Adversia
Revista Virtual de Estudiantes de Contaduria Pública
UNIVERSIDAD DE ANTIOQUIA
Facultad de Ciencias Económicas – Departamento de Ciencias Contables

Adversia (julio-diciembre), pp 15-30 ©Universidad de Antioquia-2009.

Auditoría Forense aplicada a la tecnología

Álvaro Fonseca Vivas

Contador Público de la Universidad de Bogotá Jorge Tadeo Lozano, Especializado en Administración Financiera, Magister en Docencia, docente investigador de varias Universidades a nivel de pregrado.
alvarofv1@yahoo.com

Auditoría Forense Aplicada a la Tecnología

1. Auditoria Forense

Historia de la Auditoría Forense. "El Código de Hamurabi es el primer documento conocido por el hombre que trata sobre leyes, en ellas el legislador incluyó normas sobre el comercio, vida cotidiana religión, etc. Obviamente no existía la contabilidad por partida doble debido a que el código de Hamurabi es de Mesopotamia de aproximadamente 1780 A.C. y en sus fragmentos del 100 al 126 da a entender el concepto básico de auditoría forense: demostrar con documentación contable un fraude o una mentira y también se hacen comentarios sobre cálculos de ganancias y pérdidas en los negocios para los cuales se debe utilizar un contador".

La contabilidad existe desde hace mucho tiempo, de hecho se encuentran en museos documentos relacionados con registros contables pertenecientes al antiguo Egipto, Sumer y todas las grandes civilizaciones del pasado, sin embargo, la auditoría forense nace cuando se vincula lo legal con los registros y pruebas contables y el primer documento legal conocido es el Código de Hamurabi, allí se expone por ejemplo que si un comerciante reclama un pago realizado debe demostrar el recibo, claro que este comerciante tendría su escriba o contador que fungiría como forense para presentar ante el juez el recibo correspondiente al pago y demostrar que el pago fue realizado. El Código de Hamurabi condenaba entonces al fraude o mentira del que negaba haber recibido el pago haciéndole pagar hasta seis veces el monto.

El repunte de la auditoría forense comenzó con este hecho histórico de apresar a Al Capone debido a que durante la época de la prohibición del licor y el juego, el crimen organizado prosperó como nunca antes en ese país. Millones de dólares fueron ganados usando prácticas criminales. El dinero era lavado y permitiría a los jefes principales del gangster permanecer fuera de las manos de la ley viviendo como magnates. Poco podía hacer la justicia contra la lucha de estas actividades criminales, no se podía aplicar ninguna prueba contra la gente tal como Al Capone, Lucky Luciano y Bugsy Siegel. Hasta el día que un contador en el departamento de impuesto dio con la idea de conseguir inculpar a Al Capone con la ley de impuesto, se dedicó entonces a buscar pruebas, repentinamente se encontró una abundancia de evidencia revisando las cuentas de un negocio que lavaba y hasta planchaba el dinero de Al Capone.

La Fiscalía logró traer el "lavador" de dinero y el libro de pagos y luego se pudo comprobar que el volumen de ventas superaba la capacidad teórica del negocio de los lavadores, de hecho, el volumen de ventas real y el volumen de ventas declarado iban lejanos. Aunque no se pudo probar el asesinato, extorsión y

otros crímenes cometidos por Al Capone, los contadores y auditores forenses pudieron demostrar fraude en el pago de impuesto en Al Capone y en sus lavadores y se pudo desmantelar la organización.

Por alguna razón desconocida no se dio el impulso suficiente a esta rama de las ciencias contables en esta oportunidad y el gran momento de la auditoría forense fue diferido hasta los años 70 y 80 donde surgió de nuevo en Estados Unidos como herramienta para suministrar pruebas a los fiscales, luego vinieron los auditores forenses privados y en los años 90 surgió el gran Boom de la Auditoría Forense. "[1]

Definición. "El término forense se vincula con la investigación legal para facilitar la administración de la justicia, en la medida en que se busca el aporte de evidencias para que se conviertan en pruebas en el foro, para nuestros tiempos, la corte.

