Informe de ACFE sobre el fraude corporativo – edición 2010

Por Raúl Saccani, Gerente de Forensic de KPMG en Argentina

Cuando ACFE publicó su primer Informe a la Nación sobre el Fraude Corporativo en 1996, abrió un nuevo campo en la investigación académica anti-fraude, ya que incluyó un análisis de los costos, las metodologías y los defraudadores en organizaciones de los EE.UU.

En la presente edición de 2010, por primera vez, los datos que ayudaron a construir el Informe fueron obtenidos de casos de fraude ocurridos en todo el mundo. Esto refleja la verdadera naturaleza universal del fraude corporativo.

La información contenida en este estudio se basa en 1.843 casos de fraude reportados por los CFE (Certified Fraud Examiners) que los investigaron. Estos ilícitos ocurrieron en más de 100 países en 6 continentes, y más del 43% tuvo lugar fuera de los EE.UU. Quizás lo más interesante acerca de los datos obtenidos es la consistencia que verifican los patrones de fraude a lo largo del mundo. Si bien las regiones presentan distintos matices, para la mayoría el fraude opera en forma similar, más allá de que ocurra en Europa, Asia, Sudamérica o los EE.UU.

Resumen ejecutivo

- Los respondentes de la encuesta estimaron que una organización típica pierde un 5% de sus ingresos anuales producto del fraude. Si se aplica este porcentaje al producto bruto global estimado de 2009, se traduce en una pérdida potencial de más de 2,9 billones de dólares.

- La pérdida media causada por fraudes se ubica en US$ 160.000, mientras que un cuarto de los casos involucraron pérdidas que superaron el millón de dólares.

- La duración media del fraude antes de ser detectado fue de 18 meses.

- Por un amplio margen, la apropiación indebida de activos fue la tipología de fraude más común, representando el 90% de los casos, aunque con una pérdida media de tan solo US$ 135.000. El fraude a los estados contables se ubica en el extremo opuesto, causando una pérdida media de más de 4 millones; por lejos el más costoso. Los casos de corrupción y soborno caen en el medio, representando casi un tercio de los casos y causando una pérdida media de US$ 250.000.

- El fraude tiene más probabilidad de ser detectado por el reporte de un empleado que por cualquier otro medio. Este indicio se repite en forma consistente desde el informe de 2002, cuando se empezó a consultar sobre los métodos de detección del fraude.

- Las pequeñas organizaciones sufren los efectos del fraude en forma desproporcionada, ya que carecen de suficientes controles en comparación con las grandes corporaciones. Esto hace que las compañías de menor envergadura sean más vulnerables al fraude.

- Las industrias más afectadas han sido las de servicios financieros, las de manufactura y la administración pública.

- Los controles antifraude parecen reducir tanto el costo como la duración de las maniobras. ACFE revisó la efectividad de 15 controles típicos y observó que las empresas que los ponen en práctica tuvieron pérdidas significativamente menores y una reacción más ágil que sus pares que no los practican.

- Los defraudadores de alto nivel jerárquico causan el mayor daño. En promedio, el costo de los fraudes cometidos por los ejecutivos es tres veces mayor que los que cometen los gerentes y nueve veces mayor que los de los empleados. También llevó más tiempo detectar la maniobra.

- Más del 80% de los fraudes fueron cometidos por individuos de alguno de los siguientes departamentos:

contabilidad, operaciones, ventas, comité ejecutivo, servicios al cliente y compras.

- Más del 85% de los defraudadores no tenía antecedentes de conductas similares previas, lo que resulta consistente con los estudios anteriores.

- Los defraudadores dan indicios de que están atentando contra la organización al llevar un nivel de vida por encima de sus posibilidades (43% de los casos) o al evidenciar problemas financieros (36% de los casos).

Conclusiones y recomendaciones

- El fraude corporativo es un problema global. Si bien los hallazgos difieren levemente a nivel regional, la mayoría de los resultados son consistentes respecto de las tipologías, las características de los defraudadores y los controles para detectarlos, independientemente del lugar donde ocurrió el fraude.

- Los mecanismos de reporte interno de irregularidades son un componente crítico de un programa efectivo de detección y prevención del fraude. Las organizaciones deberían implementar líneas éticas para recibir reportes, tanto de fuente internas como externas. Estos mecanismos de reporte deberían asegurar el anonimato y la confidencialidad del reportante. Asimismo, se debería alentar a los empleados a tomar esta actitud, alejando el temor a ser perseguidos luego de hacerlo.

- Las organizaciones confían demasiado en las auditorías. Si bien las auditorías externas son el método de control más extendido, evidencian resultados pobres respecto de la efectividad en la detección del fraude. Las auditorías pueden colaborar significativamente en la prevención de estas conductas, pero deberían complementarse con otras herramientas para mejorar su desempeño a la hora de detectar las irregularidades.

- La capacitación de los empleados es la piedra fundamental del sistema de prevención y detección del fraude corporativo. Siendo que los reportes internos han probado ser una herramienta efectiva para ello, los empleados deberían entrenarse para reconocer una conducta irregular en forma temprana, cómo esta acción afecta a la compañía y cuáles son los pasos que deben tomarse para reportarla. Aquellas organizaciones que capacitan a su personal y ejecutivos en estos temas han reportado menores pérdidas por casos de fraude.

