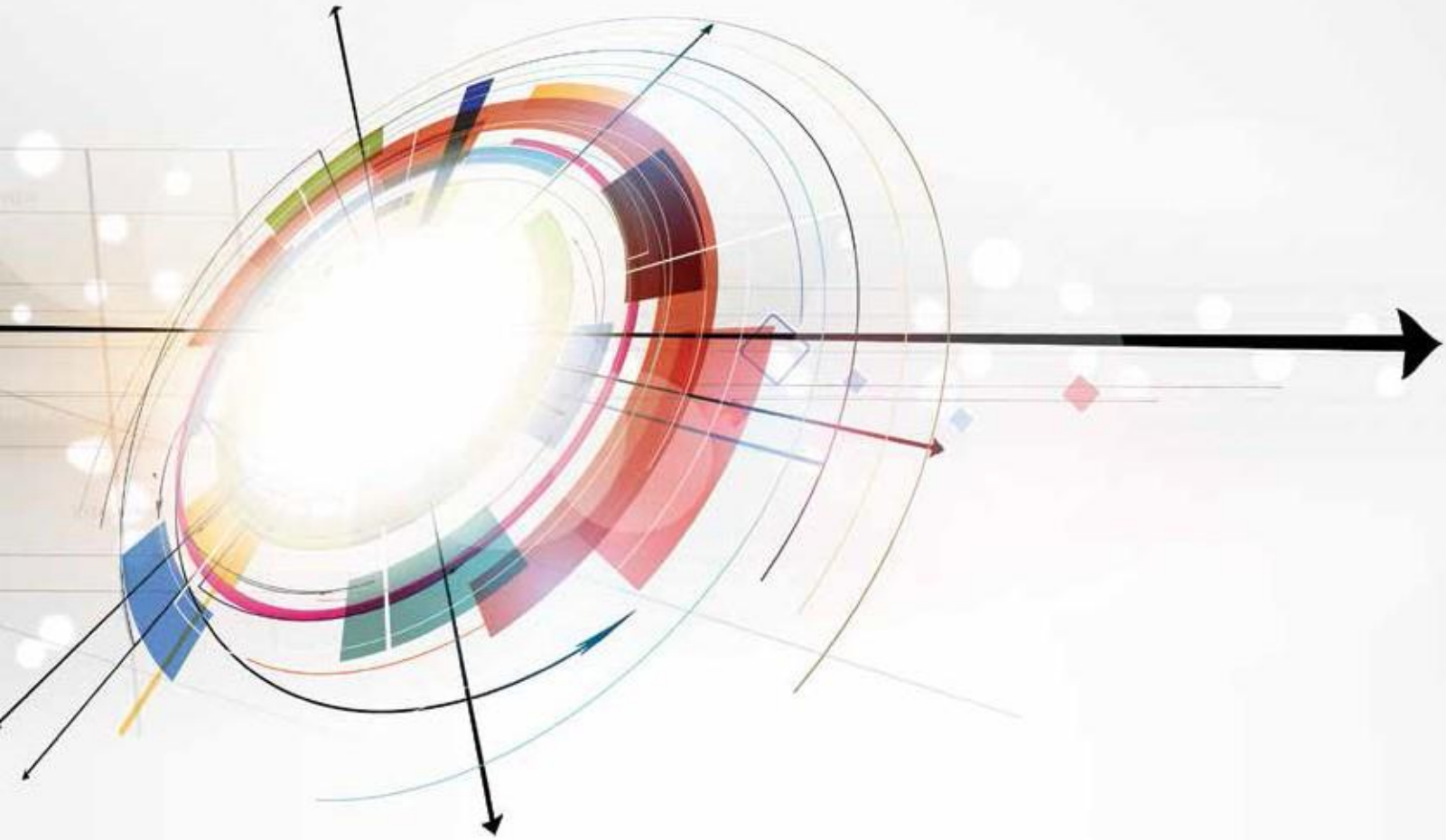

PERCEPCIONES Y PERSPECTIVAS GLOBALES

2018: Principales riesgos que enfrentan los directores ejecutivos de auditoría

The Institute of Internal Auditors

Ediciones anteriores

Para acceder a ediciones anteriores de Percepciones y perspectivas globales, visite www.theiia.org/gpi.

