Normaria

Boletín del Comité de Normas del Instituto de Auditores Internos de Argentina – Nº 20 – Septiembre de 2005

CONTENIDO

Elementos a Tener en Cuenta para Prevenir el Fraude

La Necesidad de Capacitación

Normas de Control Interno para la Tecnología de Información del Sector Público Nacional

Contáctenos

El Comité de Normas del Instituto de Auditores Internos de Argentina tiene como Misión promover el conocimiento y uso de las Normas para el Ejercicio Profesional de la Auditoría Interna por parte de los socios del Instituto y de las auditorías internas, proporcionar consejos oportunos a los socios sobre conceptos, metodologías y técnicas incluidas en el marco para la práctica profesional, y hacer comentarios o elaborar opiniones sobre otros asuntos que directa o indirectamente influyan sobre la profesión de auditoría interna. Los miembros de la Comisión son: Enrique Gonzalvo, CIA, CISA; Gustavo Rios; Guillermo Bilick, CIA; Adriana Fernández Menta, CIA; Augusto Echeguren; María de los Ángeles Novello. Puede contactarse con nosotros o hacernos llegar sus comentarios a la dirección de correo electrónico: normas@iaia.org.ar.

*Prevención del Fraude*

## Elementos a Tener en Cuenta para Prevenir el Fraude

**Por Daniel Gustavo Chalupowicz**

Uno de los métodos más útiles a la hora de identificar instancias u ocurrencias de fraude dentro de una organización es la denuncia o reclamo que proviene de un empleado, proveedor, contratista, cliente o informante anónimo.

Notoriamente, el porcentaje de detección de casos de fraude en las organizaciones pareciera ser bajo, lo cual sugiere que la efectividad de la auditoria como herramienta para prevenir las ocurrencias de irregularidades resulta efectivo. Lo que la auditoria sí detecta es un número importante de condiciones potenciales de riesgo para cometer fraude al poner en conocimiento al personal de la organización que un hecho irregular podría ser detectado, y anticiparse a los acontecimientos antes de que ocurran, mediante el análisis de situaciones de riesgo, identificación de controles débiles, inefectivos o mal diseñados e incompatibilidad en el desempeño de funciones que podría facilitar la colusión de varias personas para vulnerar las políticas y procedimientos de una organización.

El autor Ron Klein, receptor en el año 2002 del premio a la excelencia como conferencista otorgado en el estado de California, ha desarrollado un listado de puntos de control interno que si bien no abarca la totalidad de posibilidades, resulta útil como comienzo a tener en cuenta para atender y prevenir gran parte de los casos de fraude que ocurren en las organizaciones.

Dicho listado enumera los siguientes puntos a tener en cuenta por organizaciones pequeñas y medianas, a saber:

1) Separar las funciones de recepción de efectivo, desembolsos, emisión de cheques, firma de cheques, y conciliaciones bancarias. La existencia de un solo empleado responsable por más de una de las tareas enumeradas hace que la organización asuma riesgo innecesario y se encuentre más expuesta al fraude.

2) El extracto bancario debe ser enviado en sobre original cerrado sin abrir, directamente al dueño del negocio, quien debería revisarlo con el fin de identificar transacciones inusuales, nombres o destinatarios de fondos que no resultan normales o habituales en el curso del negocio.

3) Los dueños deben revisar las firmas y endosos sobre los cheques y prestar especial atención a posibles rastros o indicios de adulteración, cheques faltantes, secuencia numérica irregular de los cheques, o cheques donde el beneficiario tiene un nombre que difiere del listado conocido de nombres para los cheques que fueron emitidos.

4) Considerar la posibilidad de una revisión independiente de las cuentas de efectivo y extractos bancarios por un especialista en fraude, para identificar transacciones que pudieran sugerir la ocurrencia de irregularidades.

5) Implementar un chequeo de antecedentes sobre nuevos empleados, y notificar de esto a los mismos.

6) Los empleados que reciben entrenamiento periódico o regular sobre los aspectos perjudiciales del fraude, están más dispuestos a colaborar para controlar la ocurrencia del mismo en la organización.

7) Los empleados que se sienten correspondidos y adecuadamente compensados

en el trabajo son menos propensos a cometer fraude en comparación con los que no se sienten del mismo modo.

8) Los empleados que se sienten desconformes con su trabajo, actitud justificada o no, se encuentran más propensos a cometer fraudes y abusos.

9) Es importante insistir a los empleados en la necesidad de tomarse unas vacaciones de por lo menos una semana al año, y aprovechar dicho período de ausencia para revisar los libros y papeles de trabajo de dicho empleado para identificar posibles discrepancias o indicios de fraude.

10) Adoptar o implementar una línea telefónica o canal de comunicación para formular denuncias anónimas de modo tal de permitir a los empleados, proveedores, clientes y otras fuentes externas reportar las ocurrencias de fraude o sospechas de irregularidades, sin temor a represalias.