- Las auditorías sorpresivas han probado ser efectivas, pero no son una herramienta de uso regular. En efecto, menos del 30% de los respondentes realiza este tipo de auditorías. Las que sí las realizan han reportado menores pérdidas y mayor agilidad en la detección. El potencial más importante de las auditorías sorpresivas está en la prevención, ya que generan en el defraudador la percepción de que puede ser detectado. En términos generales, quien comete una conducta irregular lo hace a sabiendas de que no será descubierto. Este tipo de auditorías incrementan el riesgo percibido por el defraudador y, por lo tanto, se presentan como una herramienta de gran valor desde el punto de vista de la prevención.

- Las compañías más pequeñas son especialmente vulnerables al fraude. En general, estas organizaciones tienen menos recursos para ejecutar controles, por lo que deberían enfocar sus esfuerzos en aquellos que resulten eficientes, como las líneas éticas y un claro mensaje a sus ejecutivos.

- Los controles internos en solitario no alcanzan para prevenir el fraude en forma efectiva. Si bien es importante para las organizaciones contar con controles antifraude, estos no podrán prevenir todas las conductas ni tendrán capacidad para detectar todos los fraudes en el momento en que ocurren.

- Los indicios que muestran los defraudadores, al vivir por encima de sus posibilidades por ejemplo, difícilmente podrían ser detectados por los controles tradicionales. Los auditores y los empleados deben entrenarse en la detección de estos indicios ya que pueden ser la clave para detectar las irregularidades.

- Dado el alto costo que implica el fraude en las organizaciones, deberían implementarse programas de prevención efectivos que incrementen la percepción del control y, por ende, disuadan a los defraudadores de iniciar la conducta irregular.

El fraude y otras amenazas al sistema financiero latinoamericano

Por JOSE NICOLAS GOMEZ, Director GC2 Consulting, C.A., josenicolasgc@gmail.com

La idiosincrasia, conjuntamente con las costumbres y realidades históricas de los países latinoamericanos; constituyen el punto de partida y diferenciador en la construcción de los planes antifraude a ser implantados por cada una de nuestras organizaciones en el futuro inmediato. Pretender asumir erróneamente como propias, las mejores prácticas de negocios propuestas por organizaciones foráneas, pudiera abrir paso a discrepancias operativas, a nuevas acciones fraudulentas y hasta fomentar la aparición de incipientes amenazas de riesgo en la organización. En materia de planes antifraude, no basta con adecuar las recetas de terceros, ya que cada organización y cada país, requiere de metodologías ergonómicamente dispuestas para cada entidad.

Uno de los aspectos que debemos tomar en consideración dentro del sistema financiero latinoamericano, ha sido el impacto casi imperceptible que en términos generales produjo la reciente crisis financiera ocurrida en los Estados Unidos de Norteamérica. A pesar de la estrecha relación que existe entre la economía americana y el resto de países del continente, sus secuelas no se manifestaron en epidemias sistémicas o daños severos para el resto de las economías latinoamericanas, lo cual evidencia el alto grado de regulación y supervisión que las superintendencias bancarias han emprendido a lo largo de los últimos años, haciendo de nuestras instituciones, entes menos vulnerables a los embates de la económica y a los propios cambios socio políticos del hemisferio.

Sin embargo, los riesgos a los cuales se encuentra expuesto el sistema financiero latinoamericano han evolucionado en múltiples direcciones y con diversas connotaciones de probabilidad e impacto patrimonial. El fraude electrónico y la legitimación de capitales, constituyen las principales modalidades de operación transfronteriza que han alcanzado un alto grado de especialización y desarrollo. Existen adicionalmente, otras vulnerabilidades que impone el entorno regional, las cuales van a variar en atención al marco legislativo vigente en cada nación, la complejidad de las operaciones y servicios de la banca, su relación con el mercado de capitales, las acciones correctivas asumidas por los gobiernos, el papel de los auditores externos e internos y los mecanismos de control emprendidos por cada institución.

Las actividades se supervisión acometidas por las superintendencias u organismos reguladores de cada país, requieren de propuestas integradas en armonía con la gestión emprendida por los entes supervisores del mercado de capitales y del sector asegurador, a fin de minimizar la proliferación de actividades fraudulentas cruzadas y de mayor complejidad operacional. Es allí donde los planes de auditoría desarrollados en el futro cercano, deben tomar en consideración las potenciales amenazas sobre el sistema financiero local e internacional, la adecuación tecnológica a las nuevas prácticas fraudulentas, la administración de procesos bancarios críticos, la construcción de planes de continuidad del negocio e innovar con mayor frecuencia en las prácticas internas de revisión y monitoreo.

La visión sistémica del control interno bajo la perspectiva de COSO, los aportes emanados de los acuerdos de Basilea, la gestión Integral del riesgo (ERM), los lineamientos de Compliance y buen Gobierno Corporativo, constituyen la piedra angular para la confección de planes ante todas estas amenazas; pero de igual forma, urge que nuestros auditores y oficiales de cumplimiento adopten prácticas de revisión acordes a escenarios de alta exposición al fraude tanto interno como externo. Debemos asumir un papel protagónico dentro de la organización a través de recomendaciones que permitan dar continuidad al negocio, materializar el plan estratégico de nuestras instituciones y minimizar el potencial impacto de las actividades fraudulentas; para ello, debemos madurar la necesidad de incorporar revisiones internacionalmente integradas para una banca cada vez más globalizada; de no ser así, el fraude y otras amenazas al sistema financiero latinoamericano habrán ganado una batalla que desconoce de fronteras, idiomas y nacionalidades.

