

GESTIÓN DE RIESGOS DE TERCEROS

Cuando su organización confía en terceros para proveer suministros o servicios, su exposición a los riesgos se multiplica. Y mientras el término “terceros” generalmente se utiliza en referencia a grandes trabajos — tales como trabajo tercerizado, procesamiento de datos o manufactura — los riesgos asociados se pueden aplicar a toda relación contractual, sin importar cuan pequeña sea ésta. Aún pueden extenderse hasta incluir las relaciones de los vendedores con sus proveedores de servicios o suministros.

Más del 65 por ciento de las organizaciones dependen “en gran medida” de terceros, de acuerdo con una encuesta reciente llevada a cabo conjuntamente por la Fundación de Investigación del Instituto de Auditores Internos y Crowe Horwath LLP. Sin embargo, a pesar de la creencia predominante de que las relaciones con terceros plantean un riesgo significativo para la organización, una gran mayoría (80 por ciento) de las organizaciones dedican sólo una pequeña porción de sus recursos de auditoría interna para la evaluación de riesgos de terceros. Por otra parte, los

investigadores descubrieron una falta de consenso acerca de quién dentro de la organización es realmente “dueño” de cada relación de terceros y la incertidumbre respecto a qué medidas específicas se deben tomar para reducir la exposición al riesgo.

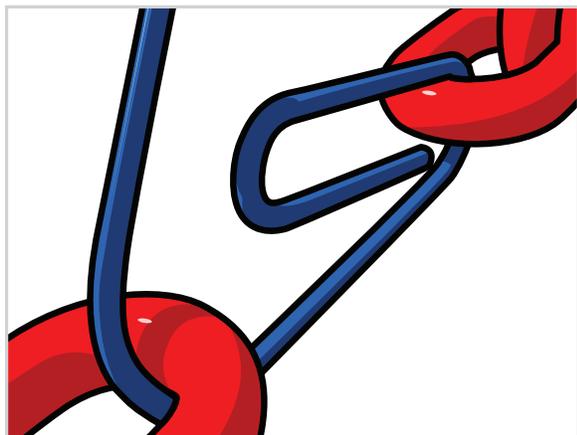
Esta edición de *Tone at the Top* explora el tema de los riesgos de terceros, aprovechando los conocimientos de tres expertos en gestión de riesgos que ofrecen varios consejos para ayudar a los líderes de la compañía a lidiar con esta creciente preocupación.

Objetivo en Movimiento

“Riesgo de terceros es uno de los mayores riesgos para nuestra organización”, dice William Vinson, vicepresidente y director ejecutivo de auditoría en Seagate Technologies, líder mundial en unidades de disco duro para computadores y soluciones de almacenamiento de datos. “Ya sea que se trate de fabricación o algún otro servicio, estamos entregando una gran cantidad de los controles típicos que esperaríamos ver internamente a otra persona.”

Seagate se basa en gran medida en los fabricantes y proveedores de terceros en China, Malasia, Corea del Sur, Tailandia, Singapur, Brasil, y otros países con una amplia gama de prácticas culturales, sistemas políticos, reglamentos, leyes laborales y expectativas de control de calidad. Navegar por este complejo y cambiante paisaje puede ser un desafío de enormes proporciones.

“Es importante que las juntas de directores y comités de auditoría reconozcan que, cuando se está hablando de la gestión de riesgos de terceros, usted está tratando con



un entorno en constante evolución”, afirma Vinson. “Las economías cambian. La política y las regulaciones cambian. Debe contarse con una revisión robusta y continua así como su correspondiente proceso de evaluación”.

El establecimiento de acuerdos o contratos integrales es un paso en la dirección correcta. Pero los programas de gestión de riesgos de terceros también deben incluir disposiciones para el control del cumplimiento y la aplicación de esos contratos.

Luchar por los Derechos

Aunque los riesgos de reputación – tales como malas condiciones de trabajo, las prácticas corruptas y la responsabilidad del producto – tienden a atraer la atención de más público, gran parte de la gestión de riesgos de terceros en realidad tiene relación con cuestiones menos provocativas tales como asegurarse que los contratos de los proveedores estén claramente redactados, los costos sean identificados y comprendidos con precisión, que los proveedores y consultores no estén abultando sus facturas, y que todas las partes estén conformes.