En términos contables y de auditoría, la relación con lo forense se hace estrecha cuando hablamos de presentar evidencias especialmente documentales.
Se define inicialmente a la auditoría forense como una auditoría especializada en descubrir, divulgar y atestar sobre fraudes y delitos en el desarrollo de las funciones públicas y privadas; es así como se abre un amplio espacio en el campo de la investigación, que irá más allá de la simple investigación administrativa de fraudes y delitos.

En la auditoría forense, las estrategias, procedimientos y métodos investigativos, son especialmente estudiados con el fin de preservar y priorizar el interés público. Un Auditor interno o externo, puede tener mucha experiencia en los procesos de evaluación de control interno y de presentación de informes con valor agregado ante el ente que contrata sus servicios, pero para el caso de investigaciones de fraudes y delitos requiere conocimientos en el campo judicial, especialmente en el levantamiento de indicios y evidencias, las cuales se deben relacionar con delitos tipificados en los códigos penales, para que fácilmente se puedan convertir en pruebas que requiere la justicia para sus sentencias.
La Auditoría Forense, es de hecho, una herramienta muy valiosa en la aplicación de la justicia, y debe por lo tanto ser un proceso legal que se deriva de una serie de

[1] CAMARGO, Nelson. Breve Historia de la Auditoría Forense, En:

http://www.redcontable.com/modules.php?name=News&file=article&sid=251

protocolos, como son la autorización de una entidad oficial (Fiscalía, Procuraduría, Contraloría, una Corte Civil o Criminal, etc.).

Este procedimiento como es de tipo investigativo y lo que se persigue es la judicialización y a la postre la penalización o exoneración, debe ser ejecutado bajo Normas Internacionales de Auditoría Especial, para evitar cometer errores que por insignificantes que puedan ser, anulen totalmente la investigación y el caso en la Corte o tribunal de Justicia pueda ser desestimado por un Juez.

Es por esta razón que la Auditoría Forense, se convierte en una herramienta eficaz para la investigación cuando se comete un delito, pero también sirve de control y prevención, pues no necesariamente la Auditoría Forense está concebida para encontrar un hecho delictivo sino también para esclarecer la verdad de los hechos y exonerar de responsabilidad a un sospechoso que sea inocente o a una empresa o entidad que haya sido acusada de un fraude con la intención de obtener beneficios económicos.

A raíz de los escándalos contables generados principalmente por el Gobierno Corporativo de empresas de clase mundial, entre muchas otras como Merck, Nortel, Worldcom, Global Crossing, AIG, Enron, Ahold, Parmalat, Drogas la rebaja y Grupo empresarial Grajales, se ha retomado la auditoría y la contabilidad forense, como una actividad que facilita desenmascarar especialmente a los delincuentes de cuello blanco que hacen parte de la alta directiva de las organizaciones y que con sus actuaciones no garantizan transparencia ni confiabilidad para preservar el interés público, por ello el auditor forense debe tener en cuenta que cualquier funcionario de una compañía tiene que informar de un hecho delictivo que descubra durante sus funciones, si de alguna forma omite, oculta o manipula la información, estará claramente en violación de la ley, incurriendo en los delitos de "Obstrucción a la Justicia", "Encubrimiento", "Omisión", "Ceguera intencional", "Complicidad", o "Falsedad". Estos delitos lo convierten automáticamente en parte comprometida en un proceso de investigación criminal y será el auditor forense el encargado de obtener evidencia para probar el conocimiento, la intención y la voluntad del imputado.

Por otra parte el auditor forense no debe estar ajeno a comprender que ante la globalización se vienen firmando acuerdos bilaterales o entre bloques comerciales; esto aceleró la estandarización de normas y leyes no solo de tipo penal para proteger los negocios, sino comerciales y de información, estos hechos ponen en plena vigencia la homologación de las Normas Internacionales de Auditoría, las Normas Internacionales de Contabilidad y las Normas de Información Financiera, conocidas como las NIA's, NIC y NIIF adicionalmente están en pleno vigor leyes extraterritoriales como "USA Patriot", "Victory Act" y "Sarbanes-Oxley" y otras disposiciones que han sido emitidas por los diferentes Países.