El ARTE de administrar riesgos

Por Martín Svarzman

1.- Introducción:

Palabras como amenaza, riesgo o incertidumbre nos producen sensaciones negativas al pensar en sus consecuencias. Es lógico que, casi instintivamente, tratemos de evitar el riesgo o reducirlo a su mínima expresión. Todo esto tiene parte de verdad pero rápidamente advertimos que no es el camino más recomendable para manejar los riesgos de una compañía cualquiera fuera su tamaño y composición.

Esa tendencia natural a evitar los riesgos nos llevaría a eliminar el emprendimiento, por lo tanto, la clave es aprender a gerenciarlos. **Aprender a Administrar los riesgos.**

Resultados económicos adversos, escándalos financieros, debacles de todo tipo a nivel mundial y global modifican el presente y condicionan el futuro generando amenazas pero también oportunidades para las compañías y para los individuos.

Así planteadas las cosas, con la concepción de riesgo asociada a la de emprendimiento, la administración de los riesgos debería resultar una práctica instalada en las distintas organizaciones con un alto nivel de eficiencia y maduración.

Los resultados están a la vista y los ejemplos son de público y accesible conocimiento.

Las empresas que ponen en práctica el gerenciamiento efectivo de sus riesgos de negocios, aprenden a controlar la incertidumbre propia, la incertidumbre de los mercados en los que operan y pueden obtener ventajas muy importantes en relación a sus competidores.

2.- Por qué ARTE?:

El título de este artículo sostiene que la administración de riesgos es **ARTE**.

La Real Academia Española define al arte genéricamente con dos acepciones:
• “Conjunto de procedimientos para realizar obras que puedan ser juzgadas estéticamente”
• “Conjunto de reglas para ejecutar bien algo”

Me resulta harto tentador desarrollar la tesis partiendo de estos conceptos tan ricos y nada despreciables, para el perfil y experiencia profesional de quien escribe pero, esta feliz coincidencia no representa el sentido que sustenta la idea central de este artículo.

ARTE, es una sigla que refiere a las cuatro acciones claves para tomar decisiones racionales a la hora de administrar los riesgos de cualquier compañía.

Dichas acciones son:

A	ASUMIR	el ejecutivo decisorio considera que dejar la situación como está es la mejor alternativa por lo cual asume el riesgo existente
R	REDUCIR	decisión de mitigar el riesgo con acciones y recursos propios de la compañía
T	TRANSFERIR	la organización busca en un socio compartir determinados riesgos, es el ejemplo de la contratación de seguros
E	ELIMINAR	el costo de mitigar el riesgo no compensa y se decide dar de baja un producto o dejar de realizar determinada actividad.

3.- Decidiendo racionalmente...:

Las opciones presentadas parecen claras, ahora bien la cuestión es la información que el ejecutivo debe tener en la mesa para tomar una decisión racional.

Intentemos entender el concepto de racionalidad, que es el uso de la razón como medio de alcanzar la verdad. Claramente estamos ante un concepto más amplio – por ende lo incluye – que el de la pura conveniencia económica de una adecuada relación de costo – beneficio, que es el sentido que se le da habitualmente.

En términos empresarios una decisión racional debería estar ligada a valores como:
- la **sustentabilidad**, es decir que las decisiones que hoy se tomen no afecten la perdurabilidad o sostenimiento en el tiempo tanto de la Empresa, de las marcas, de las relaciones estratégicas que se quiere conservar (con los clientes, con los proveedores, con la comunidad y medio ambiente, con las Instituciones Públicas, con los reguladores, etc.);
- la **legalidad**, los negocios deben ser legales y en cumplimiento de normas internas y externas;
- la **ética**, así se haya publicado o no un código de ética;
- finalmente la **rentabilidad**, siempre que la organización persiga fin de lucro o bien otros objetivos,

En otras palabras ante toda decisión el ejecutivo tendrá en cuenta primero qué posibilidad hay de afectar la Visión, Misión, Estrategias de la compañía y luego el resultado económico individual del riesgo que se está evaluando.

Por ejemplo, un pequeño ahorro por no cumplir una norma legal puede perjudicar a una compañía no sólo en la multa correspondiente sino en ver su nombre en la prensa con daños en su imagen. En este caso pesa más preservar la imagen institucional que el costo que conlleva la solución puntual.
Los ejemplos más claros se relacionan a posibles daños al medio ambiente o a temas vinculados al Lavado de dinero.

Una vez que estas cuestiones, llamémosle “superiores”, están a cubierto estamos en condiciones de abrir la discusión en términos económicos, la famosa relación de costo – beneficio.

4.- Cómo tomar decisiones racionalmente económicas?

Conforme lo explicado en el punto 3, podemos ahora acotar el proceso decisorio a una comparación entre costo y beneficio.
Vale aclarar que, como expresé al principio, todo emprendimiento conlleva algún nivel de incertidumbre y que son los mismos riesgos que se incurren con el objetivo de conseguir determinados resultados.
Nos estamos refiriendo a los riesgos como la posibilidad que si una amenaza identificada se materialice, perjudique patrimonialmente a una organización.

