# UN ENFOQUE PROACTIVO PARA COMBATIR EL FRAUDE

Extraído de la Revista Internal Auditor de Abril 2005.
***Traducción de Leticia Quiroga, CIA,*** *Instituto de Auditores Internos de Argentina*

***Siete medidas preventivas pueden ayudar a los auditores internos a noquear a la actividad fraudulenta en el primer round.***

*Por Carl Pacini y Richard Brody*

Los profesionales en Auditoría Interna deberían desempeñar un rol integral en los esfuerzos que realizan sus organizaciones para combatir el fraude. En efecto, los hechos demuestran que las organizaciones se desenvuelven mejor frente al fraude cuando los auditores internos están presentes. En su Reporte para la Nación del 2004, la Asociación de Examinadores Certificados de Fraude establece que la media de pérdidas sufridas por las organizaciones con un departamento de auditoria interna fue 50.000 dólares menor que en las organizaciones sin un departamento de auditoria. El reporte también indica que los esquemas de fraude identificados por auditores internos fueron más del doble que los detectados por los auditores externos, a pesar del hecho de que las organizaciones víctimas en el estudio eran más propensas a tener auditorias externas.

La expectativa de que los auditores internos actúen en la prevención y detección del fraude es mayor que nunca. Los riesgos incrementales asociados con malversaciones – desde reportes financieros fraudulentos hasta amenazas a la seguridad de la información – hacen que el involucramiento del auditor interno en este proceso sea imperativo. Los auditores internos pueden ayudar a la alta gerencia a perseguir agresivamente posibles conductas fraudulentas en lugar de esperar que estas situaciones sean puestas ante sus ojos. Los ejecutivos corporativos, comités de auditoria, y los inversores están al tanto de los beneficios que la experiencia de los auditores internos puede aportar en las iniciativas anti-fraude.

Los auditores pueden tomar numerosos pasos para combatir el fraude, muchos de los cuales están listados en la “lista de control para la prevención del fraude” que se muestra más adelante. Las necesidades y las circunstancias específicas de cada organización individual típicamente determinará qué medidas serán de mayor beneficio y llevarán a lograr los resultados más efectivos. Siete pasos en particular, sin embargo, pueden ser de valor casi para cualquier organización, sin importar su tamaño, industria o ubicación. Estas medidas proactivas pueden servir como una parte integrante del régimen de prevención, detección y reporte del fraude del departamento de auditoria.

## REALIZAR CHEQUEOS AMBIENTALES DE LOS EMPLEADOS

Una de las claves para mitigar la actividad fraudulenta es asegurar que la organización está compuesta de empleados de alta moral y ética. Realizando

chequeos de referencia a los empleados, las organizaciones pueden ayudar a minimizar las amenazas de robos y otras conductas fraudulentas.
Un empleado con historia de perpetración de fraude puede moverse de una organización a otra, dejando detrás de sí una pista de inconductas y abusos. Empleados deshonestos pueden defraudar a una organización inadvertida por decenas de miles de dólares y cambiarse a un nuevo trabajo antes que su fraude sea descubierto. Cuando las referencias de los empleados no son chequeadas, los malhechores pueden deslizarse en un proceso de selección.
Antes de contratar a un empleado nuevo, las organizaciones no deberían confiar en listas de teléfonos de previos empleadores provistas por ellos mismos, ya que podrían ser falsas. En cambio, deberían ser obtenidos en forma independiente. Además, las credenciales profesionales deben ser chequeadas y los títulos académicos confirmados.
Los empleadores también deben considerar realizar un segundo chequeo de referencias a los seis meses de comenzado su trabajo en la organización. La razón por la cual se hubiera despedido a un empleado de un trabajo reciente, pudo no haber tenido tiempo de convertirse en parte de sus antecedentes durante la búsqueda inicial.
Por último, los empleadores deben realizar un chequeo ambiental y criminal que permita identificar cualquier acto criminal u ofensa llevadas a cabo por el individuo. Cualquier información obtenida de la investigación permite al empleador formular preguntas directamente al candidato para obtener una evaluación completa y adecuada antes de tomar una decisión.
Los auditores pueden resultar de gran ayuda con respecto a los chequeos ambientales y otras investigaciones. Como se explica en la Ley de Creditos…” siguiente, las organizaciones pueden asegurar su cumplimiento con los requerimientos legales empleando los servicios de un auditor interno en lugar de contratar a alguien de afuera.

