ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Instituto de Ciencias Matemáticas

Auditoría y Control de Gestión

"Auditoria Forense: Metodología, Herramientas y Técnicas Aplicadas en un siniestro informático de una empresa del sector comercial"

TESIS DE GRADO

Previa a la obtención del Título de:

AUDITOR EN CONTROL DE GESTIÓN

Presentada por:

Viviana Marcela Villacís Ruiz

GUAYAQUIL – ECUADOR

AÑO

2.006

AGRADECIMIENTO

A Dios, por darme a mis padres que han sido los pilares más importantes en mi vida personal y profesional. A mis hermanos “Víctor y Carolina” por siempre creer en mi. En especial, a mi Directora de Tesis por transmitirme sus conocimientos, y ayudarme en la realización de la misma.

A Víctor Manuel, Natalia, Jennifer, Fabrizzio y David por estar siempre apoyándome en la elaboración de la tesis.

A todos…….. Gracias.

DEDICATORIA

Este trabajo está dedicada a la persona que es mi fuente de admiración, orgullo y respeto, que me dio la vida y ha seguido formándome con valores y principios “Mi mamá”.

TRIBUNAL DE GRADUACIÓN

Ing. Pablo Álvarez
PRESIDENTE

Ing. Alice Naranjo
DIRECTORA DE TESIS

Mat. Jhon Ramírez
VOCAL

Ing. Luis Rodríguez
VOCAL

DECLARACION EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado me corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL".

Viviana Villacís R.

Viviana Villacís Ruiz

RESUMEN

Las organizaciones modernas que operan o centran gran parte de su actividad en los recursos informáticos y necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y operatividad de sus actividades.

La auditoria forense informática en su concepto es metódica y se basa en acciones premeditadas para reunir pruebas, analizarlas y emitir un juicio. Para el caso del análisis forense en un siniestro informático, se trata de reunir la mayor cantidad de pruebas e información necesaria en el entorno informático, ese entorno se compone de la computadora y la red a la cual está o no conectada.

El presente trabajo tiene como una de sus metas principales, orientar a las generaciones futuras, sobre la importancia de la auditoria forense informática.

El trabajo realizado es una contribución como material de apoyo a todas las empresas, debido a que la auditoria forense informática es relativamente nueva en nuestro país y por consiguiente no existen muchos casos documentados del tema, por lo cual este trabajo pretende ser una guía para trabajos futuros.

INDICE GENERAL

Pág.

4. CASO PRÁCTICO

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCION

Con el presente trabajo doy a conocer la auditoria forense informática, sus objetivos, fines y alcance, así mismo a través de ella se encontrarán evidencias de un siniestro informático.

En el primer capítulo se revisan las vulnerabilidades del sector informático y técnicas de ataque que usan personas inescrupulosas para cometer actos prohibidos.

En la segunda parte se desarrolla el marco teórico de este trabajo.

En el tercer capítulo, se describe las normas y estándares nacionales e internacionales, que deben tenerse en cuenta a la hora de realizar un trabajo de auditoria forense.

En la cuarta parte se lleva a cabo el desarrollo de la Auditoria Forense Informática en una empresa del sector comercial.

Finalmente se dan a conocer las conclusiones y recomendaciones correspondientes.

CAPÍTULO I

1. ANTECEDENTES

En este capítulo, conoceremos sobre la evolución de la Auditoría Forense Informática, las vulnerabilidades que se presentan en el sector informático, las metodologías y herramientas de ataque, con la finalidad de encontrar las posibles soluciones a esta debilidad suscitada en el sector informático.

1.1. Evolución de la Auditoría Forense Informática

[1]La historia de la Auditoría Forense Informática, se da a conocer según la aseveración realizada por Braulio Rodríguez Castro en la publicación Cuadernos de Contabilidad, quien dice que “Se tienen algunas referencias de los detectives contables hacia 1824 en Glasgow, Escocia, donde un profesional ofrece sus servicios en forma de testimonio experto como árbitro, perito en tribunales y consejos. Hacia 1900 se enfatizó más en Estados Unidos e Inglaterra esta disciplina.

Los primeros investigadores forenses contables que fueron reconocidos como tales se asume fueron los agentes especiales del IRS (Internal Revenue Service) americano en temas de evasión fiscal, anotándose su mayor logro con la encarcelación de Al Capone.

En la Segunda Guerra Mundial, la brigada de investigación criminal del FBI empleó a más de 500 auditores y contadores como agentes, examinando toda transacción financiera.

En 1946 aparece el libro “La Contabilidad Forense: su lugar en la economía de hoy”, escrito por Maurice E. Peloubet en Nueva York. Como

[1] Publicación Cuadernos de Contabilidad, Braulio Rodríguez, Pág. 68,69,70

se observa, aunque su desarrollo se estima de corto tiempo, realmente las manifestaciones abarcan un espectro de tiempo amplio.

Según otros autores dicen que desde hace algún tiempo muchos contadores ejercen la Auditoría Forense en nuestro medio; sin embargo, ésta no ha sido debidamente identificada como tal, de tal forma que estimule su estudio e investigación

Sin embargo dentro de la gran red de redes he podido identificar algunos antecedentes respecto a fechas concretas en que se realizó el análisis forense en el campo informático, identificando casos concretos en los que participó el FBI de EEUU, los cuales se detallan cronológicamente a continuación:

1984

Fue creado el FBI Magnetic Media Program, más tarde se convirtió en el Computer Analysis and Response Team (CART)

1993

Se desarrolla la Primera conferencia sobre evidencia lógica, denominada: First International Conference on Computer Evidence held

1995

Se forma la organización internacional para evidencias, denominada International Organization on Computer Evidence (IOCE)

1997

El grupo de los ocho países denominado G8 declara que se le debe dar más importancia al tema así como entrenamiento necesario para tratar estos asuntos, la expresión vertida fue: "Law enforcement personnel must be trained and equipped to address high-tech crimes"

1998

En Marzo el grupo de los ocho G8 estableció el IICE para crear los principios internacionales relativos a los procedimientos relacionados a evidencia digital.

Se realiza el Simposium INTERPOL Forensic Science.

1999

El FBI CART analiza 2000 cases, examinando 17 terabytes de datos

2000

Se establece el primer laboratorio del FBI denominado First FBI Regional Computer Forensic Laboratory.

2003

El FBI CART analiza 6500 casos, examinando 782 terabytes de datos.
Como podemos considerar todo se circunscribe a casos vinculados a la Auditoría Forense y a la evidencia digital. El FBI ha analizado muchos y se calcula que en EEUU sólo uno de cada 100 casos es detectado. Uno de cada ocho detectados es investigado y uno de cada 33 casos investigados resulta en una sentencia de prisión.

De ahí, las pocas referencias bibliográficas respecto a la misma en esas épocas, salvo las expresamente mencionadas. En la actualidad este

tema se está tomando con mucho interés en países avanzados y ya se escucha tratar en nuestro país, debido a las múltiples vulnerabilidades en el sector informático.

1.2. Vulnerabilidades del Sector Informático

Muchas son las vulnerabilidades que se presentan en el sector informático; pero es importante recalcar, lo que es una vulnerabilidad, Para [(2)]Wilches la vulnerabilidad consiste en "la incapacidad de una comunidad para absorber, mediante auto ajuste, los efectos de un determinado cambio en su medio ambiente, o sea, su no flexibilidad o incapacidad para adaptarse a ese cambio, que para la comunidad constituye un riesgo"

[(3)]Según el profesor Sanz Caja la **vulnerabilidad de un sistema informático** es la cualidad que le hace susceptible de ser afectado, alterado o destruido por algún hecho o circunstancia indeseada, de recibir algún daño o perjuicio en cualquiera de las partes o componentes, que afecte al funcionamiento normal o previsto de dicho sistema informático.

---

(2) La vulnerabilidad social y sus desafíos,RobertoPizarro, www.cepal.org
(3) http://sans.org /top 20

Análogamente define la **seguridad de un sistema informático** como el estado de protección del mismo, establecido con el fin de evitar la aparición de las distintas amenazas posibles que puedan alterar su normal funcionamiento, o de aminorar las consecuencias negativas de los distintos riesgos, una vez producidos.

Para mi criterio vulnerabilidad es “cualquier debilidad en los sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas.”

Las vulnerabilidades que no son otras cosas que debilidades, fallas de los sistemas, los mismos que son explotados por personas mediante ataques informáticos. Estos ataques son los incrementados al punto que ya contamos con estadísticas de los mismos.

En EEUU, debido a los frecuentes ataques informáticos a empresas comerciales, se realizó una encuesta por el Instituto de Seguridad de Computadoras (CSI), quien anunció recientemente los resultados de su quinto estudio anual denominado «Estudio de Seguridad Informática»

realizado a un total de 273 Instituciones principalmente grandes Corporaciones y Agencias del Gobierno.

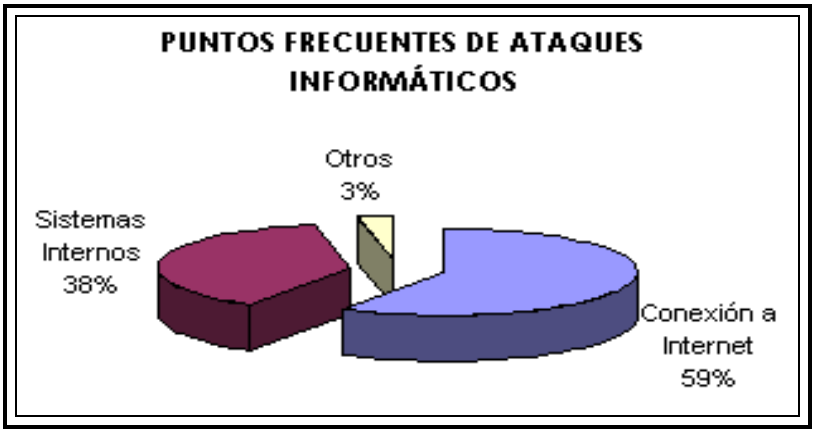


FIGURA 1.1. Puntos Frecuentes de Ataques Informáticos
[4]Fuente: Instituto de Seguridad de Computadoras (CSI)

Por tercer año consecutivo, el Estudio de Seguridad Informática, encontró que la mayoría de encuestados (59%) indicaron que los puntos frecuentes de ataques informáticos era su conexión de Internet, los que citaron sus sistemas interiores (mail, archivos, información confidencial) como un punto frecuente de ataque fue un 38%, y el 3% descubrieron que era el acceso desautorizados de terceras personas.

[4] www.segu-info.com.ar/ataquesinformatico.htm

Teniendo como base una encuesta realizada a 643 oficiales de seguridad corporaciones americanas, agencias gubernamentales, instituciones financieras, instituciones médicas y universidades, se muestra a continuación los hallazgos del «Estudio de Seguridad Informática» los mismos que confirman que los ataque por computadoras y otras violaciones de seguridad de información continúan constantes.

Los principales abusos y ataques informáticos se detallan en el gráfico a continuación:

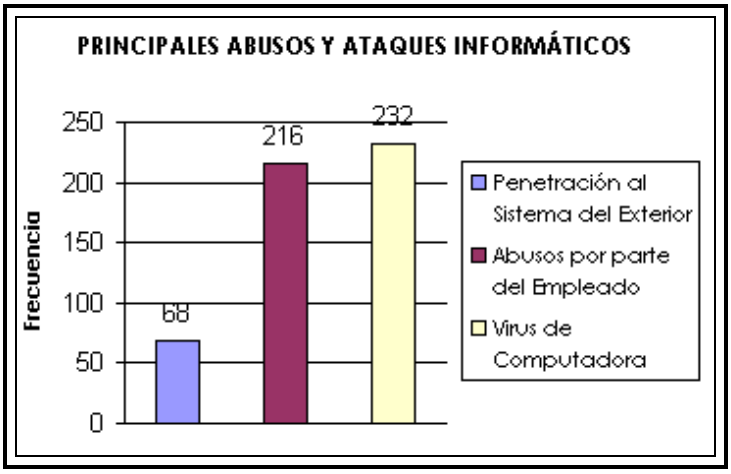


FIGURA 1.2. Principales Abusos y Ataques Informáticos
(5)Fuente: Instituto de Seguridad de Computadoras (CSI)

(5) www.segu-info.com.ar/ataquesinformatico.htm

Los encuestados detectaron una amplia gama a de ataques y abusos. De los 516 encuestados, se encontró que hay tres principales abusos que

* 68 encuestados que corresponden al 25% de encuestados descubrieron penetración al sistema del exterior.

*216 encuestados que corresponden al 79% descubrieron el abuso del empleado por acceso de Internet (por ejemplo, transmitiendo pornografía o pirateó de software, o uso inapropiado de sistemas de correo electrónico).

*232 encuestados que corresponden al 85% descubrieron virus de computadoras.

Por estos abusos y ataques informáticos han surgido diversas nomenclaturas o apelativos que se emplean para designar a personas o grupos que aprovechan estas vulnerabilidades. Los principales responsables de estos ataques son personas o grupo de personas que aprovechan las vulnerabilidades y son:

- Hackers
- Crackers
- Phreaker
- Insiders

- Outsiders

Hackers

El apelativo de hacker se crea a fines del siglo pasado cuando los Estados Unidos de América empiezan a recibir un masivo movimiento migratorio de personas de todos los países del mundo que esperaban encontrar en el "país de las oportunidades" un bienestar económico y progreso.

Los hackers eran estibadores informales que se pasaban todos el día bajando las maletas y bultos de las personas y familias completas que llegaban en los barcos a los puertos de New York, Boston, San Francisco, etc. Estos trabajadores eran infatigables, pues trabajaban muchas veces sin descansar y hasta dormían y comían entre los bultos de los muelles con el objeto de no perderse una oportunidad de ganar dinero.

La palabra "hack" en inglés tiene varios significados en español, entre ellos "hacha". Como si fuesen taladores de árboles que usan su hacha, en forma infatigable hasta llegar a tumbarlos, su tesonero propósito les mereció este apelativo.

La palabra hacker aplicada en la computación se refiere a las persona que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites. Los hackers tienen "un saludable sentido de curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas. No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos".

CRACKER

Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones

hasta lograr su objetivo. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web en Internet, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas.

Obviamente que antes que llegar a ser un cracker se debe ser un buen hacker. Asimismo se debe mencionar que no todos los hackers se convierten en crackers.

PHREAKER

El phreaker es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos.

INSIDERS

Según un reciente informe de la publicación estadounidense InformationWeek, un porcentaje sustancial de intrusiones en las redes de las empresas (ya sean chicas, medianas o grandes) proviene de ataques internos. Es decir, los mismos empleados hackean a su propia organización.

OUTSIDERS

El outsider es la persona con conoce muy bien la instalación de una organización pero no pertenece a ella. Son aquellos que ingresan a la red simplemente averiguando una password autorizada.

El aprovechamiento ilícito de las vulnerabilidades da lugar al delito informático.que pueden originar en muchos casos siniestros

informáticos. Estos delitos informáticos se presentan en diferentes maneras tales como:

Difusión de pornografía: En la mayoría de países así como en nuestro país es ilegal la comercialización de pornografía infantil o cualquier acto de desviación. Un ejemplo de conducta activa sería remitir una recopilación de imágenes pornográficas scaneadas a los mailbox de un país en donde estuvieran también prohibidos los actos de difusión o comercialización de las mismas.

Manipulación de los datos: Este fraude conocido también como sustracción de datos, representa el delito informático mas representativo ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos. De acuerdo a la información entregada por entidades de seguridad a nivel mundial, el 75% de los casos de sustracción de datos lo realiza personal interno de la organización o que pertenecieron a ellos.

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. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas. Uno de los métodos utilizados por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación informática: es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.

Existe una diferencia en las estafas informáticas cometidas dentro del sistema y las cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo, y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las manipulaciones de datos hechas antes, durante o después de la elaboración de los programas, siendo

éstas las causantes del engaño que determina una alteración intencional de la disposición patrimonial.

Los hackers, crackers, preakers, insiders, outsiders pueden cometer delitos comunes que atentan contra la seguridad informática de una organización o empresa, a continuación se dará a conocer algunas metodologías de ataque, usados por estos personajes y cualquier persona que desee aprovechar la vulnerabilidad y generar ataques.

1.3. Metodología de ataque

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

A esta altura del desarrollo de la "sociedad de la información" y de las tecnologías computacionales, los piratas informáticos que producen los ataques ya no son novedad.

Los hay prácticamente desde que surgieron las redes digitales, hace ya unos años atrás. Sin duda a medida que el acceso a las redes de comunicación electrónica se fue generalizando, también se fue multiplicando el número de quienes ingresan "ilegalmente" a ellas, con distintos fines, por eso es importante conocer la metodología de ataque que usan los atacantes.

El objetivo de la metodología de ataque es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (estos ataques a la confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde dónde), es tan importante como saber con qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos (políticas, capacitación), las cuales se describen a continuación:

1.3.1. Identificación

- **Networks Scanners.-** Hacen un mapa de la red identificando: dominios, servidores, sistemas operativos.

  Recogiendo información sin atacar y descubriendo: los servidores activos, servidores de correo, nombres de empleados, rango de direcciones IP.

1.3.2. Exploración

Ports Scanners.- Scanean las máquinas para detectar puertos abiertos, a fin de identificar posibles exposiciones o vulnerabilidades a explotar.

Sistemas activos, servicios a la escucha, sistemas operativos

1.3.3. Enumeración

Obtención de usuarios válidos o recursos compartidos mal protegidos

1.3.4. Obteniendo acceso

Passwords Crakers.- Se usan para detectar la confinación de usuarios y passwords válidos. Obteniendo la password para los usuarios/servicios

1.3.5 Escalando privilegios

Obteniendo el Super Usuario, que es el usuario administrador, que permite realizar todas las operaciones posibles en el sitio y/o la red.

1.3.6 Robando accesos

Buscando otros accesos válidos o rutas que permitan obtener información de la organización.

1.3.7. Cubriendo las huellas

Buscando logs y borrando todas las pistas de Auditoría, de manera tal que salgan sin dejar rastro.

1.3.8 Creando entradas traseras

Crear cuentas de usuario, buscando los archivos deseados.

Los métodos de ataque descritos, están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de crackear una password, un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente

también, el atacante puede adquirir derecho de acceso a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

1.4. Herramientas de Ataque

En los primeros años, los ataques involucraban poca sofisticación técnica. Los **insiders** (empleados disconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros.

Los **outsiders** (personas que atacan desde afuera de la ubicación física de la organización) ingresaban a la red simplemente averiguando una password válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño,

configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevó a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc).

Detallaré a continuación las herramientas más utilizadas en el área de un siniestro informático son:

- **Networks Scanners**.-Es la que ayuda mediante un mapa de la red identificando: dominios, servidores y sistemas operativos.

