UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA, MANAGUA

UNAN-MANAGUA

FACULTAD DE CIENCIAS ECONÓMICAS

DEPARTAMENTO DE CONTADURÍA PÚBLICA Y FINANZAS

SEMINARIO DE GRADUACIÓN PARA OPTAR AL TÍTULO DE

LICENCIADO(A) EN CONTADURÍA PÚBLICA Y FINANZAS

TEMA: AUDITORÍA FORENSE

SUBTEMA: PREVENCIÓN DEL FRAUDE A TRAVÉS DEL USO DE LAS TECNOLOGÍAS

AUTORES: BR (A). HADA MARENA SEQUEIRA PÉREZ
BR. LEONEL ERMIDES PANIAGUA LÓPEZ

Tutor: Germán Moraga

2015

Dedicatoria

Nuestra tesis la dedicamos con mucho amor y cariño:

A Dios:
Dador de la vida y de toda sabiduría, por su amor entregado a través de nuestro señor Jesucristo.

A mi mamá:
Sra. Madre; Aurora María López Valle, por su apoyo, confianza y amor.

A mi Abuelita difunta, Sra. Pastora Pérez Kauffsman y Sra. Rosibel González Herrera, que en vida brindaron fuerzas para seguir adelante, su mayor deseo era tener una hija profesional.

A todos nuestros familiares:
Con especial cariño.

Agradecimientos

El presente trabajo de tesis primeramente nos gustaría agradecerle a nuestro Dios por habernos bendecido grandemente, para llegar hasta donde he llegado, porque hizo realidad este sueño anhelado.

A nuestra Alma Máter, Universidad Nacional Autónoma de Nicaragua, en especial a la Facultad de Ciencias Económicas, por darme la posibilidad de superación profesional.

De igual manera agradecer a nuestro profesor de Investigación y de Tesis de Grado, Lic. Germán Moraga, tutor académico, por su valiosa orientación y por facilitarnos las herramientas para la culminación de este trabajo.

Valoración del Tutor

Managua, Nicaragua, 10 de diciembre de 2014.

MsC. Álvaro Guido Quiroz
Director del Departamento de Contaduría Pública y Finanzas
Su Despacho.

Estimado Maestro Guido:

Remito a usted los ejemplares del Informe Final de Seminario de Graduación titulado con el tema: Auditoría Forense y el sub-tema “El uso de la tecnología para la detección del fraude”, presentado por el bachiller(a): Hada Marena Sequeira Pérez, carnet No. 10-20578-8 y Leonel Ermides Paniagua López, carnet no. 07-04552-2, para optar al título de Licenciado(a) en Contaduría Pública y Finanzas.

Este Informe Final reúne todos los requisitos metodológicos para el Informe de Seminario de Graduación que especifica la Normativa para las modalidades de Graduación como formas de culminación de estudios, Plan 1999, de la UNAN-Managua.

Solicito a usted fijar fecha de defensa según lo establecido para tales efectos.

Sin más que agregar al respecto, deseándole éxitos en sus funciones, aprovecho la ocasión para reiterar mis muestras de consideración y aprecio.

_____
Lic. Germán Antonio Moraga
Tutor
Seminario de Graduación II Semestre 2014

Resumen

El presente trabajo se basa en la importancia del uso de herramientas tecnológicas cuyos objetivos son lograr la detención de fraudes en las empresas reuniendo la mayor cantidad de pruebas e información valiosa sin estar presentes físicamente. La necesidad de medios tecnológicos en una auditoria surge para minimizar los riesgos donde los protagonistas son los responsables de los departamentos de Contabilidad, Informáticos, Auditores y así cumplir con el objetivo deseado.

La auditoría forense es una herramienta técnica cuyo propósito es prevenir, detectar, investigar y comprobar delitos de fraudes; mediante la obtención de pruebas tecnológicas que requiera la justicia para sus sentencias.

Dentro de las Tecnologías especializadas para Análisis de Datos y Auditoría se encuentra el Software IDEA que permite utilizar el potencial de los datos disponibles, para detectar indicios de fraude que luego generen rutinas y alertas a partir de los datos y la detección de parámetros. Para demostrar lo antes mencionado se presenta un caso práctico en donde se utiliza la Ley de Benford, la escena del evento involucra a la computadora, de ahí su vinculación con la tecnología.

TEMA GENERAL:
AUDITORÍA FORENSE

SUBTEMA:
PREVENCIÓN DEL FRAUDE A TRAVÉS DEL USO DE LAS TECNOLOGÍAS

Índice General

Índice de Tablas

Pág.

Índice de Figuras

Pág.

I. Introducción

La presente investigación ha sido desarrollada con el objetivo de establecer un análisis de la Auditoria Forense como un método de prevención de fraude, partiendo desde conceptos básicos y herramientas tecnológicas que utiliza esta nueva rama de la auditoria para la detección, prevención y seguimiento de delitos financieros, los mismos que se han incrementado cada año.

Una vez comprendido y estudiado los conceptos de la auditoria forense se presentan algunas de las evidencias necesarias para enfrentar los delitos cometidos por funcionarios y empleados del sector público y privado, de esta forma se puede controlar los múltiples fraudes cometidos en perjuicio de las empresas o instituciones.

Por otra parte los profesionales con conocimientos en auditoría forense están obligados a presentar las más altas normas de conducta ya que representan a la empresa caracterizándose por custodiar los recursos y bienes de la sociedad frente al fraude y las acciones ilícitas y así mismo mejorar la responsabilidad empresarial.

Con el creciente uso de la tecnología es más probable el uso de la misma para realizar fraude al igual que para detectarlo. Pero también con el uso de tecnología y software interactivo pueden ayudar a los auditores a tener mayor precisión en las áreas de alto riesgo, dejando por fuera las transacciones de menor riesgo.

De la situación antes planteada, se determina la importancia del tema de investigación que tiene como propósito analizar la importancia que tiene el uso de la tecnología en la detención de fraudes como un proceso de control e investigación. Para el análisis del objetivo planteado el presente trabajo se encuentra estructurado de la siguiente manera: El primer acápites, comprende todo lo relacionado con la definición, objetivos, reseña histórica, características, causas y criterios de aplicación de lo que es Auditoria Forense que sustentan la investigación.

Luego en el segundo acápite, se abarcan los aspectos legales del delito, tipos de sujetos, requerimientos, preparación e investigación de una auditoría forense. El tercer acápites, contiene los aspectos generales del fraude en las empresas, concepto y definiciones, naturaleza del fraude entre otros puntos.

El cuarto acápites, se define el marco integrado al control interno (Coso), también el principio 8 y principio 11 del mismo. El quinto acápites, se presenta el análisis del fraude mediante la implementación de la tecnología, así como las herramientas y hábitos de seguridad para prevenir el fraude, la metodología para un plan de acción global contra el fraude, el control interno al proceso de aseguramiento continuo, la forma de crear y mantener una política sobre fraude, los principales indicios de fraude y las medidas preventivas de monitoreo para evitar el fraude.

En el sexto acápite, se aborda la oferta técnica y analítica de los softwares, un análisis digitalizado a la ley de Benford, los antecedentes y utilización de la Ley de Benford que se usó en el caso práctico. Finalmente en el séptimo acápite se muestra el anexo que complementa la investigación y por último el inicio, desarrollo y finalización de la auditoria forense, representándose con un caso práctico basado en el uso del software IDEA, asimismo se presenta las conclusiones, bibliografía ya anexos relacionados con el tema expuesto.

II. Justificación

Debido a la necesidad de disminuir los fraudes en las empresas, resulta necesario desarrollar procesos y procedimientos contables, con ayuda de profesionales responsables de los departamentos de Contabilidad y Auditoría e incluso del área de Informática como auxiliar (TI) con orientación a la detección y minimización de pérdidas, aportando experiencias y conocimientos a fin de eliminar este daño frecuente en beneficio de las PYMES y los Grupos Empresariales de Nicaragua. El implementar el uso de las Tecnologías del Siglo XXI permite localizar el área donde posiblemente hay fraude, dando como resultado una protección oportuna y a su vez la prevención adecuada contra los hurtos y fraudes.

La razón de este trabajo es la de presentar una guía simplificada por medio de softwares, instrumentos emitidos por Instituciones Internacionales que como objetivos tienen ayudar a prevenir este tipo de problemática y proporcionar herramientas relacionadas al ambiente tecnológico acerca de cómo los profesionales deben participar en los procesos de detección y reducción de robos y fraudes empresariales, no sólo para detectarlos sino para prevenirlos, así como determinar los efectos que dichos robos y fraudes ocasionan y la asesoría que puede brindarse en el campo.

Todo descontrol interno es una invitación a la pérdida de activos, los cuales pueden ser efectuados a través de fraudes, en especial fraudes informatizados. Las empresas pueden sufrir pérdidas todos los años por no seguir las normas y recomendaciones de los Auditores.

Se pueden considerar esas pérdidas de varias formas: como la dispensa de un funcionario que ya conoce las rutinas internas; Software´s piratas que generan fallas a los aparatos; robo o pérdidas de informaciones confidenciales.

La tecnología de la información ha evolucionado rápidamente. El tiempo y los medios disponibles se desarrollan día a día, esta evolución conlleva experiencias y procesos de negocios que están siendo guardados en software y hardware, los cuales poseen una gran capacidad de almacenamiento de datos e informaciones que pueden ser acusadas de forma irregular (fraude) por personas de la propia organización, generando así la pérdida de activos intangibles. Los posibles defraudadores pueden ser motivados por diversas formas de cometer el crimen, entre ellas, la satisfacción financiera y la satisfacción psicológica.

III. Objetivos

Objetivo General

- Determinar la importancia de la aplicación de las Tecnologías para prevenir/detectar los fraudes cometidos en las empresas.

Objetivo Específico

- Brindar una herramienta de investigación al estudiante de contaduría sobre el fraude y que en un futuro ayude por medio de sus conocimientos de la profesión identificar los responsables e informar a las entidades competentes las evidencias detectadas.

- Identificar las áreas vulnerables a través de pruebas y evidencias válidas que serán presentadas a la empresa para que puedan tomar decisiones que les permitan prevenir y manejar los riesgos de fraude.

- Demostrar mediante un caso práctico como el uso de los Softwares son un medio tecnológico que ayudan en la detención de fraudes en las empresas.

IV. Desarrollo del subtema

4.1 Auditoría Forense

4.1.1 definición de auditoría forense.

> El asunto medular de la Auditoría Forense corresponde al latín forensis, que significa público y su origen del latín forum que significa foro, plaza pública donde se trataban las asambleas públicas y los juicios; por extensión, sitio en que los tribunales oyen y determinan las causas; por lo tanto, lo forense se vincula con lo relativo al derecho y la aplicación de la ley, en la medida en que se busca que un profesional idóneo asista al juez en asuntos legales que le competan y para ello aporte pruebas de carácter público para presentar en el foro, y hoy en la actualidad en la corte, (según Ruette, R. J. 2006)

La auditoría forense es una disciplina especializada que requiere un conocimiento experto en teorías contables, auditoría, técnicas de investigación criminal. Es una rama importante de contabilidad investigativa, utilizada en la reconstrucción de hechos financieros, investigaciones de fraudes, cálculos de daños económicos y rendimientos de proyecciones financieras. La relación entre los términos contables y de auditoría con lo forense se hace estrecha cuando se habla de pruebas y evidencias de tipo penal, por lo tanto, 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.

"Una herramienta de control de la corrupción en entes gubernamentales, la preservación del patrimonio público, y el papel de la contabilidad en la lucha contra la

corrupción en los entes gubernamentales". De acuerdo a Edilma, M. (2006). Obtenido de http://www.ideaf.org.html, (Recuperado el 25-10-2014 5:05 pm),

La Auditoria Forense es: "una técnica de gran utilidad y colaboración para la investigación de cuerpos de abogados, departamentos de investigación policial, fiscal y judicial permitiendo esclarecer posibles actos ilícitos o delitos". Según Fontan, M. (s.f.). Foro de seguridad. Obtenido de http://www.forodeseguridad.com/ artic/discipl/ 4166.htm (recuperado el 12/10/2014 10:25 am).

> La labor del auditor es procurar prevenir y estudiar hechos de corrupción. Como la mayoría de los resultados del Auditor van a conocimiento de los jueces (especialmente penales), es usual el término forense. Como es muy extensa la lista de hechos de corrupción conviene señalar que la Auditoría Forense, para profesionales con formación de Contador Público, debe orientarse a la investigación de actos dolosos en el nivel financiero de una empresa, el gobierno o cualquier organización que maneje recursos. (Obtenido de http://www.forodeseguridad.com /artic/discipl/ 4166.html, recuperado el 12/10/2014 10:51 am)

La auditoría forense es aquella labor de auditoría que se enfoca en la prevención y detección del fraude financiero; por ello, generalmente los resultados del trabajo del auditor forense son puestos a consideración de la justicia, que se encargará de analizar, juzgar y sentenciar los delitos cometidos (corrupción financiera, pública o privada).

Y por último, Vega, C. (s.f.). Obtenido de http://www.forodeseguridad.com/artic /discipl/ 4166.htm (Recuperado el 12/10/2014 10:50 am), indica que la auditoría forense es:

La exploración o examen crítico de las actividades, operaciones y hechos económicos, mediante la utilización de procedimientos técnicos de La auditoría forense es una ciencia que permite reunir y presentar información contable, financiera, legal, administrativa e impositiva, que provee de un análisis contable que será aceptado por la corte, ya que formará parte de las bases de la discusión, el debate y finalmente el dictamen de la sentencia contra los perpetradores de un crimen económico.

En el mismo orden de ideas la auditoría forense por lo expuesto es una auditoría especializada que se enfoca en la prevención y detección del fraude financiero a través de los siguientes enfoques: preventivo y detectable, de acuerdo a comentarios anteriores se dice que esta sirve para analizar el fenómeno del fraude no solo en su fase de detección sino también en el estudio de la consumación y consecuencia en la empresa.

4.1.2 objetivos de la auditoría forense.

El objetivo principal de la auditoría forense según Milton, K., & Maldonado, E. (2008). "Es hacer relación a la aplicación del análisis de hechos financieros a problemas legales, asistiendo a las compañías en la identificación de las áreas claves de vulnerabilidad e implicarse en las investigaciones y en los procedimientos legales".

Dentro de los objetivos que una auditoría forense cubre, se pueden mencionar los siguientes:

- Determinar la confiabilidad de la información gerencial para la toma de decisiones.

- Salvaguardar recursos financieros, tecnológicos, etc.

- Descubrir y divulgar irregularidades y desviaciones.

- Examinar y evaluar el sistema de control interno y las estrategias que se siguen para administrar riesgos.

A como expresan ambos autores se razona que la incorporación de conocimientos y la aplicación de novedosas y probadas técnicas forenses, herramientas de Tecnología de la Información (TI), así como otras especialidades distintas de las ramas financieras, como son las legales, psicológicas y criminológicas, con el propósito de crear un nuevo perfil de profesional capaz de detectar de manera oportuna fraudes y delitos.

4.1.3 historia y causas de la auditoría forense.

Según Bardale, J. (2007). La auditoría ante la corrupción. Alternativa financiera, asevera que:

> La corrupción es una de las principales causas del deterioro del patrimonio público. La auditoría forense es una herramienta para combatir este flagelo. La auditoría forense es una alternativa, 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, especial mente en lo relativo a la vigilancia de la gestión fiscal (p27-30).

La auditoría existe desde hace mucho tiempo, hoy su protagonismo es indudable y la comunidad entera reconoce la importancia del papel que juega en la sociedad y del largo camino que aún hay por recorrer, uno de estos caminos es la auditoría forense de la cual su origen no es claro, pero se habla que ésta puede ser tan antigua que nace cuando se vincula lo legal con los registros y pruebas contables.

Con lo cual la fiscalía pudo demostrar fraude en el pago de impuestos en Al Capone y en sus lavadores, desmantelando la organización. Pero en esta época tampoco se dio el impulso suficiente a esta rama de las ciencias contables el cual fue diferido hasta los años 70 y 80; cuando con el caso Watergate en 1972 se dio inicio al análisis del fraude en los estados financieros, tan pronto como este escándalo salió a la luz, fueron reveladas una serie de actividades ilegales paralelas que dieron como resultado la dimisión del presidente Richard

Nixon y la formulación de una acusación contra el presidente o algún alto funcionario del gobierno de Estados Unidos.

En los últimos años las quiebras fraudulentas y escándalos contables en Estados Unidos, como ejemplos el caso Enron, WorldCom y Tyco, dieron como resultado que la comisión de valores de los Estados Unidos SEC investigara a cientos de empresas, y que dentro de ésta se creara un organismo para supervisar los aspectos contables y de conflictos de interés.

La auditoría forense entonces surge con los intentos de detectar y corregir los fraudes en los estados financieros, su función inicial es estrictamente económico-financiera, y los casos inmediatos se encuentran en las peritaciones judiciales y las contrataciones de contables expertos por parte de bancos oficiales; actualmente ha ampliado su campo de acción en la medida que ha desarrollado técnicas específicas para combatir el delito y trabajar estrechamente con la aplicación de justicia.

4.1.4 características de la auditoría forense.

Esta disciplina es de carácter penal debido a su génesis de orden procesal y penal, porque está considerada en el marco de las disciplinas auxiliares penales y porque su aplicación científica contribuye para conocer los hechos y llegar a las penalidades determinadas por los jueces. La auditoría forense, investiga, analiza, evalúa, interpreta, y con base en ello testifica y persuade a jueces, jurados y a otros acerca de la información financiera sobre la cual existe una presunción de delito, por lo tanto:

- Se analiza la información en forma exhaustiva.
- Se piensa con creatividad.
- Debe poseer un sentido común de los negocios.
- Domina los elementos básicos del procesamiento electrónico de datos y tiene excelente capacidad de comunicación.
- Debe tener completa discreción, amplia experiencia y absoluta confianza.
- Conocedor de temas contables, de auditoría, criminología, de investigación y legales.

Para el grupo consultor Safe Consulting Group. (2006). Fraude: Un nuevo enfoque para combatirlo. Auditoría Pública (38), Obtenido de http://www.ideaf.org (recuperado el 28-0-2014 10:50 am)

> El examen que se realiza con la auditoría forense va más allá de efectuar averiguaciones comunes a una auditoría tradicional, toda vez que investiga situaciones muy complejas y comprometedoras, por ejemplo el fraude en una entidad, el robo de activos, etc.; además que abarca áreas tan variadas como lo son la contabilidad, auditoría, derecho, criminalística, pero que en materia penal resultan ser complementarias (p.101-103).

Así como lo expresa el grupo consultor, las características de la auditoría forense, tanto los contadores como auditores tienen que tener grandes aptitudes frente a un campo de acción profesional interesante, donde se convierten en baluartes de los bienes de la sociedad común, frente a las actividades de terrorismo, fraude y corrupción.

Las características de la auditoria forense se hacen con el propósito de recabar información. Buscan sonsacar información objetiva e imparcial. Un buen entrevistador estará alerta en cuanto a inconsistencias en los hechos o comportamiento. Existen tipos generales de preguntas que se pueden hacer: Abiertas, Cerradas y que insinúan la respuesta.

4.1.5 características de validación para iniciar una auditoría forense.

Una auditoría forense, la ordena un juez, en primera instancia, o un Gran Jurado como se acostumbra en Estados Unidos de América, pero como la ley o el procedimiento legal

cambia de país en país, quizás haya países en donde es el Ministerio Público o la Procuraduría de Instituciones que toman la iniciativa de adelantar investigaciones preliminares para evaluar el caso antes de llevarlo ante un tribunal judicial. En el medio local es el Ministerio Público o el tribunal el que puede ordenar una peritación a pedido de parte o de oficio, cuando es necesario obtener, valorar o explicar un elemento de prueba y es pertinente que una persona con conocimientos especiales en alguna ciencia, arte, técnica u oficio la realice.

Primero tiene que haber una denuncia o una sospecha con fundamento para iniciar una investigación, la cual puede ser por escrito u oralmente y se presenta ante la policía, el Ministerio Público o a un tribunal el conocimiento que se tiene acerca de la comisión del delito. Ninguna institución podría arriesgarse a investigar sin bases suficientes, pues estaría violando la privacidad de las personas y allanando propiedades privadas.

