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

Viviana Marcela Villacís Ruiz, Bertha Alice Naranjo Sánchez[2].

- [1]Auditor en Control de Gestión 2006; email: evvitaz@ubbi.com

- [2]Directora de Tesis, Ingeniera en Computación, Escuela Superior Politécnica del Litoral, 1994, Postgrado Ecuador, Escuela de Postgrado de Administración de Empresas ESPAE, 1997. Profesora de la ESPOL desde 1996., email: anaranjo2408@ubbi.com

RESUMEN

El presente trabajo muestra a la Auditoria Forense en Informática, cuyo objetivo principal es tratar de reunir la mayor cantidad de pruebas e información necesaria para descifrar el siniestro, evento acontecido en un entorno informativo. La escena del evento involucra a la computadora, de ahí su vinculación con la Informática.

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. En la quinta y última parte, se muestran las conclusiones y recomendaciones correspondientes.

ABSTRACT

The present work shows to the Forensic Audit in Computer science whose main objective is to try to gather the biggest quantity in tests and necessary information to decipher the catastrophe, event happened in an informative environment. The scene of the event involves to the computer, of there it's linking with the Computer science.

In the first chapter the vulnerabilities of the computer and technical sector of attack are revised that unscrupulous people use to make forbidden acts.

In second chapter leaves it develops the theoretical mark of this work.

In the third chapter, it is described the norms and standard national and international that should be had in bill when carrying out a work of forensic audit.

In fourth chapter leaves it carries out the development of the Computer Forensic Audit in a company of the commercial sector. In the fifth and last part, it shows the conclusions and recomendations of the present work.

INTRODUCCION

Las organizaciones modernas que operan gran parte de su actividad en el negocio a través del recurso informático necesitan dotar sus sistemas e infraestructuras informáticas de medidas de protección más adecuadas que garanticen el continuo desarrollo y conservar sus actividades, en este sentido cobra especial importancia la necesidad de contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen, controlen y gestionen de manera eficaz sus sistemas.

La sociedad de la información y las nuevas tecnologías de información plantean la necesidad de mantener la integridad y confidencialidad de la información que soportan los sistemas de sus organizaciones, para ello, es especialmente importante elegir e implantar los sistemas y métodos de seguridad más idóneos, que protejan sus redes y sistemas ante eventuales amenazas, fraudes o siniestros ya sean presentes o futuros.

Este tipo de actividades deben ser estimuladas, la sociedad que está conciente de este hecho, ve con buenos ojos, aplicar esquemas de control en todo campo de acción, mas aun en el Informático, pues hasta ahora las pruebas que aportan las auditorias tradicionales no son suficientes, lo que ha dado origen a una rama de la auditoria mas especializada denominada Auditoría Forense Informática, que permite que un experto emita opiniones de valor técnico, que le permiten a terceras personas actuar con mayor certeza, respecto a acciones de control y/o sanción.

Importancia de Auditoria Forense

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 o integridad.

Definitivamente en un mundo tan automatizado como el de hoy, es indispensable el uso de la computadora y el manejo de la tecnología, sin embargo esta tecnología puede verse afectada por ciertas conductas delictivas que pueden generar, “ATAQUES”, ”FRAUDES”, "SINIESTROS", en contra de los recursos informáticos que existen en nuestras organizaciones

Por todo lo antes expuesto es necesario contar con una actividad en el campo de la auditoria pero en el entorno informático y es así como ahora con la aparición de la Auditoria Forense Informática se puede llegar a identificar al que cometió el ataque, delito, fraude o siniestro y las acciones que efectuó para cometerlo.

Estudiar este tema es particularmente emocionante para todo investigador y como estudiantes de la ESPOL tenemos un nuevo campo de acción para nuestra profesión

Presentación del Problema

Este trabajo identifica los principales causas por las cuales puede suscitarse una Auditoria Forense Informática y nos ayuda a evitar siniestros, ataques y fraudes cometidos por los empleados de la empresa.