11) Los empleadores pueden ganar información valiosa sobre posibles fraudes simplemente preguntando a los empleados de un modo no intimidatorio.

12) Si existe la sospecha de fraude se puede realizar una auditoría específica enfocada a detectar el fraude en lugar de las tradicionales auditorías internas o externas más generales.

13) El acceso a los registros de personal y base maestra de proveedores debe ser protegido con contraseña y restringido de acuerdo con la función.

14) Los sistemas informáticos deben dejar una pista de auditoria sobre los cambios efectuados en los registros de la base maestra de proveedores, incluyendo la identificación de las personas que efectuaron los cambios.

15) Los cambios efectuados a la base maestra de proveedores debe contar con documentación de respaldo, aprobación de parte de un nivel superior de supervisión y revisión independiente.

**Señales de alarma**

Algunas señales de alarma de posibles indicios de fraude son:

- Problemas financieros no resueltos,
- Estilos de vida muy por encima de las posibilidades del empleado,
- Inclinación por las apuestas y juegos de azar,
- Alcohol o abuso de drogas,
- Relación estrecha con un proveedor que pudiera prestarse o colaborar para cometer fraude,
- Nunca tomarse vacaciones,
- Trabajar hasta tarde todo el tiempo (quizás para generar la evidencia documental necesaria de ocultamiento) y,
- Mantener una exagerada discreción o tratamiento secreto sobre el trabajo que se realiza.

El lado bueno de la práctica para prevenir fraude es la oportunidad de servicio que presenta para las firmas contables o los departamentos de auditoría interna dentro de una organización. Cuando los profesionales en auditoría cumplen con la expectativa asignada, se incrementa la percepción del valor de la práctica y se crean oportunidades de mejora para las organizaciones y de crecimiento para los profesionales internos del cliente o consultoras externas.

[volver]

*Normas*

## La Necesidad de Capacitación

**Por Enrique Gonzalvo, CIA, CISA**

Una persona que necesitara realizarse una operación quirúrgica de alta complejidad difícilmente elegiría operarse con un experimentado cirujano, graduado hace veinte años con excelentes notas, si supiera que desde entonces dicho profesional no se ha seguido capacitando en su especialidad. Seguramente desconocerá los últimos adelantos de la medicina que permitan realizar operaciones más eficaces y seguras, y menos traumáticas.

Lo que puede parecer obvio en Medicina, podría no serlo tanto en otras disciplinas. Uno sale de la universidad con un bagaje de conocimientos que, si bien pueden parecer muchos, son sólo el punto de partida para lo que será una trayectoria profesional de trabajo y aprendizaje. La capacitación continua es una necesidad vital para todo profesional, y en particular para los auditores internos. Baste mencionar a título de ejemplo la evolución producida en los últimos años en temas tan diversos como gestión de riesgos, gobierno corporativo y tecnología informática, con impacto directo sobre la actividad de auditoría interna.

Si bien normalmente un auditor interno no pretenderá ser un experto en la totalidad de los temas que se manejan en una organización de cierta magnitud, también es cierto que no puede permanecer ajeno a los progresos y novedades producidos al menos en aquellas disciplinas más directamente relacionadas con la organización para la que trabaja, y en particular con el tipo de trabajo que realiza habitualmente.

Las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna explícitamente señalan que los auditores internos deben estar capacitados en:

- Identificación de indicadores de fraude
- Riesgos y controles claves en tecnología informática
- Técnicas de auditoría disponibles basadas en tecnología

Cabe destacar que este requisito alcanza a todos los auditores internos, independientemente de su especialidad. (Podría sorprender a más de un auditor, por ejemplo, el hecho de que la utilización de programas para extracción y análisis de datos no sea de la incumbencia exclusiva de los especialistas en computación.)

Las actividades disponibles para la capacitación continua de los auditores internos son diversas, y pueden estar referidas específicamente a la auditoría interna o bien a otros temas relacionados. Algunos medios apropiados de capacitación podrían ser:

- Asistencia a cursos, cursillos y conferencias
- Cursos de auto-aprendizaje
- Lectura de libros y artículos
- Participación en comités de asociaciones profesionales
- Participación en revisiones de aseguramiento de calidad.
- Dictado de clases y conferencias
- Trabajos de investigación
- Preparación de artículos, monografías y libros
- Preparación para rendir exámenes de certificación

La necesidad de capacitación se refleja en los requisitos para mantener las certificaciones otorgadas por The Institute of Internal Auditors y por otras asociaciones profesionales. Por ejemplo, para mantener vigente la certificación CIA (Certified Internal Auditor) el auditor debe estar en condiciones de acreditar su participación en actividades de Capa-

citación a razón de un promedio de 40 horas anuales. Para acumular tales horas puede ser aplicable el tiempo dedicado a algunas de las actividades de capacitación mencionadas más arriba (no todas), de acuerdo a las condiciones establecidas por The Institute of Internal Auditors para cada caso.