## INCREMENTAR EL USO DE REVISIONES ANALITICAS

El fraude puede afectar los estados financieros en sus tendencias e indicadores, y las cuentas que son manipuladas para ocultar fraudes pueden manifestar relaciones inusuales con otras cuentas que no han sido manipuladas. Más aún, los delincuentes pueden estar comprometidos sólo esporádicamente en actividades fraudulentas, creando patrones erráticos en saldos de cuentas periódicamente. A través de un análisis financiero, los auditores internos pueden revelar relaciones inesperadas o la ausencia de relaciones que debieron estar presentes.
Los auditores deberían considerar el analizar unos cuantos años de información de los estados financieros para obtener un panorama claro del impacto de cualquier esquema de fraude. Varias técnicas de revisión analítica pueden ser utilizadas, incluyendo el análisis de tendencias (horizontal), análisis de indicadores (vertical), o estados similares, comparaciones presupuestarias, comparaciones con promedios de la industria, y revisiones de los sistemas contables y sus registros de entrada. Cualquier item inusual que se encuentre

debe ser analizado para determinar si el fraude pudo o no ser la causa de la aberración.

## REALIZAR REVISIONES DE LOS CONTRATOS

Revisar los contratos y acuerdos de la compañía puede ayudar a identificar posibles fraudes contractuales, incluyendo coimas, sobornos, o conflictos de intereses entre los empleados de la organización. Los fraudes en los contratos pueden ocurrir cuando un proveedor toma fraudulentamente ventajas de un contrato para tener ganancias ilegales. También puede involucrar una conspiración entre personal de la entidad y un proveedor, o entre dos o más proveedores.

Los auditores pueden investigar fraudes en los contratos a través de la búsqueda de patrones inusuales en los registros o la actividad contractual. Un potencial signo de fraude, por ejemplo, podría ser un contratista que rutinariamente oferta último, o licita más bajo, u obtiene la recompensa contractual. Los contratos también pueden ser revisados para detectar evidencias de proveedores que siempre consiguen los contratos sin una legítima razón – la revisión puede revelar que las coimas o sobornos están motivando las adjudicaciones. Además, una revisión de los registros públicos puede revelar si un empleado tiene algún interés encubierto con un contratista.

## CONDUCIR UN ANALISIS ECONOMICO DE LAS AMENAZAS DE ESPIONAJE

Para proteger su información sensible, las organizaciones deberían llevar a cabo un análisis que convierta las amenazas en activos intelectuales. El análisis debe incluir una evaluación de los activos que se poseen y cómo podrían ser objeto de fraude. Para las entidades involucradas con e-commerce (comercio electrónico), servicios o campos orientados a la tecnología, el análisis de amenazas también debe incluir una evaluación de la exposición al espionaje económico, que involucra el robo, el mal uso, o el abuso de los secretos comerciales y de la información confidencial del negocio (activos fuera de Balance).

La ley americana sobre los Secretos Comerciales define un secreto comercial como “aquella información, incluyendo una fórmula, modelo, compilación, programa, dispositivo, método, técnica, o proceso, que (i) genera un valor económico independiente, real o potencial, el cual es preservado de que no sea divulgado, y de que no pueda ser fácilmente descubierto por otras personas que puedan obtener un valor económico por su revelación o uso, y (ii) está sujeta a esfuerzos razonables para mantenerla en secreto”. Son ejemplos de secretos comerciales la información sobre ventas y marketing, información sobre el desarrollo de productos, listas de clientes, y planes estratégicos de negocio.

Los pasos claves para proteger los secretos comerciales son, primero, identificar los conocimientos de la compañía que pueden constituir un secreto comercial, y luego implementar los pasos necesarios para asegurar que esta información sea guardada confidencialmente. Bajo la ley americana de Espionaje Económico de

1996, la información pierde su protección legal como secreto comercial si una empresa no realiza los esfuerzos necesarios para conservar su estado de confidencialidad. Un método efectivo de demostrar “esfuerzos razonables”, y consecuentemente establecer su protección legal, es implementar un plan de protección de secretos comerciales.
Según un artículo de J.H.A.Pooley publicado por Texas Intellectual Property Journal, “Entendiendo la Ley de Espionaje Económico de 1996”, un plan debería incluir los siguientes elementos:

- Acuerdos de confidencialidad – deben ser utilizados con proveedores, contratistas, clientes y empleados.
- Políticas de Documentación – para protección, guardado, y destrucción de documentos, incluyendo las provisiones para señalar documentos confidenciales.
- Controles de acceso físico – tanto para visitantes como para empleados
- Controles de acceso a computadoras – para redes de computadoras, terminales y laptops. La seguridad informática debe incluir también entrenamiento a empleados en el área de ingeniería social – la práctica de obtener ilegalmente contraseñas u otras informaciones a través de “habilidades sociales”.
- Chequeos de ambiente – deben ser realizados sobre empleados tanto como sobre proveedores y contratistas.
- Educación – la advertencia a empleados debe realizarse usando un programa que asegure la continuidad y responsabilidad.

