EL FRAUDE EN LOS SISTEMAS DE INFORMACIÓN*

Yasnyr Estévez Q.**

RESUMEN

El artículo enfatiza en los efectos del fraude en las empresas e incluye los riesgos en las transacciones en sistemas de cómputo, esquemas de fraude informático, pasos para detectar el fraude, apoyo al Contador Público en la detección del fraude, el informe de hallazgos del fraude.

INTRODUCCIÓN

Las organizaciones se exponen continuamente a diversos riesgos, entre los cuales están los de carácter económico, es decir, a perder recursos, por las actuaciones de sus propios empleados, de clientes, de proveedores, etc., por lo tanto se hace necesario la existencia de controles minuciosos para prevenir y detectar dichos riesgos.

Este ensayo pretende proporcionar a los Contadores Públicos, elementos relacionados con los aspectos informáticos que impactan las empresas y que presentan, por lo menos, dos situaciones.

La primera es el beneficio para aquellas que manejen las herramientas informáticas de forma apropiada y actualizada y, la segunda, cuando no se manejan eficientemente o se descuida su utilización, facilitando la ejecución de fraudes. Los enfoques, como el de Auditoría Forense, en un lineamiento como el tecnológico, pueden ayudar a un Contador Público para que investigue las causas de fraude y detecte las debilidades de una empresa y, por supuesto, haga mención a las recomendaciones, una vez analizados los hallazgos encontrados.

El Contador Público en su función de Auditor puede presentar debilidades

* Presentado en noviembre de 2011, aprobado en Comité de agosto de 2012.

** Contador Público, Especialista en Auditoría Forense, Docente investigador Facultad de Contaduría Pública.

en la verificación de los sistemas de información, cuando no es su campo de acción permanente. Para poder enfocarse en temas de sistemas de información, este profesional requiere de algunos conocimientos técnicos que no son difíciles de entender, pero sí requieren de habilidad.

De igual forma, este ensayo pretende orientar a los estudiantes y a los profesionales de la Contaduría Pública sobre los diferentes escenarios que se pueden presentar en las organizaciones, mediante la utilización de dispositivos electrónicos que ayudan a cometer fraude en una empresa.

También pretende relacionar algunas de las herramientas en informática para aspectos de riesgo y en temas forenses y de verificación, su aplicación y su desarrollo, teniendo en cuenta que los riesgos son algo dinámico; por lo tanto, los elementos de análisis deben ir en el mismo sentido, con el fin de poder enfrentar los desafíos que se presentan.

Por lo anterior, se pretende:

1. Describir los riesgos existentes en transacciones mediante sistemas de cómputo en las organizaciones.

2. Exponer los diferentes esquemas de fraude actuales y su incidencia en el proceso contable.

3. Relacionar y describir los pasos para poder determinar un fraude bajo sistemas de cómputo y preservar dichas evidencias para hacer un análisis que conlleve al dictamen de un caso relacionado con la auditoría forense.

Los conceptos descritos en este ensayo están basados en teorías de riesgos enfocados en el área de sistemas de tecnologías de información. Las organizaciones que apliquen dichas teorías pueden llegar a determinar cuáles son los riesgos más recurrentes y su impacto, al interior de las mismas. Éstas describen las oportunidades y su corrección obedece a las necesidades de cada empresa en particular. Es por ello que se presenta la diversidad de herramientas que pueden mitigar[1] los riesgos y otros eventos que causan catástrofes que impactan los beneficios económicos.

El desarrollo de los temas se efectúa desde los siguientes puntos de vista: riesgos en transacciones en sistemas de cómputo; definición de esquemas de fraude informático y su incidencia en las empresas; pasos para la detección de un fraude bajo sistemas computarizados; apoyo del Contador en la detección del fraude bajo sistemas de información computarizado e informe de hallazgos de fraude.

1 [www.rae.es] Mitigar: Moderar, aplacar, disminuir o suavizar algo riguroso o áspero. Junio 20 de 2012: 11:18 am

RIESGOS EN TRANSACCIONES EN SISTEMAS DE CÓMPUTO

"La seguridad no es que las situaciones te afirmen que estás seguro si no que tú afirmes a las situaciones cuán seguro estás"

Noriam[2]

Los riesgos de las transacciones en las organizaciones obedecen a la interacción de las personas con alguna influencia sobre las mismas. La delimitación de funciones y un ambiente de control, entendido como "la forma en que se estructuran las actividades del negocio, se establecen objetivos y se valoran riesgos" (Mantilla, 2005: 25), es lo que debe tener en cuenta la alta gerencia para poder mitigarlo.

Las situaciones de riesgo que se presentan en las organizaciones tienen en común que sustentan situaciones de vulnerabilidad, pero sobre todo de algunos descuidos por parte de algunas áreas.
Los sistemas de información bajo esquemas computarizados han ido evolucionando, pero a medida en que dichas herramientas presentan los adelantos, paralelamente se presentan distintas oportunidades por parte de quienes ven debilidades en los mismos.