Por supuesto que no se puede avisar a los cuatro vientos que se va a iniciar una investigación interna de una entidad, pero si se tienen que tomar todas las medidas legales para proteger el debido proceso. Normalmente hay una denuncia, de alguien que conoce un hecho doloso, sea parte de la entidad, empresa o institución. Otra fuente de la denuncia puede ser una víctima que ha sufrido pérdidas, maltrato, humillación, o un cliente insatisfecho que tiene sospechas que se está cometiendo un acto ilícito. Otras justificaciones son por parte de los socios que desconfían de sus asociados y ponen una denuncia penal por fraude, estafa, abuso de confianza y un sinnúmero de posibles delitos en contra de su patrimonio.

4.1.6 características de ejecución legal para realización de auditoría forense.

Después que se emite un nombramiento a través de una orden judicial para adelantar una investigación, el director de investigaciones del Ministerio Público, la Procuraduría, la policía según sea el país y la jurisdicción que corresponda, nombra un equipo y planifica el trabajo, la logística y la metodología a seguir, el tipo de profesionales que se necesitan, los técnicos y expertos de acuerdo a la dimensión y características del ente a investigar.

Basados en esta orden judicial, se presentan los investigadores con un documento llamado "orden de allanamiento" o también puede ser una "orden de confiscación. Si se trata de una empresa y la investigación se centra en un solo departamento, entonces quizás lo más probable es que se confisquen los equipos como computadores y documentos de archivo comprometidos, y estos sean trasladados al sitio que designe el director de la investigación, además del sellamiento de las oficinas en que se va a llevar cabo la investigación, mientras que la planta de producción puede seguir su curso normal para no perjudicar a los obreros.

Si existen órdenes de arresto, de inmediato se efectúan las capturas con la colaboración de la policía y detectives asignados. Todavía no están en función los auditores forenses, y aunque tenga la investidura oficial, se considera un civil, con tareas de experto, opina Cano, M., & Rodríguez, J. (Enero de 2005).

4.1.7 criterios de aplicación para el análisis forense.

1) Para asegurar que la evidencia digital sea obtenida, preservada, examinada o transportada de forma segura y confiable, las organizaciones forenses han establecido un sistema de calidad eficaz mediante los Procedimientos de Funcionamiento Estándar (SOP), los cuales se conforman de protocolos documentados y aceptados para el tratamiento de la evidencia, equipo y materiales propios de la investigación.

2) Todas las agencias que obtienen y/o examinan evidencia digital deben mantener un uso apropiado del SOP. Las políticas y los procedimientos de una agencia referentes a evidencia digital se deben detallar claramente en el SOP, el cual deberá ser publicado bajo supervisión de la autoridad de la agencia o unidad investigadora.

3) La gerencia de la agencia debe revisar y, en su caso, actualizar los SOP anualmente, con la finalidad de mantener los procesos y procedimientos de tratado de evidencia paralelos a la evolución tecnológica.

4) Los procedimientos realizados en el tratamiento de evidencia deben estar sustentados con base en el método científico.

5) La agencia debe mantener archivos históricos de los procedimientos técnicos apropiados para cada caso de estudio.

6) La agencia debe utilizar el hardware y el software apropiados y eficaces para el

análisis específico a realizar.

7) Toda la actividad referente a la obtención, tratamiento, manejo, análisis y transporte de evidencia debe ser registrada y estar disponible para la revisión del testimonio.

8) Cualquier acción que tenga el potencial de alterar, dañar o destruir cualquier aspecto de la evidencia original debe realizarse por personas calificadas.

"Se encontró una opinión de dichos criterios que incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos." Intermerican. (s.f.). Obtenido de http:// interame rican-usa.com/articulos/Auditoria/Audi-fore-tec-inv.html., (Recuperado el 30-10-2014 5:010 pm).

Como la definición anterior lo indica, esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido. El conocimiento del informático forense abarca el conocimiento no solamente del software sino también de hardware, redes, seguridad, hacking, cracking, recuperación de información.

Según aporta la NEPAI. (s.f.). Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna (Recuperado el 15-10-2014 9.56 am).

Adicionalmente, un examinador forense digital, dentro del proceso del cómputo forense puede llegar a recuperar información que haya sido borrada desde el sistema operativo. Es muy importante mencionar que la informática forense o cómputo forense no tiene parte preventiva, es decir, la informática forense no se encarga de prevenir delitos, de ello se encarga la seguridad informática, es importante tener claro el marco de actuación entre la informática forense.

4.1.8 atributos de un auditor forense.

Rojas, J. (s.f.). Técnicas de Auditoría Forense. Grant Thornton, indica que el autor forense debe poseer los conocimientos y habilidades que se detallan a continuación:

- Habilidades analíticas;
- Una mentalidad investigadora;
- Habilidades de mediación y negociación;
- Conocimiento de la evidencia;
- Una comprensión de motivación.
- Identificación de problemas financieros;
- Reconocimiento de riesgo y evaluación de controles;
- Creatividad para poder adaptarse a las nuevas situaciones.

En el desarrollo de una auditoría forense, en el examen y en la elaboración de los informes, se identifican además, las nuevas habilidades y competencias demandas a los auditores:

- Conocimiento del negocio, comprendiendo su funcionamiento y forma de planificar, administrar y controlar, anticipándose a la posibilidad de hechos fraudulentos.
- Conocimiento avanzado de tecnologías de información.
- Adopción de técnicas innovadoras de auditoría para prevenir hechos delictuosos.
- Desarrollar habilidades de investigación, en especial en los tipos de fraudes, delitos y operaciones ilícitas que se pueden cometer en las empresas y/o instituciones financieras.

Por otra parte (Maldonado, M., 2003), menciona que debe tener:

> Excelente salud, sereno, fuerte de carácter trabajador a presión seguro, personalidad bien formada, culto, de gran capacidad analítica y de investigación, paciente, intuitivo, perspicaz, frío y calculador, desconfiado, en el trabajo y con las personas a las cuales investiga honesto e insobornable, objetivo en independiente, imaginativo, poseer agilidad mental. Es muy importante señalar que esta auditoría produce un fuerte agotamiento físico y mental al auditor, en virtud de la presión, riesgo, dificultades en la obtención de evidencia y tiempo invertido, razón por la cual se requiere que tenga un poco de sentido del humor para que no se torne una persona amargada, en su vida personal y profesional. (p. 48-49)

Por otra parte Aditivo Fudim, A. (2003), expresa "que el auditor forense tiene que tener conocimientos y habilidades de una mentalidad investigadora, una comprensión de motivación, habilidades de comunicación, persuasión, mediación, negociación y sobre todo habilidades analíticas para poder adaptarse a las nuevas situaciones".

Conviniendo tanto con Maldonado como a Fudim, se comparte que para asegurar que el auditor forense alcance el grado de efectividad necesario, es preciso que quienes la

ejecuten, es decir los auditores forenses, estén debidamente capacitados, entrenados y que tengan la suficiente práctica en la materia, pues la misión trazada de frenar el crimen es de hecho proeza de titanes.

4.2 Aspectos Legales Del Delito

4.2.1 sujetos y objetos jurídicos de los delitos.

4.2.1.1 sujetos activos del delito.

Son todas las personas que participan de alguna manera en la realización del ilícito penal, ya sea por medio de una actividad o de una omisión, llamándoseles también procesados, reos enjuiciados o indagados. El estudio de las personas que se convierten en sujetos activos del delito, es de sumo interés, pues para los efectos de investigar la responsabilidad de quienes han cometido un ilícito, deben tomarse en cuenta las calidades del enjuiciado, como son: su grado de cultura, inteligencia ,educación, caldo social en que se ha desarrollado, etc. todo lo cual es importante, como sabemos trata de ahondar el conocimiento de todas las circunstancias que rodean los hechos ilícitos, a fin de se dicte sentencia de acuerdo a la equidad más pura.

Los sujetos activos de un delito pueden aparecer de diferentes maneras según su forma y grado de participación en el mismo; así tenemos que se puede intervenir en el hecho ilícito en calidad de autor, cómplices o encubridor, debiendo aclararse que en la autoría puede haber coautores en calidad de inductores, a los cuales comúnmente se les denomina autores intelectuales del injusto cometido.

4.2.1.2 sujetos pasivo del delito.

Se debe considerar como tal, a la persona o personas sobre quienes recae la ofensa, es decir la víctima que recibe el daño, ya sea en forma directa o indirecta. En muchos casos es difícil individualizar al sujeto pasivo del delito, pues en algunas oportunidades, los hechos delictivos producen daños a terceros, como podría ocurrir en el delito de Hurto, que a más de perjudicar al poseedor o dueño de la cosa hurtada, indirectamente también se perjudica al acreedor de éste.

Debemos estar claros que las consideraciones anteriores, no deben llevarnos a confusión entre los bienes tutelados, con las personas que puedan resultar perjudicadas, pudiéndose asegurar, que sujeto pasivo es el titular del interés cuya ofensa constituye la esencia del delito, lo cual puede recaer directamente en todos los individuos, sean o no capaces, lo mismo que en las personas jurídicas, inclusive el mismo Estado.

4.2.1.3 objeto jurídico del delito.

Se debe de entender como objeto jurídico del delito, el bien al que el Derecho otorga su protección, el cual se confunde o viene a ser la cosa que se persigue dañar. El bien jurídico puede serlo, tanto un objeto material mueble o inmueble, como también puede serlo un derecho o calidades de un sujeto, como la integridad física de las personas, su honor, su pudor, su recato, etc.

Por lo descrito anteriormente se puede decir que un sujeto es el que quebranta la norma penal positiva ; Un objeto material, la cosa u objeto sobre la que recae la acción del sujeto : la cosa en el robo; Un objeto jurídico, el derecho vulnerado: la seguridad nacional, la integridad física; Una víctima, sea individual, como en el homicidio, o abstracta, como el Estado al revelarse un secreto de armamento a otra nación; Un vínculo que enlace al autor con el hecho, y del que nace la responsabilidad. Quisiert, E., "Elementos de la relación de Derecho", 2011,http://jorgemachicado. blogspot.com/2011/02/erd.html (Recuperado el Martes, 25 Noviem bre de 2014).

4.2.2 evidencia digital.

"La evidencia digital se constituye en todos aquellos datos e información almacenada en archivos lógicos para que se pueda procesar mediante algoritmos abiertos y auditables, con la finalidad de ser expuestos de manera sencilla ante los tribunales de justicia".

Según Machicado, J. (2010). Obtenido de http://jorgemachicado.blogspot.com/ 2009/03/objeto-del-delito.html, (Recuperado 01/11/2014).

Como se ha mencionado la evidencia digital se puede encontrar en una gran cantidad de dispositivos, tales como computadores personales, en IPODS, teléfonos celulares, los cuales tienen sistemas operativos y programas que combinan en un particular orden esas cadenas de unos y ceros para crear imágenes, documentos, música y muchas cosas más en formato digital. Pero también existen evidencia digital existente en datos que no están organizados como archivos sino que son fragmentos de archivos que quedan después de que se sobrescribe la información a causa del borrado de los archivos viejos y la creación de los archivos nuevos, esto se llama SLACK SPACE, o espacio inactivo. También pueden quedar

almacenados temporalmente en los archivos de intercambio o en la misma memoria RAM.

4.2.2.1 requerimientos jurídicos de la evidencia digital.

Se puede decir que el término evidencia digital abarca cualquier información en formato digital que pueda establecer una relación entre un delito informático y su autor. Desde el punto de vista del derecho probatorio, la evidencia digital puede ser comparable con un documento como prueba legal. Con el fin de garantizar su validez probatoria, los documentos, y por ende la evidencia digital, deben cumplir con algunos requerimientos estos son:

- **Autenticidad:** La autenticidad consiste en satisfacer a un tribunal en que, los contenidos de la evidencia no han sido modificados; la información proviene de la fuente identificada; la información externa es precisa.

- **Precisión:** La precisión se refiere a que debe ser posible relacionarla positivamente con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación ante un tribunal en un proceso penal.

- **Suficiencia:** La suficiencia se debe entender que la evidencia digital debe de ser completa, que por sí misma y en sus propios términos mostrar el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

4.2.2.2 fuentes de la evidencia digital.

En muchas ocasiones se tiende a confundir los términos evidencia digital y evidencia electrónica, dichos términos pueden ser usados indistintamente como sinónimos, sin embargo es necesario distinguir entre aparatos electrónicos como los celulares y PDAS (asistentes digitales personales, por sus siglas en ingles) y la información digital que estos contengan.

Esto es indispensable ya que el foco de la investigación siempre será la evidencia digital aunque en algunos casos también serán los aparatos electrónicos. A fin de que los investigadores forenses tengan una idea de dónde buscar evidencia digital, éstos deben identificar las fuentes más comunes de evidencia. Situación que brindará al investigador el método más adecuado para su posterior recolección y preservación.

Las fuentes de evidencia digital pueden ser clasificadas en tres grandes grupos:

- **Sistemas de computación abiertos:** Son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles y los servidores. Actualmente estos computadores tienen la capacidad de guardar gran cantidad de información dentro de sus discos duros, lo que los convierte en una gran fuente de evidencia digital.

- **Sistemas de comunicación:** Estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el internet. Son también una gran fuente de información y de evidencia digital.

- **Sistemas convergentes de computación:** Son los que están formados por los teléfonos celulares llamados inteligentes o SMARTPHONES, los asistentes personales digitales PDAS (asistentes digitales personales, por sus siglas en ingles), las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puede contener evidencia digital.

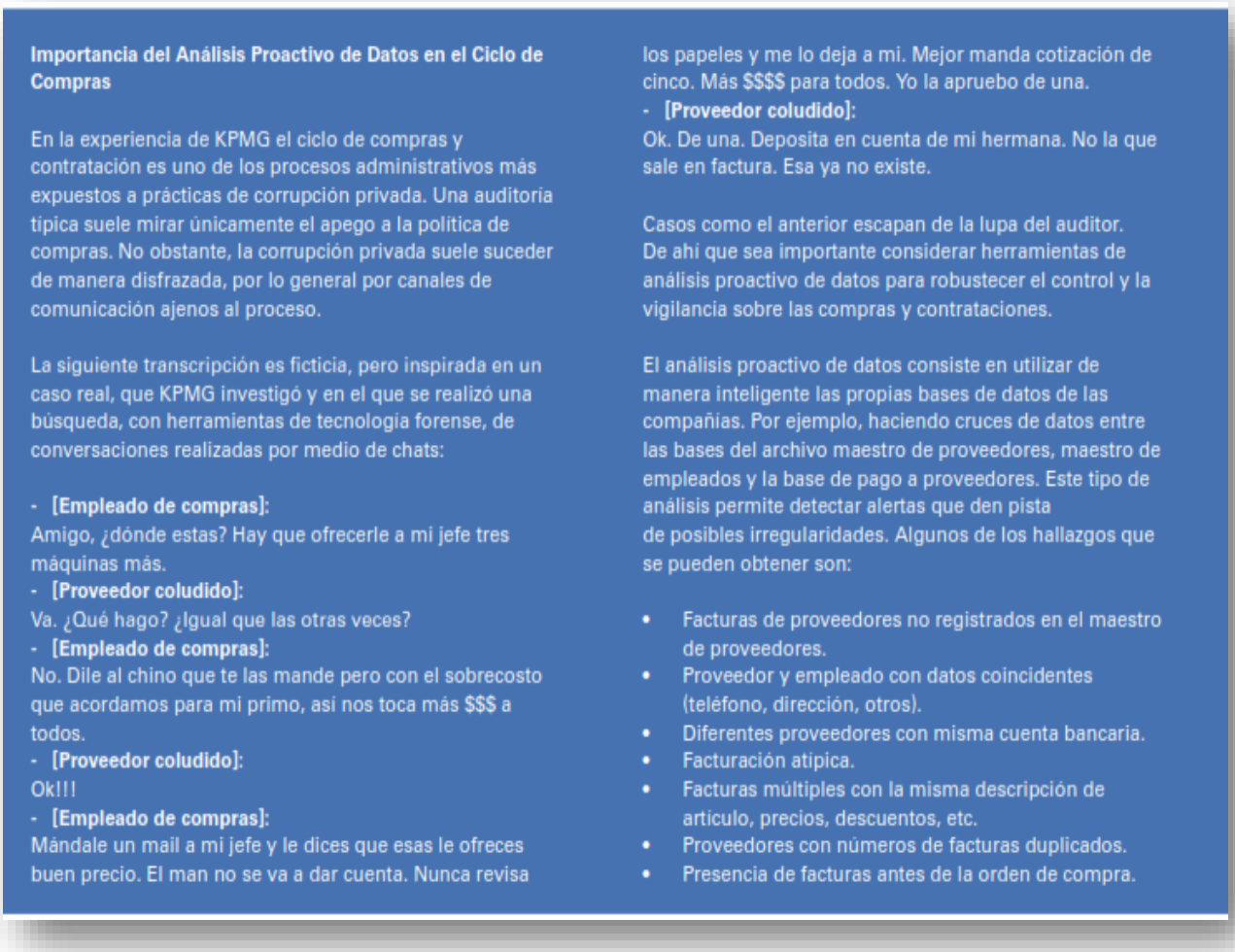
Dada la ubicuidad de la evidencia digital es raro el delito informático que no esté asociado a un mensaje de datos guardado y transmitido por medios informáticos. Un investigador entrenado puede usar el contenido de ese mensaje de datos para descubrir la conducta de un infractor, puede también hacer un perfil de su actuación, de sus actividades individuales y relacionarlas con sus víctimas.

Información financiera. El juez puede requerir a las autoridades financieras competentes o a cualquier institución financiera, pública o privada, que produzca información acerca de transacciones financieras que estén en su poder. La orden de información financiera solo procede a solicitud expresa y fundada del Fiscal General de la República o el Director General de la Policía Nacional y, una vez que el proceso ha iniciado por cualquiera de las partes, quienes deben hacer constar que han valorado los antecedentes y que la información se requiere en su criterio para fines de una investigación penal específica.

No existirá deber de informar de la solicitud y orden a la persona investigada, a menos que la información obtenida vaya a ser introducida como prueba en un proceso penal. Las

normas del secreto bancario no impedirán la expedición de la orden judicial.

Salvo su uso para los fines del proceso, todas las personas que tengan acceso a esta información deberán guardar absoluta reserva de su contenido. Los funcionarios públicos que violen esta disposición podrán ser destituidos de sus cargos, sin perjuicio de las responsabilidades civiles y penales que correspondan. Ley 406. Código Procesal Penal de Nicaragua. (2001). Managua (p.59).



Importancia del Análisis Proactivo de Datos en el Ciclo de Compras

En la experiencia de KPMG el ciclo de compras y contratación es uno de los procesos administrativos más expuestos a prácticas de corrupción privada. Una auditoria típica suele mirar únicamente el apego a la política de compras. No obstante, la corrupción privada suele suceder de manera disfrazada, por lo general por canales de comunicación ajenos al proceso.

La siguiente transcripción es ficticia, pero inspirada en un caso real, que KPMG investigó y en el que se realizó una búsqueda, con herramientas de tecnología forense, de conversaciones realizadas por medio de chats:

- **[Empleado de compras]:**
Amigo, ¿dónde estas? Hay que ofrecerle a mi jefe tres máquinas más.
- **[Proveedor coludido]:**
Va. ¿Qué hago? ¿Igual que las otras veces?
- **[Empleado de compras]:**
No. Dile al chino que te las mande pero con el sobrecosto que acordamos para mi primo, así nos toca más $$$ a todos.
- **[Proveedor coludido]:**
Ok!!!
- **[Empleado de compras]:**
Mándale un mail a mi jefe y le dices que esas le ofreces buen precio. El man no se va a dar cuenta. Nunca revisa los papeles y me lo deja a mi. Mejor manda cotización de cinco. Más $$$$ para todos. Yo la apruebo de una.
- **[Proveedor coludido]:**
Ok. De una. Deposita en cuenta de mi hermana. No la que sale en factura. Esa ya no existe.

Casos como el anterior escapan de la lupa del auditor. De ahí que sea importante considerar herramientas de análisis proactivo de datos para robustecer el control y la vigilancia sobre las compras y contrataciones.

El análisis proactivo de datos consiste en utilizar de manera inteligente las propias bases de datos de las compañías. Por ejemplo, haciendo cruces de datos entre las bases del archivo maestro de proveedores, maestro de empleados y la base de pago a proveedores. Este tipo de análisis permite detectar alertas que den pista de posibles irregularidades. Algunos de los hallazgos que se pueden obtener son:

- Facturas de proveedores no registrados en el maestro de proveedores.
- Proveedor y empleado con datos coincidentes (teléfono, dirección, otros).
- Diferentes proveedores con misma cuenta bancaria.
- Facturación atípica.
- Facturas múltiples con la misma descripción de artículo, precios, descuentos, etc.
- Proveedores con números de facturas duplicados.
- Presencia de facturas antes de la orden de compra.