**NORMAS RELACIONADAS CON LA NECESIDAD DE CAPACITACIÓN**

**1200 – Pericia y Debido Cuidado Profesional**
Los trabajos deben cumplirse con pericia y con el debido cuidado profesional.

**1210 – Pericia**
Los auditores internos deben reunir los conocimientos, las aptitudes y otras competencias necesarias para cumplir con sus responsabilidades individuales. La actividad de auditoría interna, colectivamente, debe reunir u obtener los conocimientos, las aptitudes y otras competencias necesarias para cumplir con sus responsabilidades.

**1210.A2** El auditor interno debe tener suficientes conocimientos para identificar los indicadores de fraude, pero no es de esperar que tenga conocimientos similares a los de aquellas personas cuya responsabilidad principal es la detección e investigación del fraude**.**

**1210.A3** Los auditores internos deben tener conocimiento de los riesgos y controles clave en tecnología informática y de las técnicas de auditoría disponibles basadas en tecnología que le permitan desempeñar el trabajo asignado. Sin embargo, no se espera que todos los auditores internos tengan la experiencia de aquel auditor interno cuya responsabilidad fundamental es la auditoría de tecnología informática.

**1230 – Desarrollo Profesional Continuado**
Los auditores internos deben perfeccionar sus conocimientos, aptitudes y otras competencias mediante la capacitación profesional continua.

**CONSEJOS PARA LA PRÁCTICA**

Consejo para la Práctica 1200-1: Pericia y Debido Cuidado Profesional
Consejo para la Práctica 1210-1: Pericia
Consejo para la Práctica 1230-1: Desarrollo Profesional Continuado



[volver]

*Sector Público*

## Normas de Control Interno para la Tecnología de Información del Sector Público Nacional

**Por Marina Varela, CISA**

En mayo de este año, la Sindicatura General de la Nación mediante la Res. 48/05-SGN, aprobó las normas de control interno para tecnología de información (TI) que serán aplicables en todos los organismos dependientes del Sector Público Nacional.

Para emitir tales normas, SIGEN se propuso como objetivo primordial, establecer una guía de controles mínimos a ser implementados en todas las áreas informáticas del Estado, de modo de propiciar la solución de diversas situaciones de debilidad observadas en distintos organismos y entidades.

Las normas establecidas surgieron del estudio de las prácticas y estándares recomendados internacionalmente, que fueron adaptados a la situación de los riesgos a los que

se ven expuestas las instituciones del Estado, para las cuales la informática ha adquirido gran relevancia.

Las Normas aprobadas en esta oportunidad complementan las Normas Generales de Control Interno emitidas oportunamente por SIGEN mediante su Res. 107/98, en base al modelo COSO.

Están destinadas principalmente a los responsables informáticos, que a partir de ahora disponen de un documento que describe los controles mínimos que deben cumplir, y a los auditores, que desde la aprobación de las normas, deberán incluir las revisiones de la gestión informática en sus planes de auditoría y utilizar las citadas normas como guía mínima para las auditorías a encarar.

Cabe mencionar que, además de las ya referidas Normas Generales de Control Interno, sirvieron de antecedentes para la aprobación de la Res. 48/05-SGN, las “Pautas de Control Interno para Tecnología y Sistemas de Información” publicadas por SIGEN en 1997, el Modelo COBIT (Governance, Control and Audit for Information and Related Technology) y el estándar IRAM-ISO 17799 “Tecnología de la información - Código de práctica para la administración de la seguridad de la información”, el cual fue volcado en el Modelo de Política de Seguridad de los Sistemas de Información para Organismos de la APN, impulsado por la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública.

Las Normas de Control Interno para TI abarcan objetivos de control para los siguientes temas:

1. Organización Informática
2. Plan Estratégico de TI
3. Arquitectura de la Información
4. Políticas y Procedimientos
5. Cumplimiento de Regulaciones Externas
6. Administración de Proyectos
7. Desarrollo, Mantenimiento o Adquisición de Software de Aplicación
8. Adquisición y Mantenimiento de la Infraestructura Tecnológica
9. Seguridad
10. Servicios de Procesamiento y/o Soporte Prestados por Terceros
11. Servicios de Internet/Extranet/Intranet
12. Monitoreo de los Procesos
13. Auditoría Interna de Sistemas

La aprobación de las normas en cuestión constituye un paso fundamental para que los organismos y entidades del Sector Público organicen e incrementen sus medidas de control interno y seguridad informática, tanto en forma individual como conjunta al alcanzar una mayor homogeneidad en el nivel de control implementado, todo lo cual impactará en los resultados de gestión del Estado.

[volver]

Federación Latinoamericana de Auditores Internos

Instituto de Auditores Internos de Argentina

**The Institute of Internal Auditors**