Por ello, las empresas deben tener dentro de sus esquemas de seguridad:

- Personal de confianza.
- Claves de acceso.
- Áreas restringidas.
- Manuales de funciones.
- Políticas de interacción con proveedores, prestadores de servicios, personal externo, etc.
- Control de Pirateo (Royer, 2004: 12) de los sistemas (acceso no autorizado de un tercero a todo o a una parte del sistema de información de una empresa).

Al Contador Público, dentro de su labor de Auditoría, le corresponde la verificación de las transacciones en ambientes de sistemas de información, y determinar las conclusiones sobre la razonabilidad de las mismas.

Según el portal NETMEDIA.INFO, los ataques[3] más severos, en Estados Unidos"[4], son el *spyware* y los *keyloggers*.

Dentro de los estudios adelantados por el "Reporte de Investigaciones de Brechas de Información de Verizon 2009"[5], se determinó que los ataques que suelen ser más recurrentes, entre otros se encuentran:

1. Keyloggers y Spyware. Dichos ataques permiten instalarse silenciosamente en la PC con el fin de enviar datos sobre la información que la víctima teclea o almacena en el sistema, incluso, sobre sus hábitos en Internet.

2 [www.sabidurias.com] Citas y frases célebres. Junio 18 de 2012 10:07 am.

3 http://lema.rae.es/drae/ Atacar: Perjudicar, dañar o destruir.

4 www.netmedia.info/featured/los-15-ataques-de-seguridad-mas-comunes/ mayo 31 de 2012: 20:21

5 Anatomy of a Data Breach. Verizon business. Violación de los datos de consulta. Versión 2009.

2. Backdoor o puerta trasera. Estas herramientas dan acceso remoto para controlar los sistemas infectados y, cuando son ejecutados, corren encubiertamente.

3. Inyección SQL. Es una técnica de ataque utilizada para explotar vulnerabilidades en páginas Web que tienen una ruta de comunicación con bases de datos.

4. Abuso al sistema vía acceso privilegiado. Es el abuso deliberado de recursos, accesos o privilegios concedidos a una persona por una organización.

5. Acceso no autorizado con credenciales predeterminadas. Son los métodos a través de los cuales los atacantes obtienen acceso a un dispositivo o sistema protegido con contraseñas y nombres de usuario predeterminados o estandarizados.

6. Violación de usos aceptables y otras políticas. En realidad, este ataque no distingue si fue cometido de manera accidental o premeditada; la violación a una política fue tener graves consecuencias.

7. Acceso no autorizado mediante listas de control de acceso débiles o mal configuradas (ACL). Cuando hay las condiciones el atacante puede accesar a recursos y llevar a cabo acciones sin que la víctima se dé por enterada.

8. Sniffers. Estas herramientas monitorean y capturan información a través de una red.

9. Acceso no autorizado vía credenciales robadas. Para llegar a este punto, el atacante se valió de otros métodos para ganar acceso válido a sistemas protegidos sin ser detectado.

10. Ingeniería social. Con esta técnica el atacante crea una situación para manipular las creencias o sentimientos de la víctima y persuadirla de llevar a cabo una acción, como facilitarle información confidencial.

11. Evasión de los procedimientos de autenticación. Las técnicas para evitar o evadir los mecanismos estandarizados de autenticación con el fin de obtener acceso no autorizado a un sistema.

12. RAM scraper. Una nueva forma de diseño de malware para capturar información en la memoria RAM.

13. Phishing y sus variantes. Una técnica de ingeniería social en la cual un atacante utiliza comunicaciones electrónicas fraudulentas para provocar que el destinatario facilite información.

Las empresas deben contar con las herramientas necesarias para detectar los riesgos, aunque para dañar los sistemas de información y evitar detectar a tiempo las deficiencias en éstos, algunos perpetradores insertan virus, entre los cuales se mencionan:

– Gusanos (*worms*): programas creados por un tercero con la característica de anclarse en el disco duro y una vez allí no se pueden quitar con facilidad. Se pueden adquirir por envío de archivos infectados vía e-mail, o por compartir memorias o discos con igual característica.

– Caballos de Troya (*troyan horses*): su característica particular es que inserta camuflados los virus, pero no se pueden ver con facilidad. El operador considera que todo está bien, pero al hacer sus procesos, el virus se encuentra haciendo de las suyas; es decir, dañando el equipo. El Auditor, al momento de hacer sus pruebas de verificación, debe confrontar si las claves de acceso son manipuladas por una sola persona, la separación tanto física como funcional de las áreas, la verificación de las copias de seguridad, en forma periódica y con las salvaguardas requeridas, que los funcionarios conozcan las prohibiciones de instalar *softwares* no autorizados, y que las políticas de la empresa, además de que se estén aplicando, que todos los funcionarios las conozcan.