En ese sentido, nuestro costo aquí estará representado por la erogación a realizar para mitigar esa posibilidad de pérdida, mientras que el beneficio será la NO ocurrencia de ese perjuicio.

Entonces, el primer requisito que tenemos es la necesidad de poder valorizar tanto la posibilidad de pérdida como la erogación necesaria, con un grado de precisión suficiente como para presentarlo a los niveles ejecutivos decisorios.
Esto no siempre es fácil, pero no es imposible. Recordemos que no entran en esta categoría los riesgos que afectan la imagen, las decisiones de tipo estratégico, las cuestiones legales y regulatorias, los riesgos relacionados a conceptos éticos, etc. En otras palabras, *esto no se negocia*. El resto hay que discutirlo y para discutir hay que hacerlo sobre bases ciertas, hay que medir.

Costear una posible solución mitigante de un riesgo, no parece una tarea compleja cuando una organización posee una adecuada estructura de costos. El 90% de las soluciones pasan por la automatización de un proceso existente, por cambios mayores o menores en los procesos existentes, por la creación de un nuevo proceso o parte de él, lo cual puede llevar a incorporar personal, redactar un procedimiento, etc.

Medir el perjuicio de la probabilidad de ocurrencia de un hecho es harto más complejo y requiere un adecuado sistema de gestión de riesgos, una gran cantidad de datos para poder generar proyecciones con sustento estadístico. Hay organizaciones, como por ejemplo los Bancos, que ya están recorriendo ese camino dadas las últimas regulaciones en materia de riesgos, especialmente en lo relacionado a los riesgos operacionales o riesgos operativos.
Como siempre ha sucedido, esta mejor práctica no tardará en extenderse a otras industrias.

5.- Cómo funciona el esquema decisorio (económico)?

Históricamente los empresarios han decidido de la manera más racional posible con los elementos que tuvieron en cada momento a su alcance. Algunos, probablemente por la falta o insuficiencia de esas herramientas, han tomado decisiones basadas en su "intuición", a algunos les ha ido muy bien y a otros no tanto. Claramente no se trata de despreciar esa habilidad que algunas personas naturalmente poseen pero seguramente un adecuado soporte racional hubiera mejorado aún más la performance de los más "intuitivos".

Volvamos a nuestro método de decisión racional.
Como hemos visto, los riesgos que estamos midiendo no son sino la probabilidad que se materialicen amenazas a los negocios que hemos conseguido identificar antes que se produzcan, o bien hechos que, de volver a suceder, provocarían pérdidas que afectarían la rentabilidad de la organización.

Normalmente afectamos la estructura de costos a los ingresos esperados. De la misma forma podríamos pensar en el ahorro, por evitar pérdidas, como un ingreso y poder así realizar una adecuada apropiación de costos al ahorro de gastos evitados.

Ahora bien, analicemos como se comportan las pérdidas operativas, que son aquéllas que toda organización sufre por fallas que se producen derivadas de cualquier evento interno o externo, ya sea originado en fallas provocadas por las personas.

La **Figura 1** es una representación de la curva normal de pérdidas para muestras estadísticas confiables para poblaciones altamente representativas (por ejemplo 10.000 casos).

Figura 1

El eje de las "x" muestra el impacto económico de las pérdidas y el de las "y" la probabilidad que esa pérdidas se produzca.

Claramente, las estadísticas muestran que se producen mayor cantidad de pérdidas de bajo impacto que de alto costo económico.

He aquí, en los términos antes planteados, nuestro “ingreso” como la posibilidad de disminuir estas pérdidas.

Veamos ahora como se comporta nuestro costo, que es la erogación necesaria para evitar las pérdidas, recordemos que puede ser la contratación de horas hombre, el desarrollo o cambio de un procedimiento, la automatización de una operación, remodelaciones físicas, etc.,
En ese caso, es conveniente analizar distintas estructuras de costos ya que algunas de las soluciones planteadas podrían resultar absorbidas por la estructura de costos fijos ya existente, algunas otras podrían tener un mix de costo variable a distribuir con otros procesos y aún parte fija y, en el extremo, podría tratarse de un costo marginal que de otra forma la organización no incurriría.

El costo fijo (curva CFT en la **figura 2**) es la forma más simple de comparar y representa los casos en que no hay que realizar ninguna erogación adicional ni cambio en los volúmenes de operaciones de la compañía, se aplicaría por ejemplo a una acción de control que ya existe pero no se está ejecutando correctamente y, que si se hiciera bien podría mitigar el riesgo en forma adecuada.

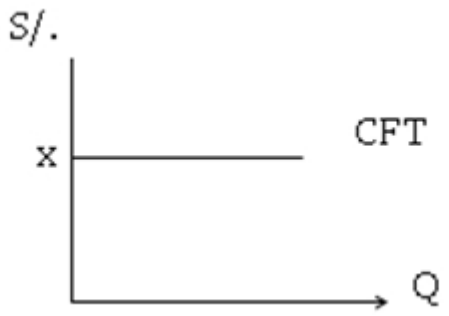

Figura 2

La experiencia indica que el 80% de las soluciones (planes de acción) resulta en mejoras sobre una base de rutinas ya existentes, la combinación de costos fijos y variables, representada en un costo medio total (C Me) es la curva más común a comparar.
La curva de Costo Marginal (C Ma) debería utilizarse para el caso de una erogación nueva realizada en forma específica para reducir una o más amenazas.