Lo anterior, obliga a los auditores forenses a prepararse no solamente en el campo contable y financiero, sino en el campo jurídico y legal, para que en sus investigaciones abarquen el entorno global y no solo el local.

Además de estas leyes, también están las normas de aplicación y las recomendaciones "mandatorias" es decir tomando un modismo anglo "Mandatory" que en su traducción al español sería como decir "recomendaciones de uso y aplicación obligada". Estas recomendaciones están compiladas en el nuevo marco del "Gobierno Corporativo", el nuevo sistema de Control Interno C.O.S.O. ERM y el acuerdo Basilea II."[2]

Por lo anterior, es importante ver que la auditoria forense se puede aplicar a lo tecnológico, con el apoyo de otros profesionales en especial en el área de lo tecnológico. Con base a ello se hacen las siguientes apreciaciones.

2. Conceptos de tecnología.

Los diferentes autores lo definen así: *Methere*: Conocimiento aplicado a propósitos prácticos. *Dupree*: Define la tecnología como un sistema de información que conecta al homo sapiens con su ambiente. La finalidad de la tecnología seria la búsqueda de una verdad útil. *Falcott*. (desde la sociología): Señala que la tecnología es la capacidad socialmente organizada para controlar y alterar activamente objetos del ambiente físico en interés de algún deseo o necesidad humana. Sábato (desde la economía) conjunto ordenado de conocimientos necesarios para la producción y comercialización de bienes y servicios. *Gallbraith* (The new industrial state) La tecnología es la aplicación sistemática del conocimiento científico o de otro tipo de conocimiento organizado, a tareas practicas.

3. Concepto de tecnología

Resulta impresionante cómo la tecnología evoluciona con cada día que pasa. Y debido a esta evolución, su conceptualización resulta cada vez más rica y variada. Muchos han sido los autores que se han decidido a sentar las bases del término. Amplias y variadas han sido estas definiciones. La gran mayoría la describen y la analizan como un fenómeno científico-social. Otras caen en la disyuntiva de considerarla como una ciencia aplicada o tomarla como un proceso autónomo, más

[2] Cano, Miguel Antonio; Lugo, Danilo. La Auditoría en la Auditoría Forense, En: http://www.redcontable.com/modules.php?name=News&file=article&sid=1258

no independiente, respecto a la ciencia. Por otro lado, hay quienes afirman que es necesario diferenciarla muy bien de la técnica. Ésta, posee una connotación más artesanal, común, sin una profunda interrelación con el hecho científico, y que busca solucionar las situaciones concretas e inmediatas a las cuales se aplica. Mientras que la tecnología no puede obviar este aspecto intrínsecamente científico.

La tecnología no solamente invade toda la actividad industrial, sino que también participa profundamente en cualquier tipo de actividad humana, en todos los campos de actuación. El hombre, moderno utiliza en su comportamiento cotidiano y casi sin percibirlo una inmensa avalancha de contribuciones de la tecnología: el automóvil, el reloj, el teléfono, las comunicaciones, etc. A pesar de que existe conocimiento que no puede ser considerado conocimiento tecnológico.

4. Interrelación entre Ciencia y Tecnología

Es interesante ver cómo en nuestros días y a través del tiempo se ha hecho difícil diferenciar la tecnología de la ciencia. Son dos actividades únicas, separadas pero no divorciadas, con naturalezas muy específicas pero con una profunda e íntima interrelación. De manera general, la ciencia sería el "por qué conocer," el "por qué llegar más allá" y el "qué de las cosas y sus circunstancias"; una incansable búsqueda de la verdad. Mientras que la tecnología es el "cómo conocer", el "cómo aplicar" los conocimientos adquiridos para resolver soluciones, crear cosas, con el fin de elevar cada día más la calidad de vida del hombre. La tecnología moderna es predominantemente científica, ya que extrae sus fundamentos teóricos de la ciencia pura o básica.

Los significados de los términos ciencia y tecnología han variado significativamente de una generación a otra. Sin embargo, se encuentran más similitudes que diferencias entre ambos términos.