Fig. 4.2.1
Evidencia digital de complicidad para cometer defalco.
Recopilado de: KPMG. (2013). Encuesta de fraude-Colombia . Sección: Tecnología, 31.

4.2.3 la investigación forense o análisis forense.

El análisis forense se entiende como el proceso formal que se encarga de recoger, analizar, preservar y presentar a través de técnicas y herramientas la información, de tal forma que el investigador forense digital pueda entregar un informe en donde presente los hallazgos de manera lógica y con un sustento claro de lo que desea mostrar. Se puede describir el proceso de análisis forense a través de las siguientes fases:

4.2.3.1 preparación.

Fase en la que, como su nombre lo indica, se prepara todo para poder realizar la investigación correspondiente, sin ser las únicas actividades están:

- Establecer lo que se necesita para realizar la investigación tanto a nivel operacional como técnico.
- Se requiere de todas las autorizaciones legales para poder adelantar la inspección y el levantamiento de la información.
- Es necesario que los protocolos de los técnicos en escena del crimen que son las primeras personas que llegan a la escena, estén claramente definidos, de tal manera que aseguren la escena del crimen que está bajo investigación.
- Definir de manera clara la estrategia con la que se debe identificar, recolectar, embalar, analizar y transportar toda la evidencia.
- Definir claramente los perfiles que van a ser involucrados en la investigación, tanto a

nivel operacional, analistas forenses y líder o líderes de los casos.

4.2.3.2 investigación.

La investigación es el componente más complejo del proceso, e involucra un gran número de actividades. Esta etapa de investigación debe tener clara la premisa de que es importante, desde el principio hasta el fin, mantener la cadena de custodia; por consiguiente, la documentación será la pieza fundamental del proceso.

4.3 Aspectos Generales Del Fraude

4.3.1 concepto y definiciones.

En sentido general, fraude significa engaño, abuso de confianza, acción contraria a la verdad o a la rectitud. Muchos conceptos de fraude han surgido y a continuación se citan algunos de ellos:

Para el autor Holmes, W. (s.f.).

> El fraude es una impostura o ardid de mala fe. Aplicado a la contabilidad el fraude consiste en cualquier acto u omisión de un acto de naturaleza dolosa y por tanto de mala fe o de negligencia grave. Consiste en despojar al propietario de lo que por derecho le pertenece, sin su consentimiento o conocimiento, o en exponer erróneamente Una situación, ya sea deliberadamente o por negligencia grave

De manera similar Castañeda, L. (s.f.), lo define de la siguiente manera: "Dolo, estafa, fraudulencia, mentira, simulación. Engaño malicioso con el que se frustra la ley o los derechos derivados de ella. Sus elementos constitutivos son la intención de perjudicar y el daño o perjuicio originado".

Del mismo modo León, L. (s.f.), dice: "El aprovechamiento ilegal de bienes, con enriquecimiento sin causas, de un funcionario público, gerente, administrador o cualquier persona de una empresa, con perjuicio para terceras personas, haciendo mal uso de la confianza conferida".

Los conceptos antes citados ponen en evidencia dos elementos constitutivos del fraude: La malicia o intención de perjudicar mediante el engaño o bien el daño ocasionado (inmediata o posteriormente). Pero que ambas conclusiones conllevan a la congruencia al abuso de confianza. El engaño puede considerarse como el medio de arribar al fraude y a este último como el fin o propósito que se propone lograr con el engaño. Estos elementos son incluyentes (deben presentarse simultáneamente), pues no puede hablarse de fraude si un perjuicio ha ocasionado una lesión en los intereses de una persona.

Corrupción: Es un sistema de comportamiento de una red en que participan actores poderosos del sector privado y público, para lograr que actores investidos de capacidad de decisión realicen actos ilegítimos que violan valores éticos, a fin de obtener beneficios particulares ilegítimos en perjuicio del bien común.

"Es el incumplimiento intencionado del principio de imparcialidad con el propósito de derivar de tal tipo de comportamiento un beneficio personal para personas relacionadas." Según asevera (Tanzi, 1995)

Actividades Fraudulentas: Conflictos de intereses, falsificación o alteración de registros y documentos, crímenes financieros, delitos monetarios, pérdida o desaparición de activos, robo, desfalco, abuso de confianza, tráfico de influencias, utilización de información privilegiada, desviaciones de fondos, estafa por uso no autorizado de tarjetas de crédito, realización de operaciones ilegales a través de cajeros automáticos (ATM), etc.

Fraude tecnológico: Es el que se da utilizando la tecnología moderna de los sistemas informáticos. Su objetivo no siempre va encaminado a apropiarse de dinero o información sino a producir pérdidas por medio de ataques cibernéticos, insertando virus a los sistemas, que pueden causar interrupción del negocio, principalmente para empresas en red o que manejan operaciones en línea o compras por internet y todo servicio de comercio electrónico, así como causar daño en la información financiera contable, que afecta la toma de decisiones importantes.

Lavado de Dinero: Es la canalización de efectivo y otros fondos generados en actividades ilegales, a través de instituciones financieras y negocios legales para ocultarla fuente de esos fondos según IFAC. (2012). Recuperado el 25/10/2014, de http://www.ifac.org

Según las NIA´s. (2009). Normas Internacionales de Auditoría. En Fraude en una Auditoría de Estados Financieros:

La malversación de activos implica el robo de los activos de una entidad y a menudo la perpetran empleados por cantidades relativamente pequeñas e insignificantes. Sin embargo, puede también involucrar a la administración quienes generalmente pueden mejor disimular u ocultar las malversaciones en formas difíciles de detectar. La irregularidad de activos puede lograrse en una variedad de formas que incluyen:

- Desfalcar ingresos (por ejemplo, malversar cobros de cuentas por cobrar o desviar entradas respecto de cuentas canceladas a cuentas bancarias personales).

- Robar activos físicos o propiedad intelectual (por ejemplo, robar inventario para uso personal o para vender, robar chatarra para reventa, coludirse con un competidor revelándole datos tecnológicos a cambio de un pago).

- Hacer que una entidad pague por bienes y servicios no recibidos (por ejemplo, pagos a vendedores ficticios, sobornos pagados por vendedores a los agentes de compras de la entidad a cambio de inflar los precios, pagos a empleados ficticios).

- Usar activos de una entidad para uso personal (por ejemplo, usar los activos de la entidad como colateral por un préstamo personal o un préstamo a una parte asociada).

- La malversación de activos a menudo se acompaña de registros o documentos falsos o engañosos para ocultar el hecho de que hay activos faltantes o de que han sido comprometidos en prenda sin la autorización apropiada (p. 209).

4.3.2 naturaleza del fraude.

El fraude es el delito más creativo: requiere de las mentes más agudas y podemos decir que es prácticamente imposible de evitar. En el momento en que se descubre el remedio, alguien inventa algo nuevo. Una persona puede llegar a merecer la confianza de otra por sus cualidades (capacidad, honradez, dedicación, etc.) y en virtud de esto llegar a desempeñar un puesto importante dentro de una institución.

En síntesis se puede decir que este grado de confianza puede llegar incluso a convertirse en excesivo y como consecuencia dejar la persona con un amplio margen de control sobre algún aspecto de las operaciones de la empresa en la que se ha desarrollado. En el momento en que una persona, por disponer de los medios propicios, obvia enfocarse en los intereses de la empresa, en búsqueda de satisfacer los propios e incluso atenta contra el patrimonio de la misma, se está convirtiendo en un defraudador.

4.3.3 actos desleales de los trabajadores cometidos a través de dispositivos tecnológicos.

Las sospechas fundadas sobre ciertas irregularidades relativas a la cartera de clientes llevaron a un empresario a exigir a uno de sus empleados la entrega de su portátil de trabajo, propiedad de la empresa.

La posterior monitorización del correo electrónico del trabajador sacó a la luz pruebas contundentes que corroboraban los recelos iniciales: el empleado había estado extrayendo información confidencial para montar otra sociedad paralela por su cuenta. Estos actos de deslealtad están a la orden del día y a veces pasan tan inadvertidos como un simple clic de ratón. En manos de las empresas está el establecimiento de límites y obligaciones relativas al uso de herramientas como Internet, las agendas PDA o los dispositivos USB, entre otros.

La utilización de dispositivos tecnológicos en el ámbito empresarial ha traído consigo unos beneficios que nadie se atreve a cuestionar hoy en día. La aplicación masiva de las nuevas tecnologías ha provocado una verdadera revolución en las organizaciones, facilitando la transferencia de información, agilizando los procesos empresariales, multiplicando la productividad y, sobre todo, mejorando la calidad de trabajo de las plantillas.

Actualmente, se estima que más de 90 por ciento por ciento de los documentos creados en el seno de una organización son electrónicos y, de todos ellos, menos del 30 por ciento se llega a imprimir. La tecnología digital es, por tanto, una herramienta indispensable para la buena marcha de un negocio, pero tampoco está exenta de riesgos frente a los que hay que saber prepararse a tiempo: la prevención y detección temprana de ciertos usos y abusos de los instrumentos como el e-mail comienza por trazar un planteamiento interno, que es fundamental para la salvaguarda de los activos intelectuales de las empresas.

Una de las infracciones cometidas con más frecuencia en el entorno empresarial es la creación de sociedades paralelas a partir de los datos, informaciones y know how extraídos de los sistemas de la empresa. El supuesto de creación de una firma paralela a la sombra de otra

(valiéndose de los activos inmateriales de ésta).

Para fines privados son dos tipos de situaciones muy frecuentes. Muchas empresas están respondiendo a este fenómeno limitando el tiempo de conexión de sus plantillas, o bien especificando aquellas franjas horarias en las que se puede hacer un uso privado de la Red. Algunas reacciones empresariales más drásticas prohíben toda utilización de Internet y del e-mail que no sea por razones puramente profesionales.

Acceder sin permiso a información confidencial de la empresa (bases de datos de clientes, por ejemplo) es un delito grave, muy propio de las capas empresariales directivas, al igual que la revelación de secretos profesionales a terceros. Sin olvidar las amenazas, injurias y calumnias vertidas a través de los medios electrónicos por parte de muchos empleados "conflictivos" con el ánimo de desprestigiar la imagen de su empresa o de insultar a potenciales clientes, por poner dos ejemplos frecuentes.

Aparte de todos estos supuestos, hay muchas otras infracciones como la destrucción, alteración o inutilización de cualquier activo inmaterial albergado en las redes o soportes informáticos de la empresa. Los causantes de estos daños informáticos a veces irreparables suelen hacer uso de virus y bombas lógicas programadas con tiempo de antelación para hacerlos "explotar" una vez que ellos ya han causado baja en su puesto de trabajo.

4.3.4 las huellas del fraude.

Las huellas de cualquier acción ilícita se pueden rastrear desde cualquier dispositivo electrónico, ya sea un ordenador de sobremesa, un portátil o teléfonos móviles, consolas de juegos y, por supuesto, en los propios servidores empresariales, que siempre dejan rastro de las acciones de sus usuarios. Ante una supuesta infracción cometida a través de estas nuevas tecnologías, es lógico que se indague sobre la autoría y, si se considera oportuno y conveniente, se iniciarán medidas legales contra el responsable, ver http://omarklinteca.foroactivo.com/t3-las-huellas-del-fraude-un-libro-cientificamente-documentado.

4.3.5 reacciones por parte de la empresa.

Insa, F. (Julio de 2007). Software y nuevas tecnologías. Fraude y actos desleales de los empleados cometidos a través de dispositivos Tecnológicos, p.212, varios síntomas pueden levantar sospechas de fraude o abuso cometido por un trabajador. A veces se advierte un consumo excesivo o inusual de recursos (envío de muchos megas al exterior). Otras veces se constata un crecimiento injustificado de datos de tráfico, el firewall de la empresa da la voz de alarma a los responsables, o bien el departamento de auditoría interna nota algún indicio raro, cuando no es otro trabajador el que informa sobre maniobras turbias.

Recordemos que la preservación del patrimonio empresarial en su conjunto es un fin legítimo de todo empresario. Así que, cuando tales sospechas están más que fundadas, se procede a investigar el ordenador de trabajo de un empleado, algo que implica realizar una

auditoría interna con el debido respeto de los derechos fundamentales de ese trabajador. El procedimiento ha de ser transparente para así evitar vulnerar estos derechos inalienables:

1) Realizar el registro de su ordenador cuando el trabajador esté presente
2) En caso de ausencia del trabajador, se reclamará la presencia de representantes de la empresa o, en su defecto, de algún compañero del investigado, preferiblemente que pertenezca a la misma categoría profesional.
3) El registro debe ser en el propio lugar de trabajo y en horario laboral.

En la hipótesis de un registro del correo electrónico, un primer análisis sólo podrá detenerse en los "elementos accesorios" como el tamaño del mensaje, la hora de envío o el asunto del mismo, pero no se podrá entrar en el contenido del mensaje si no está autorizado expresamente a través de una orden judicial (p. 94).

4.3.6 la gran oportunidad.

La tecnología nos presenta nuevos riesgos, pero también nos brinda una gran oportunidad. El más eficiente combate contra el fraude en la actualidad unido a una adecuada metodología y cultura organizacional, se logra con una metodología integral anti-fraude, y el uso de la tecnología en forma intensiva analizando universos completos de datos para identificar indicios de fraude y tomar acción sobre las mismas o bien disparar alertas en línea.

Sobre la base de la metodología indicada, el uso de una poderosa herramienta especializada de análisis de datos y auditoría orientada a la prevención y detección de fraude como IDEA se abren nuevos horizontes en esta lucha, y pone en las manos del experto en procesos operativos una herramienta de descubrimiento y creatividad, y de uso intuitivo para investigar, detectar y recuperar valor a partir de los datos corporativos analizando millones de registros de cualquier aplicación o base de datos, que también le permitirá automatizar sus procesos de Aseguramiento continuo y disparar las alertas necesarias, así como aplicar las facilidades de análisis digitalizado y cientos de funciones o prestaciones adicionales asegura Safe Consulting Group. (2006). Fraude: Un nuevo ebfoque para combatirlo. Auditoría Pública(38), 101-103. Obtenido de http://www.ideaf.org (recuperado el 28-0-2014 10:50 am).

4.4 Coso

4.4.1 concepto de coso.

Definición de Control Interno según COSO (Marco Integrado de Control Interno):El control interno es un proceso, efectuado por la junta directiva, administración y demás personal de una entidad, diseñado para proporcionar una seguridad razonable respecto al logro de objetivos relacionados a operaciones, reporte y cumplimento.

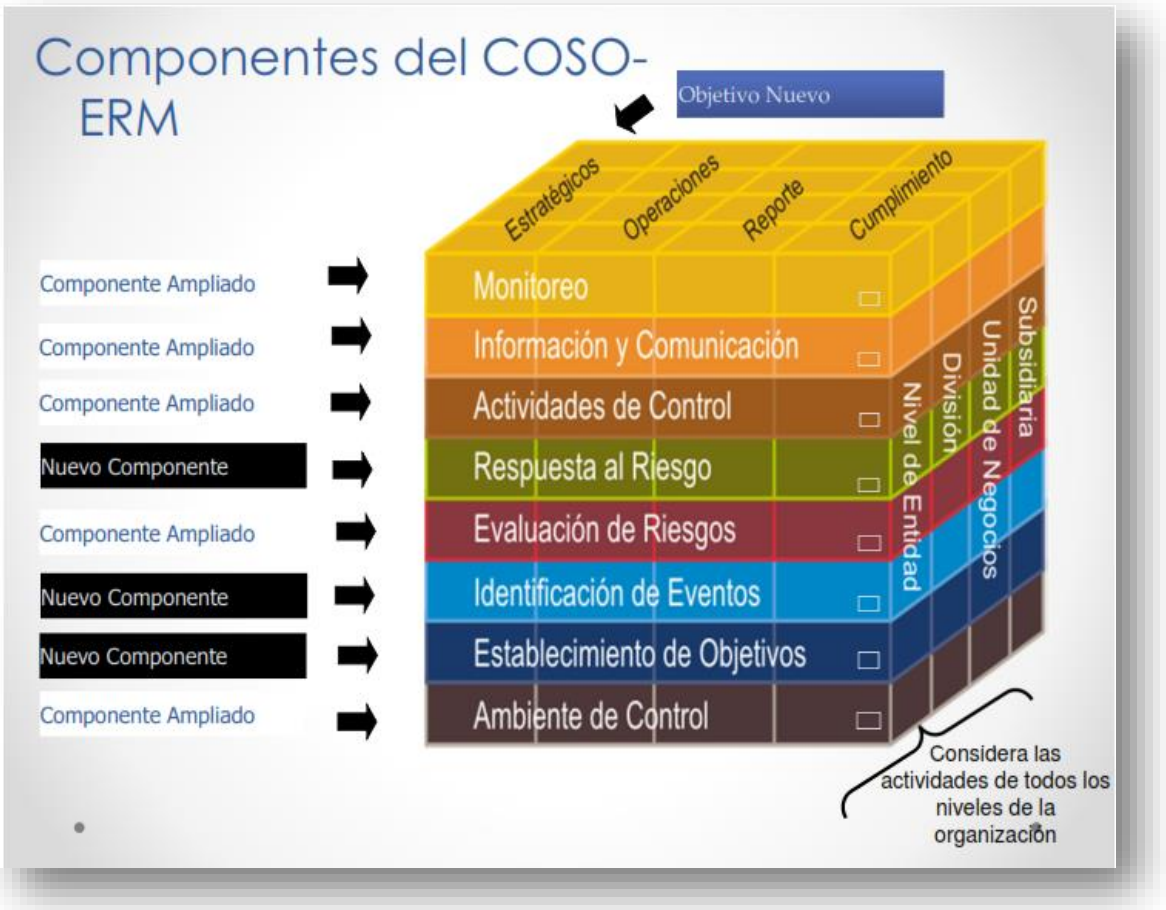


Fig. 4.4.1
Componentes del COSO-ERM.

Categorías de Objetivos:

Operacionales: Eficacia y Eficiencia en la operaciones, incluyendo objetivos de desempeño, financieros y operacionales, y la salvaguarda de activos.

Reporte: Reporte Interno y Externo, Financiero y no Financiero y puede incluir confianza, puntualidad, transparencia, u otros términos determinados por los organismos reguladores, Linares, G., & Jenith, E. (2013). COSO IV. *La Evolución del Control Interno, Basado en Principios.* Managua.

COMPONENTES Y RESUMEN DE PRINCIPIOS				
Ambiente de Control	Evaluación de Riesgos	Actividades de Control	Información y Comunicaciones	Monitoreo de Actividades
1.Demostrar compromiso con la integridad y los valores éticos. 2.Ejercitar la supervisión de manera responsable. 3.Establecer estructura, autoridad y responsabilidad. 4.Demostrar compromiso por ser competente. 5.Reforzar la responsabilidad.	6.Definir objetivos adecuados. 7.Identificar y analizar riesgos. 8.Evaluar el riesgo de fraude. 9.Identificar y analizar cambios significativos.	10.Seleccionar e implementar actividades de control. 11.Seleccionar e implementar controles generales sobre TI. 12.Desplegar a través de políticas y procedimientos.	13.Usar información relevante. 14.Comunicar Internamente. 15.Comunicar externamente.	16.Desarrollar evaluaciones propias o separadas. 17.Evaluar y Comunicar Deficiencias.

Fig. 4.4.2
Componentes y resumen de Principios del COSO-ERM.

Tomado de Valero, N., & Roa, M. (2013). Estructura de control interno COSO: Preparandose para los cambios. (pág. 13). Deloitte.

4.4.2 principio 8.

"La organización considera la posibilidad de fraude en la evaluación de riesgos para el logro de objetivos".

- Considera distintos tipos de fraude: La evaluación de fraude considera reporte fraudulento, posible pérdida de activos y corrupción resultantes de las diversas formas en que el fraude puede ocurrir.

- Evalúa incentivos y presiones para cometer fraude: La evaluación de riesgos de fraude considera oportunidades para adquisición, uso o disposición no autorizada de activos, alteración de los registros de la entidad o comisión de otros actos inapropiados.

- Evalúa oportunidades para cometer fraude: La evaluación de riesgos de fraude considera incentivos y presiones.