Opiniones de los lectores

Envíe sus preguntas o comentarios a globalperspectives@theiia.org.

Índice

Introducción

Presentando el año 2018: un año nuevo, nuevas leyes, normas, opiniones, ideas, tecnología y riesgos. El entorno de negocios actual es significativamente diferente de cómo era en el pasado; es más complejo y está más conectado. Las organizaciones se enfrentan a riesgos nuevos y desconocidos, pero también a oportunidades nuevas e inexploradas. Si consideramos en el año que tenemos por delante las nuevas oportunidades y la cantidad de posibles desafíos y riesgos (algunos de los cuales esperamos y otros que son únicos de 2018), deberíamos ver a los planes de auditoría como estructuras que cambiarán a medida que se produzcan los eventos, incluso aquellos que son disruptivos.

Con su visión que abarca toda la organización, auditoría interna ayuda a la organización a alcanzar sus objetivos aportando un enfoque disciplinado y sistemático para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno. Los organismos de control y los comités de auditoría quieren y necesitan aseguramiento de que los esfuerzos de gestión de riesgos sean adecuados para abordar las amenazas que representan los competidores poderosos, las tecnologías crecientes, las tendencias cambiantes del mercado y los desarrollos normativos (consulte Internal Audit Future Trends: Emerging Trends and High-impact Areas of Focus [Tendencias futuras para auditoría interna: tendencias emergentes y áreas principales de alto impacto]).

Dado que existe la necesidad de que auditoría interna proporcione mayor apoyo estratégico y que añada valor a todos los sectores económicos, los auditores deben asegurarse de que su trabajo esté alineado con todos los riesgos significativos, especialmente los riesgos operativos y estratégicos. Auditoría interna debe ser consciente y adaptarse a un entorno de riesgos dinámico.

Los riesgos cambian e incluso los planes de auditoría mejor preparados deberían ser flexibles y estar sujetos a cambios a medida que emergen riesgos nuevos en cada uno de los niveles de la organización. Este documento aborda los cinco riesgos principales (para la auditoría interna o la organización) que enfrentan los directores ejecutivos de auditoría (DEA), identificados por los afiliados del IIA. Estos riesgos son: gestión de talentos, análisis de datos, cibernéticos, normas y cómo responder a la disrupción.

Gestión de talentos

La gestión de talentos es consistentemente una de las principales preocupaciones de los DEA y de los profesionales de auditoría interna. Durante los últimos años, los DEA se han angustiado por la búsqueda de candidatos con las habilidades necesarias para ocupar nuevos roles y abordar riesgos nuevos y existentes. Con toda claridad, hay una reserva limitada de candidatos con las habilidades para satisfacer las necesidades cambiantes de auditoría interna.

Además, está el desafío de alinear el entorno de trabajo con los atributos únicos de la fuerza laboral de la generación del milenio, la cual tiene expectativas mayores y diferentes de apoyo y reconocimiento, un entorno de trabajo específico en mente y una preferencia por horarios de trabajo más flexibles (consulte 4 Strategies for Bridging the Internal Audit Talent Gap [4 estrategias para llenar el vacío de talentos en auditoría interna]).

«Si auditoría interna debe estar preparada para el futuro, uno de los cinco puntos imprescindibles que debe abordar es la agilidad. Debemos ser lo suficientemente ágiles para reconocer y abordar los riesgos emergentes y para evaluar los riesgos de forma continua, y entonces adaptar la cobertura de nuestra auditoría en consecuencia. Y debemos ser lo suficientemente ágiles para reconocer las deficiencias en nuestras capacidades y subsanarlas con rapidez. El éxito en el futuro lo alcanzarán aquellos departamentos de auditoría interna que tengan una estrategia dinámica de gestión de talentos».

