado. Para cada tema debe establecerse uno o más controles.

➢ Análisis de cobertura de los controles requeridos
- Este análisis tiene como propósito determinar si los controles que el auditor identificó como necesarios proveen una protección adecuada de los recursos.

2.4.5. Fase V: Evaluación de Controles

➢ Objetivos de la evaluación
- Verificar la existencia de los controles requeridos
- Determinar la operatividad y suficiencia de los controles existentes

➢ Plan de pruebas de los controles
- Incluye la selección del tipo de prueba a realizar.

- Debe solicitarse al área respectiva, todos los elementos necesarios de prueba.

- Pruebas de controles
- Análisis de resultados de las pruebas

2.4.6. Fase VI: Informe de Auditoria

- Informe detallado de recomendaciones
- Evaluación de las respuestas
- Informe resumen para la alta gerencia
  - Este informe debe prepararse una vez obtenidas y analizadas las respuestas de compromiso de las áreas.
  - Introducción: objetivo y contenido del informe de auditoria
  - Objetivos de la auditoría
  - Alcance: cobertura de la evaluación realizada
  - Opinión: con relación a la suficiencia del control interno del sistema evaluado
  - Hallazgos
  - Recomendaciones

2.4.7. Fase VII: Seguimiento de Recomendaciones

- Informes del seguimiento
- Evaluación de los controles implantados

2.5. Conclusiones

Este capítulo se encamino sobre la materia contenida para poder asegurar la adquisición, preservación, análisis y reporte sobre el estudio de la Informática Forense, así como el de conocer las fases principales para llevar a cabo una Auditoria Informática.

Por tal circunstancia, cualquier proceso que se lleve a cabo en una investigación no será sencillo, ya que el volumen de información puede ser muy grande y requiere tiempo para dar el tratamiento eficaz a los datos. Esto significa, que en la mayoría de

procesos a ejecutar el esfuerzo que la investigación demandará como los conocimientos especiales del perito serán mayores para obtener los resultados esperados.

CAPITULO III

CASO PRACTICO DE ESTUDIO

3.1 Introducción

Para efectuar el caso práctico de estudio de este Capítulo, fue necesario conocer tanto los aspectos preliminares sobre la Empresa desarrollado en el Capítulo I como el marco teórico-conceptual de la Informática Forense.

Además para poder realizar el proceso forense de la información, utilizaremos una metodología ordenada y controlada para que la evidencia recogida, preservada, analizada y presentada se la realice de forma íntegra y confiable, evitando que a lo largo del proceso se cometa algún error, lo que invalidaría todo el proceso realizado.

Durante el proceso práctico de estudio debemos recordar como peritos que cada caso a investigar es diferente, por tal motivo el proceso de análisis será ejecutado con una estructura de trabajo integral y transparente para organizar y analizar la gran cantidad de datos, para poder finalmente poder emitir los resultados pertinentes sobre las causas del incidente o hecho suscitado.

3.2 Ejecución de las Etapas de la Informática Forense

3.2.1 Identificación y adquisición

Según el problema reconocido por los directivos de la empresa Rualtim S.A y una vez determinados los riesgos evidentes detallados en el Capítulo I, se pudo determinar que el Departamento de Ventas será el área donde se ejecutará el proceso de análisis forense.

Para poder iniciar el proceso forense se debió identificar los recursos informáticos involucrados en el departamento antes mencionado, por cual relacionamos la información obtenida a través del grafico 1.2 más la constatación física del equipo, para concluir que el Ordenador 01 es el intervendrá en todo el proceso de análisis Forense. Luego de identificar los sistemas y recursos intervenidos, se tiene que obtener toda la evidencia en el Ordenador 01 por lo cual se procedió a solicitar la debida autorización al Gerente de la Empresa, para poder comenzar el día 28 de Junio del 2009 el proceso de Análisis Forense en el Departamento de Ventas.

3.2.1.1 Herramientas a utilizar:

- **Software Helix:** Herramienta poderosa utilizada en la informática forense que permite el análisis y tratamiento de la información. A través de esta herramienta realizaremos la obtención de imágenes forenses de datos del Ordenador 01. La versión de esta herramienta que utilizaremos es la 1.8, esta herramienta se la puede descargar de forma gratuita.

- Una computadora de escritorio 02 con las siguientes características:

Marca:	Clon
Modelo:	Ninguno
Serie:	Ninguno
Procesador:	2.1 Ghz
Capacidad de memoria RAM:	4GB
Sistema Operativo Instalado:	Windows XP Profesional

- Un enclosure que será utilizado para conectarlo al ordenador 01, a través de este almacenaremos la imagen en los siguientes dispositivos de almacenamiento:

Descripción	Marca	Serie	
Disco Duro 1	Maxtor	CND75126	Imagen 01
Disco Duro 2	Seagate	VT488951	Imagen 02

3.2.1.2 Preparación para la adquisición de evidencia

Una vez autorizados por el Ing. Alex Sarmiento gerente de la empresa Rualtim S.A. previo al análisis forense, se estableció que el día 28 de Junio del 2009 se iniciará el proceso para la adquisición de la evidencia. Para tal proceso intervienen como peritos el Señor Osvaldo Sebastián Zapata Avila y el Señor Andrés Oswaldo Torres Bustamante.

El Ing. Alex Sarmiento estará presente como observador durante el proceso a realizar.

Se procedió a reunir la información sobre el ordenador 01 por medio de las especificaciones que constan en el respectivo documento (anexo), que se detalla en la siguiente tabla:

Marca:	Hp Compaq
Modelo:	Dc5700 Minitower
Serie:	MXJ8160116
Procesador:	Intel Core Duo 2.20Ghz
Capacidad de almacenamiento en disco:	80 Gb
Serie Disco Duro:	9QZ48080
Capacidad de memoria RAM:	2Gb
Sistema Operativo Instalado:	Windows Xp Profesional SP3

Foto 3.1.- Ordenador 01

3.2.1.3 Sistema en el que opera el ordenador 01

Imagen 3.1.- Visualización del Escritorio del Ordenador 01

3.2.1.4 Punto de Red del Ordenador 01

El ordenador se encuentra conectado al punto de red 0-15, el otro punto de red del cajetin se encuentra desconectado, por tanto el ordenador siempre tiene la misma direccion ip.

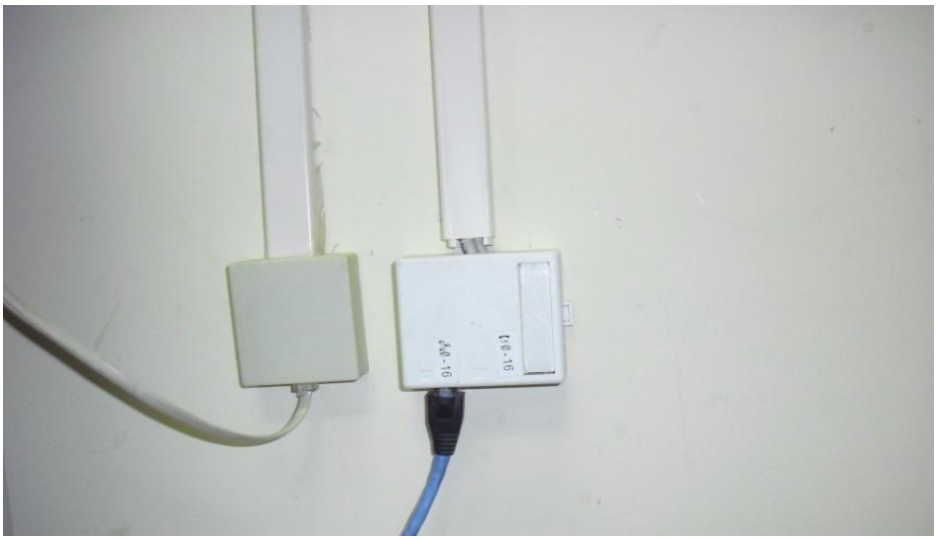


Foto 3.2.- Punto de red 0-15 del Ordenador 01

3.2.1.5 Información a través de la herramienta Hélix

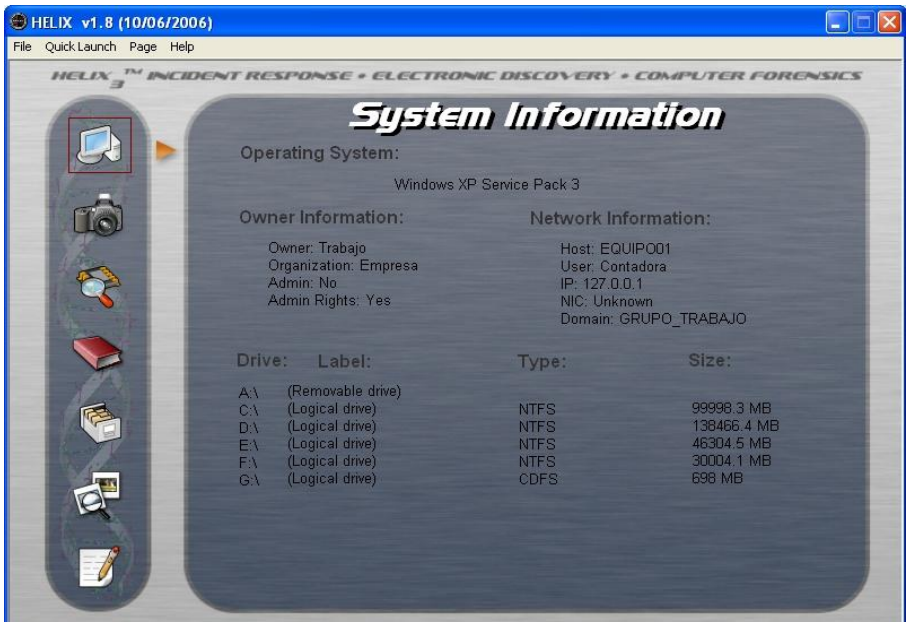


Imagen 3.2.- Nos muestra la información del Sistema Operativo

3.2.2 Preservación

3.2.1.1 Proceso para la obtención de imágenes de disco

Utilizaremos el ordenador descrito anteriormente en el punto 3.2.1.2. Como peritos comenzaremos con la adquisición forense de los datos contenidos en la prueba instrumental de carácter informatico del ordenador 01. El procedimiento a realizar se denomina comunmente “imaging” por el cual se obtienen imágenes forenses de datos. Luego de finalizar el proceso de obtencion de imágenes se debera determinar si las imágenes obtenidas se crearon correctamente, para lo cual se verifica y valida la integridad de las mismas, comprobando que los valores de hash de la prueba instrumental de carácter informatico y de las imágenes coincida.