La **Figura 3** es una representación típica de las curvas de costo medio (Cme) y costo marginal (Cma):

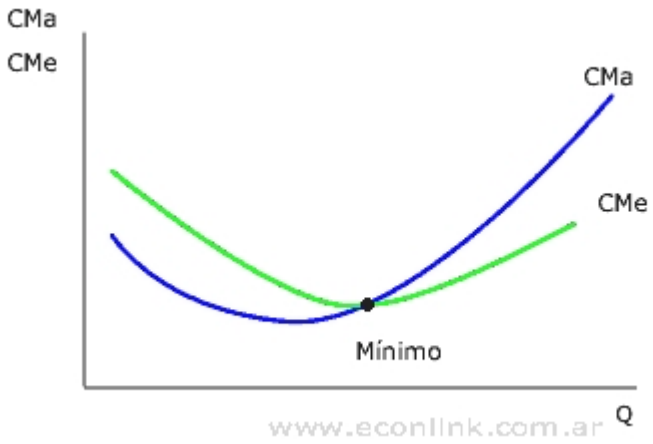

Figura 3

N del A: se evita poner valores en cantidades o en moneda ya que dependiendo del tamaño de cada organización, algunas magnitudes no serían representativas. Siendo que los conceptos enunciados son de carácter universal a cualquier compañía.

Ahora comparemos la curva de impacto de las pérdidas operativas con la curva del costo de evitarlas.
Aquí debemos tener en cuenta que no estamos comparando cantidades absolutas sino curvas que surgen relaciones ya realizadas, donde el eje de las “x” ahora son los riesgos (impacto/probabilidad) y el eje de las “y” está representado por la curva de costo (cantidad/pesos).

Observemos en la **Figura 4** la comparación mencionada en el caso más simple, es decir cuando la solución es absorbida por los costos fijos, no hay necesidad de erogaciones ni se producen cambios en la actividad de la empresa.

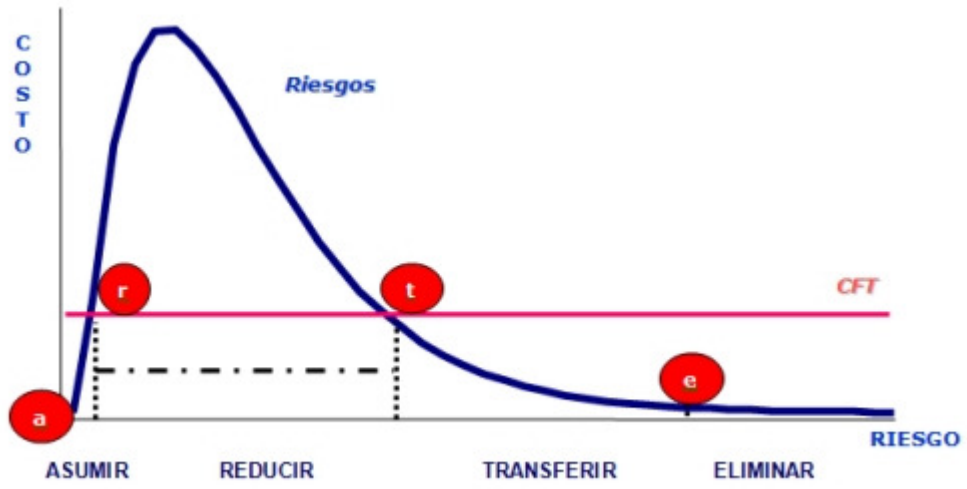

Figura 4

Siendo la línea roja la representación del costo fijo, vemos que la palabra “arte”distribuida entre los puntos de análisis nos indica la mejor decisión a tomar:

Entre los puntos “a” y “r” el costo de solucionar el riesgo es mayor que la posible pérdida por lo cual la decisión más económicamente racional sería **ASUMIR** el riesgo.

Entre los puntos “r” y “t” es más costosa la pérdida que el costo por lo cual conviene realizar las erogaciones necesarias para **REDUCIR** el riesgo.

Luego del punto “t” la curva de riesgos vuelve a estar por debajo del costo. Aquí comienza a jugar una variable que distingue la situación de la del segmento “a” – “r”:
recordemos que las absisas indican el impacto económico de la pérdida. Entre “a” – “r” si la pérdida se produce el impacto es menor pero si la pérdida se produce entre “t” y “e” el impacto podría ser muy significativo y luego de “e” podría no ser recuperable para la organización, aunque su posibilidad de ocurrencia sea menor a mínima.

Luego, cuando los puntos se encuentran entre “t” y “e” la recomendación ya no es asumir sino **TRANSFERIR** el riesgo.

Un riesgo se transfiere por ejemplo cubriendo el proceso con una adecuada póliza de seguros o bien, tercerizando alguna operación. El riesgo no desaparece pero queda atenuado.