DEFINICIÓN DE ESQUEMAS DE FRAUDE INFORMÁTICO Y SU INCIDENCIA EN LAS EMPRESAS

"*Algo llamado resolución creativa del problema tiene un nombre más corto. Se llama fraude*"

Sabiduría popular[6]

Como primera medida, es básico definir el fraude informático para luego ver su incidencia en las organizaciones.

Se puede definir como inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual quien lo comente obtendrá un beneficio porque:

1. Altera los datos que ya se han ingresado.

2. Borra archivos.

3. Manipula el *software* con la finalidad de buscar un beneficio económico personal.

Es de anotar que los anteriores esquemas requieren de un nivel, medio o alto de conocimiento en estos temas.

Colombia tiene dentro de su normativa legal la Ley 1273 de 2009, por medio de la cual se establece el sistema de la protección y la información de los datos, como uno de los bienes jurídicamente tutelados. Dicha ley es una adición al Código Penal Colombiano (título VII), la cual contiene algunas definiciones y da las penas a quienes infrinjan la ley por alguno de las causales en ella establecidas, dentro de las cuales se encuentran el acceso abusivo a cualquier sistema de información, uso de algún *software* malicioso, suplantación o violación de datos personales. Las penas varían desde 48 hasta 96 meses de privación de la libertad y hasta 1.000 salarios mínimos mensuales vigentes, de penalidad económica[7]. La parte final del presente informe contiene las normas más importantes en Colombia relacionadas con los delitos informáticos.

6 http://www.laeditorialvirtual.com.ar/Pages/Miscelanea_FrasesIngeniosas.htm 18 de junio de 2012. 10:07 am.

7 Ley 273 de 2009. Artículo 269 G. "suplantación de sitios web para capturar datos personales".

Pero, ¿qué delitos se pueden cometer mediante los sistemas de información? Estafa, piratería, falsificación, daños a los sistemas físicos (*hardware*), delitos contra tarjetas de crédito.

De lo anterior se desprende el marco jurídico o volver los actos de quienes comenten fraude, como actos típicos, es decir, los que se enmarcan dentro de una norma legar para encausar un *juzgamiento***.**

Igualmente es importante hacer la distinción en lo que se refiere a tener la intensión de cometer un acto contra un tercero, el cual es el *fraude*, y cuando ocurre un evento con ausencia de esa intensión, lo cual se denomina *error*, ocasionado este último por descuido o por falta de experiencia de quien manipula los sistemas de las organizaciones. Para ello es importante tener un alto nivel de confianza en quien opera los sistemas de información sin importar el tamaño o nivel de la misma.

Para el portal Web de Isaca[8], una empresa es una "institución cerrada donde solo un número controlado de usuarios, fundamentalmente empleados propios, interaccionan con los sistemas de información", pero "Actualmente este esquema está cambiando y son cada vez más los usuarios externos que tienen un acceso legítimo a los sistemas informáticos propios de las organizaciones, por ejemplo, clientes, ciudadanos, socios, proveedores" (Santiago, CISA).

Se considera que el primer filtro de acceso a los usuarios, ya sean de carácter interno o externo, son las claves de acceso, para controlar y detectar el número de veces de acceso, las fechas de ingreso, la duración dentro del sistema, pero lo más importante, los archivos o la información que sale de la empresa. La información es el activo más valioso de una empresa, pero debido a su característica de intangibilidad se consideran secretos que requieren el máximo cuidado.

Los esquemas de verificación del fraude informático pretenden mostrar, entre otras cosas, la autoría intelectual (individual o colectiva) y la ejecución del evento que ocasiona el fraude.

Según el autor Rodrigo Estupiñán (2010: 376), las tendencias actuales de detección de fraude están dirigidas hacia:

– Una organización de las personas y propensión al crimen como modo de vida, es decir, organizado con estructuras jerárquicas.

– Mayor propensión por parte de los propios empleados hacia la corrupción, debido a sus valores éticos y familiares.

– La oportunidad que se le presenta al interior de la actividad que realiza. Es decir, que el empleado ve las ocasiones en las que puede o no cometer un acto de la naturaleza referida.

8 www.isaca.org. Es una entidad de conocimiento, certificaciones, educación, entre otros, en temas de seguridad y aseguramiento de sistemas de información, gobierno empresarial, administración de sistemas de Tecnologías de Información.

–Ayuda de la tecnología, como por ejemplo los escáneres, o programas informáticos que ayudan a copiar o falsificar con la nitidez de un documento original, etc.

– Menores controles, o controles de baja calidad, puede ser debido a la capacidad económica de la empresa, o porque no quiere invertir sus recursos en ese rubro.