A continuación se especifican los pasos para obtener la imagen de disco, a través del FTK Imager:

a) Seleccionamos la unidad Física que contiene la información para ser analizada:

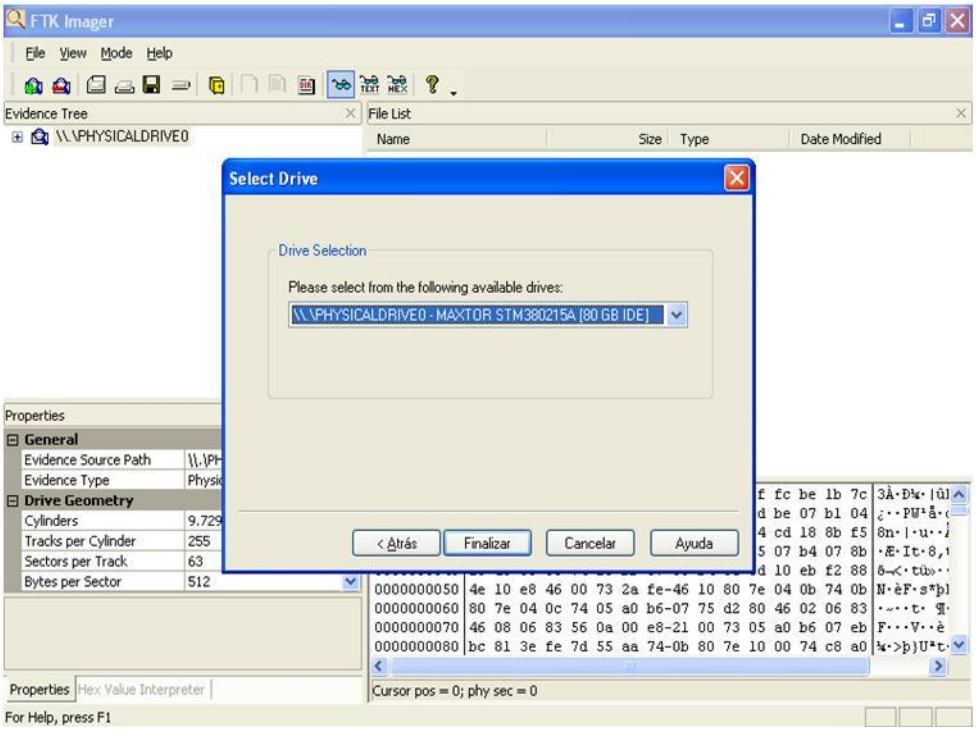


Imagen 3.3.- Selección de la unidad a través del FTK Imager

b) Se selecciona el tipo de imagen a ser creada, para nuestro caso escogimos la opción Raw(dd):

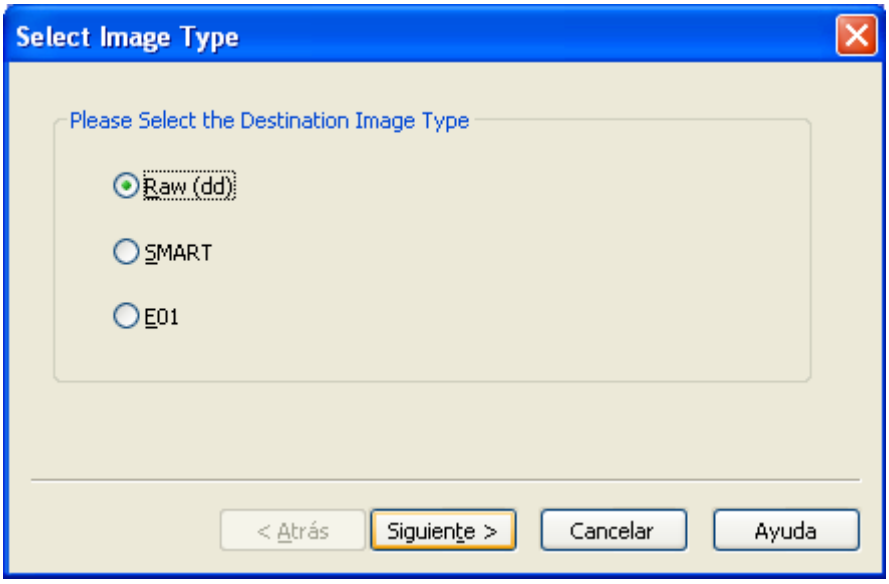


Imagen 3.4.- Opción para escoger el tipo de imagen que se creará

c) Se despliega una pantalla en la cual se añade la imagen a ser creada

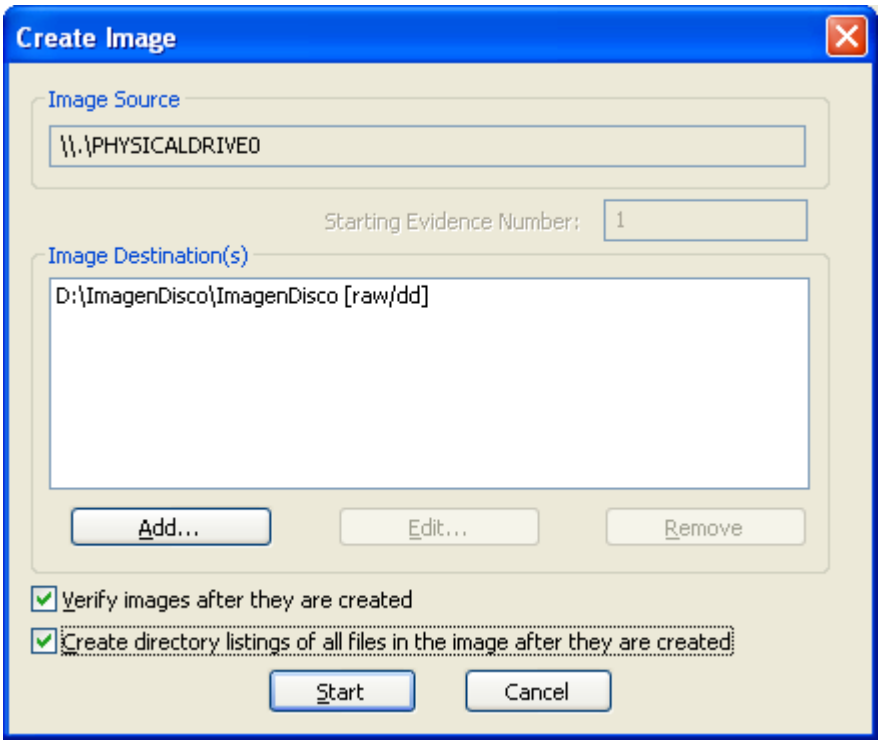


Imagen 3.5.- Escoge opciones para la imagen que será creada

d) Aquí elegimos la carpeta donde va ser almacenada la imagen de disco, además escogemos el tamaño de cada una de las imágenes a ser creadas. Para nuestro caso almacenamos en la dirección D:\ImagenDisco.

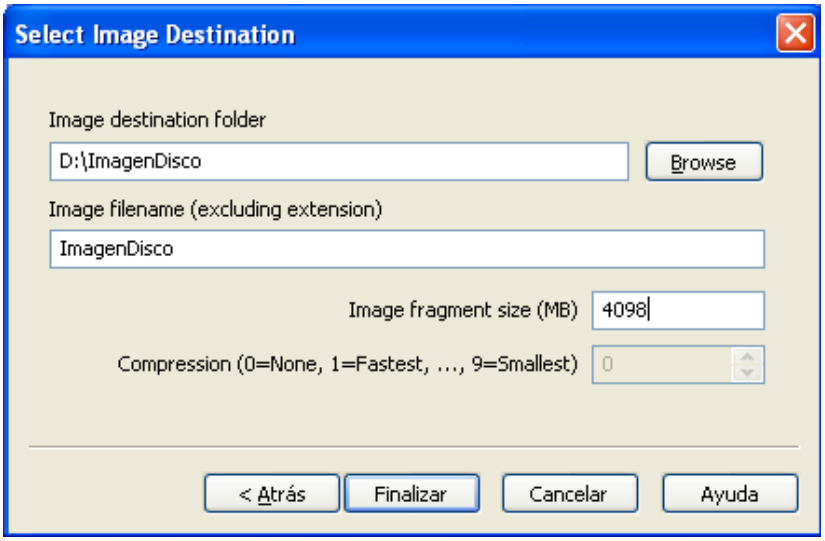


Imagen 3.6.- Selección de la carpeta donde se almacena la imagen de datos

e) Inicio de la creación de la imagen

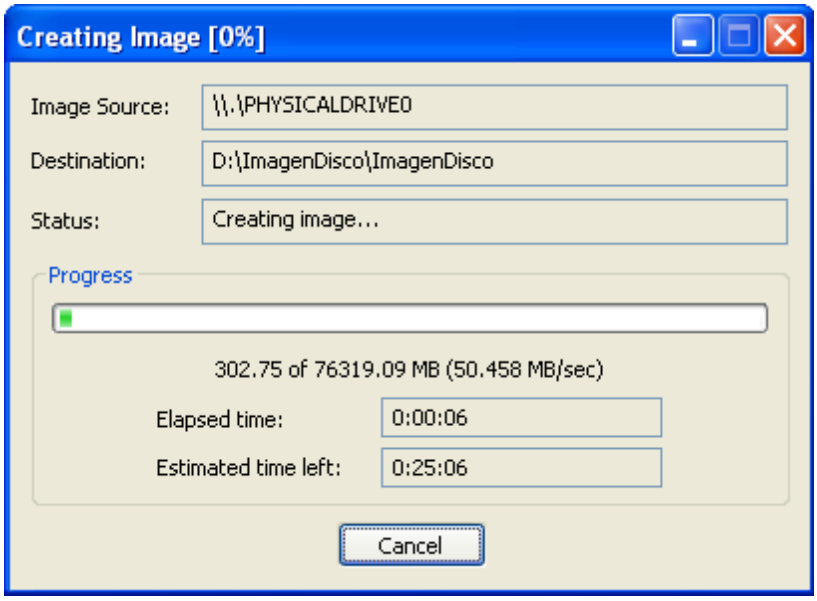


Imagen 3.7.- Progreso de la creación de imagen de datos

f) Culminación del proceso de la creación de imágenes de disco

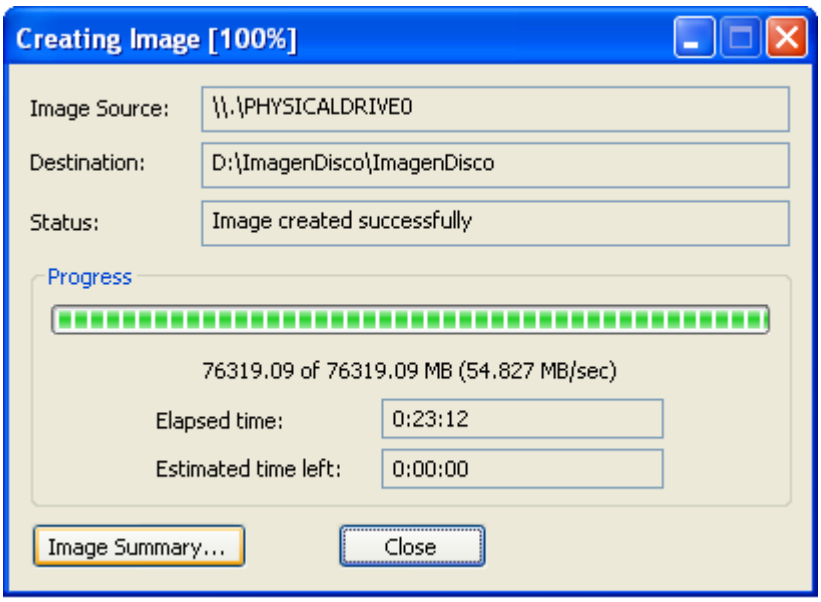


Imagen 3.8.- Finalización de la creación de imagen de datos

g) Al finalizar el proceso podemos observar un pequeño reporte del proceso finalizado.

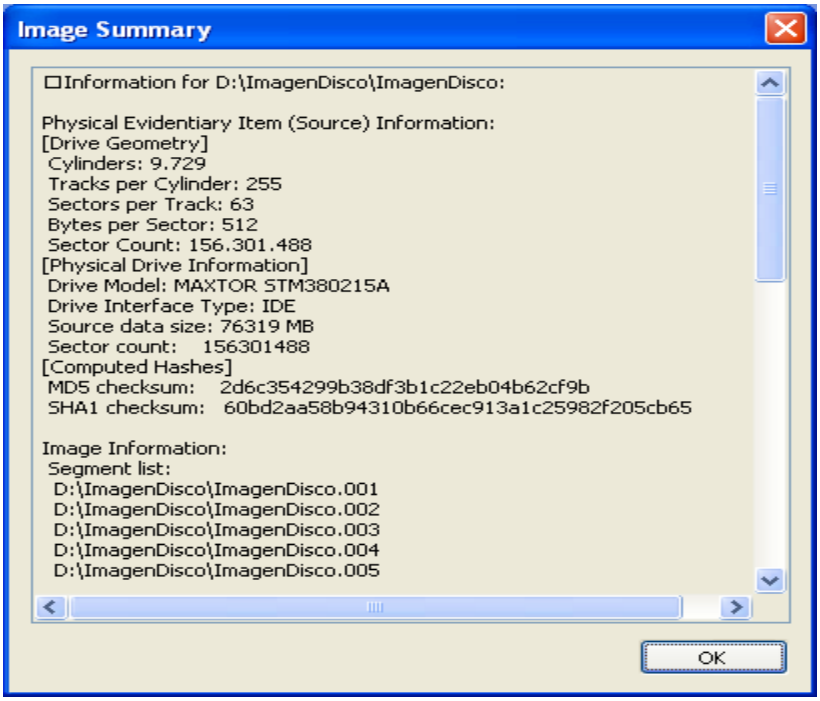


Imagen 3.9.- Sumario donde nos muestra información del proceso realizado

h) Resultado obtenido al finalizar el proceso de creación de imagen de disco 01

Descripción	
Fecha de Inicio:	28 de Junio del 2009
Hora de Inicio:	20:03:19 pm
Fecha de Finalización:	28 de Junio del 2009
Hora de Finalización:	23:14:20 pm
Archivos obtenidos:	image.dd_audit.log image.dd imagen.csv
SHA1 cheksum:	60bd2aa58b94310b66cec913a1c25982f205cb65
Archivo obtenido:	image.dd.md5
MD5 Cheksum:	2d6c354299b38df3b1c22eb04b62cf9b