La consideración de cada clase de activo, especialmente los activos extracontables, y la evaluación de la exposición a pérdidas, puede ayudar a los auditores internos a identificar las vulnerabilidades que podrían ser explotadas por ladrones.
Una vez que las categorías de información han sido identificadas, los auditores deberían determinar si la información secreta del negocio está siendo revelada a receptores no deseados. Según un artículo del New York Law Journal, “Resguardando contra el espionaje económico”, de M.G.Radigan, las potenciales fuentes de exposición incluyen los contratos de proveedores, y la literatura disponible al público, así como la existencia de filtraciones a través de socios ocasionales, empleados, trabajadores temporarios, o consultores que no han firmado acuerdos de confidencialidad. Si la exposición es detectada, los auditores internos deberían tomar los recaudos necesarios para eliminarla, minimizarla, o al menos controlarla.

## INCREMENTAR LAS EVALUACIONES Y TESTEOS DE CONTROLES INTERNOS

Muchos ejemplos de fraudes de alto perfil han sido, al menos en parte, resultado de debilidades en los sistemas de control interno. En algunos casos, los controles necesarios no existían; en otros, los controles estaban anulados,

frecuentemente por la alta gerencia. Los auditores internos están generalmente en la mejor posición para reconocer los riesgos relacionados con fraudes, y sugerir medidas correctivas. Este hecho no ha pasado desapercibido por las autoridades regulatorias, como la U.S. Securities and Exchange Comisión (SEC), que ha aprobado reglas de gobernabilidad que requieren que las compañías incluidas en la lista de la New York Stock Exchange tengan una función de auditoría interna.

El control interno debe ser integral para lograr un gobierno corporativo efectivo, y representa un área en la cual el departamento de auditoría interna puede agregar real valor y ayudar a la organización a cumplir con sus metas y objetivos. Dados los requerimientos de la Ley Sarbanes-Oxley del 2002, específicamente la sección 404 “requerimientos para reporte de control interno”, los auditores internos en una organización sujeta a dicha Ley deberían enfocar su atención en identificar debilidades y trabajar con la gerencia para corregirlas. Para que este proceso sea exitoso, sin embargo, es crítico que la auditoría interna reporte directamente al Comité de Auditoría y no a la Dirección Financiera. Ante la existencia de ejecutivos involucrados en algunos de los fraudes reportados, la auditoría interna debe mantener la independencia y objetividad para determinar qué áreas necesitan ser investigadas.

Los auditores internos deben trabajar en conjunto con los auditores externos para asegurar que los controles sean testeados y que todos los requerimientos legales sean cumplidos. Aunque las Normas de Auditoría Generalmente Aceptadas indican que el auditor externo decide en qué medida puede descansar en el trabajo del auditor interno, es claro que el mayor grado de confianza se logrará cuanto más competente y objetivo sea el auditor interno. Trabajando juntos, los auditores internos y externos pueden lograr auditorías de mayor calidad y pueden incrementar la probabilidad de detectar y prevenir fraudes.

## MEJORAR LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Los fraudes que involucran sistemas de información pueden ser categorizados como manipulación de los registros de entrada, de los registros de procesamiento, o los registros de salida. La manipulación de los datos de entrada consiste en el ingreso de datos falsos o fraudulentos en los sistemas de información, mientras que la manipulación de los registros de salida es robar datos – como listas de clientes, planes de fusión, y secretos comerciales – de los sistemas. La manipulación de los datos en el procesamiento incluye la alteración de los programas de computación o sus códigos. Muchos controles no físicos en los sistemas de información son claves para prevenir fraudes que puedan brotar de aquellos tipos de actividades.

CONTRASEÑAS. El explosivo crecimiento de Internet ha conducido a un incremento en el número de puertos de salida para las redes de computación. Los auditores internos deberían asegurar que sólo los usuarios legítimos tengan acceso a las redes y datos asociados. Aunque las contraseñas son la línea más

antigua de defensa, seguirán siendo el método más efectivo para el control de acceso. Para asegurar su efectividad, sin embargo, las contraseñas deben ser utilizadas apropiadamente.
Idealmente, las contraseñas deben ser generadas al azar por el sistema y contener una combinación de letras, números y caracteres especiales. La seguridad efectiva requiere que las contraseñas sean cambiadas periódicamente, ya que la frecuencia en su cambio depende de los niveles de riesgo. Por ejemplo, las instituciones financieras y agencias gubernamentales, que son blanco frecuente de delincuentes, deberían requerir el cambio de passwords más seguido. Los sistemas operativos de las organizaciones deben llevar registro de los intentos fallidos para acceder y limitar los intentos de acceso hasta que el usuario quede automáticamente inhabilitado. Además el empleado no debe compartir su contraseña con otros usuarios o mostrarla en cualquier lugar en que pueda ser vista por otros usuarios.
La nueva tecnología es habilitar formas de protección biométrica de passwords, como registros de voz, huellas digitales, patrones de retina, y firmas digitales. Los auditores internos, que estén al tanto de estos avances, estarán en una posición privilegiada para que su organización incremente sus controles de seguridad.