– Concepción tanto ética como moral del individuo que comete el fraude, etc.

PASOS PARA LA DETECCIÓN DE UN FRAUDE BAJO SISTEMAS COMPUTARIZADOS

> "*Casi todas las decisiones de negocio requieren que la alta dirección o los gerentes sopesen los riesgos y los beneficios. El uso común y general de las TI puede proporcionar importantes beneficios a una organización, pero también implica riesgos*"[9].

Existen varias técnicas para detectar fraudes en las empresas, pues depende de los factores que han permitido el fraude. Algunas son:

Frauditor (Vargas Madrid) hace mención a que las empresas deben tener ciertos procedimientos, a saber:

a. Análisis Estadístico: de todas las operaciones por medio de las técnicas de estadística[10], como son: regresión, correlación, dispersión, entre otras, de todas las operaciones que han ingresado, salido, o se han transformado dentro de los sistemas de información computacionales de las empresas.

b. Patrones establecidos que se han vulnerado: es aquí donde el Contador Público debe observar, bajo su criterio y experiencia, las secuencias de los documentos y operaciones, indagar por los documentos faltantes, repetidos, con un deterioro fuera de lo normal, en formatos que son diferentes a los usados habitualmente, etc.

c. Análisis histórico de las tendencias no solo de las cifras, sino de las operaciones.

d. Técnicas de análisis visual, en donde se pueden ver a mayor escala las tendencias de los procesos, si los volúmenes son lógicos con los resultados observados.

e. Procedimientos analíticos de auditoría: análisis vertical y horizontal de las cuentas de balance y de resultados y de las operaciones, ya que las solas cifras son muy importantes, pero el proceso para llegar a ellas también lo es.

Esquemas adicionales, como identificación, análisis, detección y cuantificación de las operaciones. Los controles a renovar, son igualmente importantes,

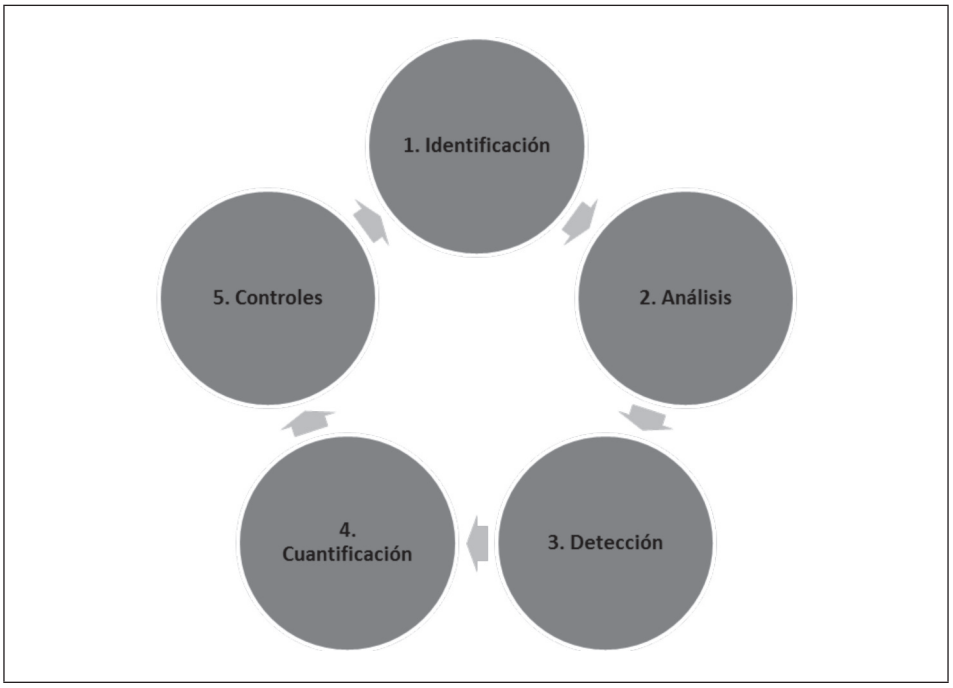
9 Tomado de http://www.info.unlp.edu.ar/uploads/docs/risk_it.pdf. ISACA. Marcos de riesgos de TI. 2009 página 11. 18 de junio de 2012 10:07 am.

10 Tomado de http://www.rae.es/RAE/Noticias.nsf/Home?ReadForm Rama de la matemática que utiliza grandes conjuntos de datos numéricos para obtener inferencias basadas en el cálculo de probabilidades.

ya que indistintamente de las empresas cada una tiene un nivel de control así sea mínimo en donde pudiese monitorear sus operaciones cotidianas.

Lo anterior es un proceso cíclico, en el que cada una de las secuencias anotadas antes se repite para dar lugar nuevamente a la fase inicial.