- Lista de imágenes obtenidas:

D:\ImagenDisco\ImagenDisco.001	D:\ImagenDisco\ImagenDisco.020
D:\ImagenDisco\ImagenDisco.002	D:\ImagenDisco\ImagenDisco.021
D:\ImagenDisco\ImagenDisco.003	D:\ImagenDisco\ImagenDisco.022
D:\ImagenDisco\ImagenDisco.004	D:\ImagenDisco\ImagenDisco.023
D:\ImagenDisco\ImagenDisco.005	D:\ImagenDisco\ImagenDisco.024
D:\ImagenDisco\ImagenDisco.006	D:\ImagenDisco\ImagenDisco.025
D:\ImagenDisco\ImagenDisco.007	D:\ImagenDisco\ImagenDisco.026
D:\ImagenDisco\ImagenDisco.008	D:\ImagenDisco\ImagenDisco.027
D:\ImagenDisco\ImagenDisco.009	D:\ImagenDisco\ImagenDisco.028
D:\ImagenDisco\ImagenDisco.010	D:\ImagenDisco\ImagenDisco.029
D:\ImagenDisco\ImagenDisco.011	D:\ImagenDisco\ImagenDisco.030
D:\ImagenDisco\ImagenDisco.012	D:\ImagenDisco\ImagenDisco.031
D:\ImagenDisco\ImagenDisco.013	D:\ImagenDisco\ImagenDisco.032
D:\ImagenDisco\ImagenDisco.014	D:\ImagenDisco\ImagenDisco.033
D:\ImagenDisco\ImagenDisco.015	D:\ImagenDisco\ImagenDisco.034
D:\ImagenDisco\ImagenDisco.016	D:\ImagenDisco\ImagenDisco.035
D:\ImagenDisco\ImagenDisco.017	D:\ImagenDisco\ImagenDisco.036
D:\ImagenDisco\ImagenDisco.018	D:\ImagenDisco\ImagenDisco.037
D:\ImagenDisco\ImagenDisco.019	D:\ImagenDisco\ImagenDisco.038

Tabla 3.1.- Imágenes de Disco

El proceso anterior se lo repitió una segunda vez para obtener una segunda imagen de los datos; por lo tanto, se generaron en total dos imágenes forenses. Los resultados de la segunda imagen nos permitieron observar que el proceso se realizó de manera confiable, obteniendo los siguientes resultados:

Descripción	
Fecha de Inicio:	28 de Junio del 2009
Hora de Inicio:	23:25:29 pm
Fecha de Finalización:	29 de Junio del 2009
Hora de Finalización:	01:45:56 am
Archivos obtenidos:	image.dd_audit.log image.dd imagen.csv
SHA1 cheksum:	60bd2aa58b94310b66cec913a1c25982f205cb65
Archivo obtenido:	image.dd.md5
MD5 Cheksum:	2d6c354299b38df3b1c22eb04b62cf9b

Una vez obtenido los resultados a través de la creación de imagen de datos, se obtuvo un archivo imagen.csv dentro del cual se encuentra un listado con todos los archivos borrados del computador 01. Para la investigación que se realiza utilizamos una selección de todos los archivos que son importantes para nuestra investigacion, es decir documentos que contengan las extensiones xls, doc, xml, por lo cual guardamos este resultado en un nuevo archivo denominado informe.xls.

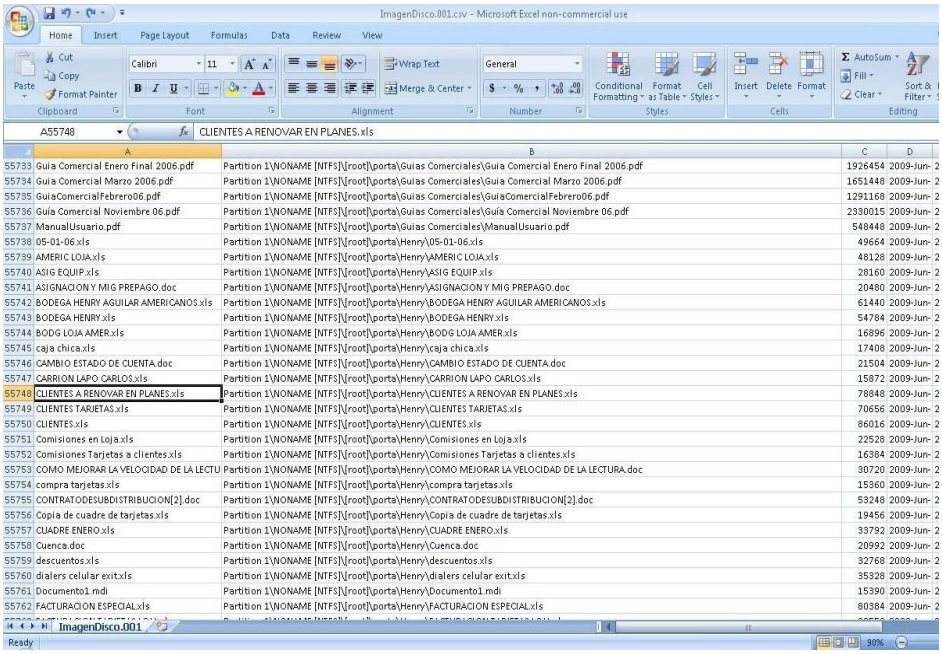


Imagen 3.10.- Archivo generado al realizar el proceso de creación de imagen

3.2.3 Análisis Forense

Una vez que se obtuvo los resultados en el punto **H** y conociendo que el proceso se efectuó de modo confiable e integro, se procede al análisis de la imagen obtenida utilizando las siguientes herramientas:

- ✓ **PC Inspector File Recovery:** Software que permite recuperar datos perdidos y soporta los sistemas de la Fat 12/16/32 y NTFS. Utilizamos la version 2.60.

- ✓ **Mount Image Pro:** Herramienta que nos permite montar imágenes obtenidas, conservando la integridad de la imagen que será analizada. Se utilizara la version 4.0 de este software.

3.2.3.1 Proceso de análisis sobre la imagen da datos obtenida

a) Agregamos la imagen de datos obtenida a través de la herramienta Mount Image Pro para ser analizada.

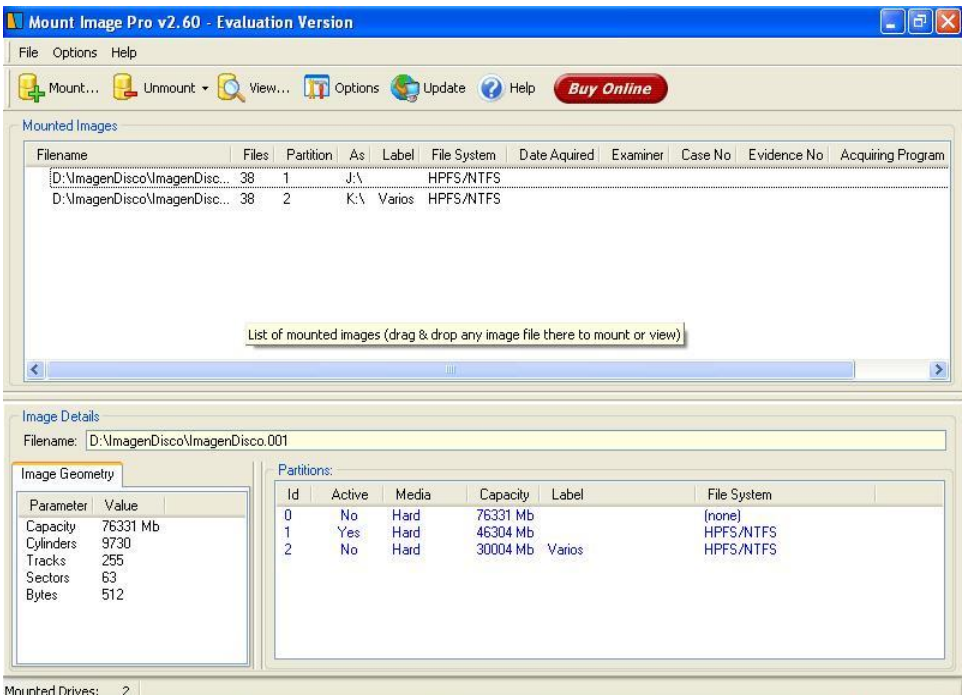


Imagen 3.11.- Montamos la imagen en el software para poder analizar los archivos

b) Seleccionamos la unidad física o lógica, por medio del cual se conseguirá a través de la herramienta PC Inspector recuperar los datos perdidos y borrados.

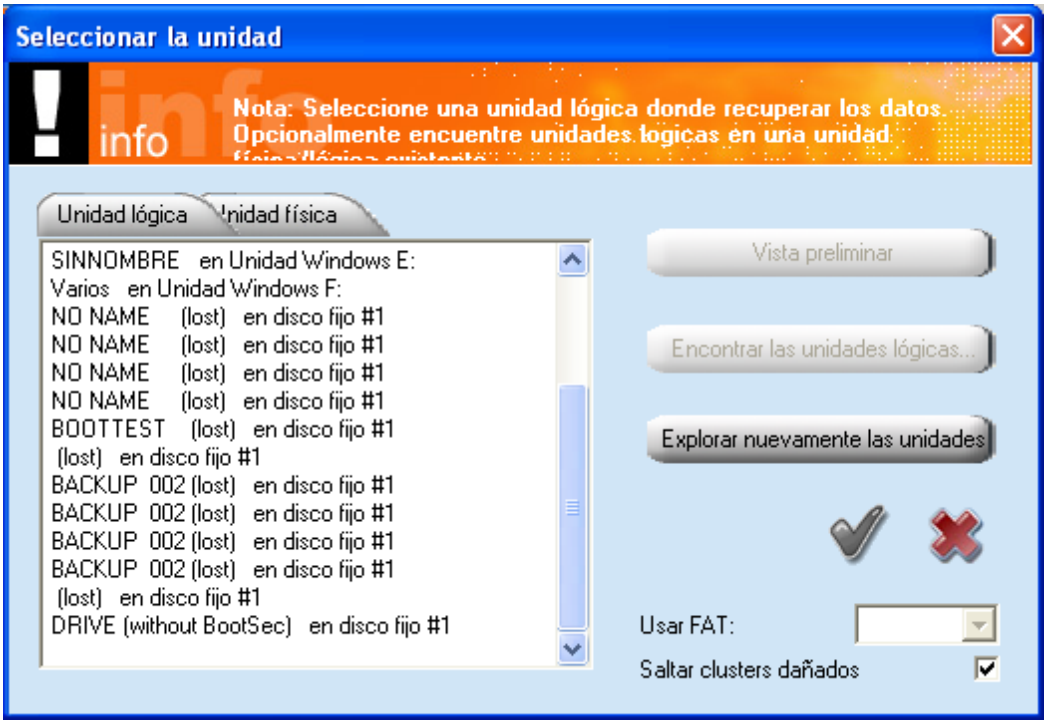


Imagen 3.12.- Selección Unidad Lógica/Física

c) Recuperación de los datos perdidos con la ayuda de la herramienta PC Inspector File Recovery

Se procede a recuperar todos los datos perdidos utilizando la Computadora 02 detallada en el punto 3.2.1.1. Por medio de la herramienta PC Inspector File Recovery 2.60 podemos visualizar la papelera de reciclaje y el contenido de los archivos que pueden ser recuperados.