- **Ports Scanners.**-Scanean las máquinas para detectar ports abiertos, a fin de identificar posibles exposiciones a explorar.

- **Passwords crackers.**- Se usan para detectar la confinación de usuarios y passwords válidos.

- **Packet Sniffers.**- Permiten leer la información de los paquetes que pasan por la red donde están instalados.

- **War Dialers.-** Son los que permiten detectar modems en las líneas de teléfono.

- **Trojans.**-Permiten introducir back doors en las redes.

El excesivo privilegio que se les ha otorgado a los empleados, ha generado debilidad en las organizaciones, que confiando en ellos, no realizan continuas evaluaciones, dichos privilegios han generado pérdidas y siniestros

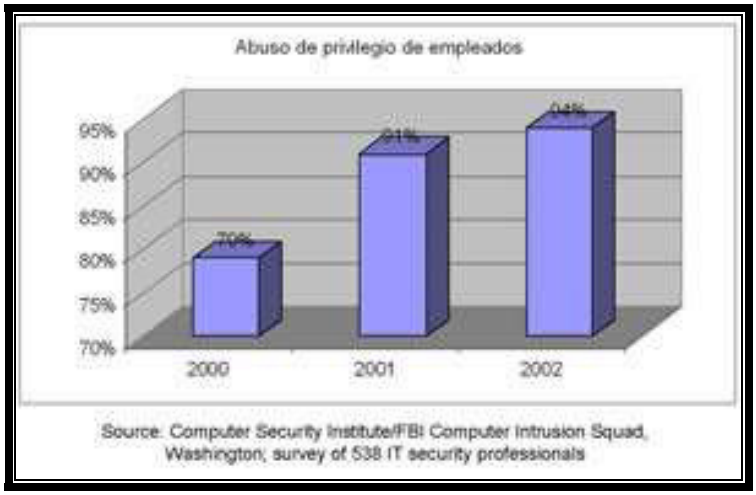


FIGURA 1.3. Abuso de privilegio de empleados
Fuente: Instituto de Seguridad de Computadoras (CSI)

[6]Este gráfico demuestra un estudio realizado por las CSI (Computer Security Institute)/FBI, en los años 2000-2002, destacando los ataques informáticos, en su mayoría producidos por el abuso de privilegio de empleados. En el año 2000 el 70% de los abusos eran cometidos por los empleados, el año siguiente (2001) se incremento al 91% el abuso del personal de la empresa, y en el último año de estudio (2002) aumento al 94% el abuso de los empleados, en cuanto a la información confidencial de la empresa.

[6] www.kneos.com/estadistica de ataques inforamáticos.htm

FIGURA 1.4. Vulnerabilidades de la Organización
Fuente: Instituto de Seguridad de Computadoras (CSI)

(7)El estudio realizado por la CSI (Computer Security Institute)/FBI, en los años 1999-2001, destaca otras variables a los cuales estaá vulnerable la organización.

En el año1999, 9% se quedaron sin servicio por más de una hora, en sus servidores, 50% sufrieron ataques por virus y el 31% por pérdidas de datos.

En el año 2000, alrededor del 61% no tuvieron acceso al sistema por más de una hora, el 63% perdieron archivos importantes porque sus equipos estaban infectados de virus, y el 40% perdieron sus datos.

(7) www.kneos.com/estadistica de ataques inforamáticos.htm

En el año 2001, cerca del70% de los servidores estuvieron fuera de servicio, 75% se infectaron de virus y el 52% perdieron sus datos.

Estas estadísticas me permiten identificar las fallas, debilidades, fortalezas y vulnerabilidades de la empresa, debido a los privilegios que se les da a los empleados, generando la pérdida de información, lo cual se convierte en una pérdida económica para la empresa.

Con el fin de evitar estas falencias, en el Capítulo dos se presentará el marco teórico de esta investigación, con el objeto de conocer más acerca sobre la Auditoría Forense Informática, la importancia, las metodología, herramientas y técnicas, para luego poder aplicar estos conceptos en la metodología del caso práctico.

CAPÍTULO II

2. MARCO TEÓRICO

En el presente capítulo se darán a conocer los diferentes temas relacionados con la auditoria forense, para que el lector comprenda la evolución de los diferentes siniestros informático que se pueden suscitar en una empresa del sector comercial, y así conseguir el entendimiento del porque las organizaciones deben revisar sus controles periódicamente con la finalidad de determinar sus seguridades tanto lógicas como físicas y además mejorar sus procesos.

2.1. Fundamentación Teórica

2.1.1. Siniestro

2.1.1.1 Concepto

Según el italiano Carlos Sarzana: “El siniestro es la destrucción fortuita o pérdida importante que sufren las personas o la propiedad, en especial por muerte, incendio o naufragio.”

Según el Ing. Cueto-López: “El siniestro es un hecho súbito, accidental e imprevisto, cuyas consecuencias dañosas estén cubiertas por las garantías dadas.”

Según el diccionario Laurrose: “El siniestro es un hecho violento, súbito, externo y ajeno a la intencionalidad del asegurado, cuyas consecuencias pueden estar cubiertas por alguna garantía del seguro. Constituye un solo y único accidente el conjunto de daños derivados de un mismo hecho.”

Para mi criterio, el siniestro es un suceso esporádico, accidental y/o planeado que pueden ser ocasionados por terceros y cuyos resultados, generan grandes pérdidas a la empresa.

2.1.1.2. Clases de Siniestros

Los siniestros dentro de una organización, empresa u organismos pueden ser causados por diferentes procedimientos, mecanismos o algunas veces por la misma mano del hombre.

Según los Consultores de Javelles S.A las clases de siniestros se derivan, según:

2.1.1.2.1. Por el grado de intensidad del daño producido

- **Siniestro Total.** Es aquél cuyas consecuencias han afectado a la totalidad del objeto asegurado, destruyéndolo completa o casi completamente.

- **Siniestro Parcial**. Es aquél cuyas consecuencias sólo afectan parte del objeto asegurado, sin destruirlo completamente.

2.1.1.2.2 Por el estado del trámite en que se encuentran:

- **Siniestro Declarado**. Aquél que ha sido comunicado por el asegurado a su entidad aseguradora.

- **Siniestro Pendiente.** Es aquél cuyas consecuencias económicas aún no han sido totalmente indemnizadas por la entidad aseguradora.

- **Siniestro Liquidado.** Aquél cuyas consecuencias económicas han sido completamente indemnizadas o reparadas por la entidad aseguradora.

2.1.1.3.3 Según lo común del siniestro

- **Siniestro Ordinario.** Es el que tiene su origen en la ocurrencia de un riesgo ordinario.

- **Siniestro Extraordinario o Catastrófico.** Es el que está originado por un riesgo de naturaleza extraordinaria o excepcional.

Los siniestros dentro de las organizaciones en algunas ocasiones, están vinculados con los fraudes, ya que pueden ser cometidos de forma intencional y afectar económicamente a la empresa

Para ejemplos mencionare algunos de ellos:

- Violación de Seguridad
- Ocultamiento de documentos
- Borrado fraudulento de archivos
- Robo de dinero
- Competencia desleal
- Destrucción de archivos
- Pérdida de datos y bienes

Hay un sin número de siniestros, que se podrán enumerar, pero he nombrado las más usuales e importantes, que se han destacado aquí en el país.

2.1.2.- Siniestro Informático

2.1.2.1.- Concepto.-Según Miguel Antonio Cano C: “El siniestro informático implica actividades criminales como robos, hurtos, falsificaciones, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho. “

2.1.2.2.- Importancia del Siniestro Informático.- En el área informática se pueden producir ataques, y esos ataques van contra algo medular que es la información la que puede sufrir distintos

tipos de intromisión para agredirla en su confidencialidad, disponibilidad e integridad.

Definitivamente es indispensable el uso de la computadora y del manejo de la tecnología para la comisión de conductas delictivas que generen un desastre informático denominadas "Siniestros Informáticos".

Cuando el siniestro informático es descubierto por un empleado (gerente, auditor, jefe), debe asegurarse que hay la máxima información disponible este intacta, clara y que sea la correcta para que el auditor forense informático pueda realizar su trabajo correctamente.

Actualmente en las organizaciones, es importante que haya un auditor forense para evitar los siniestros informáticos y así evitar la destrucción, robo o alteraciones de información valiosa para el desarrollo económico y profesional de la empresa.

2.1.2.3- Tipos de Siniestros Informáticos

El Dr. Julio Téllez Valdez menciona que los siniestros informáticos Incluye los cometidos contra el sistema y los cometidos por medio de sistemas informáticos ligados con Telemática, o a los bienes jurídicos que se han relacionado con la información: datos, documentos electrónicos, dinero electrónico, etc. Predominan:

Bomba ilícita o cronológica Exige conocimientos especializados ya que requiere programar la destrucción o modificación de datos en el futuro. Lo contrario de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso entre todos los dispositivos informáticos criminales, la bombas lógicas son las que poseen el máximo potencial de daño. Su activación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. Puede utilizarse como material de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Piratas informáticos o hackers El acceso se efectúa a menudo desde un lugar exterior, recurriendo a uno de los diversos medios como son:

Aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.

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

En todos estos casos se producen pérdidas de dinero provocadas por las conductas descritas.

Robo de información.- En principio, todos los computadores contienen alguna información de interés para alguien. Es cierto que no siempre tendrá el mismo valor, pero siempre puede existir alguien interesado en conseguirla. Por consiguiente, uno de los ataques más comunes está dirigido a extraer información confidencial de un sistema.

Destrucción de información.-Existen métodos indirectos que permiten explorar los contenidos del disco duro.

Todos poseemos datos y ficheros en nuestro computador que no quisiéramos perder. Algunos, incluso, tienen media vida en sus archivos y datos y se morirían si se les destruyera la información que guardan en su disco duro. Por estas razones es muy importante que ninguna persona sea capaz de modificar ni mucho menos destruir los datos de la máquina cliente en la que se ejecuta.

2.1.3. Auditoria Forense

2.1.3.1 Concepto

El gremio de Contadores y Auditores financieros fue un poco escéptico en aceptar este titulo de Auditoria Forense siempre había que explicar hasta la saciedad el término"forense" y desvincular la medicina legal o la patología forense o mas

comúnmente llamada necropsia forense en cadáveres para investigar las causas de muerte y dar un informe que permitiera la incriminación de algún sospechoso y recopilar las pruebas que se llevarían a un juicio en contra del acusado, o los acusados de esta muerte.

El término “forense” no se refiere a necropsia o autopsia. Es una término de origen Greco-latino, que en la antigüedad se utilizaba para denominar a un foro o “forum” la reunión de notables o el conjunto de personalidades que discutían un tema ante el pueblo y en muchos de los casos en estos “forums” también se aplicaba la ley con ejecuciones publicas ejemplarizantes de los reos que habían sido previamente juzgados y condenados. En nuestro mundo moderno la palabra forense se aplica para determinar todo lo concerniente al derecho y la ley.

2.1.3.2 Importancia

En nuestro medio son comunes los fraudes y/o siniestros estatales y corporativos, robos, desfalcos y otros conflictos donde se

requiere la ayuda de un auditor forense, para contribuir a la resolución de estos litigios.

La auditoria forense surge como alternativa para combatir la corrupción y particularmente para atacar uno de los elementos que más la favorecen: La impunidad.

2.1.3.3 Objetivo de la Auditoria Forense

La Auditoria Forense proporciona recomendaciones para asegurar la salvaguarda de los activos de los sistemas de información, manteniendo la integridad de los datos y lograr los objetivos de la organización en forma eficiente y eficaz.

Los principales objetivos de la auditoria Forense son:

1. La compensación de los daños causados por los criminales o intrusos.

2. La persecución y procesamiento judicial de los criminales.

3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

2.1.3.4 Uso de la Auditoria Forense

El uso de la Auditoria Forense puede ser de diversos casos, no tienen que ser directamente relacionadas a la informática forense:

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

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

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

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

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

2.1.4. Auditoria Informática Forense

2.1.4.1 Concepto

[6]Según la definición de Ron Weber en Auditing Conceptual Foundations and practices sobre la Auditoria Informática Forense es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente.

La Auditoria Informática Forense puede definirse, como la ciencia que se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

Es la aplicación de técnicas y herramientas de hardware y software para determinar datos potenciales o relevantes. También puede

---

[6] Auditoria en Informática, II Edición, José Antonio Echenique García, Mc Graw

servir para informar adecuadamente al cliente acerca de las posibilidades reales de la evidencia existente o supuesta.

La necesidad de este servicio se torna evidente desde el momento en que la enorme mayoría de la información generada está almacenada por medios electrónicos.

2.1.4.2 Importancia de la Auditoria Informática Forense

La auditoria informática no es sólo importante en el área corporativa sino también en el área estatal, donde se han encontrado más hechos fraudulentos. De ahí que consideremos que es necesario adquirir conocimiento sobre el tema debido a la importancia en su aplicación respecto a los fraudes económicos.

La auditoria informática forense es de importancia para:

Contadores: Pues su práctica se puede ver afectada y limitada por el desconocimiento de la auditoria forense.

Estudiantes de contaduría: Esta auditoria forense, le da una opción de especialización de la profesión.

Inversionistas, accionistas, socios, prestamistas, acreedores, empleados y otros individuos del ámbito comercial: Cualquier individuo que este involucrado con un ente económico es susceptible de requerir la auditoria forense como procedimiento para la solución de delitos económicos.

Jueces, abogados y otros involucrados en el área jurídica: La auditoria forense les sirve para presentar pruebas claras y verídicas para la solución de discusiones financieras.

La población en general: La aplicación de la auditoria forense para combatir la corrupción mejora la economía y el bienestar social.

De todo lo anterior, se deduce el incremento de la importancia de la Auditoría Forense, ya que debido al notable aumento de los

delitos económicos se hace indispensable un control y castigo de estas conductas delictivas.

2.1.5 Metodología de la Auditoria Informática Forense

El auditor forense para poder iniciar su trabajo, determinando los hallazgos de irregularidades, fraude y corrupción en las empresas del sector comercial, debe de establecer una metodología que este, acorde con las irregularidades encontradas.

2.1.5.1. Etapas de la Metodología de la Auditoria Forense

El siguiente esquema es considerado como adecuado para un desarrollo más eficiente en las metodologías de investigación.

2.1.5.1.1 Definición y reconocimiento del problema

En esta fase se determinar si hay suficientes motivos o indicios, para investigar los síntomas de un posible fraude. La sospecha es definida como la totalidad de las circunstancias que conducen a una persona razonable, prudente y profesionalmente preparada a

creer que un fraude ha ocurrido, esta ocurriendo o ocurrirá. Se debe observar que un indicio no es una prueba, ni siquiera representa una evidencia de que un fraude existe. Antes de comenzar una investigación formal, se debe obtener la aprobación del directorio de la organización ya que una auditoria de fraude es sumamente complicada, controvertida, extenuante y puede ser perjudicial para miembros de dicha organización, se debe contemplar la existencia de convenios de confidencialidad y concertar los futuros pasos a seguir con la finalidad de verificar la existencia de fraude.

Para poder cumplir con la finalidad de verificar la existencia del fraude es necesario, conocer acerca de la evidencia y lo importancia en la recuperación de sus datos.

2.1.5.1.2. Recopilación de evidencias de fraude

Después del reconocimiento del problema, comenzamos a buscar las evidencias relacionadas al fraude, siniestro o ataque, estas evidencias deben ser suficientes para que garanticen el éxito de la investigación. Las evidencias son recogidas para determinar

quien, que, cuando, donde, porque, cuanto y como se ha cometido el fraude, siniestro o ataque.

Las principales técnicas que se aplican son:

- Indagación.
- Observación.
- Inspección.
- Confirmación.
- Análisis y recálculo.

Las evidencias se deben organizar de modo que todos los elementos y variables que interactúan en el fraude sean considerados. Por lo tanto a continuación, definiremos que es una evidencia.

Evidencia

En la Auditoria Forense, el criminal deja evidencia que permite identificar lo ocurrido, lo mismo ocurre con la evidencia computacional.

La evidencia computacional es única, cuando se la compara con otras formas de “evidencia documental”. A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto, es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistido por computador, fórmulas y software propietario.

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías.

La IOCE (International Organization On Computer Evidence), define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia computacional:

1. Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.

2. Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.

3. Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.

4. Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.

5. Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Además definen que los principios desarrollados para la recuperación estandarizada de evidencia computarizada se deben gobernar por los siguientes atributos:

1. Consistencia con todos los sistemas legales.
2. Permitir el uso de un leguaje común.
3. Durabilidad.
4. Capacidad de cruzar límites internacionales.
5. Capacidad de ofrecer confianza en la integridad de la evidencia.
6. Aplicabilidad a toda la evidencia forense.

Evidencia digital

Es un tipo de evidencia física. Esta construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.

Evidencia Digital: Información de valor para el caso que es transmitida o guardada en formato digital.

- Evidencia digital original
- Evidencia digital duplicada

Objetos de datos: Información valiosa relacionada con el caso asociada a objetos físicos. Debemos procurar trabajar sobre imágenes de discos, esto es así para no trabajar a nivel de sistema de ficheros, pues podemos perder información valiosa.

Objetos físicos: Soporte físico sobre el que se guarda la información digital.

Ejemplos de evidencia digital:

- Email

- Images
- Chat rooms
- File contents
- System logs
- Network packets

Las evidencias digitales suelen pasarse por alto, o recolectarse incorrectamente o analizarse ineficientemente debido a mala formación técnica y desconocimiento de la normativa legal; sin embargo es muy importante tener el conocimiento y la pericia necesaria para usar con efectividad la evidencia digital en cualquier tipo de investigación.

Las evidencias “escritas“las podemos clasificar en:

- **Evidencia demostrativa:** Reconstruye la escena o incidente en cuestión.

- **Evidencia de documentación:** Documentos escritos que constituyen una evidencia

En el mundo digital dado la facilidad de realizar copias exactas de documentos, generalmente se considera la evidencia digital cómo evidencia demostrativa.

Existe un RFC 3227 - “Guidelines for Evidence Collection and Archiving” que establece normas para la recopilación y almacenamiento de evidencias.

2.1.5.1.3. Evaluación de las evidencias recolectadas o análisis

Esta fase sirve para determinar si son suficientes y validas las evidencias recolectadas como para comenzar a reportar eficazmente el fraude. La evidencia deber ser evaluada para determinar si es completa y precisa, si es necesario seguir recolectando mas evidencias. De la evidencia recolectada surgirá la respuesta de que acciones judiciales se pueden realizar por parte de la Organización.