Un ejemplo de un riesgo común de terceros implica acuerdos de canales de distribución, en el que un producto de marca pasa a través de varios puntos de control, asumiendo el aporte “de valor añadido” de los revendedores. Por ejemplo, un fabricante de computadoras permite que un socio del canal de producción agregue un componente, digamos la memoria. Pero éste es un componente defectuoso o deficiente, lo que genera problemas. En tal caso, el fabricante esencialmente da fe del trabajo de un tercero invisible, cuyo trabajo mediocre en última instancia, podría dañar las ventas y la reputación de la marca.

Los acuerdos de licencias para software y de regalías por música son otras dos áreas comunes donde dejar de auditar o hacer cumplir las disposiciones contractuales puede dar lugar a pérdidas económicas significativas. “Es fácil para una tienda de TI implementar más programas de lo que paga por ellos”, dice Robert Pink, socio de KPMG que se especializa en servicios de cumplimiento de contratos. “En el canal de distribución, un tercero podría subestimar las ventas para reducir las regalías adeudadas en virtud de un acuerdo de reventa”. Afortunadamente, Pink dice que está viendo un repunte en el ejercicio de los derechos de auditoría contractuales y la aplicación de las disposiciones de un solo uso.

Históricamente, ese no ha sido el caso. Mathew Behan, director de KPMG de Cumplimiento de Contratos, dice que, en más de 20 años que ha estado llevando a cabo auditorías de cumplimiento de contratos, a menudo se sorprende por la falta de seguimiento de parte de la empresa contratante después de haberse firmado un acuerdo contractual. Una vez firmado el contrato, parece que nadie lo mira de nuevo, sostiene.

Incluso, la mayoría de las veces, colapsos en la gestión de riesgos de terceros son la consecuencia de la falta de vigilancia de cerca a los vendedores y de verificar que las

Lista de Riesgos de Terceros

Los riesgos de terceros se pueden encontrar en todos los rincones de una organización. Patrick Warren, director de la unidad de consultoría de riesgos de Crowe Horwath, agrupa estos riesgos en las siguientes seis categorías:

1. **Financiero** – Divisas, riesgo de cambio, aranceles, impuestos, precio del producto, sobreprecio y devoluciones.
2. **Información** – Precisión, oportunidad, pertinencia, y la seguridad de los datos compartidos por múltiples partes.
3. **Integridad** – Fraude, cumplimiento regulatorio, conflictos de interés, marca, y reputación.
4. **Operacional** – Costo, eficiencia, problemas de contratos, interrupción del negocio, y problemas en la cadena de suministro.
5. **Estratégico** – Problemas de perspectiva general del negocio, incluyendo responsabilidad social, conciencia ambiental y el impacto económico de terceros.
6. **Tecnología** – Computadores, dispositivos de almacenamiento de datos, redes, y tecnologías emergentes.

*Adaptado del artículo de Warren, “Closing the Gaps in Third-party Risk Management,” revista *Internal Auditor*, Febrero 2014.

Profesionales Calificados

Los auditores internos y los gerentes de riesgo, particularmente aquellos que poseen la certificación del IIA en Aseguramiento de la gestión de riesgos, están calificados para identificar de manera única potenciales exposiciones a riesgos de terceros y para hacer recomendaciones sobre las políticas y procedimientos para gestionar el esfuerzo.

cláusulas contractuales se están cumpliendo. “Sabemos que los terceros cometen errores”, dice Behan. “Se aprovechan de las situaciones. Y, sin embargo, muy a menudo escuchamos: “Así es como se hacen los negocios.” Bueno, está bien – pero si esa es la manera en que vamos a hacer negocios, ¿por qué firmar un contrato?”

Frenar los Riesgos

El ritmo rápido y la aceleración de los avances tecnológicos, así como la digitalización y la monetización de la información hace cada vez más difícil poder mantener un estricto control sobre terceros. Aun así, con tanto en juego, es fundamental que las organizaciones documenten y monitoreen adecuadamente los riesgos de terceros.