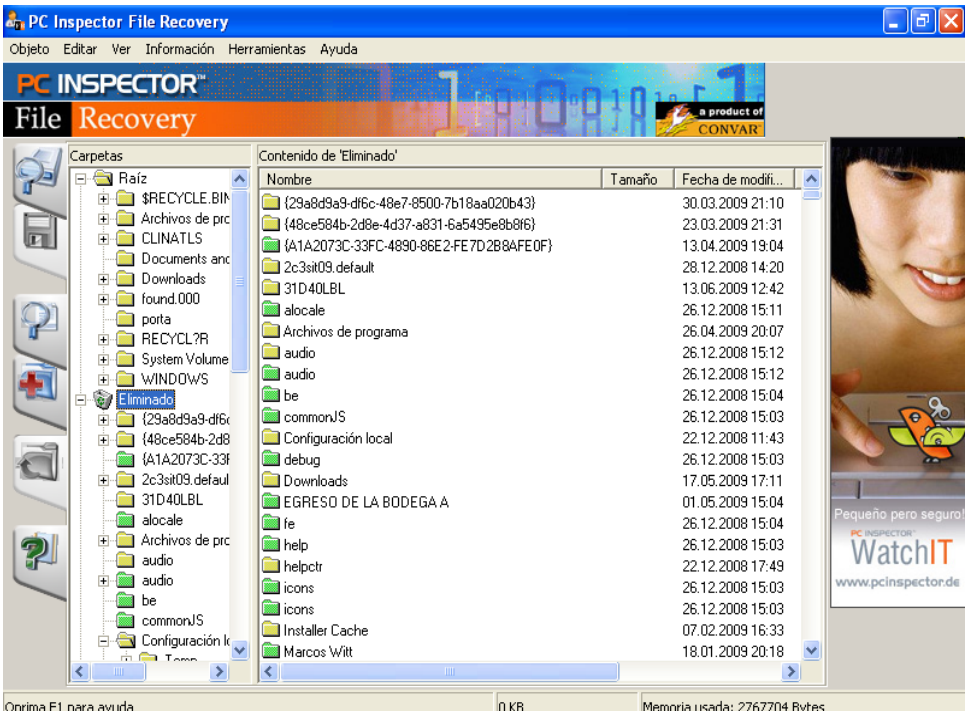


Imagen 3.13.- Visualización de los archivos eliminados a través de PC Inspector

d) Proceso de recuperación de archivos perdidos

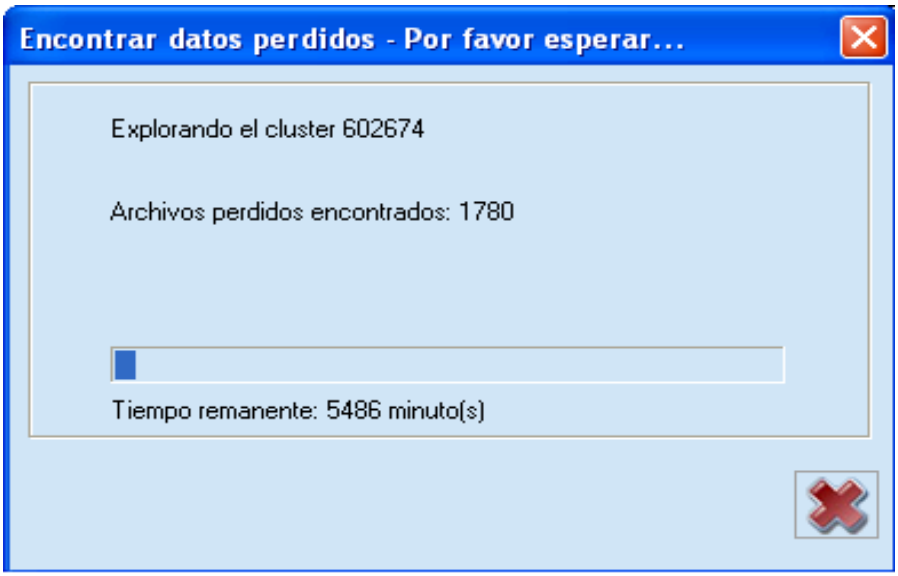
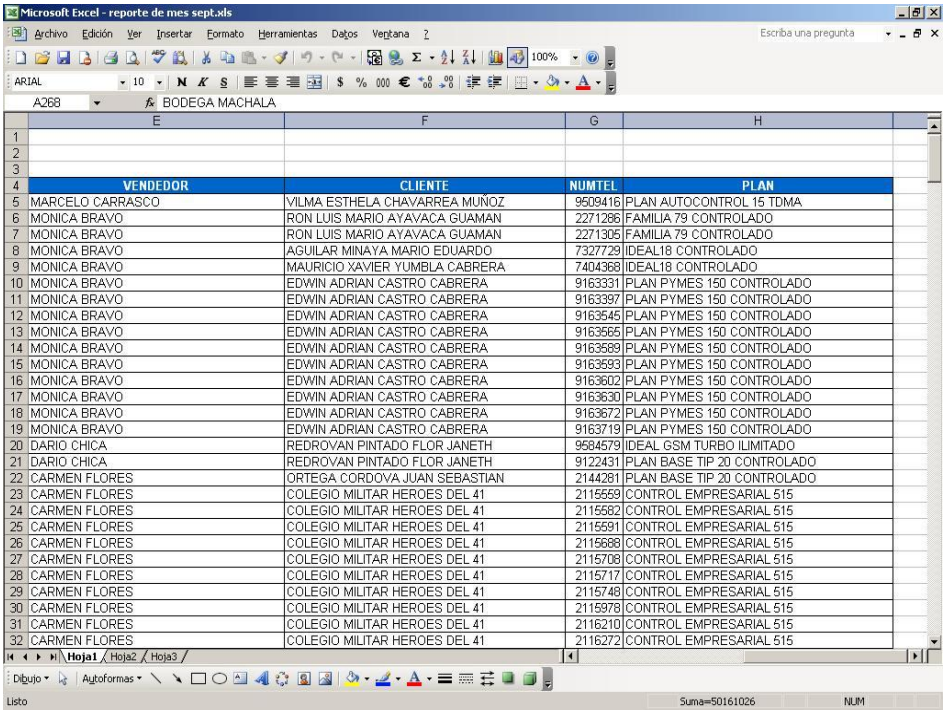


Imagen 3.14.- Inicio del proceso de recuperación de datos perdidos

Una vez que finalizó el proceso de recuperación de archivos perdidos a través de la herramienta PC Inspector File Recovery 2.60, procederemos al análisis de la información obtenida tomando como referencia todos los archivos que contengan las extensiones *.XLS; *.DOC; *.XML.

En esta parte del análisis de la información se debe tener mucho cuidado, ya que podemos descartar archivos que tengan información importante para la investigación, para el caso en concreto realizamos una abstracción de la información basandonos en las fechas de creación, modificación y acceso. Tambien se realizó una depuración de los datos obtenidos empleando los nombres que podrian contener información confidencial referente a los indicios descritos en el capitulo I como son: cartera, ventas,reporte, planes, etc.

Una vez que realizamos un profundo análisis sobre la informacián recuperada, se obtuvo dos tipos de archivos contenidos dentro de la carpeta del Vendedor 01. El primer archivo corresponde a una hoja de calculo el cual tiene el reporte de ventas para renovacion del mes de Septiembre del 2007.


Microsoft Excel - reporte de mes sept.xls

	VENDEDOR	CLIENTE	NUMTEL	PLAN
5	MARCELO CARRASCO	VILMA ESTHELA CHAVARREA MUÑOZ	9509416	PLAN AUTOCONTROL 15 TDMA
6	MONICA BRAVO	RON LUIS MARIO AYAVACA GUAMAN	2271286	FAMILIA 79 CONTROLADO
7	MONICA BRAVO	RON LUIS MARIO AYAVACA GUAMAN	2271305	FAMILIA 79 CONTROLADO
8	MONICA BRAVO	AGUILAR MINAYA MARIO EDUARDO	7327729	IDEAL18 CONTROLADO
9	MONICA BRAVO	MAURICIO XAVIER YUMBLA CABRERA	7404368	IDEAL18 CONTROLADO
10	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163331	PLAN PYMES 150 CONTROLADO
11	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163397	PLAN PYMES 150 CONTROLADO
12	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163545	PLAN PYMES 150 CONTROLADO
13	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163565	PLAN PYMES 150 CONTROLADO
14	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163589	PLAN PYMES 150 CONTROLADO
15	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163593	PLAN PYMES 150 CONTROLADO
16	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163602	PLAN PYMES 150 CONTROLADO
17	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163630	PLAN PYMES 150 CONTROLADO
18	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163672	PLAN PYMES 150 CONTROLADO
19	MONICA BRAVO	EDWIN ADRIAN CASTRO CABRERA	9163719	PLAN PYMES 150 CONTROLADO
20	DARIO CHICA	REDROVAN PINTADO FLOR JANETH	9584579	IDEAL GSM TURBO ILIMITADO
21	DARIO CHICA	REDROVAN PINTADO FLOR JANETH	9122431	PLAN BASE TIP 20 CONTROLADO
22	CARMEN FLORES	ORTEGA CORDOVA JUAN SEBASTIAN	2144281	PLAN BASE TIP 20 CONTROLADO
23	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2115559	CONTROL EMPRESARIAL 515
24	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2115582	CONTROL EMPRESARIAL 515
25	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2115591	CONTROL EMPRESARIAL 515
26	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2115688	CONTROL EMPRESARIAL 515
27	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2115708	CONTROL EMPRESARIAL 515
28	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2115717	CONTROL EMPRESARIAL 515
29	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2115748	CONTROL EMPRESARIAL 515
30	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2115978	CONTROL EMPRESARIAL 515
31	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2116210	CONTROL EMPRESARIAL 515
32	CARMEN FLORES	COLEGIO MILITAR HEROES DEL 41	2116272	CONTROL EMPRESARIAL 515

Imagen 3.15.- Archivo recuperado de la carpeta del Vendedor 01

Además dentro de la misma carpeta del vendedor 01 se pudo encontrar las conversaciones de mensajeria instantánea de uno de los mejores vendedores de la empresa, por lo cual el vendedor 01 dispuso de esa información sin la autorización pertinente.

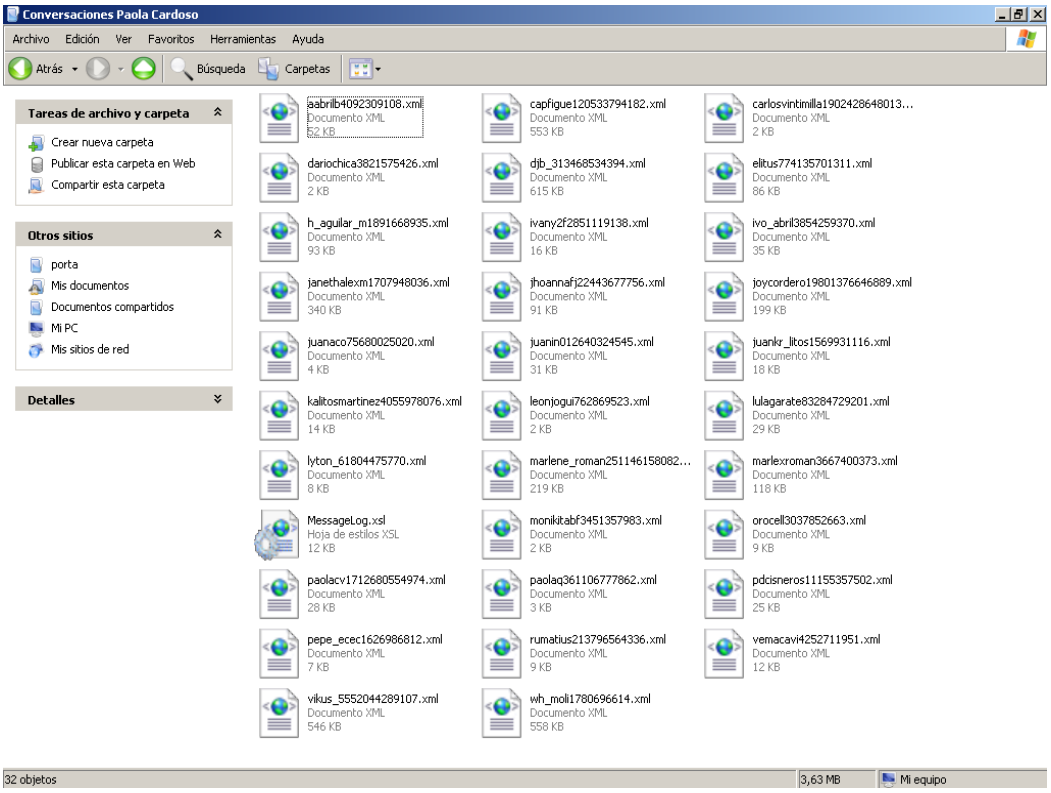
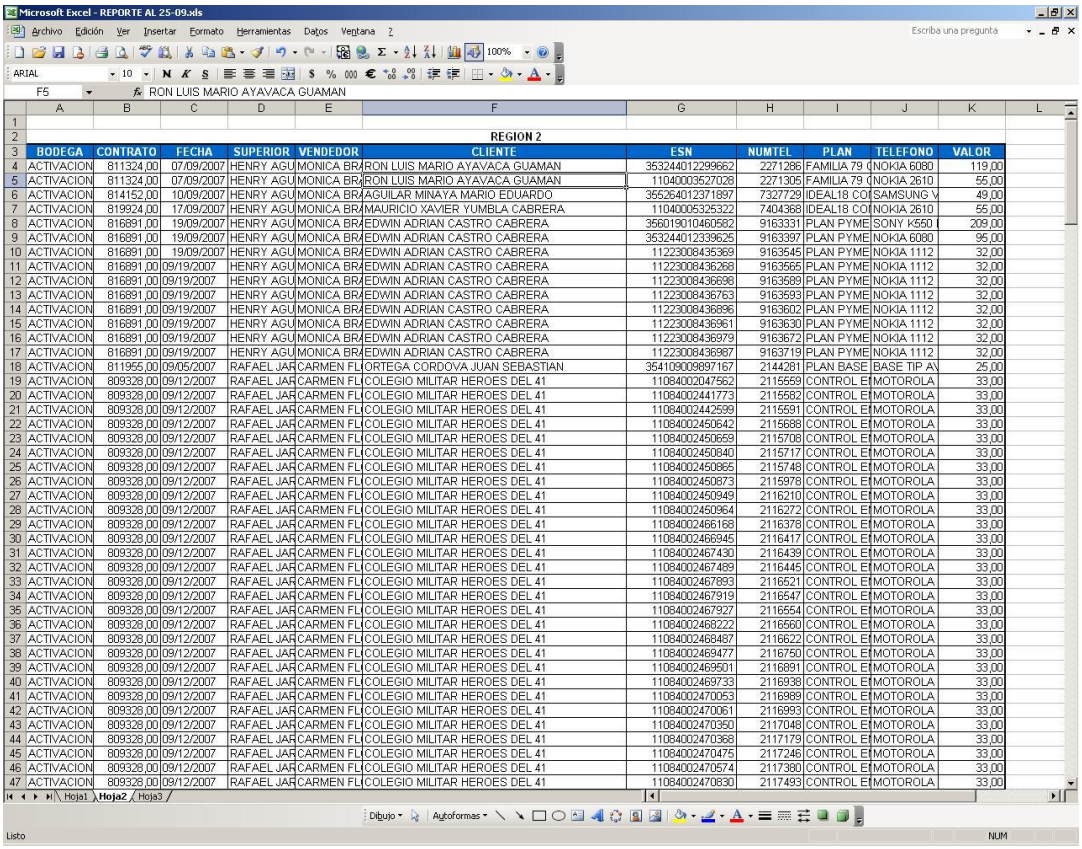