2.1.5.1.4. Elaboración del informe final con los hallazgos

La fase final de la investigación del fraude es presentar los resultados. Esto supone un reto, ya que el informe de fraude normalmente es la evidencia primaria disponible y en algunos casos única sustentatoria de la investigación realizada. El informe es de vital importancia puesto que los pleitos judiciales se ganan o se pierden mayormente en base a la calidad del informe presentado.

Características del informe

El texto del informe sobre una investigación de auditoria forense deben reunir las siguientes características:
Debe presentarse por escrito. En él debe estar claramente:

- La descripción de los hechos, objeto del peritazgo y deben distinguirse de los pronósticos o conjeturas

- Las operaciones técnicas realizadas.

- Los principios científicos en que se fundamenta.

- Las conclusiones debidamente comprobadas y sustentadas que servirán al juez para valorar la prueba.

- Si ciertos hechos parecen contradictorios, deben ser ampliamente discutidos. Un conjunto de hechos debe compararse con otro para llegar a una conclusión, y deben especificarse cuidadosamente las razones que se tengan para ignorar las implicaciones de cualquier hecho.

- El informe debe excluir toda referencia a aquellas características de las cuentas que se presten a controversia, a menos que tengan relación con las conclusiones del informe.

2.1.5.1.5.- Presentación en la corte de la evidencia relacionada

El informe junto con toda la documentación pertinente debe ser presentado ante la Corte en el juicio establecido para el suceso respectivo.

Una investigación forense es aquel estudio que se realiza bajo tales condiciones que está íntegramente documentado, es reproducible y sus resultados son verificables. Un examen forense no borra ni altera ningún dato en la evidencia original, preservando los mismos de forma precintada, e independientemente de quién lleve a cabo el examen, con qué herramientas y metodologías, debe siempre llevar a los mismos resultados.

Un principio elemental en la ciencia forense, que usaremos continuamente para relacionar un criminal con el crimen que ha cometido, es el Principio de Intercambio o transferencia de Locard, (Edmond Locard, francés fundador del instituto de criminalística de la universidad de Lion).

Este principio fundamental viene a decir que cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en la escena

o en la víctima y viceversa, por lo cual la parte más principal para recopilar la información es la evidencia digital.

2.1.6. Herramientas de la Auditoria Forense

2.1.6.1 Concepto.

Según el diccionario Aristos: “Las herramientas son instrumentos u objetos que ayuda a resolver un problema que puede ser de cualquier clase, técnico, labora, penal, etc.”

2.1.6.2. Clasificación de las Herramientas de Auditoria Forense

Las herramientas que se utilizan en la Auditoria Forense son de vital importancia en la reestructuración de la información recopilada de acuerdo al siniestro y/o fraude suscitado.

Considerando los diferentes siniestros informáticos que se pueden suscitar en una empresa del sector comercial, las herramientas tienen su clasificación:

2.1.6.2.1. Herramientas de Hardware

Para el análisis forense se requiere del siguiente hardware:

- Un equipo portable “F.R.E.D.D.I.E”, (Forensic Recovery of Evidence Device Diminutive Interrogation Equipment);
- Conjunto portable de duplicación de discos
- Impresora portable, inalámbrica
- Soporte inalámbrico para todos los dispositivos del kit
- Dispositivos varios

1.- Un equipo portable “F.R.E.D.D.I.E .- El componente principal del kit portable se denomina “F.R.E.D.D.I.E”, (Forensic Recovery of Evidence Device Diminutive Interrogation Equipment); consiste en un computador portable, diseñado para la recuperación de datos de todo tipo de dispositivos, con posibilidades de bloqueo de

discos para evitar modificaciones accidentales del material estudiado y otras características de obtener una línea temporal de eventos, tanto de los actos realizados por el equipo forense como por el autor del crimen.

2. Conjunto portable de duplicación de discos: Elemento sencillo destinado para duplicar discos IDE-IDE e IDE-SCSI, con presentación automática de un informe impreso con datos del disco (número de serie, cilindros, capacidad, fecha y hora de la copia, etc.).

3. Impresora portable, inalámbrica: se adquirió por la importancia del papel y la burocracia en todo proceso judicial, de forma que al disponer de cuadernos electrónicos podríamos llevar ahí los formularios adecuados para cada caso e imprimirlos en la impresora portable (ligera y con batería).

4. Soporte inalámbrico para todos los dispositivos del kit: es un requisito importante, ya que estudia minuciosamente cada

componente para comprobar que disponía de soporte inalámbrico, (bluetooth, infrarrojos o WiFi).

5. Dispositivos varios: llaveros de almacenamiento masivo por USB, disco USB 2.0 de alta capacidad (80 GB), etc.

Además se deben aplicar procedimientos preestablecidos según el caso, éstos son:

– Procedimientos de actuación para los centros de relación con el cliente.

– Procedimientos de actuación para asesoría jurídica.

– Procedimiento de actuación para usuario corporativo que encuentra un problema de seguridad.

– Procedimiento de actuación para administradores de sistemas que encuentra un problema de seguridad.

– Procedimiento de actuación en caso de compromiso de sistema.

– Procedimiento de recuperación.

– Scripts de recogida de información.

– Tabla/árbol de contacto para escalado de incidentes.

– Manual de procedimiento de análisis forense.

Así mismo se deben elaborar formularios según el caso, como, por ejemplo:

Formularios de incidentes tipificados: especiales, dedicados para registrar todo tipo de incidentes, ataques de ingeniería social, contacto con intruso, etc.
Recuperación y análisis.

Un análisis forense de un caso complejo puede durar meses, incluso años.

2.1.6.2.2. Herramientas de software

Software Comercial

Existe software comercial como Safeback, Norton Utilities, Forensic Toolkit, Encase, Encryption Linux Boot Disk, TCT, EnCase, FTK y otros visores de archivo, SMART (software forense comercial para plataformas linux), Autopsy de @Stake, etc

Software OpenSource

- TCT (The Coroner's Toolkit): Suite de herramientas de Auditoria Forense creada por dos de los padres de la Auditoria Forense Dan Farmer y Wietse Venema. (Ver anexo 1)
- TSK / Autopsy (The Sleuth Kit): Herramientas basadas en TCT
- Foremost: Recuperación de archivos según sus cabeceras y pies.
- ODESSA (Open Digital Evidence Search and Seizure Architecture): suite de herramientas para recuperar información en sistemas Windows (papelera de reciclaje, históricos de navegación web, etc.)

2.1.6.2.3. Herramientas para el Monitoreo y/o Control de Computadores

Algunas veces se necesita información sobre el uso de los computadoras, por lo tanto existen herramientas que monitorean el uso de los computadores para poder recolectar información. Existen algunos programas simples como key loggers o recolectores de pulsaciones del teclado, que guardan información sobre las teclas que son presionadas, hasta otros que guardan imágenes de la pantalla que ve el usuario del computador, o hasta casos donde la máquina es controlada remotamente.

KeyLogger Es un ejemplo de herramientas que caen en esta categoría. Es una herramienta que puede ser útil cuando se quiere comprobar actividad sospechosa; guarda los eventos generados por el teclado, por ejemplo, cuando el usuario teclea la tecla de 'retroceder', esto es guardado en un archivo o enviado por e-mail.

Los datos generados son complementados con información relacionada con el programa que tiene el foco de atención, con anotaciones sobre las horas, y con los mensajes que generan algunas aplicaciones.

Existen dos versiones: la registrada y la de demostración. La principal diferencia es que en la versión registrada se permite correr el programa en modo escondido. Esto significa que el usuario de la máquina no notará que sus acciones están siendo registradas.

2.1.6.2.4. Herramientas de Marcado de documentos

Un aspecto interesante es el de marcado de documentos; en los casos de robo de información, es posible, mediante el uso de herramientas, marcar software para poder detectarlo fácilmente.

2.1.7 Técnicas aplicadas para la auditoria forense

2.1.7.1 Concepto

Según el diccionario Laurrose: “Técnicas son formas por las cuales se pueden resolver diferentes problemas, mediante algunas técnicas mas especializadas que otras.”

2.1.8 Técnicas y procedimientos típicos de la Auditoria Forense

Los procedimientos de Auditoría Forense, constituyen el conjunto de técnicas que en forma simultánea se aplican para poder obtener las evidencias suficientes, competentes, relevantes y útiles que permitan sustentar las pruebas y testimonios que aporta el auditor forense, ante los tribunales o el Directorio que lo contrata.

Los tipos de evidencia que aporta el auditor forense son de carácter analítico, documental, físico y testimonial y dependerán del tipo de compromiso asumido.

Las técnicas más utilizadas para la recolección de información en una Auditoria Forense son:

Entrevistas

Esta técnica se empleará para conseguir informaciones necesarias que sirvan de aval para el buen desempeño de nuestro trabajo de investigación para la realización de la entrevista se utilizará el cuestionario de Auditoría.

Las fuentes de información que se deben consultar son las siguientes:

- Identificación de las personas
- Registros y controles que se tengan establecidos
- Establecer fuentes alternas con el propósito de analizar si el implicado o los implicados se encuentran registrados en la cámara de comercio y otros tipos de entidades financieras

- Solicitud de información, para obtener: datos completos y precisos, además de copias de documentos que soporten la información.

Cuestionario

El Cuestionario es un instrumento de investigación. Este instrumento se utiliza, de un modo preferente, en el desarrollo de una investigación en el campo de las ciencias sociales: es una técnica ampliamente aplicada en la investigación de carácter cualitativa.

Esta técnica ayudara a establecer las fortalezas y debilidades de la organización.

El Cuestionario es "un medio útil y eficaz para recoger información en un tiempo relativamente breve".

Observación

La observación es una técnica que nos ayuda en el proceso de la Auditoria Forense, nos ayuda a emitir un criterio propio sobre los hechos del suceso y tener conocimientos más amplios de lo que verdaderamente pasó.

Indagación

Esta técnica, es utilizada cuando no encontramos evidencia necesaria. La indagación nos ayuda a tener una evidencia testimonial de los empleados de la empresa.

2.1.9 Definiciones Conceptuales

1.- Auditoría Forense: es una alternativa para combatir la corrupción, porque permite que un experto emita ante los jueces conceptos y opiniones de valor técnico, que le permiten a la justicia actuar con mayor certeza, especialmente en lo relativo a la vigilancia de la gestión fiscal.

2.- Delito Informático: Según María de la Luz Lima, dice que el "delito informático en un sentido amplio es cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea con método, medio o fin".

3.-Fraude: Engaño, inexactitud, consistente, abuso de confianza, que produce o prepara un daño, generalmente material.

4.-Hallazgo: Es la recopilación de información especifica sobre una operación, actividad, organización, condición u otro asunto que se haya analizado y evaluado y que se considera de interés o utilidad para los funcionarios del organismo.

5.- Herramientas de la Auditoria Forense: Son artículos u objetos que ayuda a resolver un problema que puede ser de cualquier clase, técnico, labora, penal, etc.”

6.-Informe: Comunica a las autoridades pertinentes los resultados de la Auditoría. Los requisitos para la preparación del informe son claridad y simplicidad, importancia del contenido, respaldo adecuado, razonabilidad, objetividad entre otros.

7.- Metodología: Según el Diccionario, Método es el “modo de decir o hacer con orden una cosa”. Asimismo define el diccionario la palabra Metodología como “conjunto de métodos que se siguen en una investigación científica”. Esto significa que cualquier proceso cinético debe estar sujeto a una disciplina de proceso defina con anterioridad que llamaremos Metodología.

8.- Siniestro.- Acaecimiento dañoso del que resulta una reclamación bajo un contrato de seguro y del que habrá de responder el

asegurador en función de las garantías prestadas por la póliza y la causa del mismo

9.- Siniestro Informático: Según Miguel Antonio Cano C: “El siniestro informático implica actividades criminales que no encuadran en las figuras tradicionales como robos, hurtos, falsificaciones, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho. “

CAPÍTULO 3

3. Normas y Estándares Nacionales e Internacionales

El desarrollo de este capítulo que concierne a las normas y/o estándares internacionales, pretende difundir las normas y/o estándares internacionales que se han venido desarrollando conforme ha ido evolucionando la tecnología como una forma mas justa de ejercer la profesión de auditoria y al mismo tiempo como un marco necesario para suplir las necesidades que a este tema se refieren.

Las normativas analizadas en este capítulo constituyen el fundamento para el progreso efectivo en el campo de la Auditoria Forense Informática, con el

propósito de encontrar evidencias en un siniestro informático como el realizado y documentado en este trabajo.

A continuación se documentarán de manera textual tal y como reposan en los respectivos documentos, algunas leyes, normas y estándares internacionales vinculados a Auditoria Forense Informática.

3.1. Normas internas de auditoria

Son las condiciones mínimas del perfil que debe poseer el auditor y/o contador público, sus actitudes y aptitudes personales, para seguir obligatoriamente su aplicación en cada proceso de su actividad como auditor.

3.1.1. Clasificación de las normas de auditoría generalmente aceptadas.

1.Personales.

2. Relativas a la ejecución del trabajo.

3. Relativas a la información.

3.1.1.1. Personales: se refiere a la persona del contador público como auditor independiente; éste debe ser: experto en la materia, siendo profesional a su actuación y observando siempre principios éticos.

a. Entrenamiento técnico y capacidad profesional: el auditor debe tener conocimientos técnicos adquiridos en Universidades o Institutos superiores del país, habiendo culminado sus estudios con recepción profesional de Contador Público, adquiriendo una adecuada práctica o experiencia, que le permita ejercer un juicio sólido y sensato para aplicar los procedimientos y valorar sus efectos o resultados.

b. Cuidado y diligencia profesional: Al ofrecer sus servicios profesionales debe estar consciente de la responsabilidad que ello implica. Es cierto que los profesionales son humanos y que por lo

tanto se encuentra al margen de cometer errores, estos se eliminan o se reducen cuando el contador público pone a su trabajo (cuidado y diligencia profesional).

c. Independencia mental: Para que los interesados confíen en la información financiera este debe ser dictaminado por un contador público independiente que de antemano haya aceptado el trabajo de auditoria , ya que su opinión no este influenciada por nadie, es decir, que su opinión es objetiva, libre e imparcial.

3.1.1.2. Relativas a la ejecución del trabajo. Estas normas se refieren a elementos básicos en el que el contador público debe realizar su trabajo con cuidado y diligencia profesionales para lo cual exigen normas mínimas a seguir en la ejecución del trabajo.

a. Planeación y supervisión: antes de que el contador público independiente se responsabilice de efectuar cualquier trabajo debe conocer la entidad sujeta a la investigación con la finalidad de planear su trabajo, debe asignar responsabilidades a sus

colaboradores y determinar que pruebas debe efectuar y que alcance dará a las mismas, así como la oportunidad en que serán aplicadas.

b. Estudio y evaluación del control interno: el contador público independiente debe analizar a la entidad sujeta a ser auditada, esto, es evaluar y estudiar el control interno, con la finalidad de determinar que pruebas debe efectuar y que alcance dará a las mismas, así como, la oportunidad en

que serán aplicadas.

c. Obtención de la evidencia suficiente y competente: el contador público al dictaminar Estados Financieros adquiere una gran responsabilidad con terceros, por lo tanto, su opinión debe estar respaldada por elementos de prueba que serán sustentables, objetivos y de certeza razonables, es decir, estos hechos deben ser comprobables a satisfacción del auditor.

3.1.1.3 Relativas a la información: el objetivo de la auditoria de Estados Financieros es que el contador Público independiente emita su opinión sobre la razonabilidad de los mismos, ya que, se considera que el producto terminado de dicho trabajo es el dictamen.

a. Normas de dictamen e información: el profesional que presta estos servicios debe apegarse a reglas mínimas que garanticen la calidad de su trabajo.

b. Debe aclarar que el contador público independiente: al realizar cualquier trabajo debe expresar con claridad en que estriba su relación y cuál es su responsabilidad con respecto a los estados financieros.

c. Base de opinión sobre estados financieros: con la finalidad de unificar criterios, el IMCP por medio de su comisión de principios de contabilidad, ha recomendado una serie de criterios,

a los que los profesionales se deben de apegar y así, eliminar discrepancias, al procesar y elaborar la información.

d. Consistencia en la aplicación de los principios de contabilidad: para que la información financiera pueda ser comparable con ejercicios anteriores y posteriores, es necesario que se considere el mismo criterio y las mismas bases de aplicación de principios de contabilidad generalmente aceptados, en caso contrario, el auditor debe expresar con toda claridad la naturaleza de los cambios habidos.

e. Suficiencia de las declaraciones informativas: la contabilidad controla las operaciones e informa a través de los Estados financieros que son los documentos sobre los cuales el contador público va a opinar, la información que proporcionan los estados financieros deben ser suficiente, por lo que debe de revelar toda información importante de acuerdo con el principio de "revelación suficiente".

Como normas de auditorias internas para evitar el Fraude tenemos:

- SAS 99
- NEA 5

3.1.1.4. Normas relativas a la planificación de la Auditoria Informática

La función de auditoria estará sujeta a una planificación.

- Planteamientos y solicitudes de la entidad competente.
- Denuncias recibidas.
- A los resultados de la gestión anterior de inspección y fiscalización.
- A la situación administrativa, dimensión, importancia y áreas críticas de los organismos o entidades.

Previa a la ejecución de la auditoria se deberá:

- Programar las actividades idóneas dirigidas a conocer el área del departamento de informática de la entidad o dependencia.

- Establecer dentro de la programación los objetivos, alcance, técnicas, métodos y procedimientos a fin de alcanzar los propósitos fijados**.**

3.1.1.5. Normas relativas a la ejecución de la Auditoria Informática

Para realizar el trabajo de auditoria, el auditor debe estar formalmente acreditado ante el respectivo organismo, entidad o dependencia.

Podrán incorporarse al equipo de auditoria, en calidad de apoyo, los profesionales y/o especialistas cuyos conocimientos y experiencia se consideren necesarios para el trabajo que se desarrolla.

Según el alcance de la auditoria, se deberá evaluar el control interno del organismo, entidad, dependencia o área objeto de la misma para determinar su grado de confiabilidad e identificar los aspectos críticos que requieran examen exhaustivo y como

consecuencia de ello, establecer la naturaleza, oportunidad, métodos, procedimientos y técnicas aplicables en sus fases anteriores.

El auditor debe evaluar el cumplimiento de las leyes, reglamentos y demás normativas aplicables a la entidad y a las operaciones objeto de auditoria. El auditor debe obtener las evidencias suficientes, pertinentes, válidas, competentes y confiables que le permitan tener certeza razonable de que los hechos revelados se encuentran satisfactoriamente comprobados, con el fin de fundamentar razonablemente los juicios, opiniones, conclusiones y recomendaciones que se formulen.

Las evidencias documentales deberán obtenerse en original o en copias debidamente certificadas, en aquellos casos en que se aprecien como pruebas o indicios de hechos generadores de responsabilidad administrativa, civil o penal.