El punto “e” representa los casos en que el riesgo no puede ser transferido o si bien lo es parcialmente, la organización continua altamente expuesta. En este caso **Elimine o Evite** el riesgo. Es el caso recomendable sólo cuando no hay alternativa. Recordemos, sin riesgo no hay emprendimiento por lo cual si lo evita deja de hacer un negocio.

Las mismas conclusiones aplican al gráfico comparativo de la **Figura 5**. En este caso la comparación es contra el costo medio total que es la curva verde:

Figura 5

Recomendaciones:
Entre “a - “r”: **A**sumir
Entre “r” – “t”: **R**educir
Luego de “t”: **T**ransferir
o bien **E**liminar

El concepto es el mismo para cualquiera de las curvas de costos aplicables a cada situación, incluyendo la de costo marginal antes representada.

---

6. Conclusiones:

El **ARTE** de administrar los riesgos es una técnica de pura lógica racional aplicable al proceso decisorio de nivel ejecutivo.

Una vez atendidos valores que hemos llamado superiores como la sustentabilidad, la ética, el compliance, las compañías deberían desarrollar un proceso decisorio de carácter económico que asegure una adecuada administración de sus riesgos.
Para ello hay que enraizar en la cultura organizacional la forma en que se toman las decisiones.
La buena noticia es que se trata de un método y, como tal, se puede aprender.

Se advierte fácilmente que una aplicación eficiente de la metodología, requiere calidad de datos que soporten una adecuada y eficiente toma de decisiones. Para ello, la organización debe entrenarse en conseguir datos confiables que contribuyan al proceso decisorio. La organización debe contar con una cultura de costos y una cultura de administración de los riesgos top-down para luego obtener su feed-back.

Las modernas regulaciones en materias de gestión de riesgos. Especialmente de los riesgos operacionales u operativos, están caminando hacia estos esquemas pero aún hay un largo camino a recorrer, especialmente en la mejora en la identificación y medición de los riesgos y en los programas corporativos de respuesta a los riesgos.

La mayor dificultad radica, por el momento, en que el risk management, en el mejor de los casos, está reportando como resultado de su análisis y evaluación de riesgos, rangos que pueden estar representados por colores: rojo para lo más preocupante y decayendo en importancia en amarillo o en verde; o bien los rangos son expresados en unidades de pérdidas o en moneda corriente pero sin demasiada precisión

Dicha falta de fineza en las estimaciones de riesgos está dificultando la comparación contra números “duros” o más precisos de la contabilidad de costos.

Sin duda, los próximos pasos tendrán que darse en la búsqueda de la mayor precisión en la valorización de los riesgos de negocios.
Las organizaciones que antes comprendan que se trata, nada menos, de la materia prima del proceso decisorio ejecutivo, seguramente tomarán la delantera en esta mejor práctica.

Benchmarking Internacional 2009 - Gerenciamiento de la Auditoría Interna

Por Claudio G. Scarso, Gerente de Auditoria Interna, Banco Galicia

A principios de 2009 confeccioné cien preguntas relacionadas con nuestra profesión de Gerentes de Auditoria, las cuales fueron consolidadas en una encuesta para posteriormente ser enviadas a colegas de distintos países. El objetivo primordial fue conformar un benchmarking que nos permitiese a los Gerentes de Auditoria Interna enriquecernos mutuamente con nuevas ideas para contribuir a la mejora continua de nuestra profesión.
A continuación, adjunto un resumen de dicha encuesta y algunas reflexiones a las que he llegado a partir de estos resultados, esperando sea de vuestro interés.

Alcance de la encuesta

Se realizaron 100 preguntas a 144 encuestados (90 % Gerentes de Auditoria) de 16 países (Latinoamericanos, EEUU y España) de Entidades Financieras, Industrias, Empresas de Telecomunicaciones, Gobierno y Energía.

Highlights

De la evaluación de las respuestas obtenidas surgieron los siguientes guarismos:

• Se poseen estructuras de Auditoria Interna reducidas en relación a las necesidades existentes (menos del 1 % de la dotación total de la Empresa). Escasez de auditores de sistemas principalmente.
• El 6 % mantiene aún la Administración de Seguridad Informática dentro de su Gerencia.
• El 50 % tiene inconvenientes para lograr la aceptación de las observaciones y el 64 % para lograr la regularización de los expuestos evidenciados.
• No se ejerce un liderazgo estratégico de mediano plazo, dado que se omite la evaluación futura de potenciales amenazas, negocios y la dotación necesaria para hacer frente a dichos desafíos.
• No se ha logrado en los últimos años incorporar personal, incluso en algunos casos se ha producido el impacto inverso, es decir, se ha perdido personal valioso que migró a sectores relacionados con riesgo operacional, cumplimiento SOX, etc.
• El 61 % no cuenta con un plan de capacitación permanente, y cuando existe dicho plan, sólo en contados casos incluye la especialización sobre procesos críticos que deben ser auditados (telecomunicaciones, finanzas, etc., etc.).
• Sólo el 8 % está dedicando un tiempo importante al asesoramiento.
• El 70 % no explota adecuadamente la generación de reportes ejecutivos consolidados para la Alta Dirección sobre la regularización de expuestos detectados, reducción de costos o incremento de las ganancias a instancias de la Auditoria.
• Al 91 % no le interesa conocer la opinión de las distintas Gerencias auditadas sobre la performance de la Auditoria Interna a su cargo.
• El 71 % considera que el Informe de Auditoria es un obstáculo en su relación con el Área auditada.
• Sólo el 9 % califica los riesgos evidenciados mediante el uso de algoritmos matemáticos.
• En el 58 % de los casos, la Alta Dirección no solicita a la Auditoria Interna trabajos especiales.
• El 71 % no averigua que temas le preocupan al Gerente próximo a auditar.
• El 79 % no está satisfecho con los sistemas de seguridad física de acceso a áreas restringidas.
• El 66 % no prevé que la Auditoría Interna de Sistemas genere ethical hacking.
• El 51 % no explota adecuadamente las herramientas informáticas para lograr un incremento de las ganancias de la Empresa ni para prevenir el fraude ocupacional, sólo lo utiliza para la detección de hechos acaecidos.
• El 61 % sigue pensando que la Auditoria Interna es un Área Staff.
• Sólo el 54 % admitió conocer el Planeamiento Estratégico de Negocios de su propia Empresa. Pero, de ellos, la gran mayoría (88 %) no lo transmitía a sus auditores.
• El 41 % no tiene especialistas para auditar los procesos críticos.
• La gran mayoría (90 %) se vio en la necesidad de investigar fraudes internos y externos el último año.
• Las líneas de denuncias fueron el mejor canal para detectar un fraude.
• Los fraudes siguen siendo perpetrados mayormente por los empleados pero hay un crecimiento importante de los fraudes de Gerentes y Alta Dirección (35 % del total).

• Por distintos motivos no se lleva a juicio a los defraudadores (79 %).
• Se considera que los propios empleados serán los futuros potenciales defraudadores (59%).
• Existe plena convicción que el próximo año existirá un fraude ocupacional en la Empresa (91 %).
• El 65 % no pudo recuperar la pérdida monetaria provocada por el fraude.
• No se controla que los empleados gocen de su licencia anual ordinaria (94 %) a pesar que es un “red flag” importante para detectar fraudes.
• Casi la mitad de los delitos informáticos (46 %) fueron perpetrados por los empleados sistémicos de la propia empresa.
• Se tarda entre 6 meses y un año y medio en detectar un fraude ocupacional.
• Si se pudiera incrementar la dotación de Auditoria se tomarían auditores de sistemas (69 %)
• El 61 % no audita con especialistas el Área Financiera de su Empresa.
• El 62 % no está explotando el potencial que significa la realización de auditorias conjuntas (contables + sistemas)
• El 31 % de las Gerencias de Auditoria no depende del máximo nivel de la Empresa, sino de otra Gerencia.
• El 92 % de los Gerentes de Auditoria no está evaluando estrategias para el mediano plazo.
• El 95 % de las Auditorias de Sistemas nunca ha realizado trabajos tendientes a reducir costos tecnológicos.
• No se considera importante poseer habilidades negociadoras ni liderazgo para producir cambios.
• Se considera que las principales debilidades que presenta la Auditoria Interna están vinculadas con la carencia de especialistas para auditar los procesos críticos y con un pobre nivel de asesoramiento hacia el resto de la Empresa.
• Se considera que la mejor forma de vender el servicio de Auditoria Interna a la Alta Dirección está vinculado con trabajos que contribuyan al incremento de las ganancias y a la reducción de costos.
• El 95 % no genera benchmarking con las Auditorias Internas de la competencia.
• El 72 % considera que no existe adecuada relación con las Auditorias Externas.
• Casi el 90 % aún no está ejecutando “continuous monitoring”
• El 92 % reconoció que la dotación completa de Auditores no conoce el “core business” de su propia Empresa.
• El 81 % no realiza trabajos tendientes a incrementar las ganancias de su Empresa.
• Ante la pregunta “si se consideraban una Gerencia rentable”, sólo el 4 % dijo serlo, admitiendo que por ese motivo existían problemas para incrementar sueldos, dotación y capacitación.
• El 71 % se enteró alguna vez del lanzamiento de un nuevo producto o servicio de su empresa por medios masivos de comunicación.
• El 82 % alguna vez se enteró de un fraude ocupacional de su propia Empresa mucho tiempo después y en forma casual.
• El 92 % admitió que, alguna vez, ante un fraude acaecido la Alta Dirección dijo: “¿Cómo Auditoria no lo vio?”
• El 98 % admitió que la Auditoria Interna está en su mejor momento de los últimos 20 años, sin embargo, el 91 % admitió que no es de las Gerencias más consideradas de la Empresa.
• Respecto del punto anterior, el 80 % admitió desconocer los motivos por los cuales se encuentran en esta situación.