- Evalúa actitudes y racionalizaciones: La evaluación de riesgos de fraude considera como la administración y otro personal puede involucrarse en o justificarse actos inapropiados.

4.4.3 principio 11.

"La organización selecciona y desarrolla actividades generales de control sobre la tecnología para soportar el logro de objetivos".

- Determina la vinculación entre el uso de la tecnología en los procesos de negocio y los controles generales de tecnología. La administración comprende y determina la dependencia y vinculación entre los procesos de negocios, las actividades de control automatizadas y los controles generales de tecnología.

- Establece las actividades de control de infraestructura de tecnología pertinentes. La administración selecciona y desarrolla actividades de control sobre la infraestructura de tecnología, las que son diseñadas e implementadas para ayudar a asegurar la integridad, exactitud y disponibilidad de la tecnología de procesamiento.

- Establece actividades de control pertinentes sobre los procesos de administración de seguridad. La administración selecciona y desarrolla actividades de control que son diseñadas e implementadas para restringir el acceso a la tecnología a usuarios autorizados, adecuados a sus responsabilidades y para proteger los activos de la entidad de amenazas externas.

- Establece actividades de control pertinentes sobre la adquisición, desarrollo y mantenimiento de tecnología. La administración selecciona y desarrolla actividades de control sobre la adquisición, desarrollo y mantenimiento de tecnología y su infraestructura para alcanzar los objetivos.

PwC. (2013). COSO: Internal Control Integrated Framework. En P. España (Ed.). Madrid, España.

4.5 Prevención Del Fraude Mediante La Tecnología

4.5.1 metodología para un plan de acción global contra el fraude.

Como se ha visto el problema del fraude no puede atacarse con soluciones parciales, sino en forma integral, para lo cual, una adecuada metodología de análisis de riesgos orientado al fraude, resulta la de mayor efectividad para identificar los elementos de mayor vulnerabilidad corporativa y aplicar los recursos apropiados para atacar el problema.

Una adecuada metodología que logra identificar las vulnerabilidades del "negocio" (sea público o privado entendiendo como tal al objeto principal de las actividades) y establecer un ranking de procesos en relación al fraude, desmenuzando en detalle las vulnerabilidades y puntos de control, per- mite trazar un plan de acción preciso y alineado con los objetivos institucionales o de negocios, de manera que permita evaluar y comprender los riesgos, para establecer las técnicas y herramientas de control apropiadas para cada evento, o bien decidir si asegurar, transferir el riesgo remanente, o minimizarlo a partir de las múltiples dimensiones de las estrategias de control que mencionamos anteriormente, Ramos, D. (s.f.). Fraude un nuevo enfoque en combatirlo. Safe Consulting Group.

Otra vía preventiva es la aparición de avisos en forma de pop-up en la pantalla del ordenador cada vez que un trabajador inicia la sesión, donde se exponen las obligaciones y restricciones al uso de este dispositivo (hacer clic en "aceptar" equivaldría a firmar una cláusula, por ejemplo). Otros empresarios, mientras tanto, prefieren impartir cierta formación sobre cuáles son los derechos y las obligaciones de los trabajadores en el desempeño de sus funciones y qué posibles sanciones están asociadas a un mal uso del material empresarial.

Formar al trabajador desde el principio sobre el uso debido/indebido de las herramientas de trabajo es otra vía de prevención de usos fraudulentos y abusos de los dispositivos tecnológicos en las organizaciones. Hasta hace pocos años resultaba difícil demostrar que un empleado, por el mero hecho de estar en contacto con determinados aparatos en el lugar de trabajo, debía contraer este tipo de compromiso con la empresa que le contrataba. Antes, en caso de no respetar este compromiso, sólo se le podía acusar de negligencia, pero nunca de incumplimiento. Con la llegada de los protocolos informáticos y otras muchas medidas de control, se han fijado unas mínimas reglas de juego que están surtiendo un buen efecto en las organizaciones.

En cualquier caso, siempre se recomienda que cualquier mecanismo de control en las empresas se realice con discreción y, si es posible, se permita en general un "uso social" de los instrumentos tecnológicos, es decir, un uso sensato y moderado como, por ejemplo, autorizar a los empleados las transacciones de banca on line para evitarles desplazamientos innecesarios hasta una sucursal bancaria.

4.5.2 crear y mantener una política sobre fraude.

Toda organización debería crear y mantener una política escrita sobre fraude, para dejar en claro su posición ante comportamientos fraudulentos. La política debe ser un documento separado, diferenciado del código de conducta o de ética de la organización, estableciendo allí que el fraude es una preocupación que merece una atención especial.

El contenido de la política sobre fraude debe ser explícito y claro. Deben establecerse claramente las actitudes específicas que constituyen fraude y abuso, como así también las acciones que serán tomadas contra los perpetradores de fraude. La organización debe sustentar esta política consistentemente y asegurar que sea distribuida y comunicada a todos los empleados. Una política de fraude transmite a los empleados que la organización está con los ojos atentos en el fraude, y puede servir como disuasivo para los posibles perpetradores.

Los auditores internos están perfectamente posicionados para contribuir a la detección y prevención de actividades fraudulentas. No sólo los auditores están bien calificados en esta área, sino que pueden ayudar a la compañía a evitar potenciales conflictos con requerimientos legales asociados con la investigación. Más aún, la participación de la auditoría interna en iniciativas anti-fraude ayuda a la organización a sacar ventaja de los expertos internos que conocen mejor a la compañía.

4.5.3 indicios de fraude.

- Alteración de documentos.
- Pagos duplicados.
- Segundo endoso en cheques.
- Partidas pendientes en conciliaciones bancarias.
- Asientos contables sin documentación de respaldo.
- Ajustes no explicados a cuentas a cobrar, a pagar, ingresos o gastos.
- No salida de vacaciones de ciertos empleados.
- Falta de seguimiento de cuentas a cobrar vencidas.
- Faltantes en mercaderías entregadas.
- Empleados en la nómina que no suscriben beneficios.
- Quejas de clientes.
- Incrementos o disminuciones excesivas en ciertas cuentas.
- Relaciones inusuales en los estados financieros, como incremento de ingresos con disminución de cuentas a cobrar.
- Incremento de ingresos con disminución de compras de inventario.
- Incremento de inventario con disminución de compras o cuentas por pagar.
- Cancelaciones inusuales de cuentas a cobrar.
- Productos o servicios comprados en exceso a las necesidades.
- Gastos o reembolsos irracionales.
- Faltantes o sobrantes de caja.
- Nombres comunes, números de teléfono y direcciones en proveedores.
- Documentación extraviada.

- Excesivas anulaciones de créditos.
- Propinas de empleados.
- Cambios significativos en los índices de liquidez, apalancamiento, rentabilidad o retorno.

Quiroga, L. (Abril de 2005). Aspectos para mejorar la seguridad los sistemas de información. Instituto de Auditores Internos de Argentina.

4.5.4 medidas preventivas de monitoreo para evitar el fraude.

4.5.4.1 monitoreo permanente.

Los esquemas de control interno establecidos en los procesos deben permitir la identificación de desviaciones en los mismos de tal forma que se advierta en forma temprana la posible ocurrencia de hechos que contraríen lo dispuesto en este Código.

4.5.4.2 monitoreo continuo.

- Identifica anomalías dentro de las transacciones y archivos de datos.
- Examina el 100% de los datos.
- Identificación a tiempo Corre automáticamente (el usuario define la frecuencia);
- Reporta anomalías a personas designadas para la investigación.
- Construir un perfil de fraudes potenciales el cual pueda ser probado.
- Analizar datos para identificar posibles indicadores de fraude.
- Implementar monitoreo continuo de las actividades.

- críticas del negocio para automatizar los procesos de detección.

Otros elementos adicionales a considerar, son:

4.5.4.3 auditoría interna.

Los sistemas de auditoría y seguimiento diseñados en forma razonable para detectar fraudes y conductas irregulares son herramientas importantes utilizadas, para esto se indica como ejemplo el caso de los controles ISA y sus empresas están cumpliendo con su función.

Línea Ética: La línea ética, también es concebida, como principal elemento de comunicación de hechos sospechosos de fraude. El reporte será recibido garantizando la confidencialidad de la información y de la persona que la presenta.

4.5.4.4 investigación.

Los mecanismos de investigación están destinados a adelantar las acciones necesarias para aclarar posibles hechos de fraude. Cuando se disponga de información sobre conductas fraudulentas, bien sea potenciales o reales, ISA y sus empresas, adelantarán las verificaciones necesarias en forma objetiva y exhaustiva. El objetivo de tales verificaciones será recolectar información pertinente, de modo que la administración de la empresa pueda decidir la línea de actuación a seguir.

4.5.4.5 respuesta.

Los mecanismos de respuesta están destinados a tomar las medidas correctivas y reparar, en lo posible, el daño ocasionado por el fraude. Consecuente con lo establecido en los criterios del marco de actuación de este Código, los hechos fraudulentos, debidamente soportados y analizados por el Gerente General y con quien éste considere pertinente, tendrán la respuesta administrativa y legal acorde con lo establecido en la normatividad interna y externa aplicable en cada país.

4.5.4.6 manejo de incidentes.

En caso de presentarse un fraude, se estudiarán sus causas, las debilidades de control detectadas y se presentará un plan de respuesta, garantizando que se ha administrado el riesgo y que se fortalecerán los controles. Se generará un aprendizaje del incidente para evitar su recurrencia, teniendo en cuenta aspectos como: rediseño de procesos, planes de mejoramiento, actualización de evaluación de riesgos determinando si es necesario modificar el perfil y posibles ajustes en controles.

4.5.4.7 transferencia.

Con el objetivo de minimizar el impacto de las pérdidas y daños causados, ISA y sus empresas, mantendrán vigente los mecanismos de transferencia de riesgos que consideren pertinentes, acorde con la evaluación realizada para los riesgos que lo permitan.

4.5.4.8 utilización de tecnología.

ISA y sus empresas han dispuesto la tecnología para apoyar los procesos de negocio y facilitar el flujo de información natural entre procesos y entre sus empresas en un ámbito de seguridad tecnológica con criterios de confidencialidad, confiabilidad y disponibilidad.

Adicional a los controles de detección tradicionales, la empresa se reserva el derecho de monitorear su ambiente tecnológico con el objetivo de evitar y detectar posibles eventos de fraude en el ambiente tecnológico respectando la confidencialidad de la información en el marco de la ley aplicable. Adicionalmente, se propende por la implementación efectiva de alertas tempranas en los procesos y esquemas de monitoreo continuo. Isa. (2011). Código Antifraude. Manuscrito no publicado.

4.6 Oferta Técnica De Software's Especializados En La Detección De Fraudes

Software avalado por GAFI, BSA Y VICTORY ACT como herramientas forenses para investigar blanqueo de capitales y lavado de dinero. Existen en el mercado software diseñados para explorar bases de datos y analizar perfiles.

Entre los software's examinados vía internet y que cumplen con estas especificaciones tenemos: IDEA, ACL, monitor byte, Assist, Excel, Hana, Fico, Sas, entre otros.

El modelo se complementa con el uso creativo de herramientas especializadas para Análisis de Datos y Auditoría (como por ejemplo el Software IDEA), que permiten explotar a

fondo el potencial de los datos disponibles, para detectar indicios de fraude que luego generen rutinas y alertas en línea a partir del perfilado de los datos y la detección de parámetros excepcionales. IAIE. (Marzo de 2006). Prevención y detección de fraude y auditoría forense sector privado. Instituto de Auditores Internos de Ecuador.

4.6.1 análisis digitalizado - la ley de Benford.

4.6.1.1 introducción a la ley de benford.

Las técnicas de detección de fraudes financieros utilizadas en una auditoría financiera son diversas, algunas son simples en su forma de aplicación y otras son más complejas porque requieren del uso de técnicas de análisis estadístico.

Dentro de las técnicas estadísticas se tienen las siguientes: análisis de regresión y correlación, análisis de dispersión, la Ley de Benford, análisis de frecuencia digital, análisis de patrones y secuencias, análisis de faltantes y duplicados, análisis histórico de tendencias y análisis de ratios financieros.

Estos análisis se complementan con los procedimientos de auditoría análisis vertical y horizontal de las cuentas de balance y de resultados, los cuales corresponden a una especialidad de la carrera de Auditoria. El presente artículo se centra en la técnica de la Ley de Benford como una herramienta de análisis útil y sencillo para la detección de fraudes financieros.

4.6.1.2 antecedentes.

En un día cualquiera de 1881, el astrónomo y matemático Simón Newcomb estaba realizando unos cálculos con un viejo libro de logaritmos cuando se dio cuenta de que las páginas del libro estaban más viejas y usadas cuanto más cercanas estaban del principio, es decir, aquellos números que comenzaban con 1. La única conclusión posible es que a lo largo de los años había consultado mucho más el logaritmo de los números que comenzaban por 1.

Si pensamos en las teclas de un ascensor de un edificio, por ejemplo, sería normal que el 1 estuviera más gastado. Es claro que el 9 es el número que más vemos como último dígito en todos los catálogos de precios de productos.

Revisando los datos que él utilizaba en sus observaciones astronómicas, dedujo que los dígitos iniciales de los números no eran probables y que, de hecho, el 1 aparecía de manera más frecuente seguido del 2 y así hasta el 9 que era el menos frecuente. De esta manera empírica comprobó que la probabilidad de que un número en una serie de datos comience por el dígito d es de **log (1 + 1/d)** y enunció la "ley de los números anómalos de Benford".

Es decir, la probabilidad de que en una serie de muchos datos, el primer dígito de un número sea 1 es de alrededor del 30%, de un 17,6% para el 2, 12,5% para el 3 etc. Sin embargo, a pesar de constatar el hecho, Benford no fue capaz de explicar las causas de este fenómeno tan extraño.

4.6.1.3 utilización de la benford.

Fraude contable: De forma general, se considera que quien maquilla datos de una contabilidad u otro tipo de fraude con datos socioeconómicos tiende a distribuir por inadvertencia los dígitos significativos de forma relativamente uniforme. Mark J. Nigrini ha desarrollado eficaces test basados en la ley de Benford para detectar fraudes fiscales o contables, eso sí, que los datos sean suficientemente numerosos y con varios órdenes de magnitud, 100, 1.000, 10.000, etc.

Si a partir del conjunto de datos contables, registrados en los asientos de entradas y salidas, las primeras cifras significativas siguen la ley de Benford, la declaración no ha sido, probablemente, manipulada. Pero si la contabilidad ha sido manipulada el análisis estadístico obtendrá una distribución de frecuencias de los primeros dígitos significativos que no se ajustará a la "ley de los números anómalos".

DÍGITO	FRECUENCIA	PORCENTAJE DE OCURRENCIA COMO PRIMER DÍGITO (%)
1	0.30103	30.1
2	0.17609	17.6
3	0.12494	12.5
4	0.09691	9.7
5	0.07918	7.9
6	0.06695	6.7
7	0.05799	5.8
8	0.05115	5.1
9	0.04576	4.6

Fig. 4.6.1
Distribución de datos según la Ley de Benford.

A veces, 5 y 6 predominan con frecuencias respectivas de 40% y 20%. En algunos casos los test son muy complicados y necesitan potentes ordenadores para llevarlos a cabo en tiempo razonablemente corto pero en otros casos son muy sencillos. A ojo de buen cubero, si hay pocas cantidades que comiencen por 1 y muchas por 5 y 6 hay que desconfiar de la contabilidad que se analiza.

En forma gráfica los resultados pueden mostrarse así (Prueba del primer dígito):

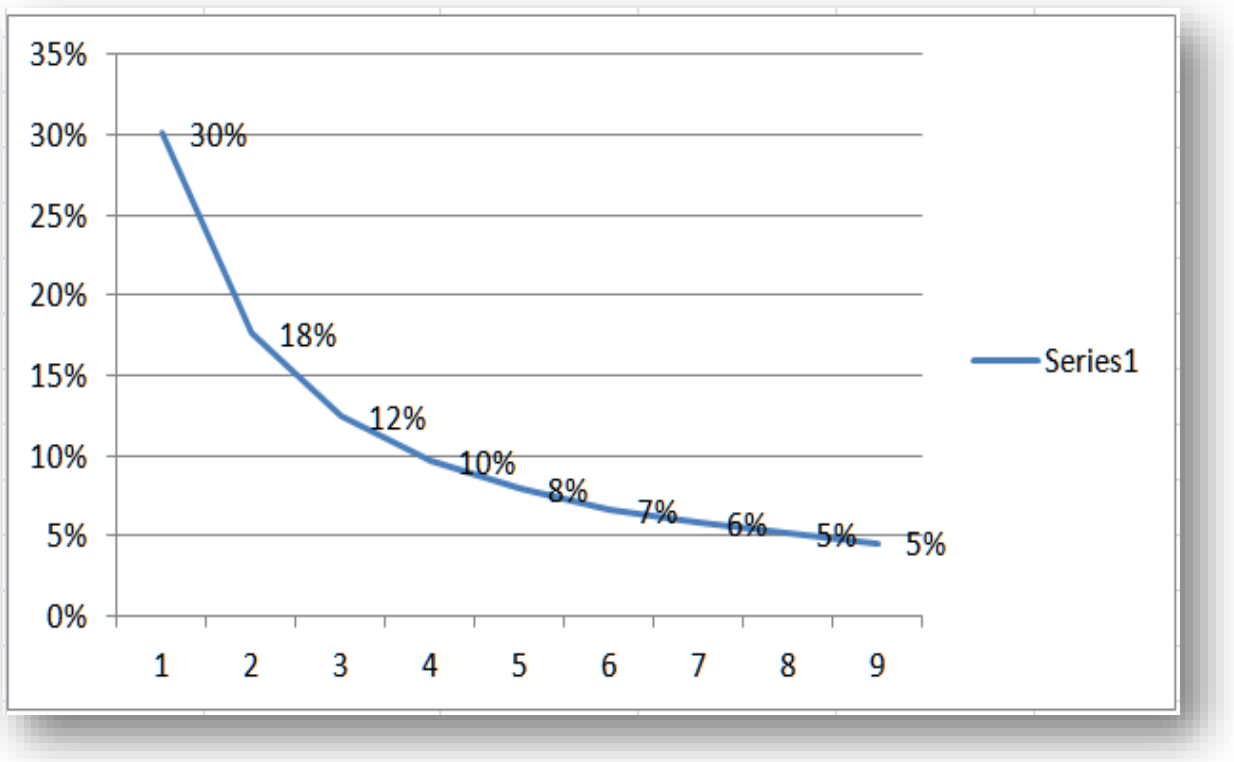


Fig. 4.6.2
Líneas de tendencia según la Ley de Benford (Véase Anexo A3.2)

El análisis digital contempla varias pruebas:

*Prueba de los primero dígitos *Prueba de los segundos dígitos	Estas son a nivel macro para evaluar la razonabilidad de los datos
*Prueba de los primeros dos dígitos *Prueba de los primeros tres dígitos	Estas son orientadas a determinar muestras de auditoría, determinan duplicados anormales, por ejemplo identifican compras realizadas por un valor justo debajo de un límite de autorización.
*Prueba de los últimos dos dígitos	Utilizada para detectar redondeos o números inventados.
*Prueba de números duplicados *Prueba de números redondeados	Busca identificar recurrencia anormal de ciertos números, busca la recurrencia anormal de redondeos en los números, para identificar estimaciones.

Cuadro 4.6.1
Análisis y prueba de los dígitos.

(Boletin Update CAATT, 2013)

4.6.1.4 conclusiones.

Revista Varianza. (Noviembre de 2012). Ley de Benforf, se puede concluir que los resultados de la aplicación de la ley de Benford no necesariamente indican que existe fraude en un grupo de datos analizados, simplemente nos dan señales de alerta de donde poner mayor atención en la auditoría, los resultados deben ser valorados de acuerdo a las particularidades del negocio, por ejemplo puede ser

que existan transacciones en depósitos a plazo fijo DPF's que las realiza un administrador de base de datos, entonces si se detecta alguna anomalía en estas transacciones de carácter operativo se deben investigar más a fondo, considerar que tipo de operaciones son, en que fechas se realizan (p. 9-12).

