Risk & Business Consulting.
Internal Audit.

Auditoría Interna

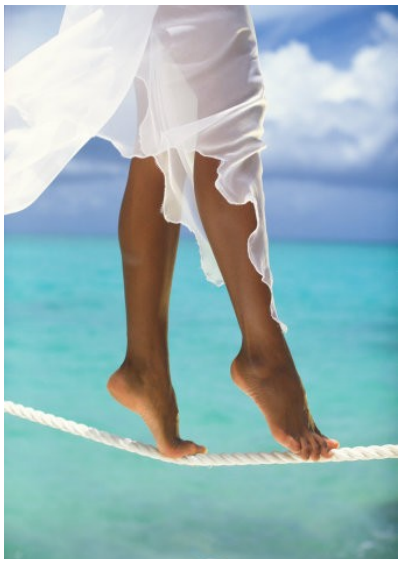
Auditoría interna de tecnología, ¿lujo o necesidad?

En este punto vista comentamos cómo los delitos digitales y riesgos tecnológicos están obligando a que organizaciones que dependen de tecnología de información para operar establezcan una función de auditoría interna de tecnología.

En este punto de vista

Fraudes y delitos informáticos, "*In Crescendo*"

A julio 2009, 262 millones de registros digitales con datos personales y privados habían sido comprometidos en los Estados Unidos según la organización *Privacy Rights Clearinghouse*. Si la cifra le sorprendió, lo siguiente quizás le preocupe aún más:



- ✓ El monto estimado de fraudes por compras en línea en los Estados Unidos y Canadá fue de 4,000 millones de dólares estadounidenses, según el *2009 Edition Online Fraud Report.*

- ✓ La principal fuente de incidentes de seguridad son los empleados (34%) y ex empleados (16%) vs hackers (28%), según *el 2008 Global State of Information Security* realizado por PwC.

- ✓ En los Estados Unidos, 50% de las compañías han sufrido incidentes de seguridad por virus en los últimos doce meses de acuerdo al *2008 CSI Computer Crime and Security Survey.*

- ✓ El 86% de las organizaciones en Panamá consideran que es probable que les ocurran incidentes de seguridad de información, según el estudio *Seguridad, Riesgo y Privacidad 2009* hecho por Deloitte Panamá.

- ✓ Entre los hallazgos de auditoría interna/externa frecuentemente identificados durante los últimos doce meses están: segregación de funciones (40%) y derechos de accesos excesivos de los usuarios en los sistemas (36%), según el estudio *Seguridad, Riesgo y Privacidad 2009.*

Continuar listando argumentos sobre cómo las organizaciones en Panamá y globalmente están siendo afectadas por los crecientes incidentes de seguridad sería innecesario para reconocer la necesidad de fortalecer o bien crear la función de Auditoría Interna de Tecnología.

Es curioso ver que a pesar que muchas organizaciones en Panamá (sector privado o gobierno) dependen literalmente de tecnología de información, redes, sistemas y comunicaciones para operar, las mismas no disponen de una función Auditoría Interna de Tecnología, y aquellas que tienen una, probablemente no disponen de herramientas, metodologías y recursos

calificados con la suficiencia necesaria para mitigar los riesgos de tecnología de información a los que están expuestos.

¿Por qué?

Como lo vemos en RISCCO, es una combinación de factores que acuñamos en el concepto “Cuando el desconocimiento alimenta la confianza”

Cuando el desconocimiento alimenta la confianza

Si usted va en una autopista a 120km/h y un camión cisterna que va enfrente de usted empieza a esparcir rápidamente gasolina (riesgo), lo más probable que usted o bien reduzca la velocidad o detenga su auto (control). Pero ¿por qué lo hace? Porque usted sabe que si no detiene el auto seguramente sufrirá un accidente y muera (impacto).

Eso es lo que de manera opuesta ocurre en la mayoría de las organizaciones en Panamá. Como desconocen los riesgos tecnológicos a los que están expuestos, difícilmente pueden advertir el impacto de los mismos y mucho menos establecer los controles para mitigarlos.

Evidentemente hay organizaciones que son la excepción, pero en términos generales muchas en Panamá, por desconocimiento edifican y alimentan una confianza en que todo está bien en cuanto a los riesgos tecnológicos. Entre otros argumentos que comúnmente escuchamos que alimentan esta confianza y que podrían ser cuestionados están:

1. Nuestra compañía nunca ha sufrido un incidente de seguridad, consecuentemente no tenemos de que preocuparnos.
2. Durante los últimos años las cartas de gerencia de nuestros auditores externos no mencionan riesgos de tecnología importantes, por lo cual asumimos que nuestras redes y sistemas están seguros.
3. Acabamos de invertir en un sistema anti virus de última tecnología y un Firewall para proteger nuestras redes y computadores.
4. Disponemos de un Departamento de Auditoría Interna con siete destacados y experimentados contadores y financistas los cuales han tomado algunos cursos sobre riesgos tecnológicos.