5. El papel social de la tecnología

Algunos historiadores científicos argumentan que la tecnología no es sólo una condición esencial para la civilización avanzada y muchas veces industrial, sino que también la velocidad del cambio tecnológico ha desarrollado su propio ímpetu en los últimos siglos. Las innovaciones parecen surgir a un ritmo que se incrementa en progresión geométrica, sin tener en cuenta los límites geográficos ni los sistemas políticos.

Lo siguiente, podría aclarar un poco la diferencia entre la ciencia y la tecnología, en cuanto al medio social en el cual se desarrollan: Las comunidades

que las sustentan, tienden a valorar tanto el "conocer" como el "hacer". Es por ello que el auditorio de la ciencia tiende a constituirse por científicos investigadores, mientras que el auditorio principal de la tecnología no está compuesto por investigadores netos sino por quienes buscan resultados de utilidad práctica.

6. Historia de las telecomunicaciones

Las telecomunicaciones se encargan del transporte de la información a grandes distancias a través de un medio o canal de comunicación por medio de señales.
La misión de las telecomunicaciones es transportar la mayor cantidad de información en el menor tiempo de una manera segura. Eso se logra por medio de varias técnicas tales como la Modulación, codificación**,** Compresión, Formateo, Multicanalización, Esparciendo el espectro, etc.

7. Ventajas y desventajas de la tecnología

En el siglo XX los logros tecnológicos fueron insuperables, con un ritmo de desarrollo mucho mayor que en periodos anteriores. La invención del automóvil, la radio, la televisión y teléfono revolucionó el modo de vida y de trabajo de muchos millones de personas. Las dos áreas de mayor avance han sido la tecnología médica, que ha proporcionado los medios para diagnosticar y vencer muchas enfermedades mortales, y la exploración del espacio, donde se ha producido el logro tecnológico más espectacular del siglo: por primera vez los hombres consiguieron abandonar y regresar a la biosfera terrestre.

Durante las últimas décadas, algunos observadores han comenzado a advertir sobre algunos resultados de la tecnología que también poseen aspectos destructivos y perjudiciales.

8. Caracterización del delincuente informático

Para algunos autores, el sujeto activo de estos delitos se encuentra conformado por un grupo de personas con una inteligencia y educación que superan el común con vastos conocimientos informáticos. Es cierto que si analizamos los casos más celebres nos encontraremos con personas dotadas de altos conocimientos de informática y tecnología. Valga como ejemplo el caso de Kevin Mitnick, quien ha pasad más de la mitad de su vida defraudando mediante ordenadores. O el caso de Roberto Morris, estudiante de informática de la Universidad de Cornell cuyo Padera era un experto en seguridad del gobierno.
Pero es un mito que el delincuente informático deba forzosamente poseer conocimientos profundos en la materia. A nuestro juicio la computación se halla tan

extendida hoy día que cualquier persona que posea conocimientos mínimos de informática y tenga acceso a un ordenador, incluso desde su casa. Puede realizar delito informático.

En 1994, en su informe al Congreso de los Estados Unidos, la oficina de Asesoramiento Tecnológico del gobierno de ese país opinaba que las redes informáticas hacen de cada usuario básicamente un incidir con el potencia para asestar un golpe letal a lo sistemas de información. D e allí las medidas de seguridad informática que se suelen tomar dentro de la empresa como ser la existencia de passwords, tarjetas magnéticas o con microchips de acceso al sistema e incluso reconocimiento de características físicas de un individuo.
A partir de la experiencia comparada e incluso la nacional, encontramos los siguientes grupos:

Clase de delito	***Sujetos***
Delitos patrimoniales contra bancos y entidades financieras.	Empleados, en especial cajero o personal del área de sistema, ex - empleados.
Delitos de acceso ilegitimo o delitos de daños menores	Hackers, phreakers, usuarios descontentos
Daño o sabotaje informativo	Empleados de la empresa, o espías profesionales o industriales
Violaciones a la privacidad, tratamiento ilícito de datos personales.	Investigadores privados, Empresas de marketing, agencias de informes crediticios y de solvencia patrimonial
Violaciones a la propiedad intelectual del software y bancos de datos, con informes o compilaciones de datos.	Piratas informáticos o también usuarios (la copia amigable), empresas que realizan competencia parasitaria.