V. Caso Práctico

Generalidades del caso y su tipo de investigación

Este es un estudio explicativo de los resultados que se obtienen al aplicar el sistema de auditoría IDEA para cada una de las cuentas en especificadas más adelante en el desarrollo del mismo, pero en sí aplicando la Ley de Benford a datos tomados de una base de datos de la cuenta de bancos de una empresa. Los resultados se miden y se toman decisiones reales. Lo que se mide es que tanto las frecuencias de los datos se acercan a las frecuencias que están dadas en la Ley de Benford, si están muy desviados, se observa cuales datos son los más alejados y a esos se les hace un análisis más detallado para ver que puede estar ocurriendo con ellos.

Diseño de la investigación

EI estudio que se está realizando es transaccional descriptivo, porque se toman los resultados de varios procesos y se evalúa en cuál de ellos se puede estar presentado problemas de fraude.

El método de investigación.

Para lograr el objetivo propuesto, se debe hacer lo siguiente: Por medio de un sistema de información (IDEA), tomar datos de una aplicación de Inventarios (devoluciones, descuentos, ventas y salidas varias) de cartera entre otros; luego a esos datos se les aplica la

Ley de Benford, si los datos cumplen con la Ley, se concluye que no existen indicios de fraude entre la información analizada, si por el contrario existe algunos datos que no cumplen la Ley de Benford, debemos hacer un análisis más profundo de la información para identificar cuales datos son los que no están cumpliendo la Ley de Benford.

Es bueno aclarar que lo último que se hace es la auditoria, porque es lo más costoso de todo el análisis, si se descubre que no es nada grave, se puede seguir evaluando la información en forma continua, hasta descubrir otro desvío que implique investigar a fondo la Información y este proceso es cíclico y continuo hasta que el investigador decida terminar y sacar las conclusiones.

Técnicas e instrumentos para la recolección de la información.

Los instrumentos para recoger la información es un programa de computador que recopila la información en una base de datos y un programa que tome esos datos y los compare con las frecuencias que están definidas en la Ley de Benford.

Análisis de la información.

La información que se obtiene en estas pruebas es cuantitativa, las muestras son datos de un proceso, la Ley de Benford exige que la muestra la cantidad de datos sea mayor a mil, esto para que se pueda tener un mejor análisis de los resultados, por eso se tomaran muestras de varios días o meses.

Las muestras son no probabilísticas ó dirigidas, porque se tornan los datos generados en un periodo de tiempo y no se deja ninguno por fuera.

Expectativas.

Se ha pensado en utilizar la investigación para realizar un curso donde los Auditores de Sistemas puedan aplicar la teoría en sus respectivas empresas. Esta idea se puede llevar a los cursos de extensión de la Universidad Nacional Autónoma de Nicaragua en especial en la Facultad de Ciencias Económicas para que el proyecto tenga más divulgación y aplicación real debido a su importancia.

Usuarios potenciales.

Los usuarios potenciales de este proyecto son las personas que estén en el campo de la auditoria, contraloría. Revisoría fiscal, control interno, control de gestión y todas aquellas personas que tengan bajo su responsabilidad el control de cualquier proceso administrativo donde exista la posibilidad de fraude.

Sistema utilizado como base fundamental de nuestra investigación:

IDEA es el acrónimo de:

I nteractive
D ata
E xtraction and
A nalysis

“Sea un auditor sobresaliente, usted tiene el conocimiento nosotros las herramientas”.

Ese es el eslogan de nuestro programa más adelante desarrollado.

Las fortalezas que tiene este programa son las siguientes en su acápite, IDEA - Smart Analyzer Financial

Análisis del Mayor General:

1. Para identificar elementos inusuales en la BD del mayor general o diario.
2. Asientos con importes redondeados.
3. Asientos con importes que terminan en 999.
4. Asientos con comentarios específicos.
5. Resumen por número de cuenta.
6. Asientos por período y fuente del asiento.
7. Asientos por período.
8. Saldos de cuenta por fuente del asiento.
9. Saldos de cuenta por período.
10. Asientos no balanceados.
11. Asientos Duplicados.
12. Asientos faltantes.
13. Asientos registrados en fines de semana.
14. Asientos registrados en fechas específicas.
15. Asientos registrados en horas específicas.
16. Asientos por usuario.

17. Resumen por combinaciones de cuenta.
18. Asientos con importes grandes.

Cuentas por Cobrar:

1. Para identificar elementos inusuales en el auxiliar de cuentas por cobrar.
2. Deudores con saldos acreedores.
3. Resumen operaciones deudor.
4. Operaciones próximas a una fecha específica.
5. Búsqueda campo duplicado.
6. Antigüedad por fecha de vencimiento.
7. Antigüedad por fecha de factura.
8. Deudores con totales de facturas mayores al límite del crédito.
9. Deudores con saldos mayores al límite del crédito.

Inventarios:

1. Antigüedad por fecha entrada.
2. Antigüedad por fecha de recepción y saldo final de existencias.
3. Antigüedad por fecha de recepción y costo unitario.
4. Recalcular saldo de existencias.
5. Calcular rotación de existencias.
6. Calcular rotación unitaria.
7. Resumen por ubicación de existencias.

8. Costo unitario cero o negativo
9. Cantidad Negativa.
10. Importes de existencias grandes.
11. Productos recibidos cerca de una fecha especificada.
12. Precio de venta inferior al costo unitario.
13. Comparación precio de venta con costo unitario.
14. Búsqueda campo duplicado.

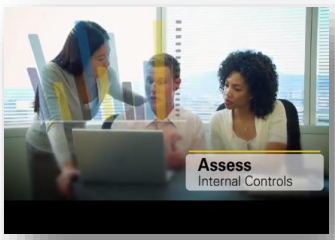
Propiedad, Planta y Equipos:

1. Para identificar errores de valuación y elementos inusuales en el archivo maestro de PPE.
2. Incorporaciones activos fijos.
3. Resumen categoría de activos.
4. Recalcular depreciación lineal.
5. Recalcular depreciación decreciente.
6. Depreciación superior al costo.
7. Búsqueda campo duplicado

Cuentas por Pagar.

1. Operaciones registradas en fines de semana.
2. Operaciones próximas a una fecha especificada.
3. Operaciones registradas en fechas especificadas.

4. Operaciones registradas en horas especificadas.
5. Operaciones por Identificador de usuario.
6. Operaciones registradas en horas especificadas.
7. Operaciones con importes redondeados.
8. Búsqueda campos duplicados.
9. Antigüedad por fecha de factura.
10. Facturas o pagos duplicados.
11. Acreedores con saldo deudor.
12. Acreedores con totales de facturas mayores al límite aprobado.
13. Acreedores con saldos mayores al límite aprobado.
14. Resumen operaciones acreedor.
15. Facturas sin orden de compra.



Evaluar controles internos que realicen auditorías operacionales

Identificar potenciales fraudes

Sección desarrollada.

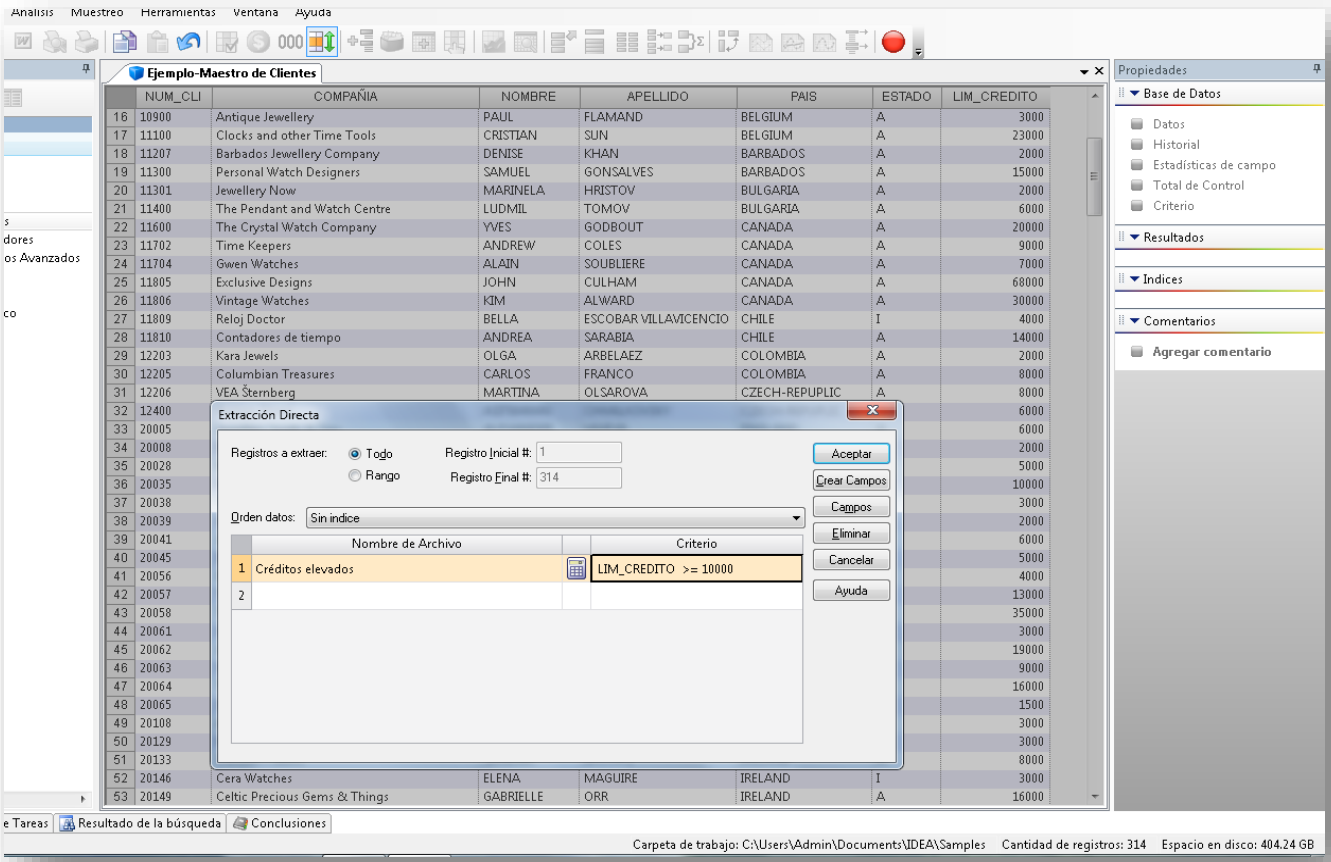
Sección Clientes[1]:

En esta sección cuando son bases de datos muy grandes el auditor no se toma la tarea de revisar uno a uno cada dato, es por eso que aquí se aplica esta herramientas para obtener dicho segmento o extraer datos que cumplan con la misma característica, es decir cuando se requiera la cartera de clientes pertenecientes a un país o región determinada.

Para obtener datos que cumplan con determinada condición[2].

[1] 2.1 billones de registros es la capacidad máxima de clientes que se puede cargar en este módulo.

[2] Estadísticas de campo aplica para valores numéricos, fecha y hora.

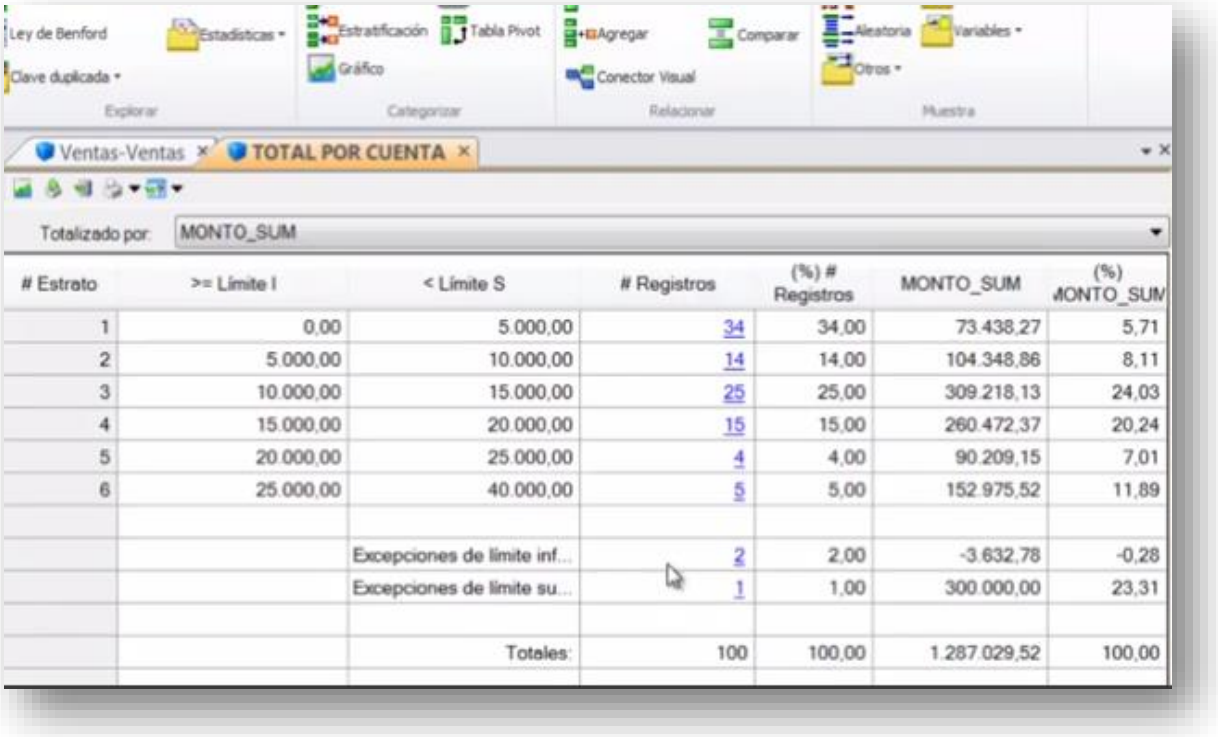


	NUM_CLI	COMPAÑIA	NOMBRE	APELLIDO	PAIS	ESTADO	LIM_CREDITO
16	10900	Antique Jewellery	PAUL	FLAMAND	BELGIUM	A	3000
17	11100	Clocks and other Time Tools	CRISTIAN	SUN	BELGIUM	A	23000
18	11207	Barbados Jewellery Company	DENISE	KHAN	BARBADOS	A	2000
19	11300	Personal Watch Designers	SAMUEL	GONSALVES	BARBADOS	A	15000
20	11301	Jewellery Now	MARINELA	HRISTOV	BULGARIA	A	2000
21	11400	The Pendant and Watch Centre	LUDMIL	TOMOV	BULGARIA	A	6000
22	11600	The Crystal Watch Company	YVES	GODBOUT	CANADA	A	20000
23	11702	Time Keepers	ANDREW	COLES	CANADA	A	9000
24	11704	Gwen Watches	ALAIN	SOUBLIERE	CANADA	A	7000
25	11805	Exclusive Designs	JOHN	CULHAM	CANADA	A	68000
26	11806	Vintage Watches	KIM	ALWARD	CANADA	A	30000
27	11809	Reloj Doctor	BELLA	ESCOBAR VILLAVICENCIO	CHILE	I	4000
28	11810	Contadores de tiempo	ANDREA	SARABIA	CHILE	A	14000
29	12203	Kara Jewels	OLGA	ARBELAEZ	COLOMBIA	A	2000
30	12205	Columbian Treasures	CARLOS	FRANCO	COLOMBIA	A	8000
31	12206	VEA Šternberg	MARTINA	OLSAROVA	CZECH-REPUPLIC	A	8000
32	12400						6000
33	20005						6000
34	20008						2000
35	20028						5000
36	20035						10000
37	20038						3000
38	20039						2000
39	20041						6000
40	20045						5000
41	20056						4000
42	20057						13000
43	20058						35000
44	20061						3000
45	20062						19000
46	20063						9000
47	20064						16000
48	20065						1500
49	20108						3000
50	20129						3000
51	20133						8000
52	20146	Cera Watches	ELENA	MAGUIRE	IRELAND	I	3000
53	20149	Celtic Precious Gems & Things	GABRIELLE	ORR	IRELAND	A	16000

Fig. 5.1
Desarrollo de la sección Clientes.

Ventas:

Lo que hace en este módulo es estratificar por montos totales, ya sean por subtotales o totales con el IVA.



# Estrato	>= Límite I	< Límite S	# Registros	(%) # Registros	MONTO_SUM	(%) MONTO_SUM
1	0,00	5.000,00	34	34,00	73.438,27	5,71
2	5.000,00	10.000,00	14	14,00	104.348,86	8,11
3	10.000,00	15.000,00	25	25,00	309.218,13	24,03
4	15.000,00	20.000,00	15	15,00	260.472,37	20,24
5	20.000,00	25.000,00	4	4,00	90.209,15	7,01
6	25.000,00	40.000,00	5	5,00	152.975,52	11,89
		Excepciones de límite inf...	2	2,00	-3.632,78	-0,28
		Excepciones de límite su...	1	1,00	300.000,00	23,31
		Totales:	100	100,00	1.287.029,52	100,00

Fig. 5.2
Desarrollo de la sección Ventas, análisis de muestras por estratos.

Al hacerlo de esta manera se puede dar cuenta perfectamente que el mayor peso de registros se encuentra en el estrato número 3, ya que cuenta con el 25 % de los registros totales. Luego, seleccionando el número sub rayado y de color azul nos lleva directamente a la base de datos de origen y ahí podemos estudiar cada caso, podemos decir que las excepciones son los valores que están por debajo del número “0”.

De manera graficada para este caso nos el siguiente resultado:

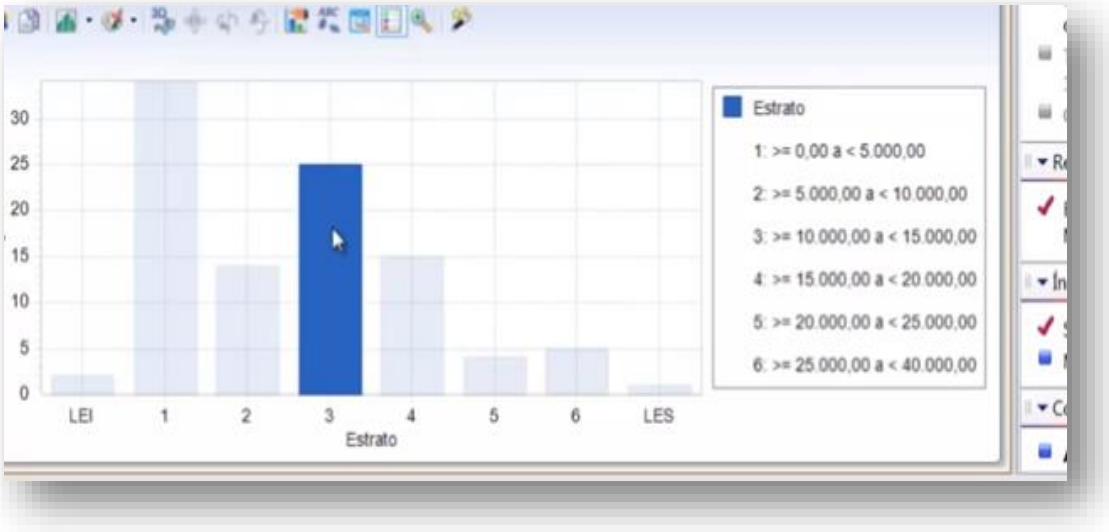


Fig. 5.3
Muestra de resultados de manera gráfica.

A como se puede observar, el estrato número 1 (0.00 < 5,000.00) tiene mayores datos, sin embargo en el estratos 3 a como lo mencionamos en el párrafo anterior es donde está la mayor concentración de datos en montos monetarios.

Facturación.

En este caso, la herramienta que permite IDEA usar es:

- Convertir al tipo de cambio del día de la contabilización o bien a la del documento, esto aplica en dado caso que la moneda que se esté utilizando no sea la moneda de operación en este caso sería el córdoba.

- Saber las facturas anuladas debido a que también hoy en día se dice que un documento esta anulado por esconder alguna malversación del flujo de dinero.