Si en el transcurso de la auditoria se determinan indicios de hechos presuntamente irregulares que pudieran generar

responsabilidad administrativa, civil y/o penal, el auditor deberá identificar el efecto de los mismos sobre las operaciones del organismo o dependencia y comunicar lo pertinente, en forma inmediata, cuando la situación lo amerite, y previa consulta formal con el supervisor respectivo, a las autoridades de la entidad o dependencia donde se desarrolle la auditoria, para que se adopten las medidas correctivas y se dispongan las demás acciones a que haya lugar. Cuando se trate de sociedades de auditores externos o profesionales independientes contratados, éstos deberán, además, comunicar tales hechos al órgano de control correspondiente.

Antes de la presentación formal de los resultados de la auditoria, las observaciones derivadas del análisis efectuado se deberán someter a discusión y consideración de los responsables de las áreas involucradas, con la finalidad de asegurarse de la solidez de las evidencias, la validez de las conclusiones, la pertinencia de las recomendaciones y la objetividad e imparcialidad del ulterior Informe de Auditoria.

El auditor debe organizar un registro completo y detallado en forma de papeles de trabajo, debidamente agrupados y referenciados, los cuales formarán parte del archivo permanente o transitorio, según corresponda. Estos papeles de trabajo pertenecen al área de control que practique directamente la auditoria o al organismo contratante en el caso de las sociedades de auditores o profesionales independientes contratados al efecto.

El archivo permanente contendrá información que se considere de interés y utilidad para auditorias sucesivas; deberá actualizarse en cada nueva auditoria y revisarse periódicamente.

3.1.1.6. Normas relativas al informe de la Auditoria Informática

Contener observaciones o hallazgos, identificando causas y efectos de los mismos, conclusiones y recomendaciones correspondientes,

con señalamiento expreso de que el trabajo ha sido realizado conforme a las Normas Generales de Auditoria.

Ser firmado por el nivel directivo o gerencial, competente para notificar los resultados.

Redactarse de manera objetiva, persuasiva y constructiva y en forma clara, precisa y concreta, insertarse los detalles necesarios que contribuyan a evitar equívocos y ambigüedades.

El informe debe ser presentado oportunamente, a objeto de que la información en él contenida tenga actualidad, utilidad y valor para que las autoridades a quienes corresponda, adopten las medidas inmediatas tendentes a corregir las deficiencias señaladas

En conclusión, las normas internas de auditoria, exigen que el trabajo realizado de auditoria, se establezcan normas mínimas para la ejecución del trabajo, ayuda a emitir una opinión razonable sobre el dictamen de dicho trabajo, evaluando el cumplimiento, leyes, reglamentos, y demás normativas aplicables a la organización a la cual se ha ejecutado una auditoria.

3.2. Norma ISO 17799:2000

La norma internacional ISO 17799:2000 esta basada en la norma BS 7799 (esta última publicada por el Instituto Británico de Normas Técnicas en 1995, y revisada y ampliada en una segunda versión en 1999). Actualmente, es un estándar a seguir dentro de la práctica de Seguridad Informática.

Propone 10 áreas o dominios de control, conteniendo una serie de recomendaciones prácticas “exitosas” de seguridad que toda organización debería poder aplicar independientemente de su tamaño o sector.

Existen programas de certificación de cumplimiento con la norma. Asimismo, la ISO 17799 puede servir de guía para definir Políticas de seguridad en la empresa y/o para implantar un programa de administración de la seguridad.

3.2.1 Estructura de la Norma ISO 17799:2000.-

3.2.1.1 Política de Seguridad de la Información.- Refleja las expectativas y el compromiso de la organización en materia de seguridad a fin de brindar administración, dirección y soporte.

3.2.1.2. Organización de la Seguridad: Relacionada con el diseño de una estructura de administración dentro de la organización que establezca la responsabilidad de los grupos en áreas de seguridad y los procesos para el manejo de respuesta a incidentes.

3.2.1.3. Clasificación y Control de Activos: Relacionado con la necesidad de inventariar y clasificar los activos de la organización en cuanto a su criticidad, grado de exposición al riesgo y nivel de protección necesario, y el nombramiento de responsables por la custodia de los mismos.

3.2.1.4. Seguridad del Personal: Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad, integrándolos de esta forma en la cadena de detección y respuesta a incidentes.

3.2.1.5. Seguridad Física y Ambiental: Responde a la necesidad de proteger las áreas de procesamiento e instalaciones de la organización.

3.2.1.6. Gestión de Comunicaciones y Operaciones:

- Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información
- Minimizar el riesgo de falla de los sistemas
- Proteger la integridad del software y la información
- Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información

- Garantizar la protección de la información en las redes y de la infraestructura de soporte
- Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

3.2.1.7. Control de Accesos

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos y externos.

3.2.1.8. Desarrollo y mantenimiento de Sistemas

En toda labor de tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad

en todas las etapas del proceso de desarrollo e implantación de software.

3.2.1.9. Administración de la Continuidad de los Negocios

La organización debe estar preparada para contrarrestar las interrupciones en las actividades y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.

3.2.1.10. Cumplimiento

Establece la necesidad de que las organizaciones verifiquen si el cumplimiento con la Norma Técnica ISO 17799 concuerda con otros requisitos jurídicos, como la Directiva de la Unión Europea que concierne la Privacidad, la Ley de Responsabilidad y Transferibilidad del Seguro Médico (HIPAA por su sigla en Inglés) y la Ley Gramm-Leach-Billey (GLBA por su sigla en inglés). Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y

consideraciones técnicas que se deben hacer en relación con el proceso de auditoria del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

En conclusión, la ISO 17799 constituye mecanismos de acción, sugiere controles en cualquier organización, aplicados en las situaciones de fraude, actos dolosos y siniestros informáticos que ayudarán a evitar cuantiosas pérdidas, razón por la cual es aplicable al tema de tesis.

3.3. COSO Report

COSO es el marco más extendido y utilizado, que se concentra en el control interno de manera integrada y comprensiva. Adoptado por el sector público y privado en USA, por el Banco Mundial y el BID, y se extiende rápidamente por todo Latino América.

COSO no solo puede ser aplicado a empresas privadas, también públicas con el objetivo de evitar siniestros tanto con empleados de la misma institución como terceras personas.

El nombre de COSO proviene del “Committee of Sponsoring Organizations of the Treadway Commission”, una iniciativa del sector privado esponsorizada por las cinco mayores asociaciones profesionales financieras de los Estados Unidos (Instituto Americano de Contadores Públicos, Instituto de Auditores Internos, Asociación Americana de Contabilidad, Instituto de Contadores de Gestión e Instituto de Ejecutivos Financieros).

3.3.1. Conceptos Fundamentales

Según el informe COSO hay ciertos conceptos fundamentales implícitos en el control interno :

- El control interno es un proceso, es decir un medio para alcanzar un fin y no un fin en sí mismo.
- Lo llevan a cabo las personas que actúan en todos los niveles, no se trata solamente de manuales de organización y procedimientos.
- Sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la conducción.

- Está pensado para facilitar la consecución de objetivos en una o más de las categorías señaladas las que, al mismo tiempo, suelen tener puntos en común.

La auto-evaluación de control interno es un proceso que guía a los gerentes y empleados dentro de la organización a través de un análisis de control interno diseñado para identificar y mejorar las fortalezas del control interno y rectificar las debilidades, lo cual impediría la vinculación de terceros y/o personas ajenas a la información de la empresa.

3.3.2. Componentes.- Los componentes presentes e interrelacionados para alcanzar los objetivos de una organización según el informe COSO son:

- Ambiente de Control: Ética de trabajo, liderazgo, trabajo en equipo, moral.
- Evaluación de Riesgos: Mecanismos para identificar riesgos para alcanzar los objetivos de trabajo, incluyendo los riesgos particulares asociados con el cambio.

- Actividades de Control: Políticas, procedimientos, atribuciones (incluyendo aquellos que pueden ser redundantes o que no agregan valor).
- Información y Comunicación: Horizontal y vertical que es crítica en todos los niveles arriba mencionados
- Monitoreo y Aprendizaje: Realizar cambios basados en ese aprendizaje.

El ambiente de control provee la base para los otros componentes. El mismo abarca factores tales como filosofía y estilo operativo de la gerencia, políticas y prácticas de recursos humanos, la integridad y valores éticos de los empleados, la estructura organizacional, y la atención y dirección del directorio.

La evaluación de riesgo en la empresa consiste en la identificación de los siniestros informáticos de cualquier magnitud, la identificación del riesgo incluye examinar factores externos tales como los desarrollos tecnológicos, la competencia y los cambios económicos, y factores internos tales como calidad del personal, la naturaleza de

las actividades de la entidad, y las características de procesamiento del sistema de información. El análisis de riesgo involucra estimar la significación del riesgo, evaluar la probabilidad de que ocurra y considerar cómo administrarlo.

Las actividades de control consisten en las políticas y procedimientos que aseguran que los empleados lleven a cabo las directivas de la gerencia. Las actividades de control incluyen revisiones del sistema de control, los controles físicos, la segregación de tareas y los controles de los sistemas de información. Los controles sobre los sistemas de información incluyen los controles generales y los controles de las aplicaciones. Controles generales son aquellos que cubren el acceso, el desarrollo de software y sistemas. Controles de las aplicaciones son aquellos que previenen que ingresen errores en el sistema o detectan y corrigen errores presentes en el sistema.

La entidad obtiene información pertinente y la comunica a través de la organización. El sistema de información identifica, captura y reporta información financiera y operativa que es útil para controlar

las actividades de la organización. Dentro de la organización, el personal debe recibir el mensaje que ellos deben comprender sus roles en el sistema de control interno, tomar seriamente sus responsabilidades por el control interno, y, si es necesario, reportar problemas a los altos niveles de gerencia. Fuera de la entidad, los individuos y organizaciones que suministran o reciben bienes o servicios deben recibir el mensaje de que la entidad no tolerará acciones impropias.

La gerencia monitorea el sistema de control revisando el output generado por las actividades regulares de control y realizando evaluaciones especiales. Las actividades regulares de control incluyen comparar los activos físicos con los datos registrados, seminarios de entrenamiento, y exámenes realizados por auditores internos y externos. Las evaluaciones especiales pueden ser de distinto alcance y frecuencia. Las deficiencias encontradas durante las actividades regulares de control son normalmente reportadas al supervisor a cargo; las deficiencias detectadas durante evaluaciones especiales son normalmente comunicadas a los niveles altos de la organización.

3.3.3. Controles.- Los Tipos de actividad de control son (Según COSO):

- Controles generales
- Ambientes de control
- Controles directos

3.3.3.1. Controles generales:

- Planeamiento de requerimientos para las instalaciones
- Controles del departamento de Sistemas

3.3.3.2. Ambientes de control:

- Enfoque hacia el control
- Organización gerencia
- Administración de Seguridad de las instalaciones

3.3.3.3. Controles directos:

- Controles de las instalaciones
- Controles de procesamiento y funciones de procesamiento computarizadas
- Controles para salvaguardar equipos

El informe COSO brinda una guía para evaluar cada uno de estos factores. Por ejemplo, la filosofía gerencial y el estilo operativo pueden ser evaluados examinando la naturaleza de los siniestros de la empresa, que acepta la gerencia, la frecuencia de su interacción con los subordinados, y su actitud hacia los informes financieros.

En conclusión, Coso es una norma que ayuda a la empresa a contar con controles adecuados, para la minimización de siniestros dentro de la empresa, por lo que su enfoque esta relacionado a la tesis y ayudaría a los directivos de las empresas a tomar medidas correctivas adecuadas, examinando los factores externos e internos implícitos en cualquier área de riesgo de la empresa.

CAPÍTULO IV

4. CASO PRÁCTICO

4.1 Información Preliminar

En el presente capitulo se desarrollará el caso práctico,con las respectivas metodologías, herramientas y técnicas a aplicar.

4.1.1 Introducción

Por razones de seguridad se han omitido el nombre real de la institución, los nombres de los empleados implicados, personas externas a la institución que se vieron involucrada en el suceso y los denunciantes, por ello el nombre ficticio que le daremos a la empresa será ETASUM.

ETASUM es una empresa ubicada en el centro de la ciudad, creada en Abril de 1998, luego de una fusión de dos compañías que se dedicaban al estudio del mercado en el área cualitativa y cuantitativa.

A lo largo de estos años, ha participado indirectamente en la toma de decisiones de importantes empresas multinacionales y nacionales dedicadas a diversas áreas dentro de los sectores productivo, comercial y de servicios, a través del servicio estadístico que brinda.

Cuenta con un equipo multidisciplinario de profesionales que incluye dos psicólogas, un ingeniero comercial, un economista, dos programadores, 5 a 7 digitadores y un número variado de consultores en otras áreas, que se unen al equipo cuando la investigación así lo requiere.

Adicional a su trabajo dentro del país, trabajan como "Preffered Supplier" de RESEARCH INTERNACIONAL, empresa multinacional de investigación de mercados cuya matriz se encuentra en Londres

y que los mantiene en contacto con sus 56 oficinas en 33 países alrededor del mundo.

Actualmente en el proceso de integración de los países del Pacto Andino al comercio sub-regional, y con las nuevas oportunidades de inversión entre países vecinos, se encuentra trabajando en buscar nuevas alternativas de mercado y desarrollo para empresas nacionales y extranjeras.

Están convencidos de que la mayor ventaja está en la calidad profesional y humana de quienes conforman ETASUM.

Los objetivos básicos de la empresa son:

- Ser líderes en el estudio competitivo del mercado a través de encuestas realizadas por personas especializadas y conocedoras del mercado.
- Aplicar técnicas de investigación de mercado para poder brindar una cobertura estratégica de los productos a los clientes

La empresa se dedica además de la ejecución de estadísticas, a la venta de software, lo que la convierte en una empresa comercial y de servicios.

Cuenta con una estructura orgánica media, (ver Anexo 2), en el que se describe los cuatro departamentos con los que son:

- De mercado
- Sistemas
- Análisis y procesamiento de datos
- Contabilidad

El Departamento de Sistemas ha desarrollado un software denominado DATALOW y actualmente están desarrollando otros sistemas acorde a las necesidades de cada departamento, esta estructurado según Anexo 3. Este departamento se encarga de dar soporte técnico a los demás departamentos.

El Departamento de Análisis y Procesamiento de Datos es el encargado de realizar, revisar e informar los resultados de las encuestas que son reportadas a la Gerencia.

El departamento de Mercado es importante, ya que la empresa esta dedicada a la investigación de Mercado y es éste el departamento que da la información necesaria, para ver el campo en que se van a realizar las encuestas

El Departamento de Contabilidad, lleva los registros contables de la empresa.

4.1.2. Justificativos del trabajo

ETASUM, se ha visto afectada por un siniestro informático originado en el Departamento de Análisis y Procesamiento de Datos es, tal cual exponen sus dueños, quienes alarmados por la situación que se ha presentado, solicitan se efectúe un estudio e investigación exhaustivo hasta lograr identificar a los responsables del suceso, pues consideran que los resultados de las encuestas han sido destruidos. Se sospecha que esta acción ha sido efectuada por uno de los colaboradores del departamento, cuya identidad se desconoce.

4.1.3 Objetivos

Los objetivos del presente trabajo de Auditoría Forense son:

- Aplicar metodologías, herramientas y técnicas que permitan identificar las causas del siniestro informático de la empresa.
- Conocer los mecanismos que usaron los empleados para la manipulación de los datos.
- Establecer controles informáticos que eviten siniestros informáticos dentro de la empresa y aseguren una mayor confidencialidad de la información.
- Identificar al o los empleado (s) que ejecutaron el siniestro.

Dentro de la escala de los objetivos, que son de especial análisis forense, se ha considerado para nuestro estudio, aquellos considerados de mayor relevancia en la Auditoria forense, por parte de la empresa. Entre éstos tenemos los siguientes:

- Aplicar metodologías, herramientas y técnicas que permitan identificar las causas del siniestro informático empresa.

De acuerdo a las causas que se identifican en un siniestro, se aplicará las herramientas y técnicas más eficientes para lograr identificar al responsable del siniestro, siguiendo las pistas dejadas por él en los equipos de computación dentro del Departamento de análisis y Procesamiento De Datos.

Las herramientas y técnicas permiten identificar a los responsables y a la vez pueden ser usadas para en el futuro monitorear otros sucesos

- Establecer controles informáticos que eviten siniestros informáticos dentro de la empresa y aseguren una mayor confidencialidad de la información.

Al establecer controles informáticos que eviten siniestros informáticos, se deben realizar los manuales correspondientes a cada uno, mediante las pruebas realizadas a éstos. Dichas pruebas deberán ser realizadas cuantas veces sean necesarias para el buen funcionamiento de los controles, evitando los siniestros informáticos dentro del departamento.

El objetivo de los controles es, que proporcionen oportuna y efectiva información al momento de presentarse un posible sabotaje de información.

Se entiende por confidencialidad el salvaguardo de la información con caracteres reservados y exclusivos a los funcionarios autorizados.

La confidencialidad de la información permite el acceso de datos e información sólo a personal autorizado de manera que las transacciones realizadas por un usuario queden registradas como responsabilidad absoluta de la persona que está autorizada a efectuar alguna transacción

- Conocer los mecanismos que usaron los empleados para la manipulación de los datos.

Uno de los objetivos principales de este trabajo, es conocer el/los mecanismo(s) que usaron los colaboradores de la empresa. Teniendo en cuenta, con que recursos el empleado contaba para manipular los datos del departamento.

Además con el conocimiento de los mecanismos, nos ayudará a evitar futuros siniestros dentro del departamento asignado o total de la empresa.

- Identificar al o los empleado(s).

Un objetivo principal dentro de una auditoria forense es identificar al o los empleados que estuvieron involucrados en el hecho, ya que ellos son la base fundamental para cualquier compañía para el desarrollo de la misma.

En el caso de la empresa, se puede observar que no hay un control adecuado al ingreso y salida de cada empleado, en la utilización de la computadora para su trabajo. Ya que el único registro que tienen es una hoja en cuyo contenido es la hora, fecha, nombre del empleado y rubrica.

4.1.4 Alcance

El presente trabajo delimita su alcance exclusivamente al caso analizado en la empresa comercial seleccionada, por la magnitud del

problema informático suscitado. La solución a presentar, no será aplicable a todos los siniestros. Así mismo la metodología, herramientas y técnicas se ajustan a este caso.

Así mismo el departamento en el que se presentó el siniestro informático, es el departamento de Análisis y Procesamiento de datos, por lo que nuestro análisis se circunscribe a este único entorno.