Ilustración 1



Fuente: elaboración propia.

Para iniciar con este esquema es importante tener de lado la observación sobre determinado proceso, la cual es básica al momento de interactuar con el sistema de cómputo.

Es indispensable tener en cuenta que si la destreza de nuestras capacidades no son los sistemas de información, podamos tener dentro del quipo a un experto que nos asesore en los temas más técnicos que podamos encontrar. Dentro de la *identificación* de los eventos es importante que al realizar una visita de auditoría se tengan en cuenta las operaciones en forma que no se salgan de la rutina. Identificar qué hace la empresa, cómo lo hace, para quién lo hace, en caso de que sean operaciones para un tercero, quién las hace, y si existen los niveles jerárquicos de autorización o validación.

Al hacer la evaluación de los controles existentes, mediante un *análisis* se puede tener una idea de las variaciones de volúmenes, horas de ingreso de datos, procesos fuera de horas establecidas, etc.

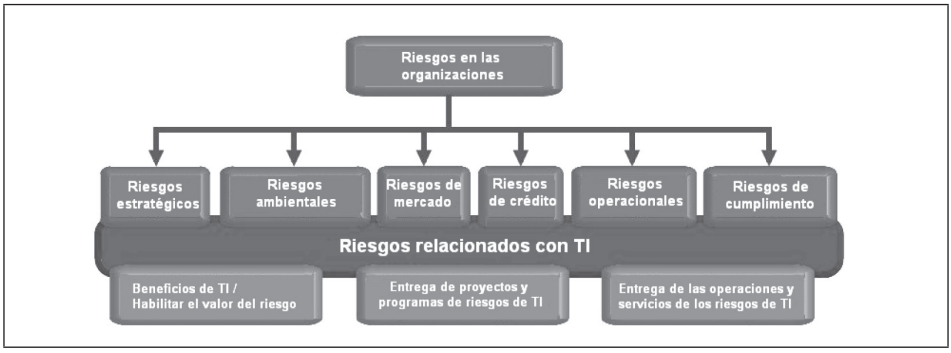
A mayor análisis, es proporcional el nivel de *detección* de las operaciones que no son usuales. Esa identificación es importante que se confronte con los manuales de procedimiento para evitar alterar o causar un pánico innecesario dentro del proceso a auditar, y que los hallazgos se comenten con el personal de coordinación al más alto nivel jerárquico, en caso de que un primer control no sea lo suficientemente claro.

A las organizaciones y a las gerencias no les interesa que se les informe si hay o no procesos inusuales, por sobre el *cuánto* le cuestan esos procesos que les ocasionan un posible impacto en las finanzas. Para determinar la *cuantificación*, es importante hacer los cálculos necesarios, mediante las planillas soporte de las pruebas de todos los hallazgos. Los Auditores son quienes hacen las revisiones con una visión independiente y es esa la que permitirá dar un informe con las cuantificaciones del caso.

El criterio del Auditor, soportado en los controles que ya tiene la empresa, con el fin de no descartarlos o desconocer los esfuerzos empresariales previos, da la pauta para reformular o *reforzarlos*.

Las organizaciones presentan diferentes riesgos dependiendo de sus estructuras internas en cuanto a procesos, los cuales se pueden clasificar o jerarquizar, pero en el caso de la industria financiera, por tomar un ejemplo, se puede esquematizar de la siguiente forma:

Ilustración 2
Riesgo de TI en la jerarquía de riesgos



Fuente: ISACA. Marcos de riesgos de TI. 2009 página 11.

- Riesgos estratégicos.
- Riesgos ambientales.
- Riesgos de mercado.
- Riesgos de crédito.
- Riesgos operacionales.
- Riesgos de cumplimiento.

Los anteriores conceptos podría decirse que están en todas las organizaciones, pero sobre todo la industria financiera tiene un componente bastante grande en el tema de sistemas de información computarizados, con los cuales están

estrechamente relacionados la entrada y salida de las operaciones, las cuales se asocian con la seguridad que ésta brinda a sus ahorradores, en cuanto a agilidad, confianza, rapidez para generar reportes, cobertura y capacidad de hacer transacciones en línea.

APOYO AL CONTADOR PÚBLICO EN LA DETECCIÓN DEL FRAUDE BAJO SISTEMAS DE INFORMACIÓN COMPUTARIZADOS

> "*El inteligente, para el bien de todos, tiene la obligación moral de vigilar al listo; lo digo porque, éste suele tender a robar o mentir sin la permanente vigilancia o auditoría del primero*"
>
> Esteves R[11].

La Contabilidad es un sistema de información que requiere del análisis de entrada y salida de los insumos que se convertirán en la base para la toma de decisiones a nivel directivo, es decir, los estados financieros.