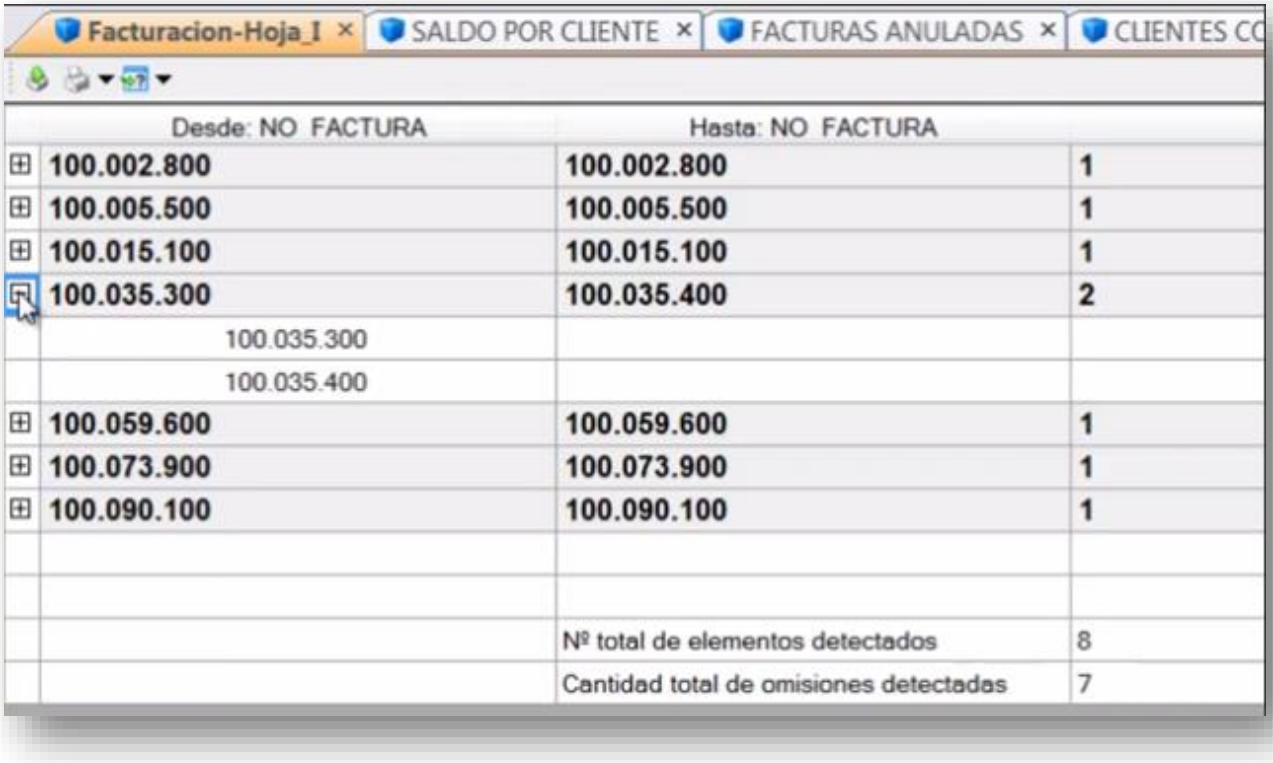
- Extraer a clientes/proveedores que tengan varias facturas, esto debido a que en el tráfico o volumen de facturas es donde hay incidencia para lo no honesto.

- Omisiones de facturas.

A cómo se puede observar, en este caso, existe una factura que no se encontraba en el reporte a simple vista en la manera correcta pero que utilizando este medio, si pudimos detectarla por medio de la numeración de la misma, por consiguiente se procede a la solicitud y análisis de la misma.

	NIT	NUM_DE_REG	MPORTE_BS_SUM
1	1037834	3	21.174,65
2	1406783	2	17.913,75
3	1407665	2	10.290,88
4	1413279	2	34.294,44
5	1414966	3	32.312,52
6	1417710	2	15.288,10
7	1421651	2	28.246,98
8	1422078	2	17.871,41
9	1424227	2	96.912,59

Fig. 5.4
Análisis de facturas por importes, sección facturación.



Facturacion-Hoja_I | SALDO POR CLIENTE | FACTURAS ANULADAS | CLIENTES CC

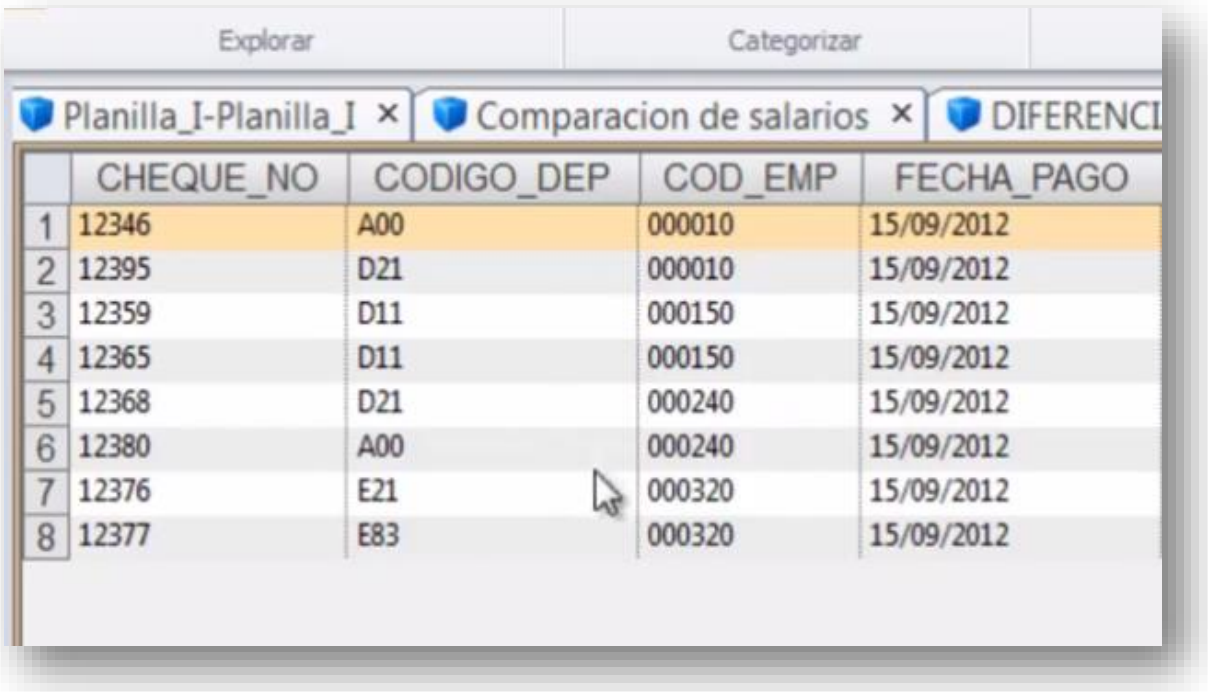
Desde: NO_FACTURA	Hasta: NO_FACTURA	
100.002.800	100.002.800	1
100.005.500	100.005.500	1
100.015.100	100.015.100	1
100.035.300	100.035.400	2
100.035.300		
100.035.400		
100.059.600	100.059.600	1
100.073.900	100.073.900	1
100.090.100	100.090.100	1
	Nº total de elementos detectados	8
	Cantidad total de omisiones detectadas	7

Fig. 5.5
Análisis de facturas en caso de duplicidad, sección facturación.

Planillas:

Aplicado a este módulo se puede decir que aquí se toman como referencia 2 tipos de planillas en dado caso sean quincenales (En Nicaragua la mayoría de las empresas utilizan este sistema de pagos), ya que esto nos permite la comparación y dar como resultado las diferencias en caso de variabilidad.

Cabe destacar que las variaciones de una u otra manera existirán siempre en el área de ventas o bien otras áreas que tengan comisiones en sus salarios.



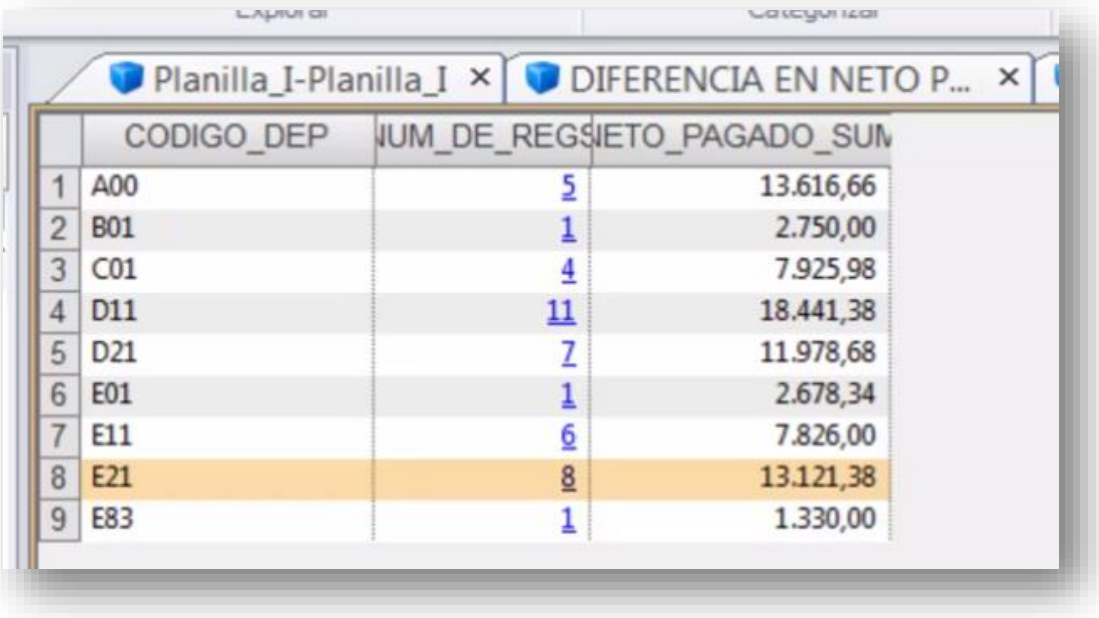
	CHEQUE_NO	CODIGO_DEP	COD_EMP	FECHA_PAGO
1	12346	A00	000010	15/09/2012
2	12395	D21	000010	15/09/2012
3	12359	D11	000150	15/09/2012
4	12365	D11	000150	15/09/2012
5	12368	D21	000240	15/09/2012
6	12380	A00	000240	15/09/2012
7	12376	E21	000320	15/09/2012
8	12377	E83	000320	15/09/2012

Fig. 5.6
Análisis de pagos efectuados a trabajadores, sección planillas.

Fig. 5.7
Muestra de variaciones de salarios, sección planillas.

A cómo se puede apreciar, el empleado número 11, aparece duplicado en las planillas.

Y como resultado total, el consolidado de las planillas de ambas quincenas.



Planilla_I-Planilla_I | DIFERENCIA EN NETO P...

	CODIGO_DEP	NUM_DE_REGS	NETO_PAGADO_SUM
1	A00	5	13.616,66
2	B01	1	2.750,00
3	C01	4	7.925,98
4	D11	11	18.441,38
5	D21	7	11.978,68
6	E01	1	2.678,34
7	E11	6	7.826,00
8	E21	8	13.121,38
9	E83	1	1.330,00

Fig. 5.8
Consolidado de planillas en períodos diferentes.

Seguridad.

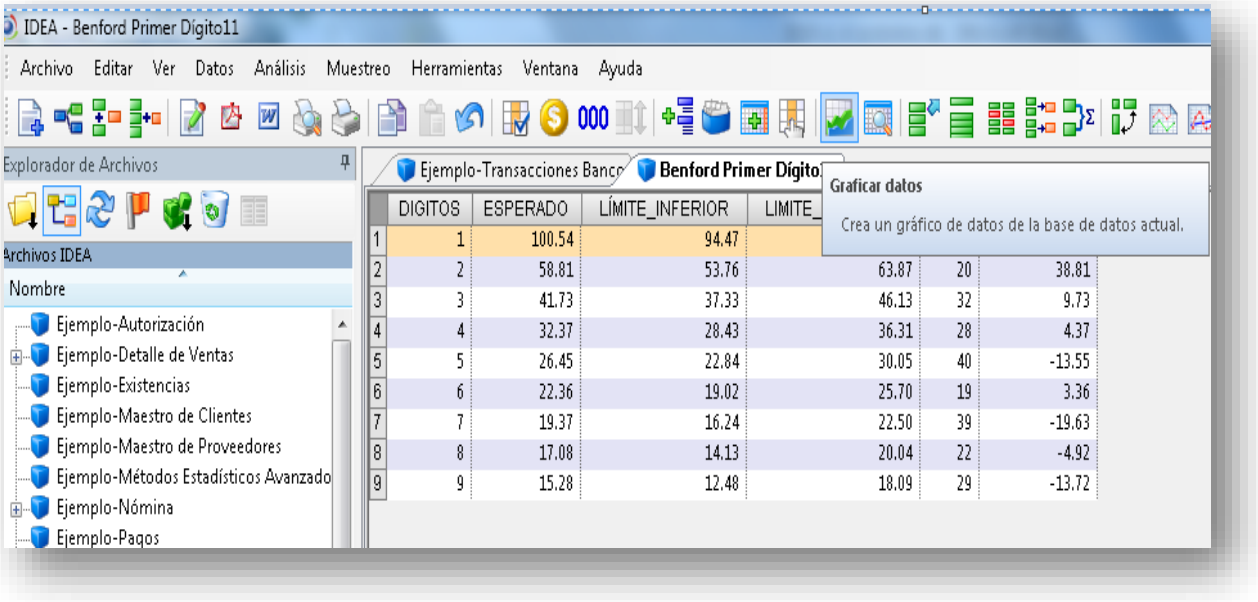
En estos casos, se observa que hoy en día a como se menciona en los temas de investigación, así como existen muchas personas que se encargan de velar por la seguridad existen algunos dentro de la organización que se encargan de violar las normas y procedimiento a fin de conseguir información de la empresa a la cual laboran para fines lucrativos y en el peor de los casos valerse de la misma para fines personales en la creación de sus propias empresas.

Se considera en la imagen anterior y posterior a usuarios dentro de la empresa que no tienen acceso a la información pero que si de una u otra manera pudieron incursionar en la misma.

Fig. 5.9
Análisis de usuarios internos de la empresa sección Seguridad.

Bancos.

Los importes a como se observan están negativos debido a que son importes de salidas (cheques) y los importes positivos (depósitos).



	DIGITOS	ESPERADO	LÍMITE_INFERIOR	LIMITE_		
1	1	100.54	94.47			
2	2	58.81	53.76	63.87	20	38.81
3	3	41.73	37.33	46.13	32	9.73
4	4	32.37	28.43	36.31	28	4.37
5	5	26.45	22.84	30.05	40	-13.55
6	6	22.36	19.02	25.70	19	3.36
7	7	19.37	16.24	22.50	39	-19.63
8	8	17.08	14.13	20.04	22	-4.92
9	9	15.28	12.48	18.09	29	-13.72

Fig. 5.10
Gráfica para el análisis de la Ley de Benford en la cuenta de Bancos.

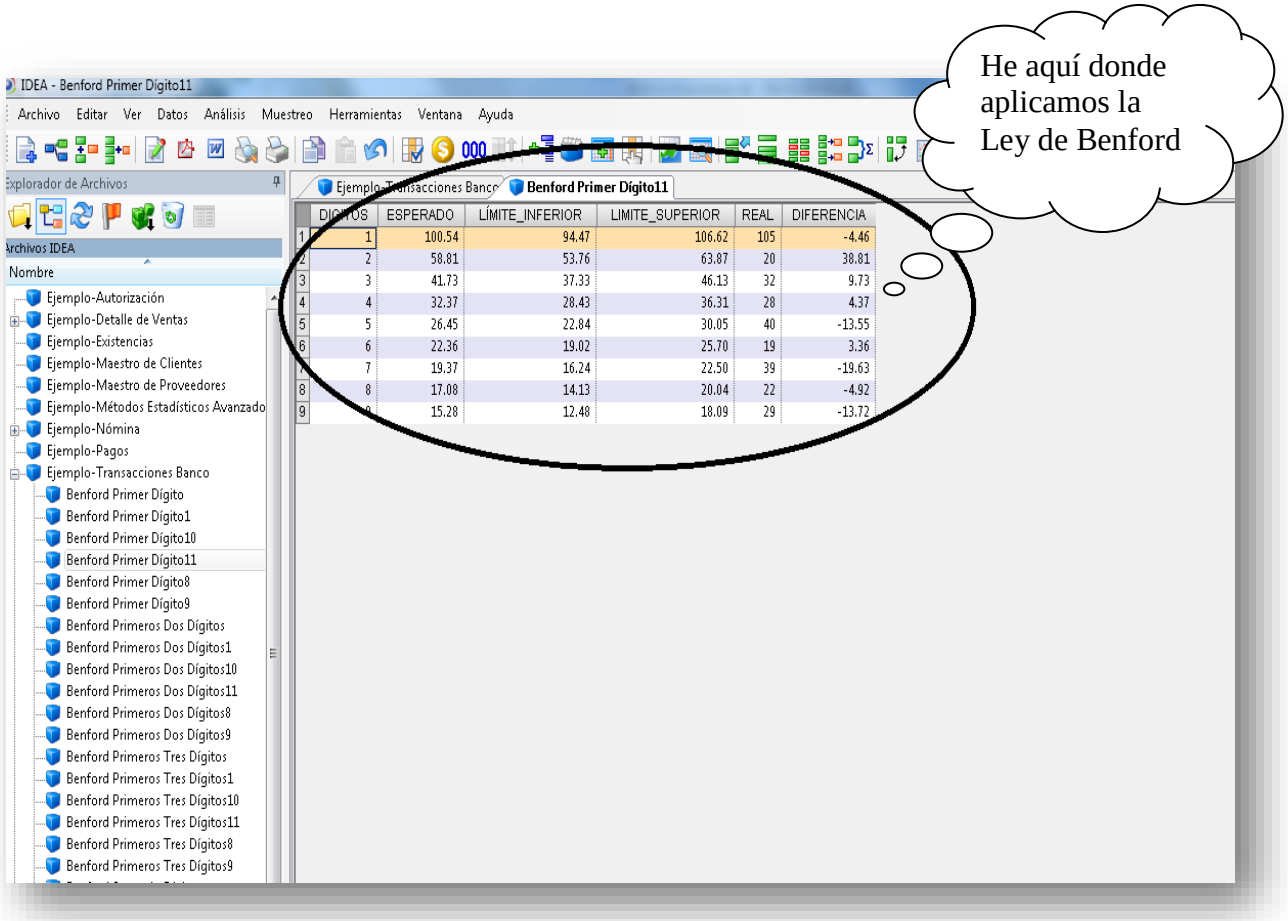


Fig. 5.11
Continuación de procedimiento para el análisis de la Ley de Benford.

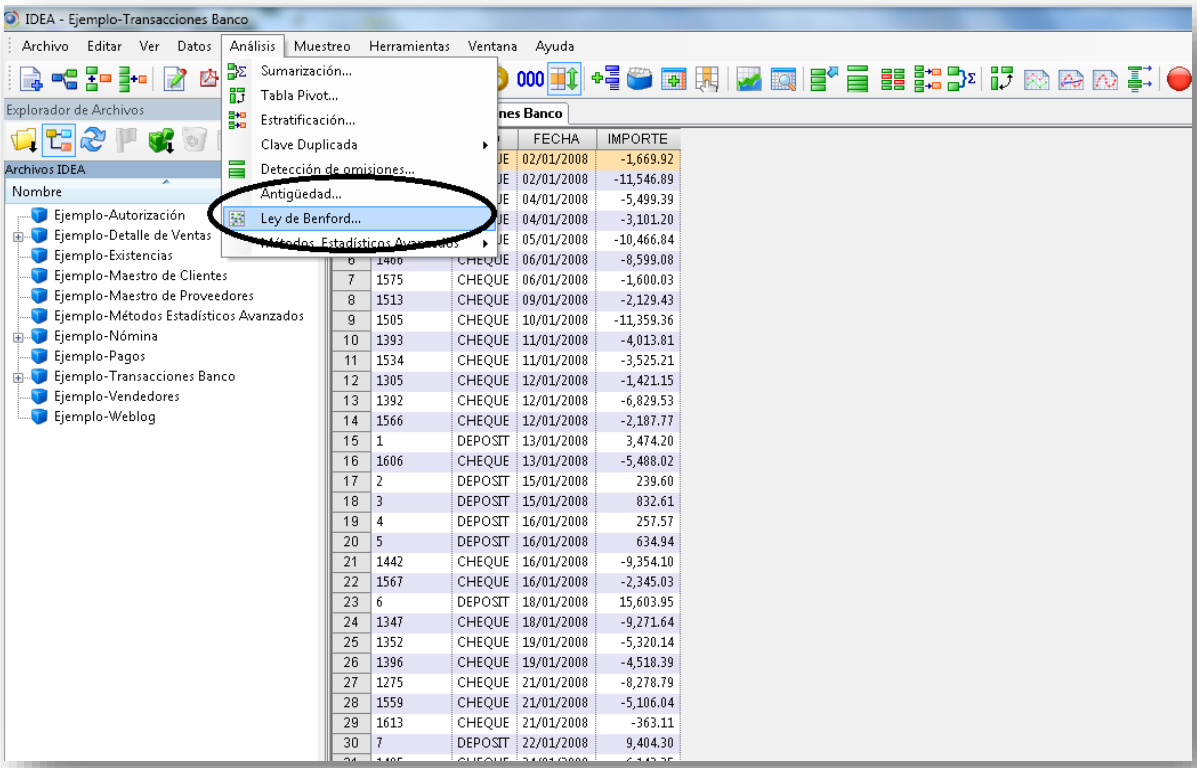


Fig. 5.12
Análisis aplicando la Ley de Benford.