4.2 Descripción del entorno informático (Anexo 4)

El entorno informático es el siguiente:

4.2.1 Arquitectura informática

4.2.1.1.- Entorno de Red

El Departamento de Análisis y Procesamiento de Datos está integrado a la red, pero el sistema DATALOW opera en cada computador en modo stand-alone.

4.2.1.2.- Equipos Disponibles

La empresa cuenta con 28 computadoras, éstas están distribuidas en los cuatro departamentos. Los departamentos que cuenta esta empresa son: Departamento de Mercado cuenta con 7 computadoras, Departamento de análisis y procesamiento de datos cuenta con 11computadoras y el Departamento de Sistema con 5 computadoras y el Departamento Contable cuenta 5 computadoras. Ver tabla I.

TABLA I

EQUIPOS DISPONIBLES EN LA LA EMPRESA

		IMPRESORAS		Scanne	Tef.	Palm
DPTO	**Comp**	**Mat.**	**Iny.**			
Mercado*	7	2	2	2	3	1
Análisis y Procesamiento Datos*	11	5	2	2	4	1
Sistemas*	5	2		1	3	1
Contabilidad	5	2	1	0	4	1
TOTAL	**28**	**11**	**5**	**5**	**14**	**4**

*existe 1 laptop

***laptop conectada a satnet

Los Equipos disponibles en el departamento de Análisis y Procesamiento de Datos, se distribuyen de acuerdo a las personas que laboran en él, así: 1 gerente, 1 analistas, 5 -7 encuestadores-digitadores, 1 secretaria y 1 supervisor. Ver Tabla II.

TABLA II

Equipos del Dpto. Análisis y Procesamiento de datos.

Analisis y Procesamiento de Datos	COMP.	Impresoras		Scanner	Telf.	Palm
		Mat.	Iny.			
Gerente*	1	0	1	1	1	1
Analistas	2	1	0	1	0	0
Encuestadores**	6	3	0	0	1	0
Supervisor	1	0	0	0	1	0
Secretaria	1	1	0	0	1	0
TOTAL	**11**	**5**	**1**	**2**	**4**	**1**

*existe 1 laptop

**existen 6-8 encuestadores

***laptop conectada a satnet

4.2.1.3.- Sistema Operativo

El Sistema Operativo que utilizan es Windows XP.

4.2.1.4 Software de Sistemas y Utilitarios

4.2.1.4.1.- Lenguaje de Programación:

E lenguaje de programación que usan es Visual Basic

4. 2.1.4.2.- Sistemas de Aplicación:

En la empresa ha desarrollado los siguientes sistemas:

- DATALOW
- Stor audit. (desarrollándose actualmente)

4.2.1.4.3. Utilitarios:

Con respecto a utilitarios la empresa utiliza el paquete Office XP.

4.2 Evaluación forense

A continuación la metodología, anteriormente mencionada en el capítulo dos, para poder hacerla evaluación forense:

4.2.1. Definición y reconocimiento del problema

Los digitadores de la empresa ETASUM, al realizar los ingresos propios de los cuestionarios respectivos para iniciar el trabajo diario y tratar de entregar la información detallada y a tiempo, se encuentra, que algunos datos han sido alterados por los empleados mismos del departamento o podemos pensar que sean terceros (intrusos) ya que este departamento no cuenta con clave personal al ingreso del sistema.

Avisado el Jefe del Departamento de Análisis y Procesamiento de Datos comprueban que algunos datos en la información han sido alterados.

Recuerdan que en un mes anterior estuvieron colaboradores del departamento en la digitación de ingresos de datos en el Departamento de Análisis y Procesamiento de Datos, debido a la gran cantidad de trabajo que había en este departamento debido a la digitación de la información.

Por lo demás cabe destacar que la empresa tiene la política, de que si el material es entregado a tiempo y la información es eficiente y efectiva el grupo de digitadores por empresa gana un porcentaje de ganancia.

Se da la circunstancia de que la empresa no acostumbra a guardar las hojas de vidas de las personas que trabajan por tarea asignada por lo que el perjuicio es bastante importante, ya que la identificación de la persona es casi nula. Solo guarda las hojas de vida cuyos empleados tienen contrato laboral indefinido.

Los pasos para definir bien el problema en el cual identificaremos, la técnica y herramienta a aplicar:

Herramienta: proyect, me ayudará hacer un cronograma para definir el problema. Ver Tabla III.

Técnicas: cuestionarios de visitas previas (Ver anexo 5), intento de factores de riesgo de fraude (Ver anexo 6) e identificación del problema de la empresa (Ver anexo 7), posibles causas para cometer un siniestro dentro de la empresa (ver anexo 8) y checklist (Ver anexo 9)

TABLA III

CRONOGRAMA DE DEFINICIÓN DEL PROBLEMA

Cronograma de Definición del Problema															
ETAPAS	MES	Marzo				Abril				Mayo					
	SEMANA	1ª	2ª	3ª	4ª	1ª	2ª	3ª	4ª	1ª	2ª	3ª	4ª		
Identificar el equipo vulnerado															
Elaborar un checklist															
Cuestionarios al gerente para identificar posibles fraudes															
Cuestionario de Visita															

Previa (gerente y empleados)				

4.2.2. Recopilación de evidencias de fraude

Para la recopilación de evidencia tenemos las siguientes alegaciones y consideraciones:

- La empresa ETASUM S. A , tiene un sistema informático configurado de la siguiente forma:
- El Departamento de Análisis y Procesamiento de Datos está integrado a la red, pero el sistema DATALOW opera en cada computador en modo stand-alone**.**
- DATALOW, es un sistema para el análisis de variables, que ayuda al ingreso de datos de las encuestas realizadas.

Los programas correspondientes al trabajo que realiza la empresa la tiene bases con extensión DTL, se encuentran ubicado en un directorio especial denominada PROYECTOS. En este directorio, además de dichos programas se encuentran otros programas necesarios para el funcionamiento de la aplicación.

Después de las alegaciones y consideraciones, tomamos fotografías a las encuestas posibles vulneradas, al computador vulnerado y su respectivo CPU.

Para seguir encontrando evidencia sigo indagando a las personas involucradas por medio de entrevistas, y observaciones al departamento que ha sido saboteado. Y es ahí, cuando el supervisor de Sistemas me da la bitácora como fuente de entrada y salida del personal y la planificación de cada encuestador-digitador.

De acuerdo con la directiva de la Empresa y a las debilidades encontradas en el Departamento de Análisis y Procesamiento de Datos, se han aplicado herramientas, las cuales ayudan a la integridad y confidenciabilidad de la información.

Las técnicas que vamos a aplicar para la recolección de la información son:

Técnicas.- entrevistas (Ver anexo 10), fotografías (Ver anexo 11)

4.2.3. Evaluación de las evidencias recolectadas o análisis

De acuerdo a investigaciones realizadas anteriormente, se puede deducir que el sistema había sido manipulado por los colaboradores de la empresa, dando una información final maquillada al Gerente del departamento, ya que el sistema que utiliza la empresa es de fácil manipulación, por lo que debe de hacerse una copia de los discos duros y de los archivo DTL, los cuales son los que guardan la información de las encuestas de todas las computadoras que han sido utilizadas para el ingreso de las variables.

De acuerdo al análisis forense realizado a continuación se detallarán las fallas que se encontraron en el departamento y cuales pudieran provocar fraudes por los mismos empleados del Departamento.

Las debilidades encontradas dentro del Departamento de Análisis y Procesamiento de Datos fueron:

- Falta de clave de acceso personal en el sistema para los encuestadores - digitadores.

- Manipulación de Datos.

- El jefe del departamento no verifica constantemente el material ingresado, lo cual afecta al informe final.

- Falta de organización por el uso de computadoras en el Departamento (cada encuestador-digitador puede utilizar cualquier computadora, lo que produce que la identificación del sospechoso sea más difícil de identificar.)

- No hay un control adecuado de las entradas y salidas de los empleados.

Las oportunidades encontradas dentro del Departamento de Análisis y Procesamiento de Datos fueron:

- El jefe y/o encargado de revisar los resultados de la información, deberá garantizarla confiabilidad mediante la revisión constante en el ingreso de la información al sistema.

- La programación del sistema debe ser corregido para de esa forma poder garantizar la confiabilidad de la información y por consiguiente los resultados obtenidos.

- Implementación de una red para así agilitar el trabajo de los digitadores.

- Diálogo entre el o los digitador (es) con el programador del sistema, para comunicar las necesidades del Departamento.

- Rediseñar el sistema implementando el menú de ayuda, y el menú de seguridad, para facilitar el arreglo de dificultades y aplicar controles en el sistema.

Conociendo las debilidades, que se han encontrado en el departamento, comenzamos a evaluar. Entre ellos tenemos: la falta de clave de acceso al personal, falta de seguridades físicas y lógicas.

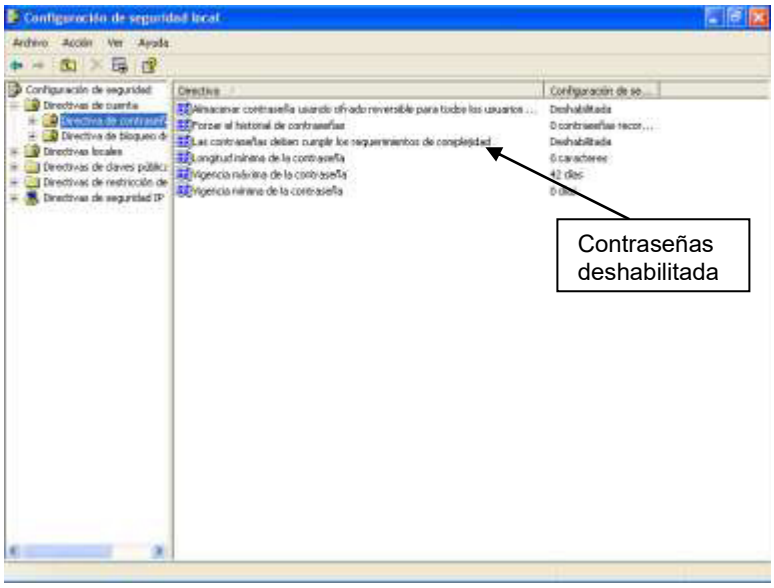


FIGURA 4.1. Falta de claves de acceso

En esta gráfica podemos observar, que en realidad las claves de acceso están deshabilitadas, es decir que el personal no cuentan con claves que identifique el ingreso al sistema.

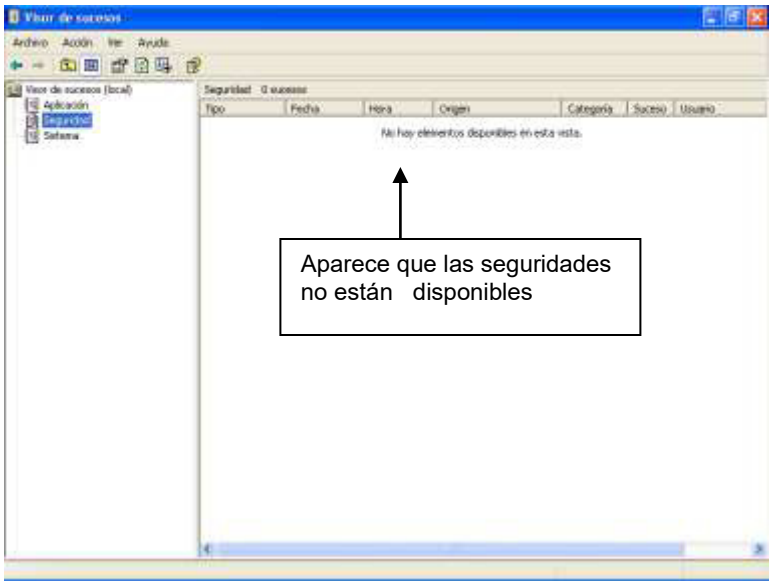


FIGURA 4.2 Falta de seguridades lógicas en las computadoras

En la gráfica 2, se muestra la falta de seguridad lógica que existe en el departamento. Podemos darnos cuenta que falta muchas seguridades y para que la información sea veraz, y que podamos obtener una información más integra y confiable.

Después de tener la evidencia de las carencias de la empresa, se inicia la evaluación, pedimos al Dpto. de Sistemas, alguna identificación y/o archivo que nos dé una pista de cómo empezar la búsqueda de la persona involucrada. A consideración de la Gerencia, para poder encontrar al culpable, el supervisor del Dpto.

afectado y el Dpto. de sistemas me entregan una bitácora de entrada y salida de los empleados (tiempo de ejecución de encuestas), la planificación del supervisor del Dpto. afectado, y el Dpto. de Sistemas me da un archivo en el cual está el ingreso de cada encuesta, con sus respectivos ingresos, modificaciones y eliminaciones.

Después de indagar y ver que no hay resultados que me ayuden a encontrar al posible culpable, comienzo a verificar los datos encontrados.

Siguiendo pistas comienzo con la evaluación del comando REGEDIT, el cual se encuentra en la siguiente dirección, detallado en el gráfico correspondiente

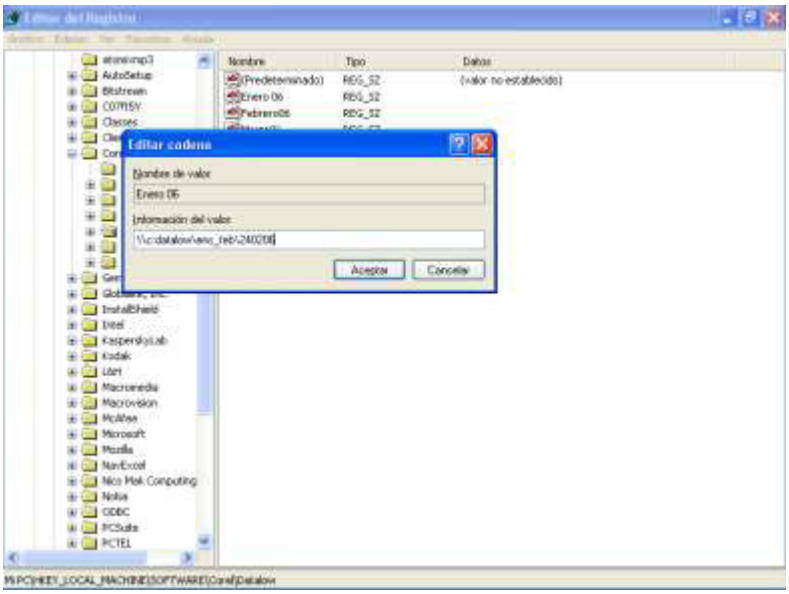


FIGURA 4.3. Comando REGEDIT

Como muestra el gráfico 3, en esta dirección del computador, que se encuentra el comando REGEDIT, encuentro el ingreso de cada encuesta, el cual tiene titulo de día ingresado, número de la encuesta, tiempo de ingreso y los campos ingresados.

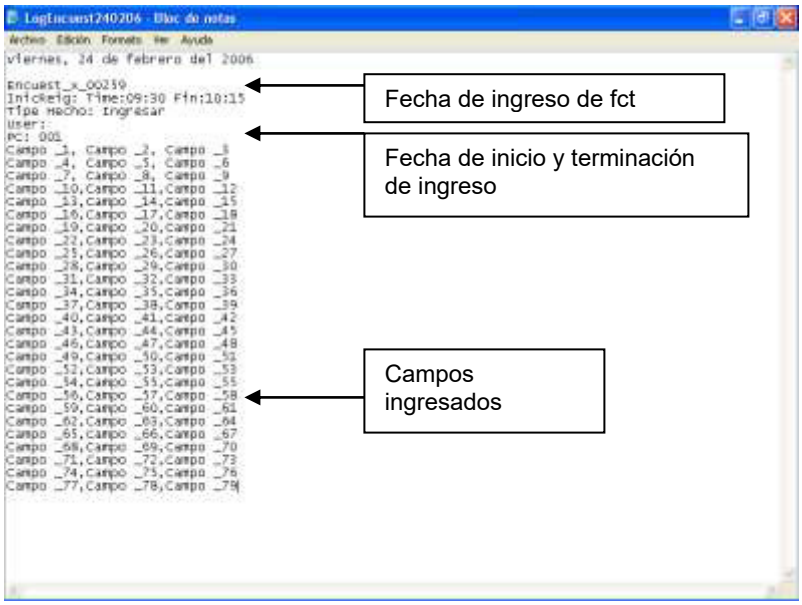


FIGURA 4.4 Ingreso de encuesta

En este gráfico, se puede observar que el ingreso de la información de las encuestas, fue realizado el 24 de febrero del presente año, la encuesta involucrada es la 259 y se la ingresó desde las 09:30 hasta las 10:15, ingresando 79 campos.

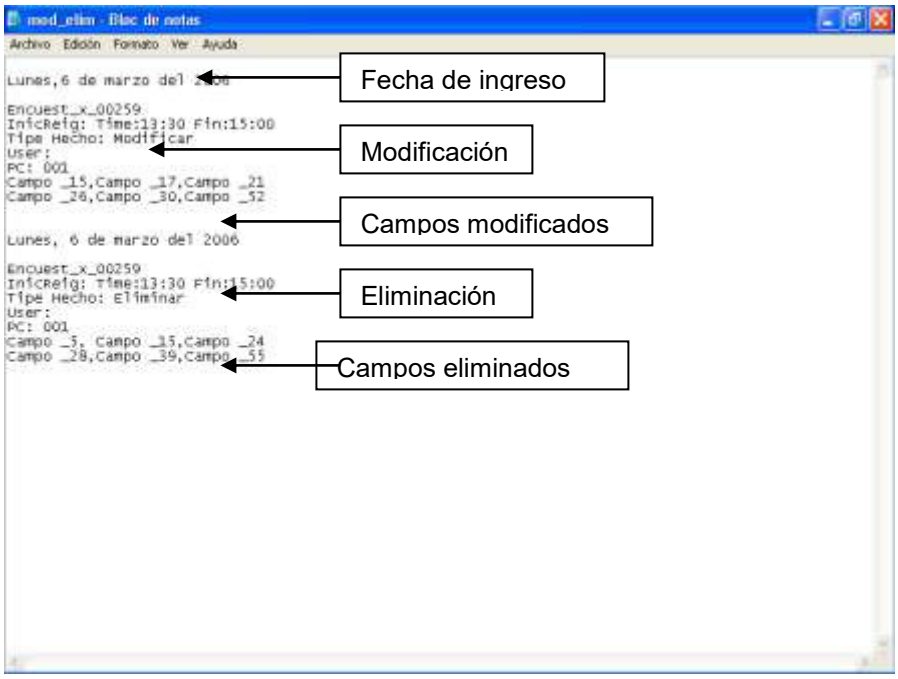
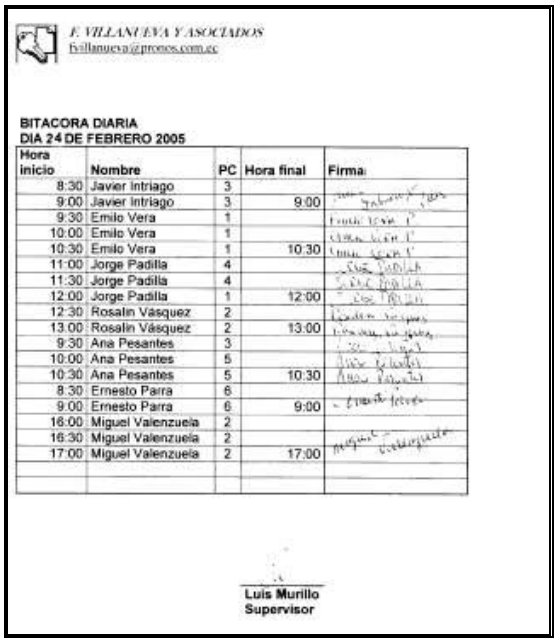


FIGURA 4 .5. Modificación y Eliminación de información

En la figura 5, ayuda a visualizar que el día 6 de marzo las alteraciones tanto modificaciones como eliminaciones, se hicieron en la encuesta 259. Con estos gráficos, podemos constatar de la alteración que se hizo en dicha encuesta, pero realmente no podemos identificar al posible culpable.