Figura 1

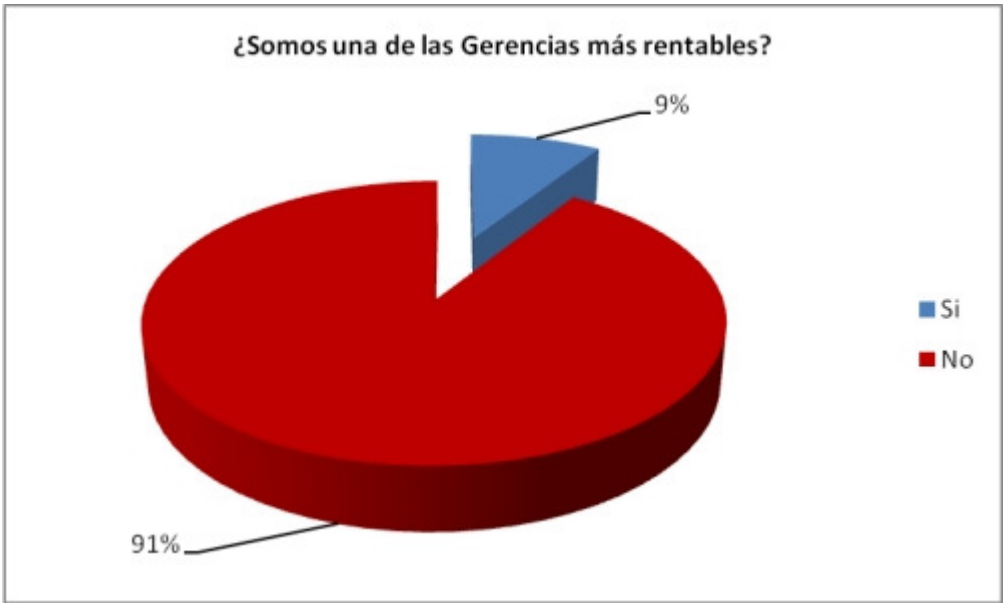

Figura 2

Conclusiones

A continuación, adjunto un detalle de ciertas reflexiones relacionadas con las respuestas que he obtenido del benchmarking internacional citado precedentemente:

• Se debe incrementar la dotación de las Auditorias de Sistemas, auditar con especialistas los procesos críticos de la Empresa, o caso contrario, proceder a su tercerización, como así también contribuir a la realización de auditorias conjuntas (contables + sistémicas).
• Las amenazas de fraude se han multiplicado exponencialmente los últimos años, pero también lo han hecho las herramientas sistémicas disponibles para su detección en forma temprana, por lo que debieran ser explotadas convenientemente.
• Debemos mejorar nuestras habilidades negociadoras para optimizar los porcentajes de regularización de los expuestos detectados.

• Es imposible como auditores contribuir al cumplimiento de los objetivos de la Empresa y a constituir un adecuado ambiente de control interno, si se desconoce el Planeamiento Estratégico de Negocios de la Compañía.
• Debemos encarar a la brevedad proyectos de “continuous monitoring”, para contribuir a la reducción del flagelo del fraude ocupacional (en continuo ascenso). No sólo por el impacto reputacional sobre la imagen de la Empresa, sino adicionalmente, porque la prevención del fraude es una de las formas más eficientes de reducir costos e incrementar las ganancias de la Compañía.
• Debemos conocer a nuestros clientes (Aéreas auditadas y Alta Dirección), saber que preocupaciones tienen, que esperan de la Auditoria Interna, cuales son sus necesidades.
• Como Gerentes de Auditoria debemos ser estrategas de nuestra función, identificando las amenazas, negocios y oportunidades de mediano plazo, y en base a ello, adecuar la dotación y el perfil de los auditores.
• Las Gerencias de Auditoria deben depender del máximo nivel de las Organizaciones.
• Debemos generar reportes periódicos ejecutivos para la Alta Dirección y el Comité de Auditoria que permitan exhibir consolidadamente el cumplimiento de los distintos objetivos de la Auditoria Interna.
• Debemos transformarnos en consultores permanentes de toda la Organización, dedicar más horas al asesoramiento y tender a cumplir funciones más proactivas que detectivas. Este nuevo perfil mejorará nuestra relación con el resto de la Organización y ello redundará en beneficios asociados con una mayor participación en los proyectos y en los objetivos del negocio.
• No generamos suficientes trabajos tendientes a contribuir a la reducción de costos ni al incremento de las ganancias de la Empresa.
• No somos más un Área Staff sino un proceso más del negocio, y por lo tanto se espera de nosotros cierta rentabilidad. Si somos realmente rentables es muy posible que logremos de esta forma adicionar valor agregado a la Auditoria y ello nos permita mejorar la dotación, sueldos, capacitación, etc., etc.

Reflexión final

Estimado colega, si Ud. se sintió identificado con el 98 % que admitió estar en el mejor momento de los últimos 20 años y con el 91 % que sostuvo que la Auditoria a su cargo no estaba entre las Gerencias más consideradas de la Empresa, pero fundamentalmente, si Ud. logró identificarse con el 80 % que admitió desconocer los motivos por los cuales le está sucediendo lo citado precedentemente, entonces, Ud. es el principal destinatario de este Benchmarking.
Por ello, dejo este material a vuestra disposición para un análisis pormenorizado que le permita dilucidar cuáles son las debilidades puntuales que podría poseer el Gerenciamiento de la Auditoria Interna a su cargo.

Si como resultado de esta evaluación, estimado colega, Ud. encuentra una idea para implementar en el corto plazo, que le permita optimizar la misión de la Auditoria Interna, adicionar valor agregado a toda la Organización, mejorar la relación con las Aéreas auditadas, pero por sobre todo, vender estratégicamente a la Alta Dirección la función de Auditoria Interna, sólo entonces, el objetivo de este Benchmarking estará cumplido.