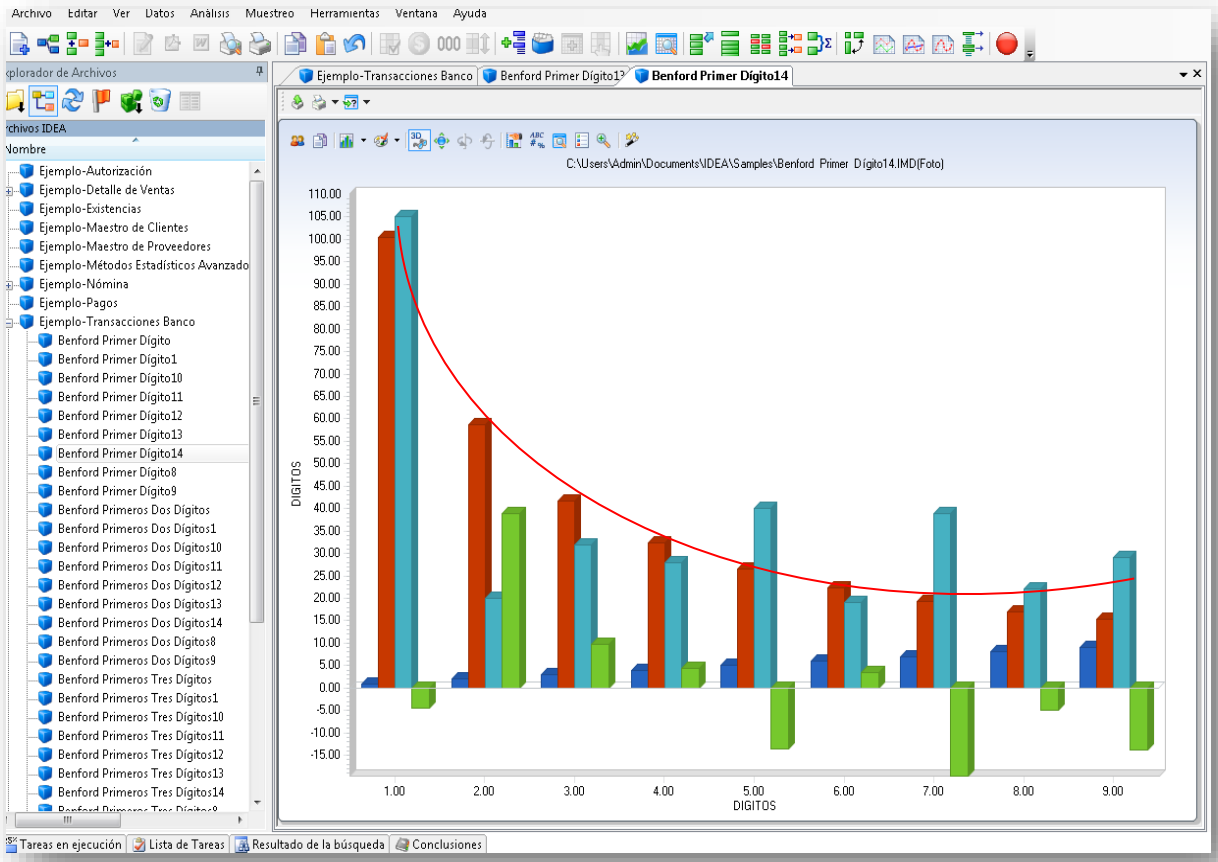


Fig. 5.13
Gráficas de la línea de tendencia según valor esperado.

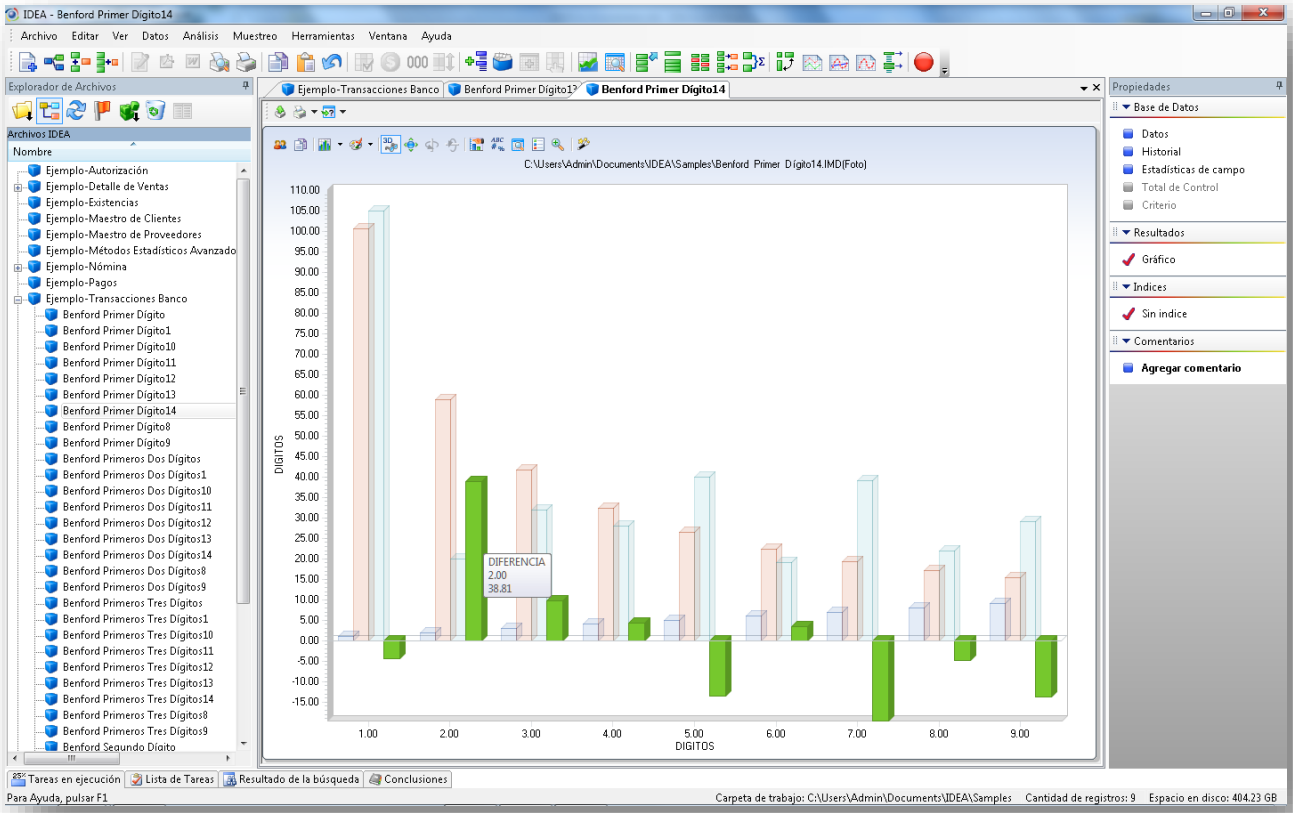


Fig. 5.14
Gráficas de resultadosla línea de tendencia según valor esperado.

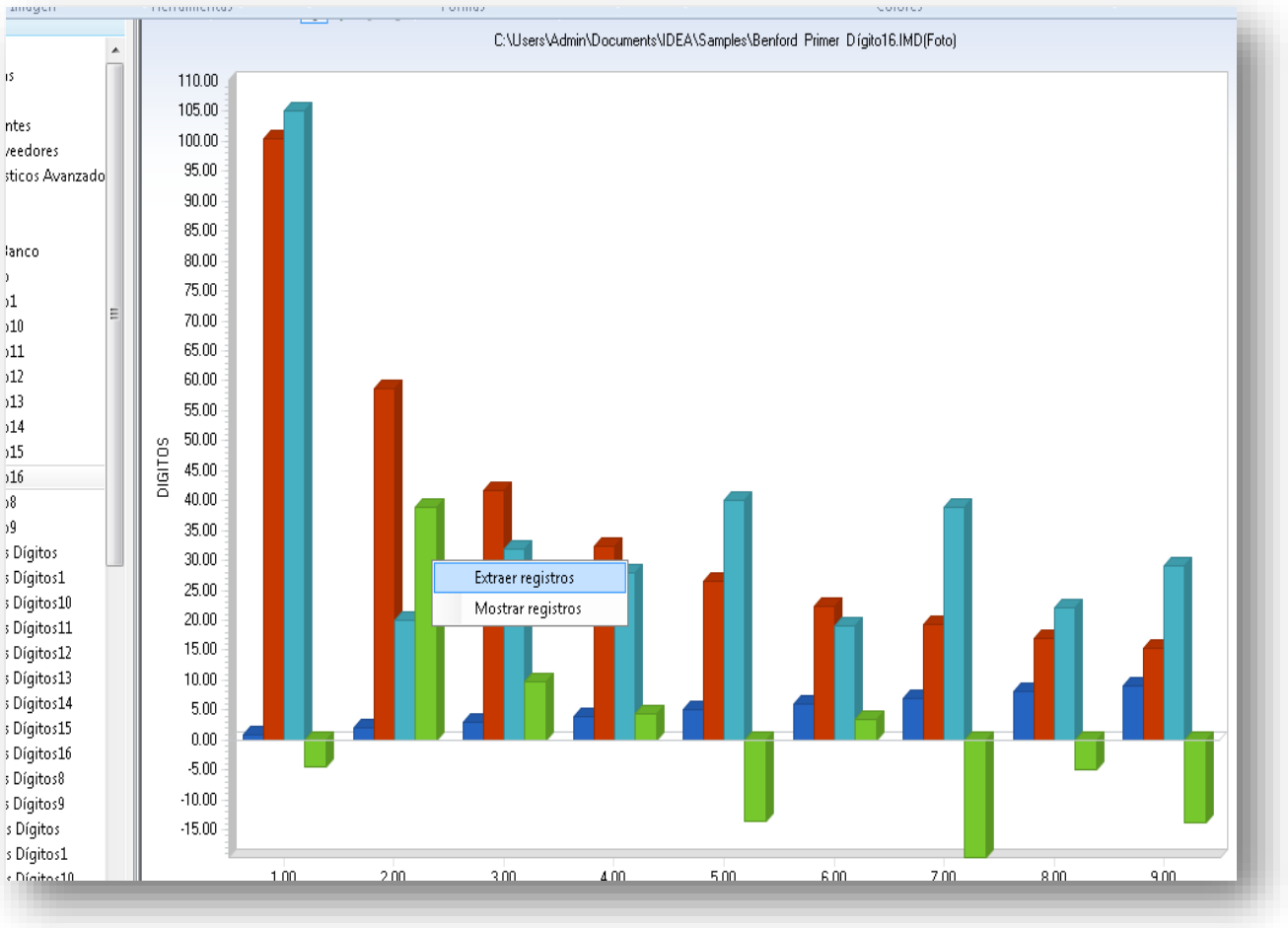


Fig. 5.15
Gráficas de datos para el análisis efectivo en cuanto a su grado de variación vrs. El valor esperado.

Aquí donde está la mayor incidencia de variaciones en cuanto a los datos de cheques por lo que para el auditor se le felicitaría y llamaría mucho la atención para revisar uno a uno cada dato, concentrado en este grupo, cabe destacar que para obtener este segmento de datos solo se ubica sobre la barra de diferencia y esta misma lo ubica de donde extrajo los datos para dar este resultado.

Análisis del caso práctico:

IDEA, una herramienta de trabajo, el cual facilita el proceso de investigación en la busca de errores o anomalías, Con este sistema se pueden visualizar, analizar, manipular, obtener muestras y extraer datos de cualquier fuente incluyendo reportes impresos que les permitirá concluir y extender el alcance de su trabajo proporcionándole funciones exclusivas y características no disponibles en otros software.

El programa puede dar información acerca de cada área de la cual se desea hacer el análisis como: bancos, clientes, ventas, etc., En este caso haremos un estudio de los salarios de los trabajadores de una empresa cotejando las planillas estas serán quincenales, ya que permite la comparación para examinar si hay duplicidad de trabajadores, si los montos de los salarios varían, si el valor del salario está siendo calculado correctamente, y otros hallazgos, al conseguir los resultados que se obtienen al aplicar el sistema de auditoría IDEA ,utilizando la Ley de Benford , los efectos se podrán medir y tomar decisiones reales.

Otros datos acerca de IDEA, que son de mucha relevancia.

A nivel mundial y de firma de Auditoría:

- KPMG.
- BDO Audit.
- Moore Stephens.
- Grant Thornton.
- Horwath Crowe Consulting Group.
- Price Waterhouse Cooper[3]

Entidades del estado, servicios públicos, industria, universidades, comunicaciones, sector financiero.

Más de 85.000 usuarios en más de 90 países utilizan el software IDEA y se encuentra disponible en 13 idiomas.

[3] Es un usuario y principal distribuidor en Centro América

VI. Conclusiones

El contenido de este trabajo expresa un enfoque sobre el uso de tecnología y software de cómo pueden ayudar a los auditores a realizar trabajos mejor enfocados a las áreas de alto riesgo, dejando por fuera las transacciones de menor riesgo de fraude. Aunque las computadoras han complicado el trabajo de auditoría, las pruebas asistidas por computador ayudan a mejorar el alcance y calidad de las mismas, así como los resultados de una investigación de fraude.

Un importante paso para la detección de fraude es la revisión de los datos disponibles para detectar síntomas de fraude. El usar tecnología proporciona un Amplio acceso a la información. Como independencia de Información, permitiendo al auditor tener mayor confianza sobre la información auditada.

Llevar a cabo análisis específicos de los datos como el cálculo de estadísticas diversas, detección de omisiones, detección de duplicados, sumas totales, etc. Importar datos desde un amplio rango de tipos de archivos, capacidad de análisis a grandes volúmenes de transacciones, desarrollo de análisis y reportes personalizados. En General, mejoras en la eficiencia, calidad, sostenibilidad y escalabilidad de los procesos de revisión.

Tener fácil acceso a toda la información permite detectar fraude realizando análisis de datos se requiere tener acceso a la información contenida en todas las aplicaciones de negocio de forma individual. Esto incluye el acceso a tablas maestras, tablas conteniendo registros en detalle e incluso tablas de configuración en algunos casos. Usar la tecnología adecuada

permitirá analizar el 100% de la información disponible sin importar el tamaño volumen y tipo, comparar datos de diferentes sistemas.

Se demostró mediante un caso práctico como La Ley de Benford permite identificar posibles errores, detectar fraudes potenciales, incumplimiento de controles y otras irregularidades. Ya que las organizaciones sufren un importante coste como resultado del fraude, por lo tanto debería ser esta la principal interesada en su prevención.

VII. Bibliografía

Badillo, J. (s.f.). *Foro de seguridad*. Obtenido de http://www.forodeseguridad.com/artic/discipl/4166.htm (recuperado el 12/10/2014 10:44 am)

Bardale, J. (2007). La auditoría ante la corrupción. *Alternativa financiera*, *4*, 27-30.

Boletin Update CAATT. (Diciembre de 2013).

Cano, M., & Lugo, D. (s.f.). Auditoría Forense en la investigación criminal del lavado de dinero y activos. *Auditoria del Siglo XXI*.

Cano, M., & Rodríguez, J. (Enero de 2005).

Castañeda, L. (s.f.).

Código Penal de Nicaragua. (1998). Managua.

Deloitte. (Noviembre de 2007). Diez cosas acerca del control del fraude. *Deloitte Forensic Center*, 14.

Edilma, M. (2006). Obtenido de http://www.ideaf.org.html, (Recuperado el 25-10-2014 5:05 pm)

Fontan, M. (s.f.). *Foro de seguridad*. Obtenido de http://www.forodeseguridad.com/artic/discipl/4166.htm (recuperado el 12/10/2014 10:25 am).

Fudim, A. (2003).

Holmes, W. (s.f.).

IAIE. (Marzo de 2006). Prevención y detección de fraude y auditoría forense sector privado. *Instituto de Auditores Internos de Ecuador.*

IFAC. (2012). Recuperado el 25/10/2014, de http://www.ifac.org

Insa, F. (Julio de 2007). Software y nuevas tecnologías. *Fraude y actos desleales de los empleados cometidos a través de dispositivos Tecnológicos*, *212*, 94.

Intermerican. (s.f.). Obtenido de http://interamerican-usa.com/articulos/Auditoria/Audi-fore-tec-inv.htm., (Recuperado el 30-10-2014 5:010 pm).

Isa. (2011). Código Antifraude. *Manuscrito no publicado*.

KPMG. (2012). Informe de fraude en el Perú 2012. *Cutting through Complexity*, 24.

KPMG. (2013). Encuesta de fraude-Colombia . *Sección: Tecnología*, 31.

León, L. (s.f.).

Linares, G., & Jenith, E. (2013). COSO IV. *La Evolución del Control Interno, Basado en Principios.* Managua.

Machicado, J. (2010). Obtenido de http://jorgemachicado.blogspot.com/2009/03/objeto-del-delito.html, (Recuperado 01/11/2014)

Maldonado, M. (2003).

Maldonado, M. (s.f.). Obtenido de http://www.forodeseguridad.com/artic/discipl/4166.html (Recuperado el 12/10/2014 10:42 am)

Milton, K., & Maldonado, E. (2008). El objetivo principal de la auditoría forense. *2da Edición*.

NEPAI. (s.f.). *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna (recuperado el 15-10-2014 9.56 am).*

NIA´s. (2009). Normas Internacionales de Auditoría. En *Fraude en una Auditoría de Estados Financieros.*

PwC. (2013). COSO: Internal Control Integrated Framework. En P. España (Ed.). Madrid, España.

PwC. (2014). Global Eonomic Cime Srvice. *Survey 2014*, 46.

Quiroga, L. (Abril de 2005). Aspectos para mejorar la seguridad los sistemas de información. *Instituto de Auditores Internos de Argentina.*

Ramos, D. (s.f.). Fraude un nuevo enfoque en combatirlo. *Safe Consulting Group.*

Revista Varianza. (Noviembre de 2012). *Ley de Benford*, 9-12.

Rojas, J. (s.f.). *Técnicas de Auditoría Forense.* Grant Thornton.

Ruette, R. J. (2006). *http://www.ideaf.org*. Obtenido de http://www.ideaf.org.html, (Recuperado el 25-10-2014 4:55 pm)

Safe Consulting Group. (2006). Fraude: Un nuevo ebfoque para combatirlo. *Auditoría Pública*(38), 101-103. Obtenido de http://www.ideaf.org (recuperado el 28-0-2014 10:50 am)

Tanzi, V. (1995).

Valero, N., & Roa, M. (2013). Estructura de control interno COSO: Preparandose para los cambios. (pág. 13). Deloitte.