Éstos, con el apoyo de la Contabilidad, son el producto final de una serie de procesos que, de no estar bien soportados, analizados y sustentados no tendría la base de objetividad requerida, no solo por la misma técnica, sino que de la Contabilidad se soportan las bases impositivas y presupuestarias.

El ideal es que las operaciones de salida para preparar los estados financieros (de final del periodo o intermedios), sean lo más accesibles y sobre todo fiables. Pero para ello se requiere de la Auditoría como filtro último para dar la seguridad requerida de que ésta es lo suficientemente válida para no admitir cuestionamientos en contrario.

El lenguaje de los sistemas de información, aunque hoy en día es más cotidiano, no es extraño que algunos Contadores no tengan la facilidad de manipulación tanto de lo elementos físicos como de los lógicos sin un entrenamiento previo, que le pueda dar los soportes necesarios para poder hacer su Auditoría.

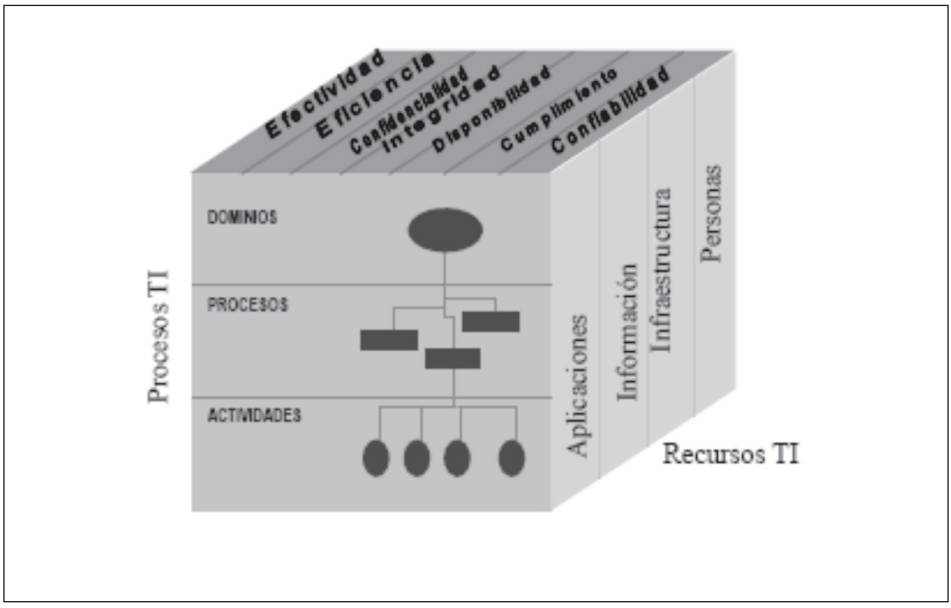
Es importante que si no se tiene la destreza requerida, por ejemplo en una visita inicial a un cliente nuevo, se cuente con el apoyo de un experto en temas de sistemas de información computarizados. Desde la logística, digitación, procesamiento, elaboración de informes, recuperación de datos, accesos restringidos, aunque aparentemente sean actividades operativas, hoy en día llevan un alto componente de sistemas computacionales, de tal forma que el Contador Público debe estar inmerso en las actualizaciones en estos temas.

A pesar de que en un proceso de Auditoría el profesional lleve su "programa de ejecución", el cual incluye la metodología a seguir, es importante que se tengan en cuenta las características del sistema COBIT, para evaluar el control interno, pero dirigido a los sistemas de información computarizados.

11 Tomado de: http://www.citasyrefranes.com/vuestras/buscar/auditoria. 18 de junio 18 de 2012, 10:07 am.

A través de él se unen los procesos de *Tecnología de Información* (dominios, procesos, actividades), los requerimientos del negocio y los recursos asociados (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad, los cuales son muy parecidos a los que trata el sistema de control interno COSO), bajo el esquema de tecnologías de información (aplicaciones, información, infraestructura y personas).