Vinson de Seagate ofrece los siguientes consejos para gestionar el esfuerzo:

- 1 Llevar a cabo un inventario completo de las actividades de terceros calificados por factores de riesgo, incluyendo el valor del contrato, el potencial de corrupción, riesgo financiero y la regulación.
- 2 Asignar un proceso adecuado y equilibrado para gestionar cada riesgo de terceros / relación identificada.
- 3 Establecer reglas claras e inequívocas para mantener la responsabilidad de los vendedores y medir el desempeño.
- 4 Asegurar que los controles y herramientas de evaluación de riesgos se adaptan a los cambios en el perfil de riesgo.

En muchas organizaciones, la responsabilidad de la realización de estas tareas recae en los gerentes de riesgo y los profesionales de

la auditoría interna, que trabajan en conjunto para asegurar que las muchas exposiciones de riesgo de la organización sean identificadas y resueltas adecuadamente. Los gerentes de riesgo establecen controles y procedimientos para minimizar los riesgos, mientras que los auditores internos proporcionan una evaluación objetiva de los controles, recomiendan mejoras y ofrecen garantías a la dirección ejecutiva y a la junta directiva que los abordan adecuadamente.

En última instancia le corresponde a los ejecutivos, directores y comités de auditoría asegurar que la gestión de riesgos de terceros esté en su radar. Los líderes de la compañía deben entender y ser capaces de cuantificar estos riesgos para determinar si se asignan recursos suficientes para proporcionar la seguridad de que las relaciones con terceros se gestionan adecuadamente.

Pregunta para la Encuesta Rápida

¿Qué tan seguro está usted de que los riesgos de terceros de su organización están siendo atendidos adecuadamente?

Visite www.teiia.org/goto/quickpoll para responder esta pregunta y ver lo que otros están respondiendo.

Preguntas que los directorios deberían hacer

- ¿Son los riesgos de terceros considerados en el enfoque global de la organización para la gestión del riesgo empresarial?
- ¿Se ha realizado un inventario y clasificado los riesgos?
- ¿Están las funciones y responsabilidades de gestión de riesgos de terceros claramente definidas dentro de la organización?
- ¿Están asignados los recursos apropiados para abordar los riesgos de terceros?
- ¿Los gerentes de riesgos y los auditores internos consideran el riesgo de terceros en sus evaluaciones de riesgos y planes de auditoría?

Sobre El IIA

El Instituto de Auditores Internos Inc. (IIA) es una asociación profesional mundial con 180.000 miembros en 190 países. El IIA sirve como defensor de la profesión de auditoría interna, pionero de las normas internacionales y principal investigador y educador. www.globaliia.org

Suscripciones a disposición

Visite www.globaliia.org/Tone-at-the-Top o llame al: +1-407-937-1111 para solicitar su suscripción gratuita.

Comentarios de los lectores

Envíe sus preguntas / comentarios a tone@theiia.org.

Contenido del Consejo Consultivo

Con décadas de experiencia en la alta dirección y consejo de administración, los siguientes apreciados profesionales proporcionan orientación sobre el contenido de esta publicación:

Martin M. Coyne II
Michele J. Hooper

Nancy A. Eckl
Kenton J. Sicchitano



TONE
— at the —
TOP

RESULTADOS DE LA ENCUESTA RÁPIDA:

¿Cuán seguro está usted que los controles de su organización pueden prevenir una amenaza significativa a su seguridad cibernética?

*Basado en 497 respuestas. Los encuestados sólo podían elegir una respuesta.



34%

Poco a No
Confiado

54%

Cierto grado de
Confianza

12%

Muy
Confiado

Derechos de autor © 2013 por The Institute of Internal Auditors, Inc., ("El IIA") estrictamente reservados. Toda reproducción del nombre o del logo del IIA llevará el símbolo de registro de la marca registrada federal de los EE. UU. ®. Ninguna parte de este material podrá reproducirse de ninguna forma sin el permiso escrito del IIA.

El permiso se ha obtenido del titular del derecho de autor, The Institute of Internal Auditors, Inc., 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201, U.S.A., para publicar esta traducción, que es la misma en todos los aspectos materiales, como el original, a menos que se apruebe como fue modificado. Ninguna parte del presente documento puede ser reproducida, guardada en ningún sistema de recuperación o transmitida en forma alguna ni por ningún medio, sea electrónico, mecánico, fotocopia, grabación, o cualquier otro, sin obtener previamente el permiso por escrito del IIA.

El presente documento fue traducido por el IIA ECUADOR el 15/4/2014.