En el campo forense informático, el trabajo destaca la importancia de definir acertadas metodologías, herramientas y técnicas ligadas de forma inseparable a los objetivos de la organización, planteados en su estrategia empresarial, en su misión y visión.

El problema en sí, se basa en la modificación y/o eliminación de archivos, el objetivo primordial es reconstruir lo hechos del siniestro, para asi poder encontrar al o los culpables del suceso.

CONTENIDO

Como bosquejo de lo que se encontrara en este trabajo, describiré algunas ideas principales a continuación.

Primero es necesario dejar en claro ciertas definiciones que son consideradas como relevantes para un mejor entendimiento del trabajo.

Definiciones:

1.- Siniestro: Según el italiano Carlos Sarzana: “El siniestro informático es cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo.”

2.- 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. "

3.- Delito Informático: Según María de la Luz Lima, dice que el "delito informático en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en 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".

4.- 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.

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

6.- 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.

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

8.-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.

9.-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.

PROCESO DE LA AUDITORIA FORENSE

Aunque no hay un procedimiento cierto para la Auditoria Forense es importante seguir una metodología, de acuerdo al caso suscitado, aplicando las técnicas y herramientas adecuadas para poder evitar un siniestro, fraude o ataque. Por lo cual hay procedimientos como los que detallamos a continuación:

1.-Definición y reconocimiento del problema,

Primero definimos el problema que se ha suscitado, identificando las causas y las consecuencias que se presentan por el o lo(s) problema(s) suscitado(s).

Este problema, fue reconocido por la gerencia de la empresa, debido a malos entendidos con clientes que ya tenían credibilidad en el sector comercial, debido a que hubo una pérdida, maquillaje o adulteración de información confiable para un informe final.

Para el reconocimiento del problema, nos valemos de técnicas como visitas previas, entrevistas, etc y la herramienta apropiada seria Proyect, ayudándonos con un cronograma para reconocer el problema.

2.- Recopilación de evidencias de fraude.-

Una vez, identificado el problema, comenzamos a la recopilación de la información, nos valemos de técnicas utilizadas como entrevistas a las personas involucradas, mails de directivos o empleados de la empresa, bitácora, planificaciones, observaciones, etc.

Se toma foto al equipo vulnerado, para tener como evidencia cual fue el equipo a investigar con sus respectivos archivos.

3.- Evaluación de las evidencias recolectadas o análisis.-

Al tener las evidencias correspondientes al problema, comenzamos a analizar cada una de ellas, haciendo relación una con otra para descubrir el o los culpables de este hecho.

La evaluación de las evidencias se puede hacer por medio de softwares especializados en la detección de fraude, comando, pistas, log, todas relacionadas entre si. Después de analizarlas causas y dar con el criminal damos el resultado de la auditoria forense informática.

CONCLUSIONES

1. La Auditoria Forense en los siniestros informático, ayuda a conocer el motivo porque el cual se ha suscitado el fraude o siniestro presente en un momento dado, anticipando posibles perdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir.

2. Las metodologías, herramientas y técnicas que se aplican para prevenir un siniestro informático en las empresas comerciales se hacen cada vez más un objetivo primordial para evitar los siniestros dentro de una empresa del sector comercial cometido por los mismos empleados.

3. La Auditoria Forense Informática, en esta tesis, nos muestra los principales controles y seguridades que deben implementarse en uno de los departamentos de la empresa como es el caso del departamento de Análisis Y procesamientote Datos.

4. Esta tesis ayuda a conocer la importancia de la auditoria forense, especialmente para los estudiantes quienes con este nuevo conocimiento pueden desarrollar un perfil profesional de la mano con la era digital actual y futura en el ambiente de la Auditoria.

5. 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.

REFERENCIAS

1. V. Villacís, "Auditoria Forense: Metodología, Herramientas y Técnicas Aplicadas en un siniestro informático de una empresa del sector comercial" (Tesis, Instituto de Ciencias Matemáticas, Escuela Superior Politécnica del Litoral, 2006).

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

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

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

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