Ilustración 3
Requerimientos de negocio



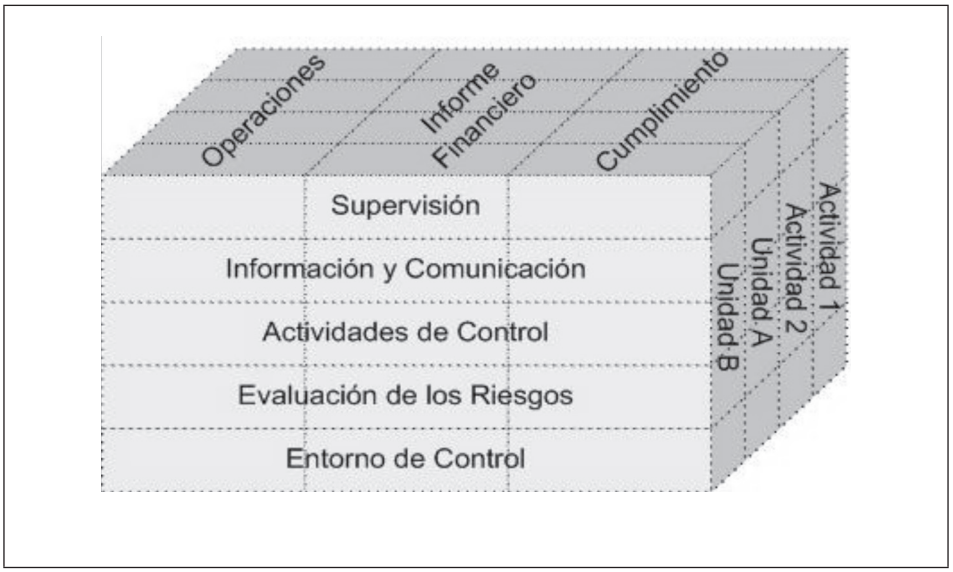
Fuente: Cubo de Cobit 4.1[12]

"COBIT es un marco de referencia de Gobierno TI y un conjunto de herramientas de soporte que permite a los gerentes reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio"[13].

De igual forma se presenta el sistema de control interno COSO, el cual incluye los sistemas de información computarizados y dentro de sus cinco ambientes ejerce influencia para las auditorías de los sistemas de información.

12 www.itgi.org COBIT (Control Objectives for Information and related Technology). Objetivos de Control para Tecnología de Información y Tecnologías relacionadas.
13 www.isaca-bogota.net. 4 de junio de 2012. 23:41.

Ilustración 4
Relación entre objetivos y componentes



Fuente: mercadotendencias.com.

Estos dos procesos de control interno se pueden comparar con algunas equivalencias, las cuales pueden en un momento dado llegar a ser similares, mas no quiere decir que sean excluyentes, como es el caso de los objetivos (de operaciones, de información financiera y de cumplimiento), pero en su esencia fundamental tienen un enfoque diferente.

El modelo COSO cuenta con cinco ambientes (ambiente o entorno de control, evaluación de riesgos, actividades de control, información y comunicación y, por último, monitoreo) y tres objetivos (operacionales, financieros y de cumplimiento) todos muy relacionados. Pero son las actividades de control las que evidencian los pasos que debería hacer un funcionario soportado en sus manuales de funciones para llevar su labor de acuerdo con los lineamientos institucionales.

INFORME DE HALLAZGOS DE FRAUDE

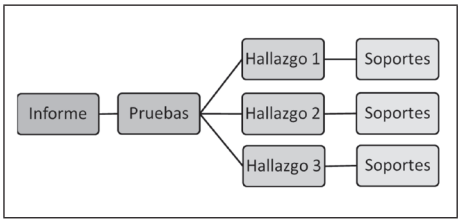
"*El pensamiento es el corcel; la razón, el jinete.*"

George Sand[14]

Para el informe de hallazgo bajo un esquema de fraude, el Contador puede utilizar los diferentes modelos, para rendir sus conclusiones, soportado en las pruebas encontradas.

14 Tomado de: http://www.polseguera.com/cgi-bin/phrases/castella/frasesesp.cgi?Asunto=Pensamiento. 18 de junio de 2012. 10:25 am.

Ilustración 5



Fuente: elaboración propia.

El informe debe estar soportado en unas pruebas y éstas, a su vez, en unos hallazgos, los cuales de forma general se extraen de unos soportes. En el caso de una Auditoría bajo sistemas de información computarizado, los soportes son los que resultan del cumplimento de los parámetros de acuerdo con los procedimientos establecidos.

La Declaración Internacional de Prácticas de Auditoría –IAPS– 1006 emitida por el IFAC en 2010, relacionada con las Auditorías a los estados financieros de los bancos, hace mención a los tres componentes de los riesgos de auditoria[15], los cuales se deben documentar en debida forma:

– *Riesgos inherentes*, es decir, el que es propio del proceso y por lo tanto, por ser inseparable, no se puede evitar, pero sí se puede controlar.

– *Riesgos de control*, son los que se establecen por el "sistema" de control mismo. Las debilidades del sistema se van a ver reflejadas en él, ya que pudo haberse diseñado con errores, o la profundidad para la elaboración de los controles fue muy poca.

– *Riesgos de detección*, una vez establecida esa barrera que es el "control", cuyo procedimiento es ejecutado por el Auditor, existe el riesgo de que éste no lo pueda evidenciar. Es decir, que este es el último filtro para poder detectar un riesgo. En caso de que la detección no sea eficaz, corresponde a uno de los vacíos más grandes de lo cual hace que puedan ocurrir eventos con un altísimo grado de impacto negativo para la operación.