Imagen 3.16.- Conversaciones de mensajeria instantanea guardadas dentro de la carpeta del vendedor 01

Para poder corroborar que la información obtenida pertenece a la Empresa Rualtim S.A, procedimos a pedir el informe de las ventas realizadas en el mes de Septiembre del 2007. Por lo cual el Gerente de Ventas nos facilitó el archivo fuente con la siguiente Información:



Microsoft Excel - REPORTE AL 25-09.xls

F5: RON LUIS MARIO AYAVACA GUAMAN

REGION 2

BODEGA	CONTRATO	FECHA	SUPERIOR	VENDEDOR	CLIENTE	ESN	NUMTEL	PLAN	TELEFONO	VALOR
ACTIVACION	811324,00	07/09/2007	HENRY AGU	MONICA BRA	RON LUIS MARIO AYAVACA GUAMAN	353244012299662	2271286	FAMILIA 79	NOKIA 6080	119,00
ACTIVACION	811324,00	07/09/2007	HENRY AGU	MONICA BRA	RON LUIS MARIO AYAVACA GUAMAN	1104000327028	2271305	FAMILIA 79	NOKIA 2610	55,00
ACTIVACION	814152,00	10/09/2007	HENRY AGU	MONICA BRA	AGUILAR MINAYA MARIO EDUARDO	356264012371897	7327729	IDEAL18 CO	SAMSUNG V	49,00
ACTIVACION	819924,00	17/09/2007	HENRY AGU	MONICA BRA	MAURICIO XAVIER YUMBLA CABRERA	1104000325322	7404368	IDEAL18 CO	NOKIA 2610	55,00
ACTIVACION	816891,00	19/09/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	356019010460582	9163331	PLAN PYME	SONY K550	209,00
ACTIVACION	816891,00	19/09/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	353244012339625	9163397	PLAN PYME	NOKIA 6080	95,00
ACTIVACION	816891,00	19/09/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	1122300843536 9	9163545	PLAN PYME	NOKIA 1112	32,00
ACTIVACION	816891,00	09/19/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	1122300843626 8	9163565	PLAN PYME	NOKIA 1112	32,00
ACTIVACION	816891,00	09/19/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	1122300843669 8	9163589	PLAN PYME	NOKIA 1112	32,00
ACTIVACION	816891,00	09/19/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	1122300843676 3	9163593	PLAN PYME	NOKIA 1112	32,00
ACTIVACION	816891,00	09/19/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	1122300843689 6	9163602	PLAN PYME	NOKIA 1112	32,00
ACTIVACION	816891,00	09/19/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	1122300843696 1	9163630	PLAN PYME	NOKIA 1112	32,00
ACTIVACION	816891,00	09/19/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	1122300843697 9	9163672	PLAN PYME	NOKIA 1112	32,00
ACTIVACION	816891,00	09/19/2007	HENRY AGU	MONICA BRA	EDWIN ADRIAN CASTRO CABRERA	1122300843698 7	9163719	PLAN PYME	NOKIA 1112	32,00
ACTIVACION	811955,00	09/05/2007	RAFAEL JAR	CARMEN FL	ORTEGA CORDOVA JUAN SEBASTIAN	354109009897167	2144281	PLAN BASE	BASE TIP AV	25,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400204756 2	2115559	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400244177 3	2115582	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400244259 9	2115591	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400245064 2	2115688	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400245065 9	2115708	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400245084 0	2115717	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400245086 5	2115748	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400245087 3	2115978	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400245094 9	2116210	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400245096 4	2116272	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246616 8	2116378	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246694 5	2116417	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246743 0	2116439	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246748 9	2116445	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246789 3	2116521	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246791 9	2116547	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246792 7	2116554	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246822 2	2116560	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246848 7	2116622	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246947 7	2116750	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246950 1	2116891	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400246973 3	2116938	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400247005 3	2116989	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400247006 1	2116993	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400247036 0	2117048	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400247036 8	2117179	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400247047 5	2117246	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400247057 4	2117380	CONTROL E	MOTOROLA	33,00
ACTIVACION	809328,00	09/12/2007	RAFAEL JAR	CARMEN FL	COLEGIO MILITAR HEROES DEL 41	1108400247083 0	2117493	CONTROL E	MOTOROLA	33,00

Hoja1 Hoja2 Hoja3

Dibujo Autoformas

Listo NUM

Imagen 3.17.- Reporte de Ventas del mes de Septiembre del 2007

Por lo cual al analizar el archivo eliminado que se obtuvo a través del análisis forense así como el fuente que mantiene la empresa, se puede determinar que la información que se obtuvo en el ordenador 01 dentro de la carpeta del vendedor 01, fue obtenida a través de la información que mantiene el Gerente de Ventas en dicho ordenador.

Por lo cual se deja establecido el precedente para realizar el proceso legal o civil que solicitare la Empresa.

3.2.4 Presentación Judicial

Informe Pericial realizado por los estudiantes de la Universidad del Azuay escuela de Ingeniería de sistemas previo a la obtención del Título que suscribe en relación con el Oficio enviado al Decano de la Facultad de Ciencias de la Administración Eco. Luis Mario Cabrera González el día 10 de Marzo del 2009, seguido en contra del Señor(a) Vendedor 01 solicitado por la Empresa Rualtim S.A. a petición del Ing. Alex Sarmiento.

Sr. Andrés Oswaldo Torres Bustamante

CI: 0103731113

Sr. Osvaldo Sebastián Zapata Avila

CI: 0103861795

Contenido

Informe Pericial realizado por los estudiantes de la Universidad del Azuay escuela de Ingeniería de sistemas previo a la obtención del Título que suscribe en relación con el Oficio enviado al Decano de la Facultad de Ciencias de la Administración Eco. Luis Mario Cabrera González el día 10 de Marzo del 2009, seguido en contra de la Señor(a) Vendedor 01 solicitado por la Empresa Rualtim S.A. a petición del Ing. Alex Sarmiento

Los peritos que suscriben Andrés Torres, Sebastián Zapata declaran decir la verdad y que ha elaborado el presente informe en forma objetiva y teniendo en consideración, por tanto, todos los elementos que influyen en el objeto estudiado**.**

Los peritos que suscriben Andrés Torres, Sebastián Zapata declaran decir la verdad y que se elaboró el presente informe en forma objetiva teniendo en consideración todos los elementos críticos que influyen en el objeto de estudio.

Objetivo

Conforme el Acta de Posesión del día 18 de Febrero del 2009, en virtud del escrito CARTA dirigida a Empresa Rualtim S.A. de proceso (anexo), se deberá proceder a establecer lo siguiente:

"Según oficio recibido por ustedes y luego de haber presentado su propuesta a la reunión pertinente de nuestro directorio, hemos tomado la decisión de aceptar la solicitud con mucho agrado dando la apertura para realizar cualquier proceso o investigación, de la misma manera se les pide que toda información que se obtenga se la maneje con reserva debido a que cualquier decisión que se tome ya sea legal o empresarial será tomada en cuenta basándonos en los resultados obtenidos así como en la decisión tomada por todos los directivos de nuestra empresa"

Metodología Empleada

Para la realización del presente peritaje se ha utilizado una metodología técnica especializada y de conformidad a la ley, siguiendo cada momento los principios fundamentales de la informática forense, documentando totalmente y a fondo el proceso investigativo, utilizado herramientas hardware adecuadas y herramientas software forenses especializadas.

Para la consecución del objeto de este peritaje se utilizaron las aplicaciones: Hélix 1.8, PC Inspector File Recovery 4.0, Mount Image Pro 2.60, para el análisis se utilizaron las aplicaciones: Microsoft Excel 2007, Microsoft Word 2007 y la aplicación de Búsqueda de Windows XP.

Descripción del proceso

El proceso informático forense se lo realizó en dos etapas esencialmente: la primera basada en la recuperación de archivos perdidos o eliminados del ordenador 01 y la segunda parte en la verificación de archivos que se encuentren contenidos dentro del ordenador 01. Todo archivo que no esté enmarcado dentro de la información permitida por la empresa o la existencia de indicios sobre alguna irregularidad de información confidencial de la empresa será analizada.

Proceso de la obtención de la prueba

El día 28 de Junio del 2009 a las 11h45 AM en la ciudad de Cuenca, en la Oficina de la Empresa Rualtim S.A, ubicado en las calles Remigio Crespo 2-160 y Federico Proaño, en el Departamento de Ventas de la mencionada empresa como parte del peritaje efectuado y bajo la presencia del Ing. Alex Sarmiento, se procedió a reconocer el computador 01 que se encuentra en dicho departamento con el número de serie MXJ8160116.

Se solicitó la presencia del Ing. Alex Sarmiento, con CI 0391006199 como delegado para la supervisión del proceso a realizar (anexo).

A las 20 horas 03 minutos 19 segundos del día 28 de Junio del 2009 se procedió a obtener una imagen lógica del disco duro del computador 01 mencionado, para lo cual se utilizó la aplicación FTK Imager que viene contenida en la herramienta forense HELIX 1.8, proceso que culminó a las 23 horas 14 minutos 20 segundos del día 28 de Junio del 2009, una vez obtenida la imagen se verificó su originalidad y autenticidad utilizando el algoritmo MD5, obteniendo el siguiente hash: 2d6c354299b38df3b1c22eb04b62cf9b (anexo).

A las 23 horas 25 minutos 29 segundos del día 28 de Junio del 2009 se procedió a obtener una segunda imagen lógica del disco duro del computador mencionado para lo cual se utilizó la aplicación software FTK Imager que viene contenida en la herramienta forense HELIX 1.8, proceso que culminó a las 01 horas 45 minutos 56 segundos del día 29 de Junio del 2009, una vez obtenida la imagen se verificó su

originalidad y autenticidad utilizando el algoritmo MD5, obteniendo el siguiente hash: 2d6c354299b38df3b1c22eb04b62cf9b

Para constancia de lo mencionado, la actividad realizada durante este día se la registro en un Acta Pericial (anexo), suscrita por los peritos: Señores Andrés Torres CI: 0103731113, Sebastián Zapata CI: 0103861795 y por el Ing. Alex Sarmiento con CI 0391006199.