En definitiva, nos inclinamos por considerar que el delincuente informático no tiene necesariamente profundos conocimientos de computación, sino que es inducido a delinquir por la oportunidad que se le presenta frente al uso diario del ordenador y la impunidad que éste le brinda, o por los conocimientos que éste tiene frente al resto del personal.

9. Tipos de fraude en el área tecnológica

Suele ser un programa pequeño alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece

realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o anti troyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

9.1. Troyanos. Los troyanos de conexión directa son aquellos que el cliente se conecta al servidor. Una bomba lógica es un programa informático que se instala en un ordenador y permanece oculto hasta cumplirse una o más condiciones pre-programadas para entonces ejecutar una acción. A diferencia de un virus, una bomba lógica jamás se reproduce por sí sola.

Ejemplos de condiciones predeterminadas:

- Día de la semana concreto.
- Hora concreta.
- Pulsación de una tecla o una secuencia de teclas concreta.
- Levantamiento de un interfaz de red concreto.

Ejemplos de acciones:

- Borrar la información del disco duro.
- Mostrar un mensaje.
- Reproducir una canción.
- Enviar un correo electrónico.

9.2. Programas espías o de conexión directa. Son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.
Los programas espía pueden ser instalados en un ordenador mediante un virus, un troyano_(informática) que se distribuye por correo electrónico, como el programa Magic Lantern desarrollado por el FBI, o bien puede estar oculto en la instalación de un programa aparentemente inocuo.

Los cookies son un conocido mecanismo que almacena información sobre un usuario de internet en su propio ordenador, y se suelen emplear para asignar a los visitantes de un sitio de internet un número de identificación individual para su reconocimiento subsiguiente. Sin embargo, la existencia de los cookies y su uso generalmente no están ocultos al usuario, quien puede desactivar el acceso a la

información de los cookies. Sin embargo, dado que un sitio Web puede emplear un identificador cookie para construir un perfil del usuario y éste no conoce la información que se añade a este perfil, se puede considerar a los cookies una forma de spyware. Por ejemplo, una página con motor de búsqueda puede asignar un número de identificación individual al usuario la primera vez que visita la página, y puede almacenar todos sus términos de búsqueda en una base de datos con su número de identificación como clave en todas sus próximas visitas (hasta que el cookie expira o se borra).

Se trata de un programa que marca un número de tarificación adicional (NTA) usando el módem, estos NTA son números cuyo coste es superior al de una llamada nacional. Estos marcadores se suelen descargar tanto con autorización del usuario (utilizando pop-ups poco claros) como automáticamente. Además pueden ser programas ejecutables o ActiveX (Estos programas sólo funcionan en Internet Explorer).

Los marcadores telefónicos son legítimos siempre y cuando no incurran en las malas artes que los han definido como Malware que son los siguientes trucos:

1. No se avisa de su instalación en la página que lo suministra.
2. Hace una re-conexión a Internet sin previo aviso, o lo intenta.
3. Se instala silenciosamente en el ordenador utilizando vulnerabilidades del navegador, programa de correo electrónico, otros programas de acceso a Internet o el propio sistema operativo.
4. Puede dejar un acceso directo al escritorio sin conocimiento del usuario.
5. Puede instalarse unido a otros programas como barras de mejora para el navegador.
6. No informa de los costes de conexión. Afortunadamente hay varios programas que pueden detectar y eliminar los dialers, entre ellos la mayoría de los antivirus actuales, sin olvidar los programas gratuitos que podemos encontrar en los enlaces que se pueden encontrar en esta misma página.

Un ***cracker*** es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.

El término deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al término hacker, en defensa de estos últimos por el uso incorrecto del término.
Se considera que la actividad de esta clase de *cracker* es dañina e ilegal.