Entonces, el paso siguiente es examinar la bitácora y la planificación del supervisor, observando, cuales de los empleados se encontraban en la empresa esos días.



F. VILLANUEVA Y ASOCIADOS
fvillanueva@pronos.com.ec

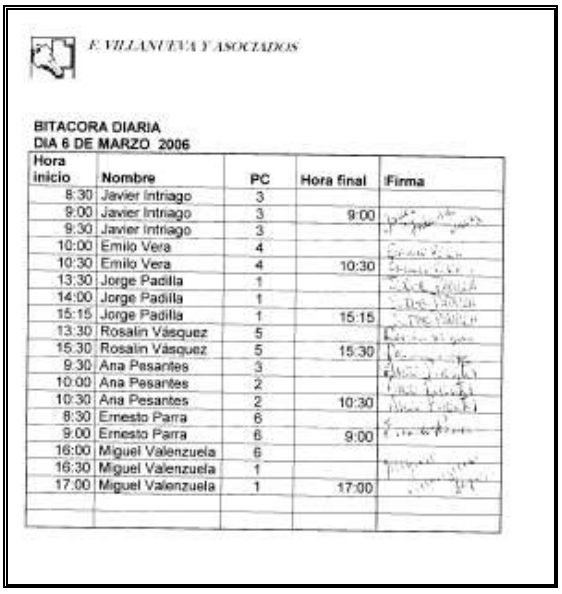
BITACORA DIARIA
DIA 24 DE FEBRERO 2005

Hora inicio	Nombre	PC	Hora final	Firma
8:30	Javier Intriago	3		
9:00	Javier Intriago	3	9:00	
9:30	Emilo Vera	1		
10:00	Emilo Vera	1		
10:30	Emilo Vera	1	10:30	
11:00	Jorge Padilla	4		
11:30	Jorge Padilla	4		
12:00	Jorge Padilla	1	12:00	
12:30	Rosalin Vásquez	2		
13:00	Rosalin Vásquez	2	13:00	
9:30	Ana Pesantes	3		
10:00	Ana Pesantes	5		
10:30	Ana Pesantes	5	10:30	
8:30	Ernesto Parra	6		
9:00	Ernesto Parra	6	9:00	
16:00	Miguel Valenzuela	2		
16:30	Miguel Valenzuela	2		
17:00	Miguel Valenzuela	2	17:00	

Luis Murillo
Supervisor

FIGURA 4.6. Bitácora 24 Febrero

En la figura 6 podemos observar, quien fue el responsable del ingreso de los datos, el PC que utilizó y el tiempo estimado.



F. VILLANUEVA Y ASOCIADOS

BITACORA DIARIA
DIA 6 DE MARZO 2006

Hora inicio	Nombre	PC	Hora final	Firma
8:30	Javier Intriago	3		
9:00	Javier Intriago	3	9:00	
9:30	Javier Intriago	3		
10:00	Emilo Vera	4		
10:30	Emilo Vera	4	10:30	
13:30	Jorge Padilla	1		
14:00	Jorge Padilla	1		
15:15	Jorge Padilla	1	15:15	
13:30	Rosalin Vásquez	5		
15:30	Rosalin Vásquez	5	15:30	
9:30	Ana Pesantes	3		
10:00	Ana Pesantes	2		
10:30	Ana Pesantes	2	10:30	
8:30	Ernesto Parra	6		
9:00	Ernesto Parra	6	9:00	
16:00	Miguel Valenzuela	6		
16:30	Miguel Valenzuela	1		
17:00	Miguel Valenzuela	1	17:00	

FIGURA 4.7. Bitácora 6 marzo

En esta figura podemos observar que el día 6 de marzo hubo modificaciones de la información ya guardada, ya que en la bitácora, está especificando el día, hora y quien está utilizando el PC.

F. VILLANUEVA Y ASOCIADOS

PLANIFICACION SEMANA 21-25 FEBRERO DEL 2006

Supervisor : Luis Murillo No.encuestas 250-400

#	Horario	Sector	Lugar		Encuestador
1	08:30-11:30	Sur	Mall del Sur	Megamaxi	Javier Intriago
2	10:00-13:00	Sur	Rio Centro Sur	Hipermarket	Luis Rendón
3	11:00-12:00	Sur	Rio Centro Sur	Patios Comida	Emilo Vera
4	14:00-17:00	Centro	Unicentro	Puerta 1	Jorge Padilla
5	09:30-12:30	Centro	Unicentro	Puerta 2	Rosalin Vásquez
6	13:30-16:30	Norte	Policentro	Megamaxi	Ana Pesantes
7	09:00-12:00	Norte	Alborada puerta 1	Mi comisariato	Ernesto Parra
8	12:30-15:30	Norte	Alborada puerta 2	Mi comisariato	Miguel Valenzuela

Luis Murillo
Supervisor

Revisado y aprobado

FIGURA 4.8. Planificación del Supervisor (día 24/02/06)

En esta figura, se puede observar, quien realmente esta en campo, y quien realmente se quedo en la oficina ingresando la información.

F. VILLANUEVA Y ASOCIADOS

PLANIFICACION SEMANA 06-10 MARZO DEL 2006

Supervisor : Luis Murillo — No.encuestas 603-720

#	Horario	Sector	Lugar		Encuestador
1	14:00-17:00	Sur	H.del Niño	Puerta 1	Javier Intriago
2	10:00-13:00	Sur	H.del Niño	Puerta 2	Luis Rendon
3	11:00-12:00	Norte	H.Solca (niños)	Puerta 1	Emilo Vera
4	08:30-11:30	Norte	H.Solca (niños)	Puerta 2	Jorge Padilla
5	09:30-12:30	Sur	H. IESS	Puerta 1	Rosalin Vasquez
6	13:30-16:30	Sur	H. IESS	Puerta 2	Ana Pesantes
7	09:00-12:00	Norte	H.Enrique Gilbert	Puerta 1	Ernesto Parra
8	12:30-15:30	Norte	H.Enrique Gilbert	Mi comisariato	Miguel Valenzuela

Luis Murillo
Supervisor

Revisado y aprobado

FIGURA 4.9. Planificación del Supervisor (día 06/03/06)

En esta figura, ya tenemos tres evidencias, de quien realmente fue el que adulteró la información. Constatando con la persona encargada, encuentro que el culpable ya no labora en la institución.

4.2.4. Elaboración del informe final con los hallazgos.

Al término del análisis, podemos determinar que quien hizo las modificaciones y eliminaciones fue quien estuvo en el horario estipulado entre 13:00 – 15:00 , y en el PC vulnerado fue el 1.

Cabe destaca que la máquina vulnerada fue el PC 1 y la encuesta 259 entonces relacionamos todas las evidencias (bitácora, planificación del supervisor, comando REGEDIT) que tenemos con ese PC y dicha encuesta, tomamos fotos al equipo y elabore el informe.

Por lo que podemos determinar, que el digitador Jorge Padilla (nombre ficticio), es el culpable de la adulteración de la información, con las evidencias presentadas.

Es todo cuanto puedo decir, en honor a la verdad. (Ver anexo 12) donde se incluyen conclusiones y recomendaciones.

CONCLUSIONES

DEL CASO PRÁCTICO

1. El presente trabajo permitió detectar algunas novedades que se encuentran registradas en el informe a manera de hallazgos, que si bien es cierto no están relacionadas directamente con el caso, influyen en la organización y son vulnerabilidades dignas de tomar en cuenta en toda organización mediana o pequeña. Estos hallazgos fueron:
    - Ausencia de seguridades física
    - Inexistencia de Planes de Contingencia
    - Inexistencia de seguros para la protección de los Equipos
    - Carencia de seguridades en la empresa
    - Inexistencia de documentación y de seguridad de la Información
    - Falta de rutinas de validación (Ingreso incorrecto de variables, Ingreso de códigos no permitidos)
    - Falta de control y Seguridades lógicas como Claves de Acceso (Manipulación de Datos)
    - Falta de organización en el Departamento

2. Este trabajo así como es un apoyo a la empresa, también es una guía para quienes en un futuro desarrollen actividades sobre la Auditoría Forense en un determinado siniestro informático.

3. El desarrollo de esta tesis, me ha permitido adquirir una mejor y mayor percepción de los problemas típicos por la falta de herramientas y técnicas para evitar los siniestros dentro de las empresas.

4. Este trabajo tiene como una de sus metas primordiales el orientar a las generaciones futuras, sobre los aspectos importantes que se deben considerar en la Auditoría Forense de las empresas del sector informático.

5. Los profesionales de hoy en día, tenemos los conocimientos y hemos desarrollado habilidades que nos permiten encontrar evidencia suficiente en una Auditoría forense, empleado herramientas y técnicas básicas de Auditoría.

6. Este trabajo pretende contribuir con la difusión y uso de la Auditoría Forense Informática en nuestro país y su aplicación en distintos tipos y tamaños de empresas.

DE LA AUDITORÍA FORENSE

7. La Auditoría Forense en los siniestros informáticos es importante porque permite encontrar las evidencias necesarias y suficientes de un fraude o siniestro, así mismo actúa como un enfoque correctivo y preventivo pues permite detectar vulnerabilidades adicionales que pueden ser tratadas mediante la aplicación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que pudiesen ocurrir.

8. Las metodologías, herramientas y técnicas que se aplican en Auditoría Forense Informática son comunes a otros tipos de Auditoría, pero así mismo utiliza herramientas particulares en su enfoque que ayudan a dilucidar hechos ocurridos.

9. Las empresas comerciales medianas o pequeñas se enfrentan hoy a una dura batalla, pues la proliferación de fraudes, robos y siniestros provocados por empleados de la organización es muy frecuente en nuestro medio dada la grave crisis que afecta a nuestro país y es en la Auditoría Forense Informática que los Directivos pueden encontrar una alternativa para llegar a dilucidar hechos pasados o presentes que les ayude a tomar una adecuada decisión.

10. La Auditoría Forense, en esta tesis, tuvo entre sus alcances incluir recomendaciones a la Gerencia, lo cual nos permite establecer los principales controles y seguridades que deben implementarse en la empresa.

11. Esta tesis ayuda a conocer la importancia de la Auditoría forense, especialmente a los estudiantes. Debido a que la ciencia forense integra conceptos de temas de auditoría, contabilidad, informática, así como aspectos legales que se enmarcan en el perfil profesional integral

12. Si bien en estos últimos tiempos en nuestro país se han dictado unas pocas conferencias, respecto al tema, poco o nada se conoce de la “Auditoría Forense Informática”.

13. A mi criterio muy personal, la auditoría informática forense es una disciplina que debe desarrollarse en forma integral y considero que debe delinearse en forma concreta y por consenso, el entorno completo de operación con metodologías comunes, procedimientos, herramientas y técnicas.

14. Se debe fortalecer la seguridad en el área de sistemas contando como herramienta de monitoreo continuo o de resolución de incidentes a la auditoría informática forense.

15. La auditoría informática forense es un puente para comprender las pruebas judiciales y su impacto en el mundo informático.

16. La práctica de la auditoría informática forense difiere de las demás disciplinas forenses en que la primera las metodologías y herramientas no solamente cambian con el tiempo sino también debido a la evolución en hardware y software, por lo que subyacen naturalmente en los sistemas informáticos bajo investigación. Para quien se embarca en una carrera en este campo es importante destacar el valor de estar preparado para el cambio.

17. Para todo lo relacionado con crímenes de alta tecnología y mala conducta, nunca es tarde para comenzar a prepararse de cara a los desafíos que se presentan. Uno de esos desafíos es incursionar en la Auditoría Forense Informática.

18. Las herramientas para realizar Auditoría Informática Forense se presentan en varias y diferentes formas y tamaños, desde grandes, costosas, paquetes con multi-características comerciales hasta utilitarios gratuitos para tareas sencillas. Lo importante es saber elegir la herramienta para el caso específico y no dejar que la herramienta elegida

por sí sola de un diagnóstico sino que el analista sepa interpretar adecuadamente los resultados.

19. La clave del éxito en el uso de software forense es, donde sea posible, identificar cuáles son las herramientas más apropiadas para cada caso y ganar familiaridad con las mismas antes que la investigación lo requiera.

RECOMENDACIONES

1. La mejor forma de evitar situaciones engorrosas de fraudes, robo y siniestros informáticos es estableciendo controles, pero por sobre todo, promover una cultura de seguridad en las organizaciones

2. Se deben desarrollar prácticas y procedimientos de programación y control que busquen disminuir los problemas de seguridad en los productos de software y hardware.

3. Previsibilidad, debido cuidado y diligencia son palabras claves de control en el entrono empresarial.

4. Definir prácticas y políticas de seguridad informática, como pruebas preconstituidas para la organización.

5. Una de las normas legales es garantizar la confiabilidad de la información y por consiguiente los resultados obtenidos, debe ser una meta de los Jefes departamentales.

6. Adecuar a la empresa con seguridades físicas y lógicas básicas

7. Revisiones periódicas constituyen una buena práctica de control interno y deben aplicarse en las organizaciones incluso para el entorno informático.

8. Capacitar continuamente al personal de la empresa para fomentar y mejorar la cultura organizativa con el propósito de establecer objetivos de control para que a su vez esto contribuya a la obtención y cumplimiento de metas y objetivos institucionales.

9. Fomentar al personal de la organización la importancia de poseer y trabajar con información efectiva, oportuna y verdadera para adecuadas y acertadas toma de decisiones.

10. Los cambios tecnológicos y procesos globalizados demandan mayor rapidez, eficacia, efectividad y un mayor control, por lo cual los profesores y estudiantes vinculados a la investigación, así como los directivos de las instituciones educativas deben profundizar en estos temas de actualidad.

11. Difundir el uso de las herramientas, técnicas y mecanismos necesarios para evitar los posibles fraudes, robos y siniestros que se pueden cometer dentro de un sistema de información.

12. Concientizar sobre las responsabilidades jurídicas de estas situaciones a los colaboradores de la empresa.

13. Implantando Mecanismos de Seguridad Informática
    a. Firmas digitales
    b. Certificados digitales
    c. Algoritmos de encripción simétrica y asimétrica
    d. Intrusion detection systems, Control de intregridad de archivos
    e. Logs de auditoría

14. Establecer enfoques de Seguridad Informática de acuerdo a los aspectos legales del país incluyendo:
    a. Principios
        i. Confidencialidad
        ii. Integridad
        iii. Disponibilidad
    b. Servicios
        i. Autenticación
        ii. Autorización
        iii. No-repudiación
        iv. Auditabilidad

15. Ante los continuos cambios tecnológicos se recomienda que el analista esté constantemente actualizándose en el uso de herramientas y técnicas hasta ganar la experiencia requerida para resolver casos con mayor facilidad.

ANEXOS

ANEXO 1

PADRES DE LA AUDITORIA FORENSE

WIETSE VENEMA

Wietse Venema es conocido por el software que ha desarrollado, como el TCP Wrapper y el sistema de correo POSTFIX. Es coautor del escaner de red SATAN y del conjunto de herramientas para análisis forense denominado Coroner's Toolkit, y escribió un libro sobre análisis forense en computadoras junto a Dan Farmer.

Wietse recibió premios del gremio de los administradores de sistemas (SAGE) y del Grupo de usuarios UNIX de Holanda (NLUUG). Se desenvolvió durante dos años como director del Foro Internacional de grupos de Seguridad y Respuesta a Incidentes (FIRST).