ENCRIPCIÓN. Los datos almacenados en archivos y transmitidos a través de líneas de comunicación están sujetos a invasión por empleados no autorizados y otros individuos. Un control que combate este problema es la encriptación, o traducción de la información a un código secreto. El esquema de encriptación más popular para la transmisión de datos basados en la web es SSL – Secure Sockers Layer --, un protocolo para la transmisión de documentos privados para Internet. Los sistemas de comunicación más comunes para transmisión de paquetes de información contienen la habilidad para encriptar los datos, y las organizaciones deberían tomar ventaja de estos controles cuando estén disponibles.

CONSOLE LOGS. Los auditores internos deberían evaluar la posibilidad de que los sistemas operativos de sus organizaciones mantengan un registro seguro de cada transacción o ingreso en el sistema. La identificación del usuario, la hora y fecha de los ingresos, y la transacción misma deberían ser capturados. Con las recientes mejoras que han tenido las tecnologías de guardado de datos, los registros de consola se han convertido en un control efectivo. Un registro de consola bien mantenido puede ayudar a los auditores internos a testear combinaciones de usuarios y transacciones, así como proveer soporte para la detección de futuros posibles fraudes. El log también puede servir como un disuasor de fraudes, si los empleados saben de la existencia de registros de toda la actividad que se realiza.

CONTROLES DE SEGURIDAD DE REDES. Los auditores internos – o nuestros especialistas en fraude con habilidades en seguridad informática – deberían realizar una revisión periódica de los controles de seguridad en los sistemas o

redes. Los auditores pueden identificar los controles de seguridad establecidos realizando un cuestionario preliminar sobre todos los aspectos de los sistemas operativos de una entidad, incluyendo las políticas y prácticas del personal. Obtener información sobre los procedimientos también puede ayudar a entender las razones para incluir o no ciertos controles, así como a determinar la efectividad de los mismos. Esta revisión también puede revelar qué pasos adicionales deben seguir los auditores para reducir la posibilidad de fraude informático.

BACKUPS. Los archivos de datos y los sistemas deben estar protegidos de delitos o destrucción por parte de empleados infieles o agentes externos. Una de las formas más efectivas de asegurar los datos importantes es establecer un sistema de resguardo (backup). Aunque muchas firmas tienen procedimientos de backup, los auditores internos deben periódicamente evaluarlos. Los auditores deben determinar si los archivos de datos actualizados están a buen resguardo, en lugar seguro, alejado del acceso por agentes operacionales de la empresa.

## CREAR Y MANTENER UNA POLITICA 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.

## UN POCO DE PREVENCIÓN

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 auditoria interna en iniciativas anti-fraude ayuda a la organización a sacar ventaja de los expertos internos que conocen mejor a la compañía.
Los siete pasos proactivos descriptos representan sólo una pequeña muestra de las áreas en las cuales la auditoria interna puede agregar valor y asistir en la prevención y detección del fraude. Existen numerosas oportunidades para

individuos deshonestos para cometer fraudes, y los auditores deberían trabajar en conjunto con la gerencia para considerar las mejores alternativas para mantener a la organización al resguardo de posibles daños. Cuando resultan exitosas para combatir el fraude, las medidas preactivas cosechan su mejor resultado. Como dice el viejo adagio, una onza de prevención es mucho más valiosa que una libra de cura.

SEÑALES DE FRAUDE

- Alteración de documentos
- Pagos duplicados
- Segundo endoso en cheques
- Partidas pendientes en conciliaciones bancarias
- Asientos contables sin documentación respaldatoria
- 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

---

Este artículo fue seleccionado por el Comité de Publicaciones del IAIA, de la revista **INTERNAL AUDITOR** de **Abril 2005**, y su traducción autorizada por el IIA.

**CARL PACINI, PHD, CPA, CPA, CFSA, JD** es profesor asociado a Marguerite y Guy Howard profesor de negocios de Florida Gulf COSAT University.

**RICHARD BRODY, PHD, CPA, CFE** es profesor asociado, College of Business de University of South Florida– Saint Petersburg.