También se denomina *cracker* a quien diseña o programa *cracks* informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo. Esta acepción está más cercana al concepto de *hacker* en cuanto al interés por entender el funcionamiento del programa o hardware, y la adecuación a sus necesidades particulares, generalmente desarrolladas mediante ingeniería inversa.
No puede considerarse que la actividad de esta clase de cracker sea ilegal si ha obtenido el software o hardware legítimamente, aunque la distribución de los *cracks* pudiera serlo.

El cracker también es una persona de amplios conocimientos como el hacker pero éste los utiliza para su bien o el bien de todos, por ejemplo se podría representar como un Robbin Hood, que altera programas para el uso público y que sean gratis.

Por ello los crackers son temidos y criticados por la mayoría de hackers, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos (Haffner y Markoff, 1995). Pueden considerarse un subgrupo marginal de la comunidad de hackers.

Otros crackers, más sofisticados, penetran en sistemas informáticos para desafiar personalmente a los poderes establecidos, por ejemplo, a la empresa Microsoft o las grandes empresas. Y algunos utilizan su capacidad tecnológica como forma de protesta social o política, como expresión de su crítica al orden establecido. Ellos son quienes se introducen en sistemas militares, administraciones públicas, bancos o empresas para reprocharles alguna fechoría. Entre los ataques de crackers con motivación política hay que situar los practicados por movimientos políticos o por servicios de inteligencia de los gobiernos, como la guerra informática desarrollada entre los crackers islámicos e israelíes o entre los pro-chechenos y los servicios rusos.

10. Fraudes en la telecomunicaciones

- Fraude de suscripción
- Clonación de servicios
- Call Back
- By pass

11. Tipos de transacciones

Son formas de utilización y pago con tarjeta en los cajeros y establecimientos afiliados en donde se acude a la utilización de diferentes dispositivos como Data fono Inteligente, y Maquina Imprinter.

- Transacciones manuales
- Transacciones electrónicas
- Transacciones sin la presencia del plástico.
- Tarjeta hurtada o extraviada
- Utilización indebida (autoría del tarjeta habiente).
- Tarjeta emitida con documentos falsos
- Suplantación del tarjeta habiente en el retiro del plástico
- Doble facturación
- Fraude con tarjeta antes de ser entregada al titular
- Fraude con tarjeta después de ser devuelta por el titular.
- Fraude realizado con tarjeta alterada
- Tarjeta alterada en el realce
- Tarjeta alterada en la banda magnética
- Fraude realizado con tarjeta integralmente falsa
- Fraude por internet y telemercadeo

Para efectuar una transacción por Internet con cargo a una tarjeta de crédito se necesitan un computador y la información básica de una tarjeta de crédito (nombre del titular y número de tarjeta).

12. Formas de operar de los delincuentes

- Consecución de información privilegiada (mínima) de tarjetas de crédito (nombre del titular y número de tarjeta); la cual puede ser obtenida a través de los comercios, tarjeta habiente, proveedores, entidades financieras o sistemas.
- Con la utilización de programas de computador utilizan algunos bines de entidades financieras para crear números de tarjetas, las cuales son probadas posteriormente hasta que obtengan una que se encuentra emitida por la entidad la que es afectada con operaciones fraudulentas.
- Ubicación y acceso a tiendas virtuales.
- Realización de la compra, suministrando el número de la tarjeta, el nombre de titular, el número de cuotas, la fecha de vencimiento y a dirección de entrega.
- Recepción de la mercancía:
    - Los delincuentes alquilan un inmueble por espacio de tiempo corto para recibir la mercancía y luego desaparecen.

- Cuando las compras son hechas en páginas virtuales de comercios ubicados en el exterior, los delincuentes suministran direcciones que no existen, ya que la mercancía no está destinada a salir del país de origen.
- La mercancía es recibida por un encargado a la entrada de conjuntos residenciales, edificios de apartamentos, parqueaderos, tiendas de barrio y oficinas de apuestas u otros establecimientos públicos pequeños en los cuales la persona que recibe señala no conocer al destinatario.
- En algunas ocasiones el receptor de la mercancía es el estafador quien se hace pasar por otra persona y de esta manera intenta evadir su participación en el ilícito argumentado ser un tercero de buena fe.
- La dirección de entrega no existe sin embargo cuando la empresa que entrega recorre el lugar es abordado por una persona que le indica que el sector sufrió un cambio de nomenclatura y que él es el receptor de los artículos.
- La entrega de la mercancía se hace directamente en las oficinas de la empresa de mensajería que transporta el artículo y una persona con el número de guía lo reclama en el lugar.