Wietse tiene un Doctorado en Física y es investigador del Centro de Investigación T.J.Watson de IBM en los Estados Unidos de América

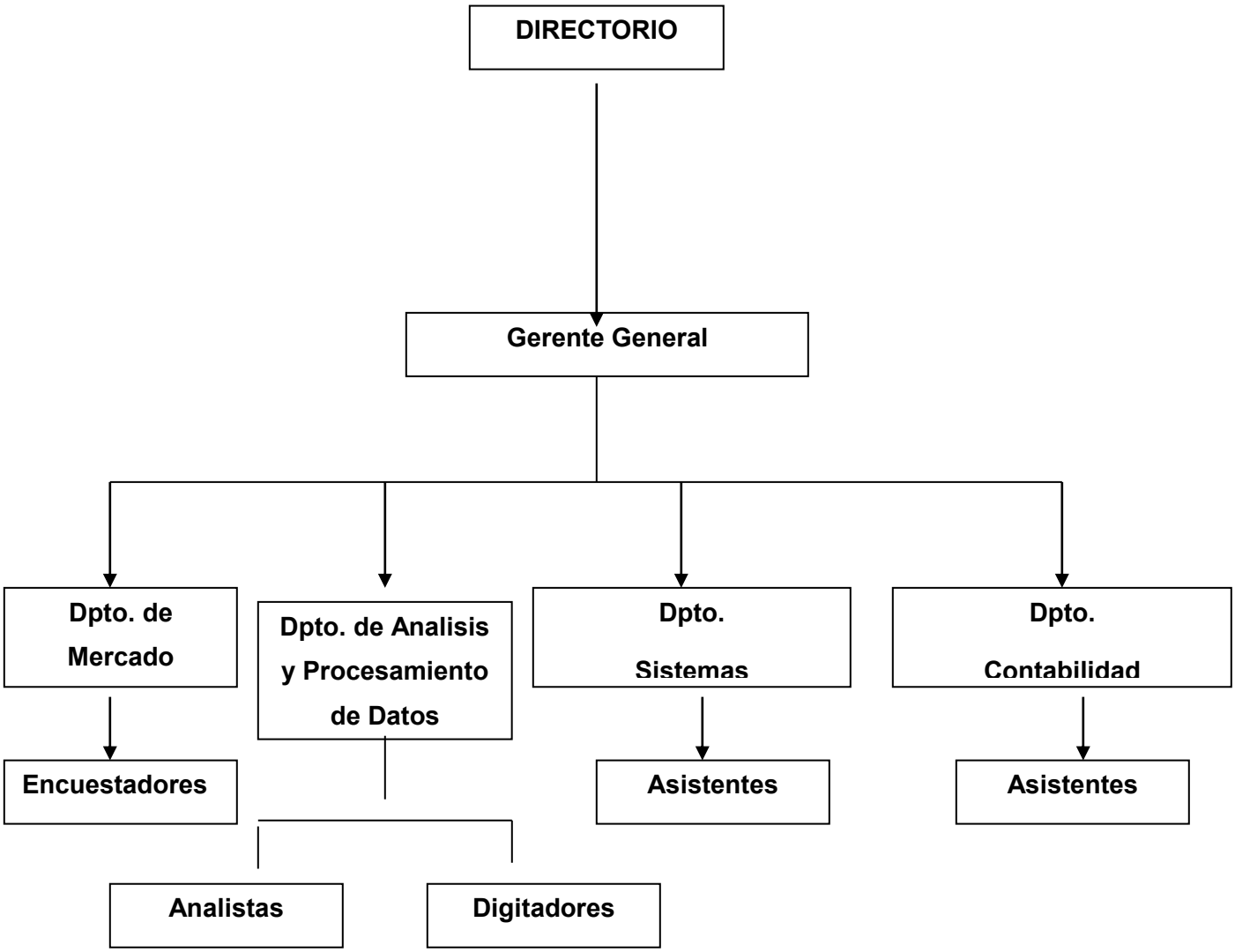
DAN FARMER

Pionero en la programación de herramientas de seguridad, trabajó junto con Spafford en el desarrollo de COPS,así como en el desarrollo de SATAN junto con Venema. Dentro del análisis forense en sistemas de cómputo, diseñó la herramienta The Coroner Toolkit (TCT).

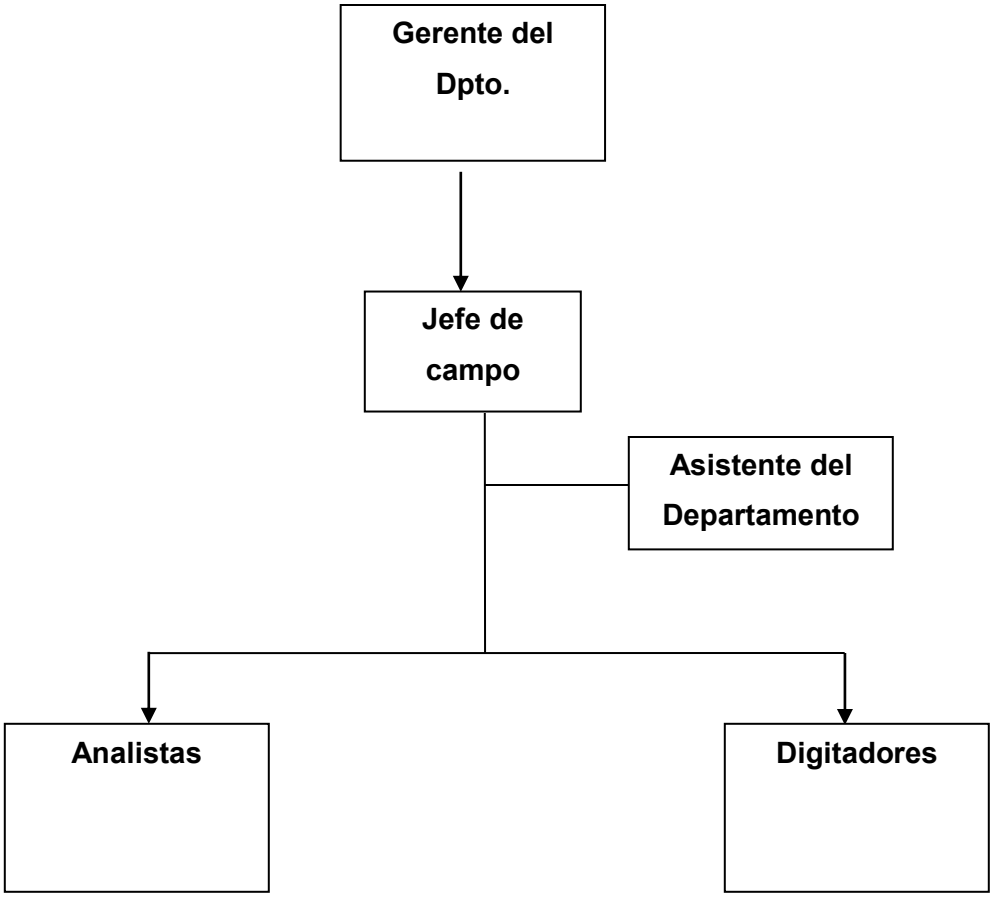
Wietse Venema, Dan Farmer, *Computer Forensic Analysis class :* Trasparencias sobre una sesión impartida por Dan Farmer y Wiete Venema en Verano de 1999 sobre análisis forense en equipos Unix, con referencias a la herramiente TCT.

ANEXO 2

ORGANIGRAMA DE ETASUM S.A.



ANEXO 3
ORGANIGRAMA DEL DEPARTAMENTO DE ANALISIS Y PROCESAMIENTO DE DATOS



ANEXO 4

DESCRIPCIÓN DEL ENTORNO INFORMÁTICO

Empresa: ETASUM
Persona Entrevistada: Gerente General
Fecha: 24/02/05

1. ¿Cuándo fue creada la empresa? ¿Con qué finalidad fue creada?

En Enero de 2004, en Guayaquil, se realizó un consenso, sobre la importancia del estudio del mercado para sastifacer las necesidades de otras empresas.

Definiendo esto como un reto importante, tres ingenieros estadísticos, deciden formar una empresa que analiza el estudio competitivo de los productos en el mercado a través de encuestas.

Es así, que ese mismo año, el 1 de octubre de 2004, deciden formar Empresa ETASUM, haciéndose socios con importantes empresas reconocidas en el mercado.

Los objetivos básicos de la empresa son:

- Ser líderes en el estudio competitivo del mercado a través de encuestas realizadas por personas especializadas y conocedoras del mercado.
- Aplicar técnicas de investigación de mercado para poder brindar una cobertura estratégica de los productos a los clientes

El directivo de la empresa como conocedor del entorno del mercado, cuenta con clientela, debido a que está asociada con una empresa líder en el mercado. Esta empresa cuenta con tres departamentos importantes que son:

- Mercado
- Sistemas
- Análisis y procesamiento de datos
- Contable

2. ¿Qué servicios presta la Empresa (Detalle el / los servicio(s) y cómo funciona(n))?

La empresa con el fin de sastifacer las necesidades de las empresas clientes brindan los siguientes servicios:

- Investigación de mercado.- analiza el producto y da la información pertinente a los directivos de la empresa.

- Cuantitativos: Imagen y posicionamiento, Store audit., hábitos y costumbres, Customer satisfaction, etc.

3. ¿Qué software es utilizado por la empresa por medio del cual interactúan todos los sistemas?

La empresa actualmente cuenta con el sistema Data low, pero debido a las ineficiencias encontradas se desarrollará nuevo sistema, de acuerdo a las necesidades de cada departamento de la empresa.

4. ¿Con qué equipos cuenta la empresa?

La empresa cuenta con 28 computadoras, scaner, telefonos, impresoras matriciales y laser.

5. ¿Cómo están distribuidos los equipos con que cuenta la empresa?

Los equipos disponibles en el departamento de Análisis y Procesamiento de Datos, se distribuyen de acuerdo a las personas que laboran en él, así: 1 gerente, 1 analistas, 3 digitadores, 1 secretaria y 1 supervisor. Este departamento cuenta con los siguientes equipos:

El Supervisor del Dpto. Análisis y Procesamiento de Datos:

- 1 laptop
- 1 impresora inyección a tinta
- 1 palm
- 1 Teléfono

Los analistas:

- 2 computadoras
- 1 Impresora matricial
- Scanner

Los digitadores de encuestas

- 1 computadora cada uno
- 3 impresoras matricial
- 1 teléfono

Supervisor del departamento

- 1 computadora
- 1 teléfono

La secretaria:

- 1 computadora
- 1 Impresora matricial
- 1 Teléfono

6. ¿Qué sistema operativo utilizan?

El sistema operativo con el se maneja la empresa es Windows XP

7.- ¿Con qué sistemas desarrollados cuenta la empresa?

El sistema Datalow, debido a las fallas se esta desarrollando el sistema Stor audit, (Visual y Sql)

8. ¿Cuáles son los utilitarios que se utilizan en el departamento?

Office XP

ANEXO 5

GUIA DE VISITA PREVIA

Nombre de la entidad: ETASUM
Nombre del Departamento: ANALISIS Y PROCESAMIENTODE DATOS
Persona Entrevistada: GERENTE DEL DPTO
Auditor Responsable: Viviana Villacís

1. **¿Cuál es la misión de la empresa?**

   La misión de la empresa es: Ser líderes en el estudio competitivo del mercado a través de encuestas realizadas por personas especializadas y conocedoras del mercado. Además aplicar técnicas de investigación de mercado para poder brindar una cobertura estratégica de los productos a los clientes.

2. **Cuáles son los procesos críticos de la empresa?**

   Uno de los procesos críticos de la empresa es que no cuenta con un manual de procesos, además que no contamos con respaldo de información, los empleados han manipulado información, maquillando los valores de las variables,

3. **Cuenta la empresa con un organigrama?**

   Si No

4. **Qué sistemas se utilizan en la empresa?**

   El sistema Datalow, debido a las fallas se esta desarrollando el sistema Stor audit, (Visual y SQL)

5. **Qué hardware usa?**

   Usa computadoras, scanner, teléfonos, impresoras matriciales y láser.

6. Qué esquemas de seguridad existen en la empresa?

Seguridades Físicas	( )
Alarmas	( )
Plantas de energías auxiliares	( )
Reguladores	(**x**)
Cables de ingreso	( )
Extintores	(**x**)
Respaldo de información	( )

ANEXO 6

INTENTO DE FACTORES DE RIESGOS DE FRAUDES

Empresa: ETASUM
Persona Entrevistada: Gerente General
Fecha: 06-02-06

1.- ¿Qué riesgos de Fraudes considera que hay o pueden haber en su empresa?
Debido a la creación de empresa no hay seguirdades físicas para evitar riesgos naturales creados por el hombre, es decir, no hay alarmas de seguridad de ingreso para la oficina, no hay plantas de energia auxiliares.
Tampoco cuenta con seguridades logicas en los departamentos es decir, no hay UPS, el sistema de data low con elque opera eldepartamento de Análisis y procesamiento de datos no tiene cables de ingresos y cualquiera puede entrar a las bases

2. ¿Dichos riesgos en que área(s) de la empresa se encuentran (o podrían encontrarse)?

Debido a la falta de seguridades fisicas, la empresa corre un riesgo natural que puede ser ocasionado por el hombre. Un área que esta vulnerable al riesgo son dos departamentos el de Sistemas y el de Análsis y procesamiento de Datos.
Debido a la falta de seguridades lógicas y a que no contamos con respaldo de información, los empleados han manipulado información, maquillandolos valores de las variables, debido a que si el informe da una respuesta sastifactoria, los directivos de la empresa dan un porcentaje como incentivo a los empleados. Pero no se ha podido conocerla identidad del empleado que pudo haber maquillado ya que los digitadores no tienen una computadora destinada para cada empleado y eso hace más dificil identificar al posible sospechoso que ha usurpado identidad del digitador.

3. ¿Qué causas considera Ud. por las que están latentes esos riesgos?
Ausencia de seguridades fisicas y lógicas.
Falta de dinero
Ausencia de estructura organizativa
No hay niveles de autoridad

ANEXO 7
IDENTIFICACION DEL PROBLEMA DE LA EMPRESA

Empresa: ETASUM
Persona Entrevistada: Gerente General
Fecha: 10-02-06

1) **Cuál es el problema que ha ocurrido en la empresa? Descríbalo brevemente**

El problema suscitado en la empresa, es debido a una serie de irregularidades como alteraciones de información en las computadoras, robos de encuestas ya revisadas, alteración de la información.

2) **Cuál es la afectación que ha generado dicho problema a su empresa?**

Ha generado una pérdida económica del 65% de un contrato con empresas de alto reconocimiento en el Ecuador, ya que la información entregada no fue la acertada,y esto se fue lo que produjo una perdida cuantiosa para la empresa.

3) **Cuáles considera Usted pueden ser las causas del problema suscitado?**

- Mala supervisión del jefe de ese departamento
- Ausencia de seguridades físicas y lógicas.
- Ausencia de estructura organizativa
- No hay niveles de autoridad

4) **En qué departamento se ha originado el problema?**

Departamentote análisis y Procesamiento de datos.

5) **Qué proceso ha sido afectado?**

El proceso final el cual es la entrega de la información al cliente.

6) **Cuáles son las persona(s) involucrada(s) en el proceso?**

Todos los empleados del personal, esto incluye los digitadores, analistas y el jefe del departamento.

7) **Considera Usted, que la Auditoria Forense le ayudara a resolver dicho problema suscitado en su empresa?**

Tengo conocimiento acerca de la auditoria forense, la cual creo que es la de recopilar o encontrar la información que ha sido robada y/o alterada. Además porque ayudara ala empresa a poner controles para evitar mas fraudes en un futuro.

ANEXO 8

CUESTIONARIO DE POSIBLES SINIESTROS DENTRO DE LA EMPRESA

Área: Análisis y Procesamiento de Datos
Persona Entrevistada: Gerente General
Fecha: 10-02-06

Escriba del 1-5 según su criterio, las posibles causas que se pueden cometer un siniestro dentro de la empresa ETASUM S.A.

5 más importante
4 importante
3 neutral
2 poco significativo
1 no significativo

Causas	Nivel
Alteración, Destrucción y/o Pérdida de información relevante para la empresa	5
Inundaciones	2
Ausencia de claves de accesos en el sistema	3
Ausencia de alarmas de incendios	1
Falta de seguridades en el acceso a la empresa (fisicas)	4

ANEXO 8

CUESTIONARIO DE POSIBLES SINIESTROS DENTRO DE LA EMPRESA

Área: Análisis y Procesamiento de Datos
Persona Entrevistada: Encuestador -Digitador 1
Fecha: 10-02-06

Escriba del 1-5 según su criterio, las posibles causas que se pueden cometer un siniestro dentro de la empresa ETASUM S.A.

5 más importante
4 importante
3 neutral
2 poco significativo
1 no significativo

Causas	Nivel
Alteración, Destrucción y/o Pérdida de información relevante para la empresa	4
Inundaciones	1
Ausencia de claves de accesos en el sistema	3
Ausencia de alarmas de incendios	2
Falta de seguridades en el acceso a la empresa (fisicas)	5

ANEXO 8

CUESTIONARIO DE POSIBLES SINIESTROS DENTRO DE LA EMPRESA

Área: Análisis y Procesamiento de Datos
Persona Entrevistada: Encuestador- Digitador 2
Fecha: 10-02-06

Escriba del 1-5 según su criterio, las posibles causas que se pueden cometer un siniestro dentro de la empresa ETASUM S.A.

5 más importante
4 importante
3 neutral
2 poco significativo
1 no significativo

Causas	Nivel
Alteración, Destrucción y/o Pérdida de información relevante para la empresa	5
Inundaciones	1
Ausencia de claves de accesos en el sistema	3
Ausencia de alarmas de incendios	2
Falta de seguridades en el acceso a la empresa (fisicas)	4

ANEXO 8

CUESTIONARIO DE POSIBLES SINIESTROS DENTRO DE LA EMPRESA

Área: Análisis y Procesamiento de Datos
Persona Entrevistada: Encuestador-Digitador 3
Fecha: 10-02-06

Escriba del 1-5 según su criterio, las posibles causas que se pueden cometer un siniestro dentro de la empresa ETASUM S.A.

5 más importante
4 importante
3 neutral
2 poco significativo
1 no significativo

Causas	Nivel
Alteración, Destrucción y/o Pérdida de información relevante para la empresa	5
Inundaciones	1
Ausencia de claves de accesos en el sistema	4
Ausencia de alarmas de incendios	2
Falta de seguridades en el acceso a la empresa (fisicas)	3

ANEXO 8

CUESTIONARIO DE POSIBLES SINIESTROS DENTRO DE LA EMPRESA

Área: Análisis y Procesamiento de Datos
Persona Entrevistada: Encuestador-Digitador 4
Fecha: 10-02-06

Escriba del 1-5 según su criterio, las posibles causas que se pueden cometer un siniestro dentro de la empresa ETASUM S.A.

5 más importante
4 importante
3 neutral
2 poco significativo
1 no significativo

Causas	Nivel
Alteración, Destrucción y/o Pérdida de información relevante para la empresa	4
Inundaciones	1
Ausencia de claves de accesos en el sistema	5
Ausencia de alarmas de incendios	2
Falta de seguridades en el acceso a la empresa (fisicas)	3

ANEXO 8

CUESTIONARIO DE POSIBLES SINIESTROS DENTRO DE LA EMPRESA

Area: Analisis y Procesamiento de Datos
Persona Entrevistada: Encuestador-Digitador 5
Fecha: 10-02-06

Escriba del 1-5 según su criterio, las posibles causas que se pueden cometer un siniestro dentro de la empresa ETASUM S.A.