Vega, C. (s.f.). Obtenido de http://www.forodeseguridad.com/artic/discipl/4166.htm (Recuperado el 12/10/2014 10:50 am)

VIII. Anexos

Anexo 1: Auditoría Forense y el uso de la Ley de Benford

Fig. A1.1

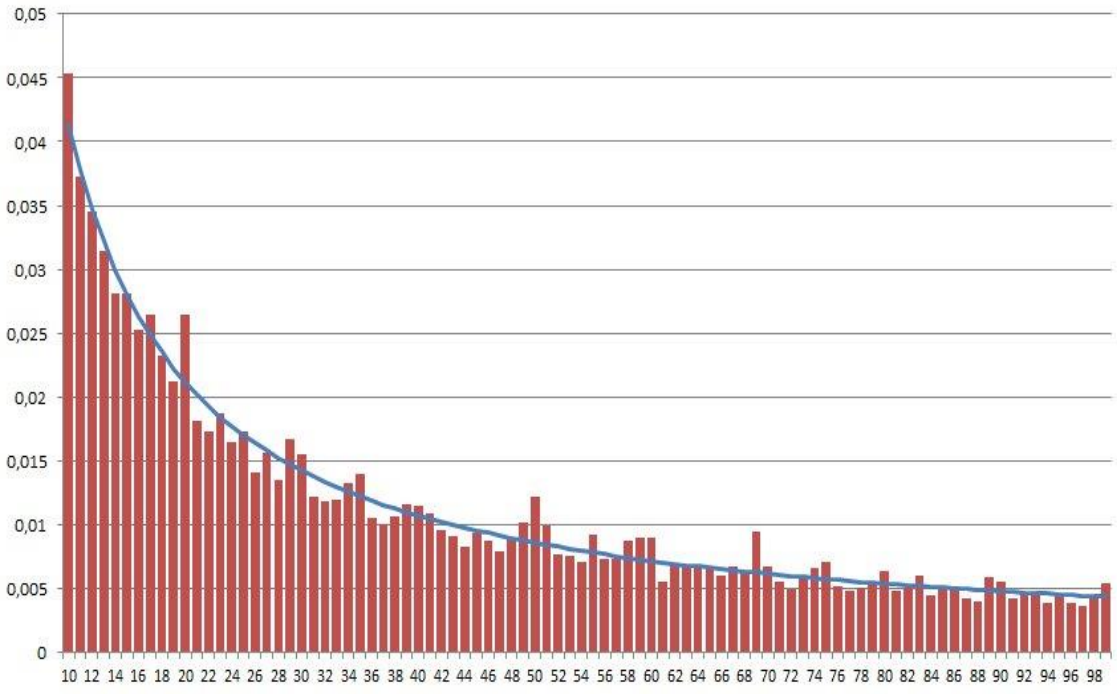


Fig. A1.2

Anexo 2: Software utilizado IDEA y su relación con la Ley de Benford

Fig. A2.1

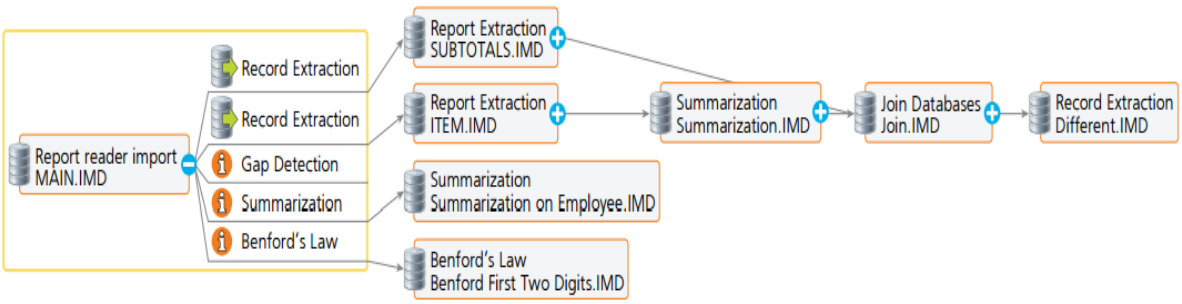


Fig. A2.2

Anexo 3: Aplicación de la Ley de Benford en una hoja de cálculo

De una serie de 2,000 números del 1-9, se ejecutó un comando en Visual Basic, quedando de la siguiente manera:

```
Sub Benfore()
Dim Arrayone(0 To 9) As Integer
Dim Arraytwo(0 To 9) As Integer
Dim Arraythree(0 To 9) As Integer
Dim Arrayfour(0 To 9) As Integer
Dim Arrayfive(0 To 9) As Integer
Dim Arraysix(0 To 9) As Integer
Dim Arrayseven(0 To 9) As Integer
Dim Arrayeight(0 To 9) As Integer
Dim Arraynine(0 To 9) As Integer
Dim Arrayzero(0 To 9) As Integer
Dim Arraywotest(10 To 99) As Integer
Dim I

Dim Row As Long, Col As Long, Step As Long, Colcells

Dim Digits As Long, Total As Long

Worksheets(1).Select

Col = Application.CountA(ActiveSheet.Range("1:1"))

For Step = 1 To Col
   Cells(1, Step).Select
   Selection.End(xlDown).Select
   Row = ActiveCell.Row

For Colcells = 1 To Row

For Digits = 1 To Len(Cells(Colcells, Step))

Select Case Mid(Cells(Colcells, Step), Digits, 1)
   Case 1
      Arrayone(Digits) = Arrayone(Digits) + 1

   Case 2
      Arraytwo(Digits) = Arraytwo(Digits) + 1

   Case 3
      Arraythree(Digits) = Arraythree(Digits) + 1

   Case 4
      Arrayfour(Digits) = Arrayfour(Digits) + 1
```

```
    Case 5
       Arrayfive(Digits) = Arrayfive(Digits) + 1

    Case 6
       Arraysix(Digits) = Arraysix(Digits) + 1

    Case 7
       Arrayseven(Digits) = Arrayseven(Digits) + 1

    Case 8
       Arrayeight(Digits) = Arrayeight(Digits) + 1

    Case 9
       Arraynine(Digits) = Arraynine(Digits) + 1

    Case 0
       Arrayzero(Digits) = Arrayzero(Digits) + 1


    End Select
   Next Digits
  Next Colcells
Next Step

Worksheets(2).Range("C5").Value = Arrayone(1)
Worksheets(2).Range("C6").Value = Arraytwo(1)
Worksheets(2).Range("C7").Value = Arraythree(1)
Worksheets(2).Range("C8").Value = Arrayfour(1)
Worksheets(2).Range("C9").Value = Arrayfive(1)
Worksheets(2).Range("C10").Value = Arraysix(1)
Worksheets(2).Range("C11").Value = Arrayseven(1)
Worksheets(2).Range("C12").Value = Arrayeight(1)
Worksheets(2).Range("C13").Value = Arraynine(1)

Worksheets(3).Range("C5").Value = Arrayone(2)
Worksheets(3).Range("C6").Value = Arraytwo(2)
Worksheets(3).Range("C7").Value = Arraythree(2)
Worksheets(3).Range("C8").Value = Arrayfour(2)
Worksheets(3).Range("C9").Value = Arrayfive(2)
Worksheets(3).Range("C10").Value = Arraysix(2)
Worksheets(3).Range("C11").Value = Arrayseven(2)
Worksheets(3).Range("C12").Value = Arrayeight(2)
Worksheets(3).Range("C13").Value = Arraynine(2)
Worksheets(2).Select

End Sub
```

		PORCENTAJES			
Dígito	Total de Datos	Benford	Datos	Diferencia	Significancia
1	196	30%	11%	-19%	568.69
2	201	18%	11%	-6%	332.96
3	193	12%	11%	-2%	235.49
4	196	10%	11%	1%	182.72
5	193	8%	11%	3%	149.05
6	222	7%	12%	6%	127.10
7	172	6%	10%	4%	108.31
8	194	5%	11%	6%	96.13
9	217	5%	12%	8%	86.57
Totales	1784				1,906.51

Fig. A3.1 Resultado numérico

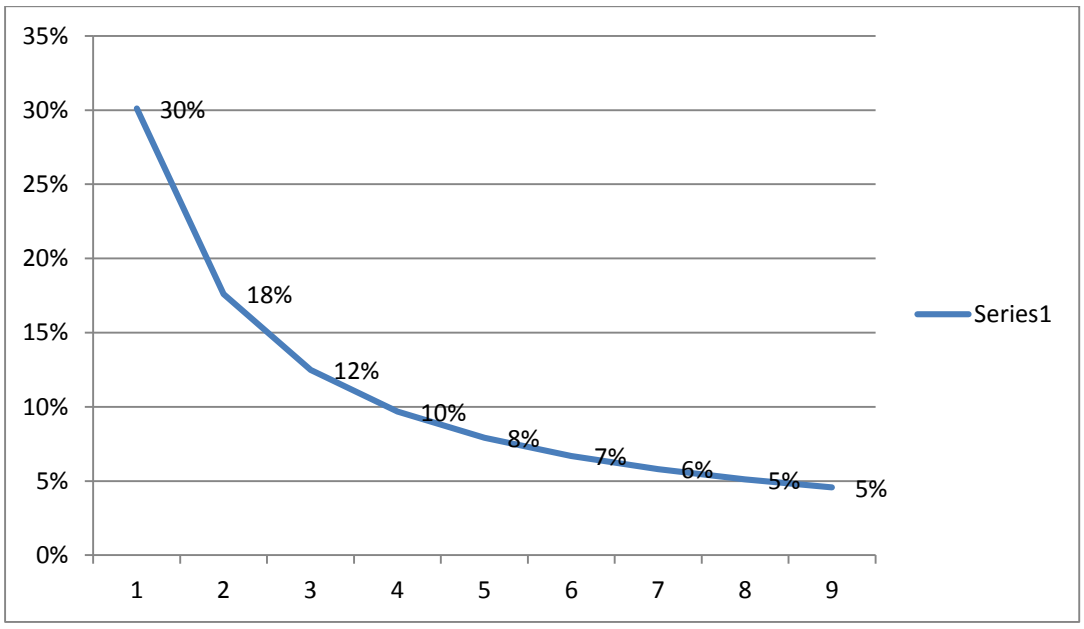


Fig. A3.2 Resultado gráfico porcentual:

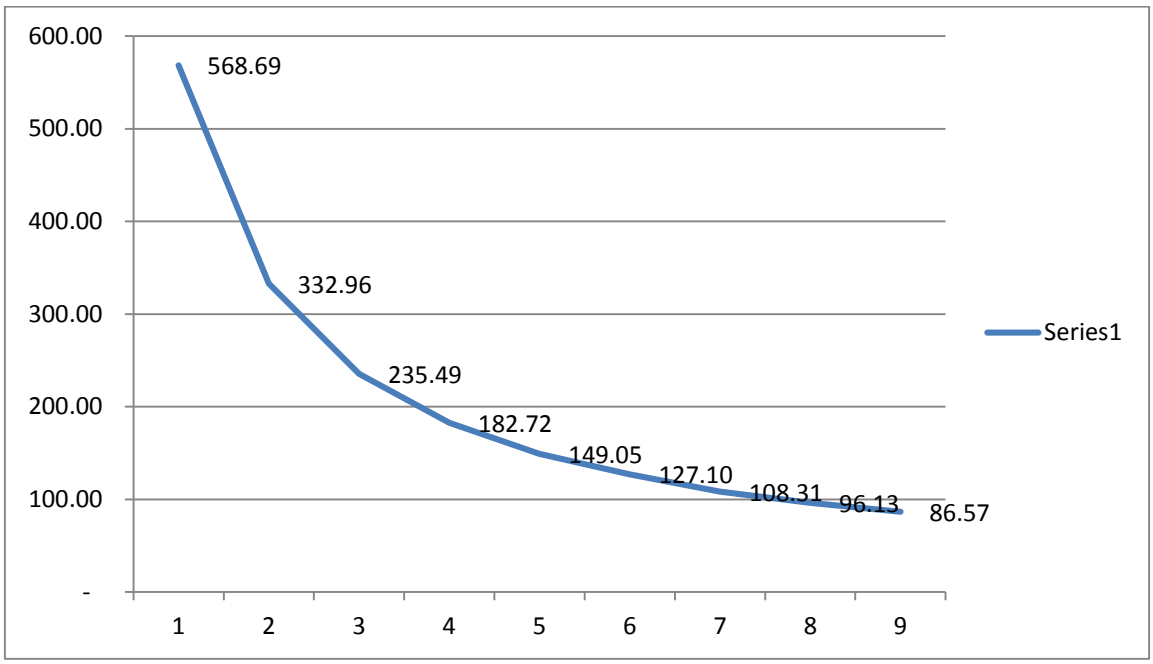


Fig. A3.3 Resultado gráfico números enteros

Anexo 4: Estadísticas relevantes en cuanto al fraude

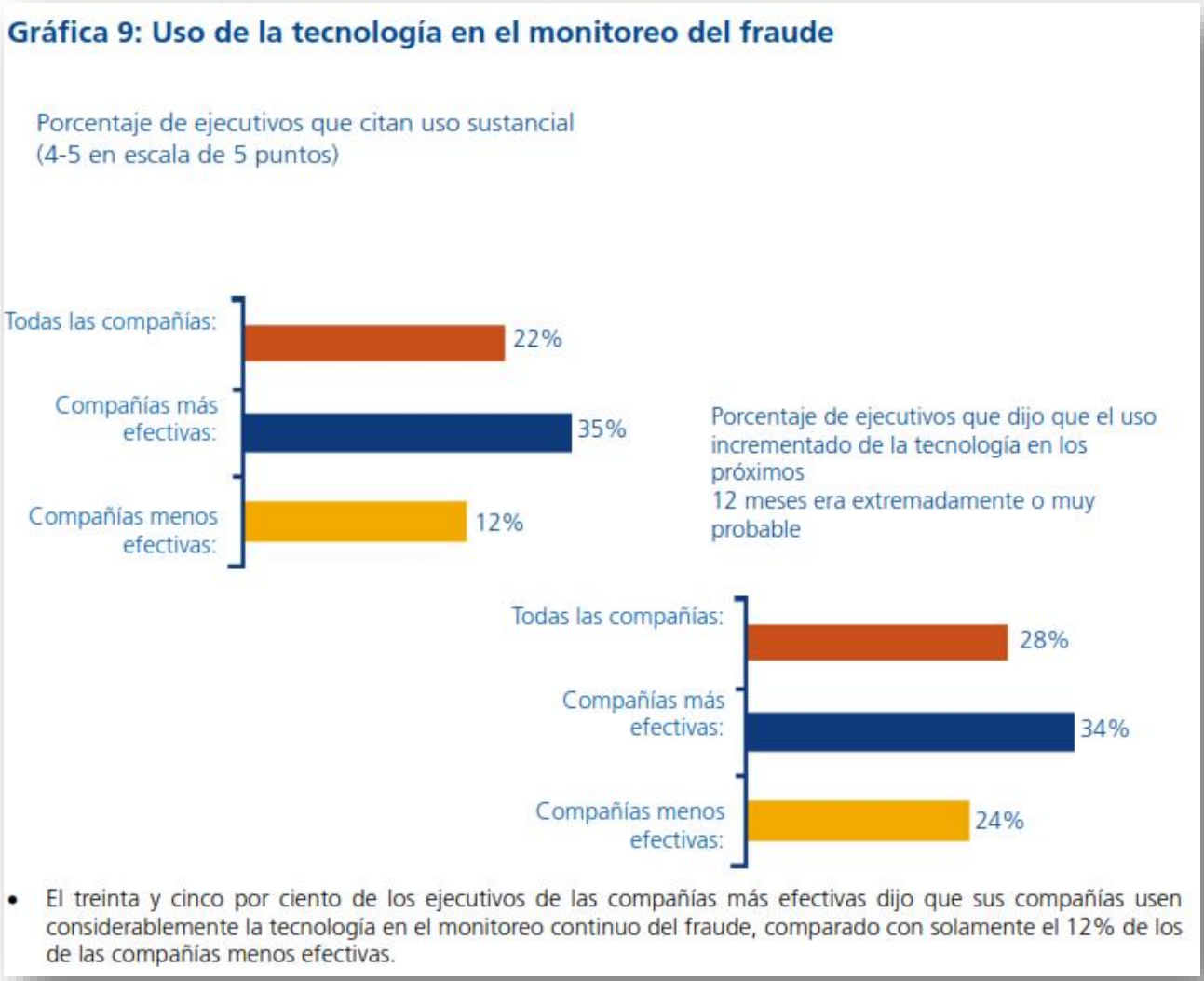


Fig. A4.1

Uso de la tecnología en el monitoreo del fraude.

Deloitte. (Noviembre de 2007). Diez cosas acerca del control del fraude. Deloitte Forensic Center, (p.14).

Detección

La mayoría de los casos fueron detectados a partir de informantes a través de línea ética y otros métodos de denuncias. En segunda instancia figuran los casos detectados a partir de los controles vigentes en los procesos de la compañía. Se observa que los casos detectados por auditoría interna ascienden al 22%. En muchos casos, las expectativas del público y los ejecutivos son mayores respecto a la función de auditoría interna en materia de fraude. Cuando se detecta un caso, debido al desconocimiento de la función del auditor interno, la pregunta recurrente es ¿por qué no lo vieron los auditores? La función primaria del auditor interno es evaluar y asesorar. Trabaja por muestras y existen diferencias metodológicas entre su trabajo y el trabajo de un auditor forense.

Funciones del Auditor Interno

El Instituto de Auditores Internos define la actividad de auditoría interna como "una actividad **independiente** y **objetiva** de aseguramiento y consulta para **agregar valor** y mejorar las operaciones de una organización." En cuanto al fraude dice que "el Auditor Interno debe tener suficientes conocimientos para identificar **indicadores de fraude (RED FLAGS)**, pero no es de esperar que tenga conocimientos similares a aquellas personas cuya responsabilidad principal es la detección e investigación del fraude." (www.theiia.org)

¿Cómo fue descubierto el acto fraudulento?*

*Pregunta de respuesta múltiple

Fig. A4.2
Estadísticas del fraude.

KPMG (2012). Informe de fraude en el Perú 2012. Cutting Through Complexity(p.24).

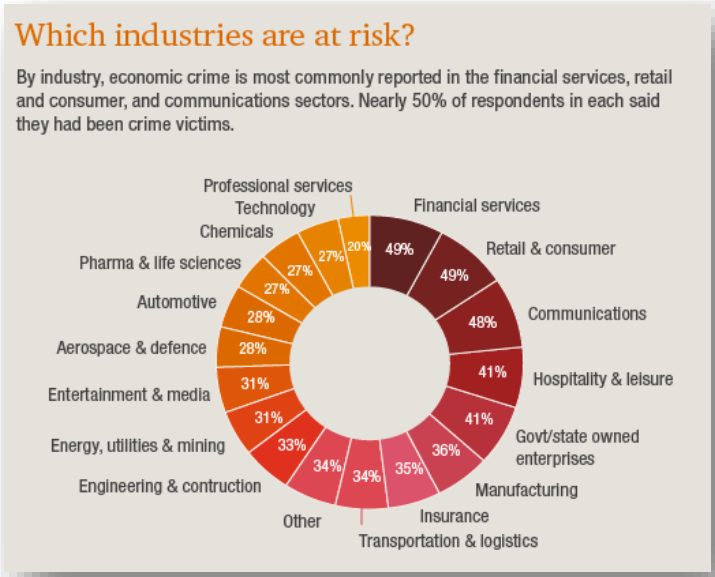


Fig. A4.3
Gráfico de las Industrias con mayor riesgo.

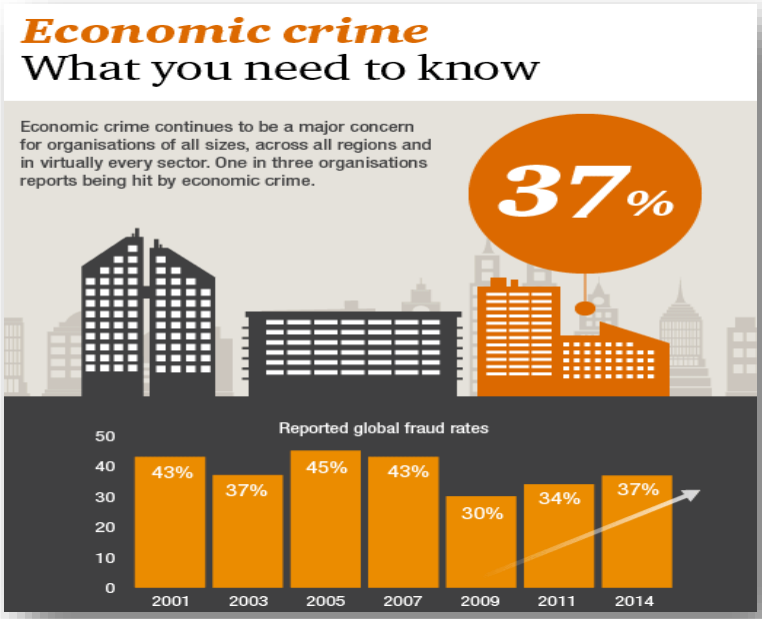


Fig. A4.4
Gráfico de las Industrias con mayor riesgo.

PwC (2014), Global Economic Crime Service, *Survey 2014*, (p.46).