13. Casos internacionales

Transferencia de fondos a otras cuentas: Vladimir Levin, un graduado en matemáticas de la Universidad Tecnológica de San Petersburgo, Rusia, fue acusado de ser la mente maestra de una serie de fraudes tecnológicos que le permitieron a él y la banda que conformaba, substraer más de 10 millones de dólares, de cuentas corporativas del Citibank.

En 1995 fue arrestado por la Interpol, en el aeropuerto de Heathrow, Inglaterra, y luego extraditado a los Estados Unidos.

Las investigaciones establecieron que desde su computadora instalada en la empresa AO Saturn, de San Petersburgo, donde trabajaba, Levin irrumpió en las cuentas del Citibank de New York y transfirió los fondos a cuentas abiertas en Finlandia, Israel y en el Bank of América de San Francisco.

Ante las evidencias y manifestaciones de sus co-inculpados, Vladimir Levin se declaró culpable. Uno de sus cómplices, Alexei Lashmanov, de 28 años, en Agosto de 1994 había hecho alarde entre sus conocidos, en San Petersburgo, acerca de sus abultadas cuentas bancarias personales en Tel Aviv, Israel.

Otros tres cómplices, entre ellos una mujer, también se declararon culpables. Esta última fue descubierta "in fraganti" cuando intentaba retirar dinero de una

cuenta de un banco de San Francisco. Se estima en un total de 10.7 millones de dólares el monto substraído por esta banda.

Las investigaciones y el proceso tuvieron muchas implicancias que no pudieron ser aclaradas ni siquiera por los responsables de la seguridad del sistema de Administración de Dinero en Efectivo, del propio CITIBANK. Jamás se descartó la sospecha de participación de más de un empleado del propio banco.

A pesar de que la banda substrajo más de 10 millones de dólares al CITIBANK, Levin fue sentenciado a 3 años de prisión y a pagar la suma de US $ 240,015 a favor del CITIBANK.

CONCLUSIONES

El control organizacional es una herramienta básica que sirve para el cuidado, la protección, el seguimiento, el sostenimiento, y el aseguramiento de los recursos humanos, financieros y físicos de una compañía.

Es importante el llevar a cabo las pruebas de cumplimiento, la eficiencia y la efectividad de los procesos de la compañía con el fin de implementar las prácticas y políticas de control adecuadas para revisar constantemente las conciliaciones de saldos de bancos, clientes, proveedores, acreedores, vinculados entre otras.

Los Contadores Públicos, cómo únicos profesionales garantes de la fe pública, debemos conocer los diferentes fraudes que se pueden cometer en una compañía para que en el momento de dictaminar los estados financieros, tengan la seguridad que los procedimientos de auditoría aplicados sean los suficientemente efectivos para evitar los fraudes en una compañía.

A medida que las empresas crecen, sus operaciones aumentan, creándose la necesidad de implementar medios de control que permitan ejercer una completa y adecuada vigilancia sobre el desarrollo de las operaciones; y es en este aspecto en el que la Auditoria auxilia en forma definitiva a las empresas.

La Auditoria es un instrumento eficaz e idóneo para llevar a cabo el ejercicio de una adecuada vigilancia.

La Criminalística contribuye a la solución de todo tipo de casos criminales, por su profundo estudio técnico y aplicación de las diferentes ramas de la ciencia.

La auditoria forense es especializada en descubrir, divulgar y atestar sobre fraude en el sector público y privado como apoyo legal a la JUSTICIA, se enfoca en la prevención y detección del fraude financiero.