Verificación de existencia, borrado o destrucción de archivos

Se solicito al Ing. Alex Sarmiento proceda a prender la computadora e ingresar a la misma, una vez ingresado en la computadora, se procedió a obtener información referente a actividades realizadas en el computador a través del visor de sucesos (anexo).

Posteriormente se reviso el perfil de usuario y confirmación de las propiedades del mismo (anexo).

Se procedió a buscar archivos (.xls), (.doc), (.xml) que puedan tener relación con la información sobre los reportes de ventas postpago de la empresa, específicamente se busco lo siguiente:

- Archivos tipo (.xls), (.doc), (.xml) modificados o creados entre julio 2007 y Noviembre 2007. Se obtuvieron 165 archivos.

Con la finalidad de analizar el objeto de la pericia, encaminada a la verificación de borrado o destrucción de archivos, se realizo el proceso de recuperación de información el día 29 de Junio del 2009 a las 02 horas 05 minutos 10 segundos y se analizó el registro de aplicaciones y lista de programas instalados para buscar la existencia de algún tipo de software destructor de información.

En presencia del Ing. Alex Sarmiento se procedió a realizar el proceso de recuperación de información utilizando el siguiente software.

Software de recuperación	Resultado
PC Inspector File Recovery	1780 Archivos

El proceso realizado durante este día se lo registro en una Acta Pericial (anexo), y para constancia de lo actuado suscribieron la mencionada acta, junto a los peritos, Ing. Alex Sarmiento con CI 0391006199 como observador y testigo del proceso.

Proceso de estudio de las pruebas obtenidas

Para analizar las imágenes obtenidas se utilizo el software Mount Image Pro y Microsoft Excel.

Se procedió a realizar una copia de archivos desde el disco duro hacia un dispositivo de almacenamiento externo y se pudo comprobar que existe un reporte realizado en el mes de Septiembre del 2007 perteneciente al Gerente de Ventas el cual se encontró dentro de una carpeta del vendedor 01(anexo).

Análisis de la prueba pericial

El dictamen pericial se presenta en forma conclusiones e indicios.
Las conclusiones son aseveraciones inequívocas que no están sujetas a validación o refutación, por encontrarse apoyadas en principios doctrinales y técnicos irrefutables.

Los Indicios son los que quedan supeditados a otros trabajos de peritaje o validación mediante presentación de pruebas de partes que apoyen o descarten los mismos. No generan una conclusión por sí mismo, solo abren posibles líneas de investigación.

Conclusiones

Aplicación

- Del reporte generado (anexo) se pudo observar que el vendedor 01 durante el mes de septiembre del 2007 obtuvo información confidencial del Gerente de Ventas de la empresa. Según el análisis realizado, la información fue guardada en un dispositivo de almacenamiento para

luego ser guardada y revisada por el vendedor 01 en el computador 01, el cual luego procedió a borrar dicho archivo.

Verificación de la información en formato Excel.

- En la computadora del departamento de ventas con número de serie MXJ8160116, marca Hp Compaq, Modelo Dc5700 Minitower, se pudo observar la existencia de archivos relacionados con la pericia (anexo).
- Se pudo observar la existencia de archivos creados en Septiembre del 2007.
- De los archivos tipo .XLS que se encuentran en el computador 01 se realizo un análisis sobre los datos contenidos desde julio hasta noviembre del 2007, lo cual aparentemente indica que existen archivos que fueron copiados en el transcurso de este tiempo.
- Se pudo observar que la información que se encontró en la carpeta del vendedor 01, a través de la recuperación de archivos es igual a la información que el Gerente de Ventas nos facilito para la respectiva comprobación.
- Del proceso de recuperación de información se encontraron 1780 archivos eliminados, algunos relacionados con el objeto del presente peritaje, de lo cual se concluye que se abría eliminado archivos de tipo .xls, .xml.
- Del proceso de análisis sobre el contenido de los datos, se pudo encontrar el log de conversaciones de mensajería instantáneo que guardó el vendedor 01 en su carpeta.

Indicios:

Se presentan indicios en el estudio pericial de la evidencia.

Observaciones finales:

Dentro de las funciones para las cuales se me ha posesionado, se puede precisar las siguientes observaciones:

- Se intentó en todo momento cumplir con la labor pericial dentro de un marco de respeto y legalidad, explicando a todas las partes los alcances y limitaciones de la tarea pericial.
- Se realizaron las diligencias escritas que se consideraron oportunas y pertinentes, con objeto de certificar la tarea realizada y evitar posteriores mal entendidos.

Anexos y Sustento Legal

El presente informe cumple con los Art. 98 y 110 del código de procedimiento penal 2000 en lo que respecta a la prueba material y Art.257 del código de procedimiento civil.

Cumpliendo con el Art. 98 Art.257 del antes mencionado cuerpo, se adjunta al presente las pruebas obtenidas, consistentes (anexo).

3.3 Conclusiones

Luego de haber concluido el caso de estudio desarrollado en este capítulo, se obtuvo la evidencia necesaria que indica que el "Vendedor 01" tenía en su poder el archivo "reporte de mes sept.xls" generado el 01/10/2007 5:28 Pm y 31 archivos de conversaciones de mensajería instantánea de carácter privado de otro vendedor de la empresa.

Con la finalidad de que el caso de estudio sea tomado en cuenta por la empresa, el proceso ejecutado se lo realizó en base a la metodología adecuada del proceso Informático forense. Además se espera que la empresa tome cartas en el asunto para poder prevenir otro fraude informático y poder evitar tener una pérdida económica significativa.

CAPITULO IV

ESTABLECIMIENTO DE CONTROLES

4.1. Introducción

El entorno informático en las organizaciones esta caracterizado por sistemas y redes computacionales de alta complejidad, por lo que se debe emplear normativas que presten atención a la implementación e inspección de procesos que operen con información confidencial así como de los recursos de la Empresa.

Por lo tanto, el avance de la tecnología y debido a que la información es considerado hoy en día como uno de los mayores activos, pues tiene un valor substancial para la organización y en consecuencia necesita ser protegido, se debe establecer controles en la organización incrementando los niveles en los sistemas de información así como el uso adecuado de los recursos empresariales.

En lineas generales, la problemática creada a partir del manejo inadecuado de controles como de vulnerabilidades presentes en los sistemas de informacion, causan perjuicios economicos evidenciables en el Capitulo I que afectaron a los ingresos de la empresa, por consiguiente si la empresa no implementa de forma inmediata controles para los recursos que maneja será victima de un nuevo delito informatico.

4.2. Evaluación de Costo-Beneficio

4.2.1. Costo

Desde el punto de vista informático, saber que valor se le atribuye a la información ha sido siempre difícil y más complejo es poder convencer que los costos que intervienen en el establecimiento de controles para asegurar la información son justificables.

Debemos tomar en cuenta que el valor de la información es algo absolutamente relativo, puesto que la información constituye un recurso que en muchos casos no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.

Inicialmente debemos respondernos si los costos en los que vamos a incurrir serán plenamente justificados mediante los beneficios que obtendremos por estos, cada control implementado incidirá de cierta manera en costos, por lo tanto este tendría que brindar un beneficio. Por eso es importante entender que los esfuerzos invertidos en la seguridad son costeables.

Para poder realizar una evaluación de costos se tiene que cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta todas las posibilidades. El planteamiento viable para desarrollar esta política es analizar qué recursos se desea proteger, la importancia de estos recursos, el tipo de amenazas al que está expuesto y de que personas necesita proteger los recursos

Una vez que realizamos el análisis sobre la política empleada para el manejo y protección de los recursos sumada a una evaluacion de riesgos, se debería conocer que tipo de recursos valen la pena proteger y justificar su costo, tomando en cuenta que ciertos recursos son mas importantes que otros.

Ahora que se tiene los costos en los cuales la empresa esta dispuesto a incurrir y analizado las vulnerabilidades que presenta la empresa, se tiene que llegar a obtener un punto de equilibrio basandonos en el costo, riesgo y seguridad.

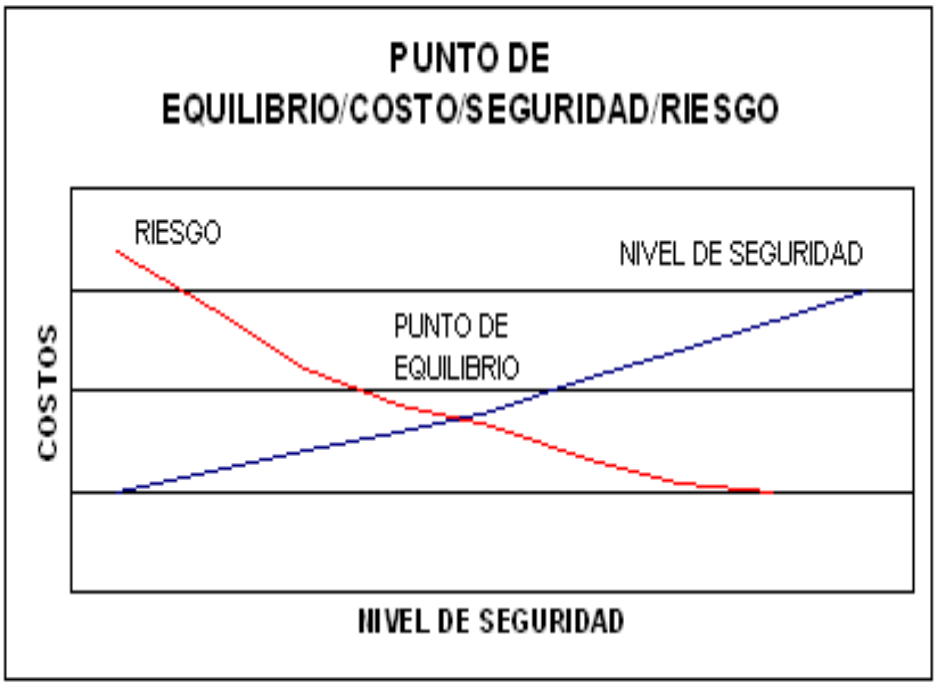


Grafico 4.1.- Punto de equilibrio Costo/Seguridad/Riesgo

Como se puede apreciar según el grafico 4.1, los riesgos disminuyen al aumentar la seguridad y los costos en los que incurre, pero como se tiene conocimiento, los costos tenderán al infinito sin llegar al 100% de seguridad y por supuesto nunca se logrará no correr algún tipo de riesgo. Lo importante es poder conocer cuan seguro estará la organización conociendo los costos y los riesgos que se corren.

El costo de perdida que mantuvo la empresa Rualtim S.A. al no manejar y tener en cuenta la seguridad en sus sistemas informáticos fue de $5440, según el delito informático analizado en el capítulo 3. Por lo tanto el costo de la implementación de seguridad para tratar de impedir el hecho suscitado hubiera sido mucho menor que la pérdida obtenida.