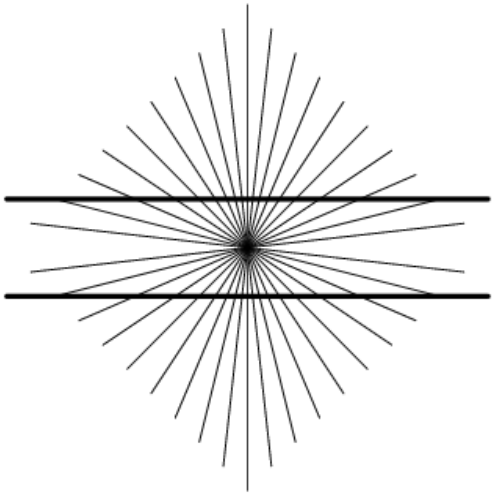
   Vale la pena aclarar que seguridad de información es un tema técnico. Las buenas intenciones y voluntad no son suficientes. Es el mismo efecto que en una Auditoría Interna para revisar los riesgos financieros

de ciertos “Hedge Fund” contratados, usted asigne a un Auditor Interno de Tecnología.

5. A pesar que no tenemos una función de Auditoría Interna de Tecnología, nuestro Gerente de Tecnología en las reuniones semanales de Gerencia nos comenta que nuestras redes y sistemas son seguros.

6. Recientemente realizamos pruebas de vulnerabilidad externa a nuestro sitio web y los resultados fueron bastante favorables, por lo cual consideramos que no tenemos por qué preocuparnos.

   Aunque pueda ser cierto que desde Internet no puedan acceder a las bases de datos internas de la organización, esto en lo absoluto mitiga el riesgo que un empleado con derechos de acceso excesivos pueda copiar a un USB la base de datos de clientes con depósitos a términos o de costos de su inventario.



Estos argumentos con regularidad son esbozados y contribuyen a crear una ilusión de confianza (como la ilusión de Hering) que los riesgos tecnológicos están mitigados y que consecuentemente, la función de Auditoría Interna de Tecnología no tendría sentido y aportaría poco valor.

Creando valor a través de la Auditoría Interna de Tecnología

La norma 1210 del Instituto de Auditores Internos Internacional (IIA) establece que el Auditor Interno debe reunir los conocimientos y competencias necesarias para cumplir con sus responsabilidades. De hecho, la IIA ha creado guías (Global Technology Audit Guide) para que los Auditores Internos de Tecnología dispongan de herramientas para su labor.

Una función de Auditoría Interna de Tecnología efectiva advierte riesgos tecnológicos que puedan afectar los procesos críticos de negocio, ayuda a verificar que las políticas de seguridad de la compañía se cumplan, a fortalecer la estructura de control interno a través de recomendaciones, a verificar el cumplimiento de regulaciones locales o internacionales, entre otros.

Si su organización adolece de un Oficial de Seguridad de Información, con mucha más razón la función de Auditoría Interna de Tecnología, debe existir. Si no fuese importante, ¿por qué en la Comunidad Europea y los Estados Unidos existen regulaciones que apuntan a crear dicha función?

¿Qué puedo hacer?

Si su organización depende de tecnología de información para operar, o si opera en un ambiente regulado, o si procesa cientos de transacciones diarias, o si depende de servicios basados en la web o aunque procese pocas transacciones pero de montos altísimos, es muy probable que necesite la función de Auditoría Interna de Tecnología. Dependiendo de las variables anteriores su organización puede estar en las siguientes situaciones:

1. Requerir una función permanente en su organización con recursos calificados que apoye al resto del equipo de Auditoría Interna.
2. Crear una función permanente que atienda a todas las compañías de su grupo de empresas. Esto es muy útil ya que redeuce costos y crea consistencia en el enfoque de trabajo.
3. Requerir una función no permanente que una o dos veces al año realice una revisión sobre los riesgos y controles de tecnología y que esté alineado con el plan de Auditoría Interna de la organización.
4. Necesitar una función no permanente que apoye al Departamento de Auditoría Interna en revisiones específicas durante el año, como por ejemplo, revisar la seguridad del sistema de inventario o captaciones.

Para las opciones una y dos tendrá que crear la función y lo que ello conlleva. Para la tres y cuatro podría considerar darlas en outsourcing, algo que cada día toma más aceptación en las organizaciones dado su importancia y lo dificil que resulta identifcar recursos con tales habilidades.

¿Lujo o necesidad? En nuestro criterio, es una necesidad si su organización depende de tecnología de información para generar ingresos, para brindar servicio o para reducir costos. Si su organización puede funcionar perfectamente sin redes y sistemas, pues no la necesita.

En ocasiones ejecutivos indican que están convencidos que necesitan la función pero que es un lujo tenerla. Sobre el supuesto que dicha afirmación sea cierta, pregúntese qué otros lujos su organización se da, sin probablemente necesidad alguna.

Independencia. Integridad. Conocimiento. Credibilidad.

RISCCO es una compañía independiente dedicada de manera exclusiva a la consultoría en riesgo, negocios y auditoría interna.

Para mayor información sobre el contenido de este documento o conocer más sobre la forma cómo estamos ayudando a las organizaciones a enfrentar sus desafíos en materia de administración de riesgo, riesgos de tecnología o auditoría interna, por favor contáctenos.

info@riscco.com

Teléfono: +507 279-1410

RISCCO
Ave. Ricardo J. Alfaro
Panamá, Rep. de Panamá

www.riscco.com