Es importante que dentro del informe se incluyan aquellas partidas que son materiales[16] y que tengan las consideraciones, si es del caso, de otros profesionales que ayudaron a la obtención de las pruebas.

Uno de los modelos de informe puede involucrar, entre otros:

- Un alcance.
- Un objetivo general y varios específicos.
- Las etapas del trabajo, o planeación del mismo.
- Evaluación y determinación de la evaluación del control, bajo sistemas de información.
- Procedimientos a verificar.
- Hallazgos encontrados durante el proceso auditado.

15 IASP 1006, versión 2011, párrafo 45. Riesgo de auditoría. Fuente: texto emitido por [www.IFAC.org]. Versión 20120

16 Marco conceptual de IASB 2010. Párrafo CC11. Materialidad: Las decisiones de los usuarios tienen un imparto por la omisión o la expresión inadecuada información financiera presentada, ya sea cifra o revelación.

– Recomendaciones y sugerencias de mejora (Oportunidades de mejoramiento).
– Conclusiones.
– Entrega y discusión definitiva del informe.

CONCLUSIONES

Indistintamente de su tamaño, las organizaciones presentan riesgos en sus sistemas de información, a pesar de los controles que tengan. Lo importante es el monitoreo que se les haga a estos controles, en forma permanente. A todo el personal, sin importar si se trata de empleados o no, se le deben entregar los manuales de las funciones propias a su actividad. Una de las restricciones que deben estipularse en dichos manuales es la prohibición de instalación de *software* no autorizados.

La contabilidad es un *sistema de información*, relacionada con la informática. Estas herramientas ayudan a que la labor del Contador y del Auditor, aunque sean más ágiles, también tengan más complejidad al momento de hacer sus pruebas. Una de las ayudas con que cuentan las empresas es la ley, la cual impone penas para hacer frente a los delitos informáticos.

Existen varias herramientas probadas para hacer frente al fraude, bajo sistema de información, pero por sí solas no son efectivas: se requiere que la empresa, previamente a unas políticas, las establezca como mecanismo de obligatorio cumplimiento. Igualmente es importante la experiencia y actualización del Auditor o Contador en temas relacionados.

Existen varios modelos de control, uno de los cuales es el COBIT, orientado al fraude, que establece unos lineamientos aplicados especialmente a los sistemas de información bajo sistemas de cómputo. Para mayor información se pueden referir a [www.isaca.org].

Los pasos para un informe de Auditoría bajo sistemas de información no son diferentes, de lo que habitualmente hace el Contador Público, pero sí requieren de que los análisis estén valorados por un experto en caso de que el Contador no tenga un conocimiento amplio en esos temas. Algo específico es el lenguaje claro que debe proporcionar quien elabore un informe para que cualquier interesado, sin excepción, lo pueda comprender, aun si no tienen conocimientos específicos.

BIBLIOGRAFÍA

Textos

Anatomy of a Data Breach. Verizon business. Violación de los datos de consulta. Versión 2009. *Ataques más frecuentes mediante sistemas de cómputo.*

Estupiñán Gaitán, Rodrigo (2006). *Control interno y Fraudes*. Bogotá: Ecoe Ediciones, Biblioteca Luis Ángel Arango. Pág. 376. *Se definen las tendencias de los fraudes en las organizaciones.*

IASP 1006, versión 2011. *Definen los riesgos en auditoría en las organizaciones, según el IFAC (International Federation of Accountants), o Federación Internacional de Contadores, organismo que emite las normas de*

auditoria a nivel internacional con sede en EEUU.

Mantilla, Samuel. Informe COSO. Bogotá: Ed. Ecoe. 4ª Edición. 2005. Página 25. *Definición de ambiente de control*.

Royer, Jean Marc (2004). *Seguridad en la informática de empresa*. Ediciones ENI. 2004. Página 12. *Definición de pirateo*.

Páginas en internet

www.netmedia.info/featured/los-15-ataques-de-seguridad-mas-comunes/ mayo 31 de 2012: 20:21. *Artículo publicado en diciembre 10 de 2009. Define los ataques informáticos más recurrentes en los EEUU*.

www.isaca.org. *Define que es delito informático*.

www.isaca.org/Journal/Past-Issues/2009/Volume-4/Pages/Fraude-o-Error1.aspx. Junio 9 de 2012. 12:20. *Definición de Organización*.

www.nobosti.com. VARGAS Madrid, Daniel. Técnicas de Detección de Fraudes, publicado en 21 de febrero de 2008. *Técnicas de detección de fraude*.

www.rae.es *Se toman las definiciones como: atacar, mitigar.*

www.itgi.org. *Definición de Cobit. (Control Objectives for Information and related Technology)*

www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html. Ley 273 de 2009. Artículo 269 G. *La ley modifica al código Penal en su título VII, y crea y bien jurídicamente tutelado denominado, la protección de la información y de los datos*.