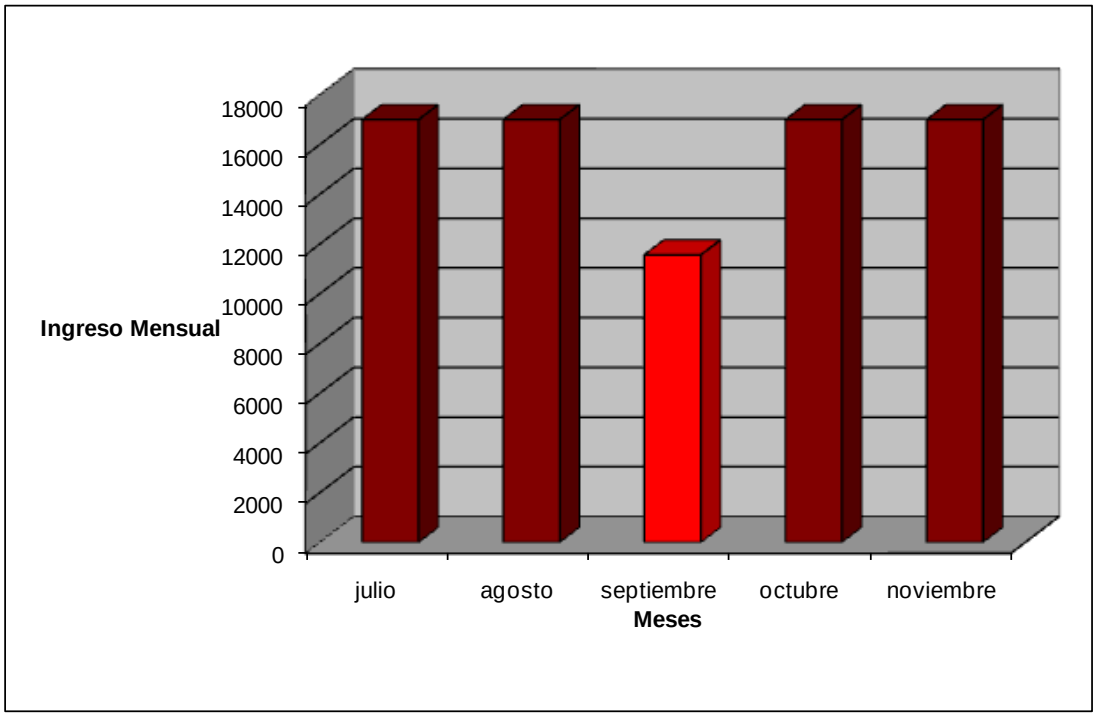


Grafico 4.2.- Ingresos obtenidos durante los meses de Julio a Noviembre del 2007

4.2.2. Beneficio

Los beneficios que se obtienen al incurrir en la implementación del manejo de normativas y controles puede clasificarse en cuantificables y no cuantificables. Los cuantificables son aquellos datos que se obtienen a través de un análisis sobre los costos reales que la empresa tendrá que invertir para poder crear niveles de seguridad

mas altos. Mientras que los beneficios no cuantificables que obtiene la organización pueden llegar a ser:

- Mayor seguridad sobre la información y recursos de la emrpesa
- Rápida reacción frente a incidentes informáticos
- Mayor control sobre la información proporcionada a terceros
- Control de seguridad informática mas precisos y confiables
- Reducción de los riesgos involucrados al manejo de información en medios informáticos
- Planeamiento de la seguridad informática mas efectivo

4.3. Comparación entre diferentes normativas empresariales

Para el correcto manejo de la información en las empresas se crean normativas empresariales tanto para el manejo de los sistemas informáticos/electrónicos como para el manejo interno de la organización, los cuales son puestos a disposición del trabajador para su fiel cumplimiento. Para nuestro caso nos interesa revisar diversas normativas empresariales que están siendo implementadas en las organizaciones, para lo cual realizaremos una comparación entre la empresa (A) que pone énfasis en la implementación de controles para su organización y la empresa (B) que mantiene los sistemas a la deriva:

Descripción Normativas	**Empresa A Cumplimiento**		**Empresa B Cumplimiento**	
	SI	NO	SI	NO
- Control sobre el acceso a Internet	X			X
- Filtro de control para el bloqueo o borrado automático de correo electrónico, que cumplan o incumplan los requisitos implementado por la empresa	X			X
- Creación de cuentas personales de correo electrónico para cada empleado que tenga acceso a internet	X		X	

- Inspección de correo y/o la navegación en internet	X			X
- Creación de cuentas personales de usuario dependiendo del área en el que se encuentre	X		X	
- Prohibición del uso de hardware y software ajeno a la empresa	X			X
- Se prohíbe extraer de su ubicación cualquier elemento hardware, salvo autorización expresa	X		X	
- No se deberá instalar software sin previa autorización del debido departamento	X			X
- Cada usuario es responsable del manejo de la contraseña entregada a cada trabajador, asumiendo la responsabilidad de las consecuencias derivadas de este	X		X	
- Queda prohibido la entrada a los sistemas utilizando la contraseña de otro usuario		X		X
- Se prohíbe la modificación o alteración de cualquier medida de seguridad implantada en la empresa	X			X
- El usuario será responsable de la perdida de toda documentación guardada en el ordenador	X		X	
- Control automático para la prevención y detección de programas no deseados(spyware, virus)	X			X
- Los permisos a usuarios serán reevaluados normalmente		X		X
- Efectuar auditorias informáticas cada cierto periodo de tiempo	X			X

Tabla 4.1.- Comparación de Normativas Empresariales

Según la tabla comparativa 4.1 se puede observar que pueden existir brechas de seguridad en las organizaciones, por medio de las cuales puede haber o se puede realizar un fraude informático, por esto los responsables de las empresas tienen la

obligación de tomar las debidas precauciones y realizar los debidos ajustes sobre los controles a la información con la que opera la organización.

Evaluacion de controles de la Empresa Rualtim S.A

Nro	Descripción	Efectividad del control
01	Protección del hardware y de los soporte de datos	Bajo
02	Recursos informáticos debidamente protegidos de factores físicos que los puedan dañar	Medio
03	Instalacciones adecuadas para preservar los equipos informáticos como sus periféricos	Medio
04	Control de acceso para cada usuario que utilice un equipo informatico	Bajo
05	Control de privilegios sobre los accesos de los usuarios	Nulo
06	Elaboración de planes de manejo de los recursos para el personal	Nulo
07	Control de validación, integridad, almacenamiento para el procesamiento de los datos	Bajo
08	Control de transmisión y distribución de los datos	Nulo
09	Control y evaluación de la información que se maneja por departamento	Bajo
10	Control de la disponibilidad, integridad y confidencialidad de la información	Bajo
11	Procedimientos para la administración del software y de los sistemas operativos	Bajo
12	Control para garantizar la seguridad mínima requerida en cuanto a los sistemas de información que se desarrollan en la empresa	Bajo
13	Procedimiento formal para asegurar que los cambios efectuados al realizar un mantenimiento de sistemas no afecte la información contenida dentro de los ordenadores	Bajo
14	Procedimiento para identificar las responsabilidades en cuanto al uso de los sistemas y recursos donde sera implantado	Bajo
15	Política relativa al uso y protección del hardware de la empresa	Bajo
16	Control del tráfico existente en la red	Bajo
17	Control del Internet e Intranet en la empresa	Bajo
18	Control del correo electrónico no deseado asi como de filtros para evitar suplantaciones de identidad	Bajo

Tabla 4.2.- Evaluación de Controles

4.4. Conclusiones

Una de las conclusiones más importantes al realizar la ejecución de las fases IV y V de la Auditoria Informática sobre el manejo de la información en las empresas, es que las pérdidas por el inadecuado control de sistemas informáticos son representativamente altos, mientras que en la mayoría de casos el ejecutar planes e implementar controles para prevenir fraudes o delitos en relación al costo económico es muy bajo.

La empresa Rualtim S.A. nunca realizo una evaluación de los riesgos a los cuales está expuesto, por tal motivo el delito informático cometido en dicha empresa afecto al cumplimiento de los objetivos específicos y globales de la entidad.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La Informática Forense asociada con la Auditoria Informática, nos permite conocer el motivo por el cual se ha suscitado un fraude o delito en un momento dado, lo cual podría ayudar a evitar posibles pérdidas de información que tienen principalmente un impacto económico.

- El delito informático se está convirtiendo en uno de los principales problemas dentro de las empresas, ya que existe un control inadecuado de los recursos informáticos como del acceso a los mismos.

- La Auditoria Informática nos permitió analizar los riesgos que se presentan con respecto al manejo de la información, con el objetivo de identificar el nivel de seguridad existente en la empresa.

- Para lograr el control adecuado de la información, se requiere el análisis pertinente y enfocado a lo que realmente quiere la empresa, es decir, no se trata de realizar un simple análisis con el fin de obtener un resultado, sino de utilizar la metodología y las herramientas más apropiadas

- La seguridad no solo dependerá de las herramientas que se utilicen para la ejecución de los controles pertinentes a la seguridad de la información, un factor que posee un nivel de importancia significativo, es el usuario.

- En el desarrollo de esta monografía, se pudo identificar los riesgos y vulnerabilidades existentes en la empresa Rualtim S.A. lo que afecto seriamente al desarrollo normal de sus actividades, por lo cual se expone algunas recomendaciones que pueden disminuir el impacto de los riesgos antes mencionados.

- La importancia de conocer los aspectos legales y civiles que tienen relación con el cometimiento de un delito o fraude informático, es de suma

importancia hoy en día, ya que los alcances de los actos delincuenciales son inimaginables.

5.2. Recomendaciones

- Se debe crear normativas internas dentro de la empresa, tanto para el manejo de los recursos informáticos como para el establecimiento de controles, que permitan debilitar los posibles ataques a los cuales puede estar expuesta la organización.

- Incorporar cámaras de seguridad dentro de la empresa para poder vigilar en todo momento cualquier irregularidad que pueda darse.

- Mantener una seguridad proactiva teniendo como base fundamental las aplicaciones y comunicaciones realizadas a nivel organizacional.

- Redefinir la estructura de la red informática de la empresa, con la finalidad de poder controlar de manera eficiente las áreas y procesos que por el momento se encuentran desprotegidos.

- Crear documentación sobre el uso y manejo de los recursos informáticos a cada una de las personas que laboran dentro de la empresa, lo que responsabilizara el uso de los mismos si se llegara a dar algún acontecimiento.

- Crear normativas internas para el uso y administración de información dentro de la empresa, las cuales deberán estar por escrito y contar con el apoyo de la organización.

- Considerar la creación de procedimientos informáticos para el manejo de incidentes de seguridad y destinar un responsable que coordine a las personas involucradas en un incidente.

- Dar mantenimiento a los recursos informáticos tratando de controlar toda la información contenida en los mismos, para evitar futuros fraudes o el manejo inadecuado de los mismos.

Bibliografía

- Constitución Política del Ecuador
- Legislación Ecuatoriana
- Código Penal Del Ecuador
- PEDRO MIGUEL LOLLETT R, "Auditoria Forense"
- "Manual de Gestión de Seguridad de la Información de la Universidad Técnica Particular de Loja."
- "Legislación y el Manejo de la Información en la era del conocimiento"
- GLIN, "Nicaragua Corte Suprema de Justicia Nicaragua"
- ANA ROSA CHAVARRÍA, JOSÉ ANTONIO PEREIRA VEGA, LENIN ERNESTO DÁVILA, "MSc.", Managua Nicaragua, Noviembre, 2005
- RAFAEL HERNANDO GAMBOA B, "Validez procesal de la información digital"
- CÉSAR FELIPE RODRÍGUEZ PARRA, "Documentos electrónicos como pruebas claves en litigios empresariales"
- CANO MARTINES JEIMY JOSÉ. "Introducción a la informática forense" Revista ACIS, Junio de 2006
- CASEY, EOGHAM, "Handbook of Computer Crime Investigation: Forensic Tools and Technology", 2003
- [HBIT03] "Handbook Guidelines for the management of IT evidence"
- www.asambleanacional.gov.ec
- www.lexis.com.ec
- www.eiidi.com
- www.derechoecuador.com
- www.mitecnologico.com/Main/FasesAuditoriaInformatica

ANEXOS

Anexo1

Normativa Legal

Introducción

Con el desarrollo de la tecnología en todo el mundo, y la falta de algunos controles, se generan riesgos que la hacen vulnerable a la ocurrencia de los Delitos Informáticos. La red de computadoras provee muchas ventajas para quienes las usan, sin embargo también poseen ciertos niveles de vulnerabilidad. El hecho de que la red permita compartir información, transferir archivos y acceder remotamente, hace que estos servicios puedan ser utilizados para fines ilícitos. Acceso a base de datos no autorizada, revisión y modificación de información sensible, copia de archivos y documentos privados, propagación de virus, son algunos de las formas en que las redes facilitan el trabajo a los denominados delincuentes informáticos.

Los Delitos Informáticos se encuentran en constante crecimiento convirtiéndose en un problema global para todas las empresas que utilizan Sistemas de Información y redes de comunicación como Intranet e Internet, una gran parte de las organizaciones tienen el pensamiento de que “Esto nunca nos ocurrirá a nosotros, si ocurre estamos bien preparados para enfrentarlo”, no obstante este es un pensamiento erróneo porque el peligro de que sean víctimas de algún incidente o ataque está latente.

En la actualidad con la creación de la denominada "autopista de la información", el INTERNET, las posibilidades de comunicación e investigación se han acrecentado, se tiene acceso a un ilimitado número de fuentes de consulta y entretenimiento. El problema radica en que, la conducta humana parece ser que está inclinada al delito, a conseguir satisfacción a sus deseos a toda costa. Con el desarrollo de la informática, aparece también lo que se denomina como: “DELITO INFORMATICO.”