5 más importante
4 importante
3 neutral
2 poco significativo
1 no significativo

Causas	Nivel
Alteración, Destrucción y/o Pérdida de información relevante para la empresa	5
Inundaciones	3
Ausencia de claves de accesos en el sistema	2
Ausencia de alarmas de incendios	1
Falta de seguridades en el acceso a la empresa (fisicas)	4

ANEXO 8

CUESTIONARIO DE POSIBLES SINIESTROS DENTRO DE LA EMPRESA

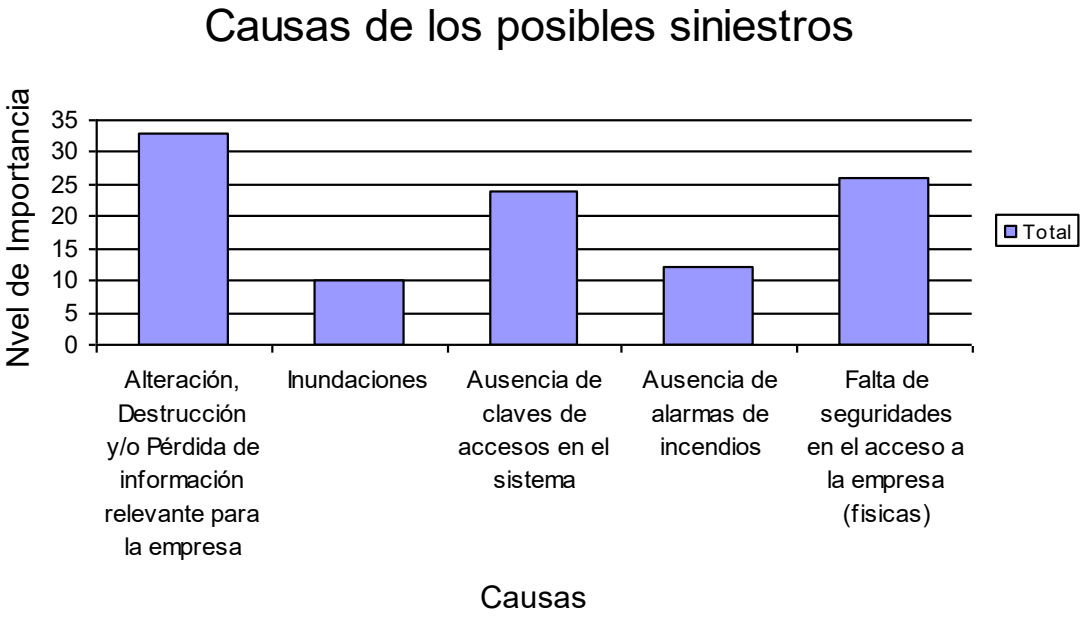
Área: Análisis y Procesamiento de Datos
Persona Entrevistada: Encuestador-Digitador 6
Fecha: 10-02-06

Escriba del 1-5 según su criterio, las posibles causas que se pueden cometer un siniestro dentro de la empresa ETASUM S.A.

5 más importante
4 importante
3 neutral
2 poco significativo
1 no significativo

Causas	Nivel
Alteración, Destrucción y/o Pérdida de información relevante para la empresa	5
Inundaciones	1
Ausencia de claves de accesos en el sistema	4
Ausencia de alarmas de incendios	2
Falta de seguridades en el acceso a la empresa (fisicas)	3

Causas	Total
Alteración, Destrucción y/o Pérdida de información relevante para la empresa	33
Inundaciones	10
Ausencia de claves de accesos en el sistema	24
Ausencia de alarmas de incendios	12
Falta de seguridades en el acceso a la empresa (fisicas)	26



ANEXO 9

Área	Si	No	Comentarios
Administración			
Existe un organigrama de la estructura organizacional del personal de Departamento de análisis y procesamiento de datos. Si existe, verificar a que nivel se encuentra el departamento.	**X**		No está establecido a que nivel se encuentra
Se realizan reuniones periódicas con la Alta Gerencia. Se hacen divulgación de resultados.		**X**	Se realizan siempre y cuando tengan que dar resultados
Cuentan con presupuesto		**X**	
Cuentan con descripción de funciones del personal del Departamento de Análisis y Procesamiento de Datos.	**X**		Las políticas no se revisan periódicamente, para verificar si se están cumpliendo
Se realizan evaluaciones de desempeño		**X**	
Existen políticas y procedimientos de seguridad de lógicas y fisicas.		**X**	
Cuentan con antivirus. Es actualizado periódicamente. Cada que tiempo?	**X**		Todas las computador, se lo realiza trimestralmente
Disponen de inventario de software y hardware.	**X**		
Existe un departamento de auditoría Interna.		**X**	
Se realizan auditoría de sistemas. CHECKLIST		**X**	

Área	Si	No	Comentarios
Seguridad Física y Ambiental Cuentan con extintores de fuego.		**X**	
Existen detectores de humo.		**X**	
Disponen de protección de cables de red.		**X**	
Existe un regulador de poder instalado y adecuadamente protegidos contra fallos eléctricos?	**X**		
Cada que tiempo se prueban las condiciones de la fuente de poder o UPS		**X**	No cuentan con UPS.
Están los equipos de humo y fuego aprobados por una autoridad reconocida?		**X**	No hay
Robo de equipos Existe un procedimiento aprobado para retirar las computadoras de la empresa		**X**	
Acceso Lógico Existen mecanismos de control de acceso a los sistemas		**X**	No existe claves de acceso
Cuál es la periodicidad de cambio de las contraseñas. Longitud.		**X**	No hay
Se almacenan en algún lugar seguro. Quienes la conocen.		**X**	No hay
Existe procedimientos para la eliminación, modificación de los datos o información del sistema	**X**		Debido a que no existen claves de acceso.
Que tipo de controles de acceso se utilizan (puertas de combinación de cifras o claves de acceso o lectores de carnet, utilizados para controlar el acceso al área de tecnología?		**X**	No hay
Área	**Si**	**No**	**Comentarios**
Disponen de registros de control de entrada y salida de personal visitante al área?	**X**		Existe una bitácora diaria

Continuidad de operaciones			
Se cuenta con un plan de contingencia actualizado.		**X**	
Existen procedimientos de respaldos de datos.	**X**		Solo en el Dpto. de Sistemas
Se cuentan con registro de control de respaldos realizados en forma correcta.	**X**		El Dpto. de Sistemas utiliza log de encuestas ingresadas diariamente.
Cuentan con un equipo de contigencia	**X**		

ANEXO 10

PAPELES DE TRABAJO

Empresa: ETASUM
Persona Entrevistada: Encuestador-Digitador 1
Fecha: 16-01-06
Auditor Responsable: Viviana Villacís

1) **Qué cargo usted ocupa dentro de la empresa y en qué departamento labora?**

Encuestador - Digitador en el departamento de Análisis y Procesamiento de datos.

2) **Cuál es su participación dentro de la entrega de información?**

Facilito la información ya digitada y procesada por los analistas, verificando Qué los campos en el sistema estén correctos al Jefe del Dpto.

3) **Qué sistema de información utiliza en dicho proceso?**

El sistema DATALOW

4) **Como accede al sistema de información, seleccione una opción**

- **Directamente en el PC (X)**
- **Red ( )**
- **Clave personal ( )**
- **Conexión remota ( )**

5) **El sistema Qué Ud. Usa cuenta con respaldos?**
Si ( ) No (X)

6) **Al sistema puede tener acceso cualquier usuario sin conocimientos estadísticos?**

Si, ya qué no existe una clave personal, y cualquier persona puede modificar la información.

7) **Existen controles necesarios para Qué la información no sea adulterada?**

NO

8) **El sistema es íntegro, confiable y está disponible?**

No, el sistema tiene muchas falencias

ANEXO 10

PAPELES DE TRABAJO

Empresa: ETASUM
Persona Entrevistada: Encuestador-Digitador 2
Fecha: 16-01-06
Auditor Responsable: Viviana Villacís

1) **Qué cargo usted ocupa dentro de la empresa y en qué departamento labora?**

Encuestador - Digitador en el departamento de Análisis y Procesamiento de datos.

2) **Cuál es su participación dentro de la entrega de información?**

Digito las encuestas y verifica qué la información sea confiable, de acuerdo a una ponderación dentro de la información solicitada.

3) **Qué sistema de información utiliza en dicho proceso?**

El sistema DATALOW

4) **Cómo accede al sistema de información, seleccione una opción**

- **Directamente en el PC (X)**
- **Red ( )**
- **Clave personal ( )**
- **Conexión remota ( )**

5) **El sistema Qué Ud. Usa cuenta con respaldos?**
Si ( ) No (X)

6) **Al sistema puede tener acceso cualquier usuario sin conocimientos estadísticos?**

Si, y esto es lo Qué conlleva a la alteración de la información, ya Qué el departamento tampoco cuenta con seguridades físicas como alarmas dentro del departamento.

7) **Existen controles necesarios para qué la información no sea adulterada?**

La empresa no cuenta con seguridades lógicas.

8) **El sistema es íntegro, confiable y está disponible?**

NO es integro, pero esta disponible a cualquier usuario Qué tenga acceso al departamento.

ANEXO 10

PAPELES DE TRABAJO

Empresa: ETASUM
Persona Entrevistada: Secretaria
Fecha: 16-01-06
Auditor Responsable: Viviana Villacís

1) **Qué cargo usted ocupa dentro de la empresa y en qué departamento labora?**

Secretaria del Dpto. de análisis y procesamiento de datos

2) **Cuál es su participación dentro de la entrega de información?**

Entrega de cartas a empresas Clientes, elaboración de cartas, entrega de la información relacionada del Dpto. al Gerente, archivos de encuestas y/o información relevante, pago de movilización de los encuestadores, movimientos de caja chica.

3) **Qué sistema de información utiliza en dicho proceso?**

Paquete Office

4) **Cómo accede al sistema de información, seleccione una opción**

- **Directamente en el PC (X)**
- **Red ( )**
- **Clave personal ( )**
- **Conexión remota ( )**

5) **El sistema Qué Ud. Usa cuenta con respaldos?**
Si (X) No ( )

6) **Al sistema puede tener acceso cualquier usuario sin conocimientos estadísticos?**

Si

7) **Existen controles necesarios para que la información no sea adulterada?**

No, pero los archivos elaborados por mi, los guardo con clave, debido a qu no existe un control, dentro del departamento.

8) **El sistema es íntegro, confiable y está disponible?**

Si

ANEXO 10

PAPELES DE TRABAJO

Empresa: ETASUM
Persona Entrevistada: Analista
Fecha: 16-01-06
Auditor Responsable: Viviana Villacís

1) **Qué cargo usted ocupa dentro de la empresa y en qué departamento labora?**

Analista en el departamento de Análisis y Procesamiento de datos.

2) **Cuál es su participación dentro de la entrega de información?**

Analizo y evaluó los resultados qué se obtienen por medio del sistema, proporcionando mi criterio qué luego es analizado por el supervisor del departamento.

3) **Qué sistema de información utiliza en dicho proceso?**

El sistema DATALOW

4) **Como accede al sistema de información, seleccione una opción**

- **Directamente en el PC (X)**
- **Red ( )**
- **Clave personal ( )**
- **Conexión remota ( )**

5) **El sistema que Ud. Usa cuenta con respaldos?**
Si ( ) No (X)

6) **Al sistema puede tener acceso cualquier usuario sin conocimientos estadísticos?**

Si, eso es lo Qué ha originado la alteración de la información.

7) **Existen controles necesarios para que la información no sea adulterada?**

No hay controles Qué aseguren la confidencialidad de la información, pero ahora se están tomando medidas necesarias.

8) **El sistema es íntegro, confiable y está disponible?**

El sistema posee muchas falencias, cuales han afectado a la información final.

ANEXO 10

PAPELES DE TRABAJO

Empresa: ETASUM
Persona Entrevistada: Encuestador-Digitador 3
Fecha: 16-01-06
Auditor Responsable: Viviana Villacís

1) Qué cargo usted ocupa dentro de la empresa y en Qué departamento labora?

Encuestador - Digitador en el departamento de Análisis y Procesamiento de datos.

2) Cuál es su participación dentro de la entrega de información?

Ingresar la información recolectada al sistema.

3) Qué sistema de información utiliza en dicho proceso?

DATALOW

4) Cómo accede al sistema de información, seleccione una opción

- **Directamente en el PC (X)**
- **Red ( )**
- **Clave personal ( )**
- **Conexión remota ( )**

5) El sistema Qué Ud. Usa cuenta con respaldos?

Si ( ) No (X)

6) Al sistema puede tener acceso cualquier usuario sin conocimientos estadísticos?

Si, debido a las falencias que se puede encontrar en el momento que uno va ingresando la información.

7) Existen controles necesarios para qué la información no sea adulterada?

No

8) El sistema es íntegro, confiable y está disponible?

NO es integro, pero en Sistemas creo que guardan cierta información.

ANEXO 10

PAPELES DE TRABAJO

Empresa: ETASUM
Persona Entrevistada: Encuestador-Digitador 4
Fecha: 16-01-06
Auditor Responsable: Viviana Villacís

1) Qué cargo usted ocupa dentro de la empresa y en qué departamento labora?

Encuestador - Digitador en el departamento de Análisis y Procesamiento de datos.

2) Cuál es su participación dentro de la entrega de información?

Recolectar información y luego procesar la información en el sistema.

3) Qué sistema de información utiliza en dicho proceso?

DATALOW

4) Cómo accede al sistema de información, seleccione una opción

- **Directamente en el PC (X)**
- **Red ( )**
- **Clave personal ( )**
- **Conexión remota ( )**

5) El sistema Qué Ud. Usa cuenta con respaldos?
Si ( ) No (X)

6) Al sistema puede tener acceso cualquier usuario sin conocimientos estadísticos?

Si, porque no cuenta con seguridades lógicas el sistema

7) Existen controles necesarios para qué la información no sea adulterada?

No

8) El sistema es íntegro, confiable y está disponible?

No

ANEXO 11

CONSTATACION DEL EQUIPO VULNERABLE EN EL ANALISIS FORENSE

- Computadora
- Teléfono
- Impresora Láser

CPU

MONITOR

- PAPELES DE TRABAJO.-
  ENCUESTAS REALIZADAS

ANEXO 12
OBSERVACIONES

Hallazgo 1.- Ingreso incorrecto de variables

Condición.- Ingresan incorrectamente las variables al sistema.
Criterio.- El jefe y/o encargado debe revisar periódicamente el ingreso de variables de acuerdo con las encuestas realizadas.
Causa.- Todas las personas tienen acceso al sistema, dando la posibilidad de modificaciones o alteraciones en la información.
Efecto.- El informe final es adulterado y la información es falseada.
Conclusión.- El informe final con datos falseados puede ocasionar pérdidas aún mayores para la empresa en caso de no ser corregida a tiempo
Recomendación.- La programación del sistema y los esquemas debe ser corregido para garantizar la confiabilidad de la información y el jefe y/o encargado debe revisar los resultados de la información y deberá garantizar la confiabilidad mediante la revisión constante y una rúbrica de aceptación previo, durante y después del ingreso de la información al sistema.

Observación 2.- El sistema carece de Clave de Acceso

Condición.- Falta de clave de acceso personal en el sistema para el digitador.
Criterio.- El sistema debe tener una clave de acceso para cada digitador
Causa.- Todas las personas tienen acceso al sistema, dando la posibilidad de modificaciones o alteraciones en la información sin la respectiva identificación del culpable.
Efecto.- El ingreso de terceros al sistema con fines fraudulentos.
Conclusión.- La falta de claves de acceso puede ocasionar pérdidas aún mayores para la empresa en caso de no ser corregida a tiempo
Recomendación.- La programación del sistema debe ser corregido para de esa forma poder garantizar la confiabilidad de la información y por consiguiente los resultados obtenidos.

Observación 3.- Falta de autoridad de los jefes y/o encargados

Condición.- El jefe de la empresa no verifica constantemente el material ingresado, lo cual afecta al informe final.
Criterio.- El Departamento debe tener políticas de autoridad para revisar periodicamente las encuestas realizadas e ingresadas.
Causa.- Todos los digitadores tienen acceso a todas las computadoras lo que ocasiona modificaciones o alteraciones en la información sin descubrir al posible culpable en la manipulación de datos.
Efecto.- Manipulación de los datos

Conclusión.- La falta de autoridad los jefes y la revisión periódica de las tareas encomendadas a los empleados pueden ocasionar pérdidas aún mayores para la empresa en caso de no ser corregida a tiempo.
Recomendación.- Elaborar una estructura organizativa que defina claramente los niveles de autoridad y responsabilidad y provea una apropiada segregación de funciones.

Observación 4.- Falta de organización en el Departamento

Condición.- Falta de organización respecto al uso de las computadoras.
Criterio.- El Departamento debe tener una estructura organizativa, para el uso adecuado de sus activos.
Causa.- Falta de comunicación entre los digitadores y el jefe para solucionar los problemas suscitados.
Efecto.-Resulta difícil identificar al empleado que manipuló los datos en la computadora.
Conclusión.- Cada empleado debe de tener a cargo una computadora. El digitador deberá ser responsable de cada activo fijo que se le entregue.
Recomendación.- Elaborar un informe donde se especifique la entrega de un computador a cada digitador cuya información sirva de respaldo para el empleado.

BIBLIOGRAFÍA

1. Betancourt López Eduardo, Teoría del delito, Editorial Porrúa. S.A., México 1994. Páginas 304.-305

2. Comité Directivo de COBIT**,** 1998. COBIT. Directrices de Auditoría**,** Segunda Edición, EE.UU, Páginas 8-18, 23-27, 70-73.

3. Echenique García José Antonio, Auditoria en Informática, Segunda edición, Mc Graw - Hill, México. Páginas 17-22.

4. Gutiérrez Abraham, 1998, Métodos y técnicas de investigación, Segunda edición, Mc Graw Hill, México, páginas 12-65.

5. Gill Morell M., 2000. Informática y Comunicaciones, GIGA Nº 2, Revista Cubana de Computación, Cuba.

6. Piattini Mario y Del Peso Emilio**,** 2004. Auditoría Informática: Un Enfoque Práctico, Segunda Edición, Editorial RA-MA, España, Páginas 45-89, 310-317, 394-401, 570-581, 616

PAGINAS WEB

2005

http://www.vnunet.es/Actualidad/Noticias/Seguridad/Vulnerabilidades/20030911031

http://www.alfa-redi.org/revista/data/20-9.asp

http://his.sourceforge.net/honeynet/papers/forensics/http://www.snort.org/

http://www.gestiopolis.com/recursos/experto/catsexp/pagans/fin/46/clasnormaaudit.htm

2006

http://www.monografias.com/trabajos16/auditoria-deinformacion/auditoria-de-informacion.shtml

www.cops.org/forensic_examination_procedures.htm

- **Asociaciones**
  - http://www.gocsi.com - Computer Security Institute
  - http://www.acfe.org - Assoc. Certified Fraud Examiners
  - http://www.icsa.com - International Information Systems Security Assoc.
  - http://www.htcia.org - High Technology crime investigation Assoc.
  - http://www.cops.org - International Assoc. of Computer Investigative Specialist (IACIS)

- **Ciencias Forenses**

  - http://www.aafs.org - American Academy of Foreinsic Science.

  - http://www.forensics.com - Computer Forensics, Inc.

  - http://www.computer-forensics.com - Computer Forensics Ltd.

  - Http://www.forensics-intl.com - New Technologies, Inc.(NTI).

  - SANS Institute (SANS InfoSec Reading Room):

  - www.sans.org/rr/

- **Forensics Science Communications:**

  - http://www.fbi.gov/hq/lab/fsc/current/index.htm