El autor de los delitos informáticos difícilmente, es descubierto y por ende sancionado, existe una indiferencia en la opinión pública sobre los daños ocasionados en la sociedad, debido a que esta no los considera delincuentes, no los segrega, no los desprecia ni desvaloriza, por el contrario el autor se considera respetable, y generalmente las sanciones son medidas de carácter administrativo y no privativas de la libertad.

Las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras, lo que ha generado la necesidad de la tipificación de nuevas conductas en el ámbito penal para la regulación y control de las mismas.

Se necesita de habilidades y conocimientos profundos en materia jurídica, investigativa, contable y que faciliten obtener las pruebas convincentes que requiere la justicia para sus sentencias ante delitos económicos y financieros, como la corrupción administrativa, el fraude corporativo y el lavado de dinero y activos, blanqueo y legitimación de capitales entre otros.

BIBLIOGRAFÍA

- PEÑA BERMUDEZ, Jesús María, Control, Auditoria, y Revisoría Fiscal.
- ZOLTHERS, Greg, La firma obesa.
- CANO, Miguel, LUGO, Danilo, Auditoria Forense en la investigación criminal del lavado de dinero y activos.
- CANO, Miguel y LUGO, Danilo AUDITORIA FORENSE en la Investigación Criminal del lavado de dinero y activos. Bogotá D.C. 2006. En: http://www.mincomercio.gov.co/eContent/NewsDetail.asp?ID=4590.
- CERNA APAZA, Luis Alfonso. Norma internacional de auditoría fraude y error Universidad Nacional de tumbes Facultad de ciencias económicas. En: http://www.monografias.com/trabajos11/fraer/fraer.shtml.
- ENCICLOPEDIA, Wikipedia, Definiciones de: Fraude - Auditoria – Error En: http://www.wikipedia.org/wiki/Fraude.
- MICROSOFT CORPORATION, Enciclopedia Encarta 2007, Definiciones de: dolo, delito, fraude.
- Lugo, Danilo. Auditoria Forense Una Perspectiva De Investigación Científica En: http://www.interamericanusa.com/articulos/Auditoria/Audt-For-Art.htm.
- El Perfil Profesional del Auditor Forense En: http://auditoriaforense.net/index2.php?option=com_content&do_pdf=1&id=.

- CAMARGO, NELSON. Breve Historia de la Auditoría Forense, En: http://www.redcontable.com/modules.php?name=News&file=article&sid=251.
- SUPERINTENDENCIA FINANCIERA DE DE COLOMBIA. En http://www.superfinanciera.gov.co/ SARLAFT.
- PERIODICO EL TIEMPO En http://www.eltiempo.com.
- Una perspectiva de investigación científica. En http://www.interamericanusa.com.
- MARTINEZ LÓPEZ Mario, Aprendamos Jugando con las Ciencias, 1998, Tomo II p. 62-80 Editorial del Valle México de C.V.
- SALGADO, Manuel B. Delincuentes Informáticos, 2007, En: hppt://www,monografías.com.
- ZUCKERMANN, JOHN, Revistas Hacker, Todas las distribuciones. 2004 En: http://www.dragonjar.us/revistas-hacker-todas-las-distribuciones.xhtml.
- LONDOÑO, Guillermo, Trabajo de Normatividad de Comercio Electrónico, Universidad Jorge Tadeo Lozano 2006.
- EL CONGRESO DE COLOMBIA, Ley 599 de 2000, Delitos Contra El Patrimonio Económico, titulo VII capítulo primero artículo 240, 2000.
- MASTERMAGAZINE, Publicación marzo 16 de 2006, En: http://www.mastermagazine.info/termino/4478.php.
- FERANDEZ DE SOTO, María Clara, Tesis de Grado, Atipicidad Relativa En Los Delitos de Falsedad, Hurto, Estafa, y daño informáticos, Universidad Sergio Arboleda, Santa Martha, 2004.
- QUIROGA, Milton. Especialización en Seguridad de la Información, Universidad de los Andes, 2007, En: http://sistemas.uniandes.edu.co.
- CANO Miguel A. Auditoria Forense, En: http://www.interamericanusa.com/articulos/Auditoria/Audi-fore-tec-inv.htm.