Revisión Legal del delito Informático

Encontramos tantos conceptos de Delito Informático, que citaremos algunos de ellos:

Para Carlos Sarzana, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".[13]

Carlos Sarzana

María de Luz Lima dice que el "delito electrónico" en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".[14]

María de Luz Lima

Rodolfo Herrera. "Conducta típica, antijurídica y culpable que atente contra el soporte lógico de un sistema de procesamiento de información, sea programas o datos relevantes a través del uso natural de las tecnologías de la información."[15]

Rodolfo Herrera

Sujetos que generan los delitos informáticos

Las personas que pueden cometer "Delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Estas características nos remiten a:

[13] *Carlos Sarzana*
[14] *María de Luz Lima*
[15] *Rodolfo Herrera*

- Operadores, que se pueden poner en relación con el Sistema para modificar, agregar, eliminar, sustituir información y/o programas, copiar archivos para venderlos a competidores.
- Programadores, que pueden violar o inutilizar controles protectores del programa y/o sistema; dar información a terceros ajenos a la empresa, atacar el sistema operativo, sabotear programas, modificar archivos, acceder a información confidencial.
- Analistas de sistemas, que pueden unirse con usuarios, programadores y/u operadores para revelarles la operación de un sistema completo.
- Analistas de comunicaciones, que enseñan a otras personas la forma de violar la seguridad del sistema de comunicaciones de una empresa, con fines de fraude.
- Supervisores, que pueden manipular los archivos de datos y los ingresos y salidas del sistema.
- Personal técnico y de servicio, que por su libertad de acceso al centro de cómputo puede dañar el sistema operativo.
- Personal de limpieza, mantenimiento y guardias, que pueden vender el contenido de papeles, fotocopiar documentos, sabotear el sistema.
- Usuarios Finales, que pueden modificar, omitir o agregar información con fines fraudulentos.

En el Ecuador, el 11 abril de 2002, expide la Ley de Comercio, Firmas Electrónicas y Mensajes de Datos, instrumento que da un marco jurídico a las innovaciones tecnológicas relacionadas con la transmisión de información utilizando medios electrónicos. El objeto de la Ley es la de regular los mensajes de datos, firmas electrónicas, servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico (e-business) y lógicamente la protección a los usuarios de estos sistemas de cualquier mecanismo de distorsión.

Gracias a la expedición de esta Ley, nacen como delitos con características propias el sabotaje (SPAM) y los daños informáticos (CYBER CRIME). Diremos que estas infracciones se incorporan al Código Penal ecuatoriano, logrando así una protección concreta y específica a este tipo de actos, considerados desde abril de 2002 como delitos. Ahora bien, dentro de la regulación propia de los mensajes de datos, también se prevé mecanismos de protección propios en donde se enuncian principios y procedimientos que se deben respetar.

La Ley establece principios sobre confidencialidad y reserva: "se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o

intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia".[16] Se establecen principios que armonizan con disposiciones constitucionales. La inviolabilidad y el secreto de la correspondencia es una garantía establecida en la Constitución Política.

Resumiendo, vemos que existen principios constitucionales y legales de protección a la información que consta en una base de datos. Los mensajes que se generen, deben estar acompañados siempre de criterios y parámetros de respeto al bien ajeno y a la propiedad privada. La Ley considera que si se recopila y usan datos personales sin el consentimiento previo, existe una violación flagrante a los derechos de la privacidad, confidencialidad e intimidad que se encuentran garantizados por la Constitución.

El campo de aplicación de la Ley de Comercio y Firmas Electrónicas está dado básicamente por relaciones contractuales amparadas en el campo civil, aunque también, de menor manera, tiene injerencia dentro del ámbito penal. Este ámbito está dado concretamente dentro de lo que ésta misma considera como infracciones informáticas. La Ley agregó al Código Penal una serie de infracciones antes no contempladas para sancionar este tipo de delitos.

Legislación del Ecuador

LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.

Tipos de delitos informáticos reconocidos por Naciones Unidas

a.- Fraudes cometidos mediante manipulación de computadoras

16 Constitución Política del Ecuador

- **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.

- **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.

- **Manipulación de los datos de salida**. Se efectúa fijando un objetivo al funcionamiento del sistema informático.

b.- 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.

c.- Falsificaciones informáticas

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

- **Como instrumento.** Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

Código de Procedimiento Penal

Código Penal Del Ecuador

Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos innumerados:

"Art. ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un alío y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. - Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica"

Art. 61.- A continuación del artículo 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art. - Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

Art. ....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.'

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena previste en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

Art.- 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:

Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Anexo2

Information for D:\ImagenDisco\ImagenDisco:

Physical Evidentiary Item (Source) Information:
[Drive Geometry]
Cylinders: 9.729
Tracks per Cylinder: 255
Sectors per Track: 63
Bytes per Sector: 512
Sector Count: 156.301.488
[Physical Drive Information]
Drive Model: MAXTOR STM380215A
Drive Interface Type: IDE
Source data size: 76319 MB
Sector count: 156301488
[Computed Hashes]
MD5 checksum: 2d6c354299b38df3b1c22eb04b62cf9b
SHA1 checksum: 60bd2aa58b94310b66cec913a1c25982f205cb65

Image Information:
Segment list:
D:\ImagenDisco\ImagenDisco.001
D:\ImagenDisco\ImagenDisco.002
D:\ImagenDisco\ImagenDisco.003
D:\ImagenDisco\ImagenDisco.004
D:\ImagenDisco\ImagenDisco.005
D:\ImagenDisco\ImagenDisco.006
D:\ImagenDisco\ImagenDisco.007
D:\ImagenDisco\ImagenDisco.008
D:\ImagenDisco\ImagenDisco.009
D:\ImagenDisco\ImagenDisco.010
D:\ImagenDisco\ImagenDisco.011
D:\ImagenDisco\ImagenDisco.012
D:\ImagenDisco\ImagenDisco.013
D:\ImagenDisco\ImagenDisco.014
D:\ImagenDisco\ImagenDisco.015
D:\ImagenDisco\ImagenDisco.016
D:\ImagenDisco\ImagenDisco.017
D:\ImagenDisco\ImagenDisco.018
D:\ImagenDisco\ImagenDisco.019
D:\ImagenDisco\ImagenDisco.020
D:\ImagenDisco\ImagenDisco.021
D:\ImagenDisco\ImagenDisco.022
D:\ImagenDisco\ImagenDisco.023
D:\ImagenDisco\ImagenDisco.024
D:\ImagenDisco\ImagenDisco.025
D:\ImagenDisco\ImagenDisco.026
D:\ImagenDisco\ImagenDisco.027
D:\ImagenDisco\ImagenDisco.028
D:\ImagenDisco\ImagenDisco.029
D:\ImagenDisco\ImagenDisco.030
D:\ImagenDisco\ImagenDisco.031

D:\ImagenDisco\ImagenDisco.032
D:\ImagenDisco\ImagenDisco.033
D:\ImagenDisco\ImagenDisco.034
D:\ImagenDisco\ImagenDisco.035
D:\ImagenDisco\ImagenDisco.036
D:\ImagenDisco\ImagenDisco.037
D:\ImagenDisco\ImagenDisco.038

Sun Jun 28 20:03:19 2009 - Image Verification Results:
MD5 checksum: 2d6c354299b38df3b1c22eb04b62cf9b : verified
SHA1 checksum: 60bd2aa58b94310b66cec913a1c25982f205cb65 : verified

Anexo3

Identificacion de Riesgos

Numero Riesgo	Descripcion	Probabilidad	Impacto	Puntaje
01	Modificacion de los archivos del sistema operativo	5	4	20
02	Instalacion de programas espia, keylogger, virus, etc	5	5	25
03	Acceso remoto al ordenador	5	5	25
04	Eliminacion de informacion personal de los vendedores	4	4	16
05	Robo del ordenador del departamento	2	5	10
06	Interrupcion del sistema operativo	4	3	12
07	Robo de recursos por terceras personas	1	5	5
08	Alteracion de informacion confidencial	3	4	12
09	Falla en el servicio de la red	3	2	6
10	Manejo inadecuado del ordenador	4	3	12

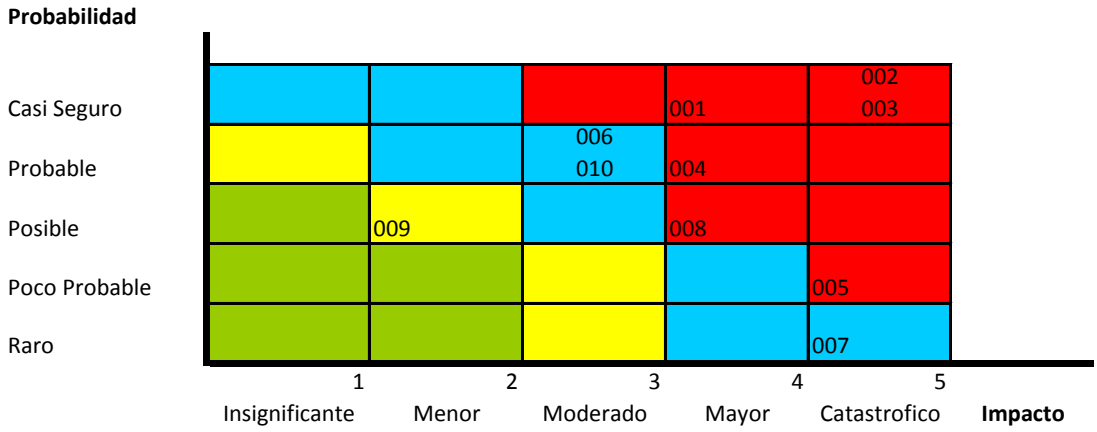
CALIFICACION DE LA FRECUENCIA

Valor	Frecuencia	Descripcion
1	Baja	Un caso en mas de cuatro años
2	Media	Hasta dos casos en dos años
3	Alta	1 Caso por año
4	Muy Alta	Mas de dos casos por año

CALIFICACION DE IMPACTO

Valor	Impacto	Descripcion en terminos economicos
5	Leve	Pequeño daño economico
10	Moderado	Daños entre 500 y 4000 dolares
20	Grave	Daños entre 4001 y 9999 dolares
40	Catastrófico	Mas de 10000 dolares

Matriz de Riesgo



Bajo	
Moderado	
Alto	
Extremo	

Codigo	Probabilidad	Impacto	
001	5	4	Extremo
002	5	5	Extremo
003	5	5	Extremo
004	4	4	Extremo
005	2	5	Extremo
006	4	3	Alto
007	1	5	Alto
008	3	4	Extremo
009	3	2	Moderado
010	4	3	Alto

Matriz evaluacion riesgo

4	Muy Alta	20	B	60	C	100	D	160	D
3	Alta	15	B	45	C	75	C	120	D
2	Media	10	B	30	B	50	C	80	D
1	Baja	5	A	15	B	25	C	40	C
		Leve		Moderado		Grave		Catastrofico	
		5		15		25		40	

IMPACTO

Matriz de evalluacion de riesgo y medida de tratamiento

Frecuencia	Valor				
Muy Alta	4	20 Zona Tolerable Pv, R	60 Zona de Riesgo Grave Pv, Pt, T	100 Zona de Riesgo Inaceptable Pv, Pt, T	160 Zona de Riesgo Inaceptable E, Pv, Pt
Alta	3	15 Zona Tolerable Pv, R	45 Zona de Riesgo Grave Pv, Pt, T	75 Zona de Riesgo Grave Pv, Pt, T	120 Zona de Riesgo Inaceptable E, Pv, Pt
Media	2	10 Zona Tolerable Pv, R	30 Zona Tolerable Pv, Pt, R	50 Zona de Riesgo Grave Pv, Pt, T	80 Zona de Riesgo Inaceptable Pv, Pt, T
Baja	1	05 Zona de Inaceptabilidad	15 Zona Tolerable Pt, R	25 Zona Tolerable Pt, T	40 Zona de Riesgo Grave Pt, T
	Impacto	Leve	Moderado	Grave	Catastrófico
	Valor	5	15	25	40

Pv= Prevenir el riesgo
Pt= Proteger los recursos
T= Transferir el riesgo
E= Eliminar la actividad
R= Retener las perdidad
A= Aceptar el riesgo

Areas	Impacto
Gerencia General	Moderado
Gerencia Administrativa	Considerable
Gerencia de Ventas	Considerable
Ventas	Alta