Richard Chambers,
Presidente ejecutivo del IIA

En 2015, *atraer y retener talentos* fue una prioridad alta o crítica para más del 40 por ciento de los encuestados de una encuesta global del IIA, donde más de la mitad de los encuestados atribuyen la *insuficiencia de conocimientos* a la reserva limitada de auditores habilidosos. Nuevamente en 2017, en respuesta a una encuesta del Audit Executive Center® (AEC®) del IIA, una clara mayoría (79 por ciento) de casi 200 DEA identificó a la gestión de talentos como el riesgo principal extremadamente importante o muy importante para la profesión de auditoría interna. Según KPMG, los consejos de administración consideran que los talentos (o la falta de estos) son un *riesgo empresarial*. A medida que las organizaciones se hacen más globales, la fuerza de trabajo que las respalda continúa evolucionando, razón por la cual la gestión de talentos es tan crucial. El impacto y las implicaciones posibles de la escasez de talentos globales incluyen la inhabilidad para mantener habilidades de liderazgo, dado que ya no hay un canal saludable de futuros líderes, y las entregas estratégicas de la empresa están en duda porque los candidatos no son capaces de asumir roles críticos. Las organizaciones están descubriendo que no son capaces de preparar y orientar a las nuevas generaciones ni de retener a los talentos superiores o especializados, lo cual hace que se pierda el capital intelectual y la ventaja competitiva. Además, y constantemente, la población jubilada desencadena una escasez de habilidades (consulte Boardroom Questions: Talent Management...or Talent Risk? [Preguntas para el consejo de administración: ¿gestión de talentos... o riesgo de talentos?)

Para añadir leña al fuego, debido a los riesgos emergentes (como el análisis de datos, la gestión de terceros, la seguridad cibernética, la sostenibilidad y las incertidumbres políticas y de otro tipo), las organizaciones esperan más de sus auditores internos. Atrás quedaron los días en los cuales el enfoque de auditoría interna estaba limitado a tareas e intereses financieros tradicionales y basados en el cumplimiento.

Aunque auditoría interna no está en el negocio de los recursos humanos, debería evaluar *qué tan bien* la dirección está abordando estos riesgos. Las organizaciones actuales necesitan, y esperan que los auditores internos asuman, un enfoque más holístico hacia la auditoría, lo cual incluye vigilancia del riesgo integral y creación de valor. Debido a esto, la búsqueda de los mejores talentos, habilidades y fortalezas en auditoría interna se ha tornado muy competitiva.

Sin habilidades adecuadas, auditoría interna está vulnerable a pasar por alto, o no auditar con suficiente minuciosidad, riesgos específicos y no tradicionales, como tecnología, geopolítica, economía, presentación de informes

empresariales cambiante, cultura y normas globales y nacionales. Según la Asociación para la gestión de recursos humanos (Society for Human Resource Management), la habilidad de auditoría interna para evolucionar más allá de los conjuntos de habilidades tradicionales financieras, operativas y de TI generales, y concentrarse en un panorama más general, es crucial.

Una actividad de auditoría interna que expande concienzudamente sus competencias y asume su trabajo con base en una comprensión más amplia del perfil de riesgo de la organización estará mejor preparada para servir a la organización. Parte de esa preparación es incluir personas con capacidades avanzadas de razonamiento crítico y perspicacia fuertes de negocios, combinadas con experiencia en áreas específicas o con conocimientos específicos del sector económico. Los riesgos emergentes no tradicionales influenciarán el universo de la auditoría; por lo tanto, auditoría interna debe intentar alcanzar y expandir el alcance y la profundidad de sus habilidades.

Es imprescindible que los DEA guíen a los auditores hacia la ampliación de su experiencia y sus habilidades y consideren la «nueva normalidad» de los riesgos a la hora de evaluar y llevar a cabo los planes de auditoría. No se equivoque, la formación tradicional en auditoría es relevante y siempre lo será; pero la educación y exposición continuas, la adaptabilidad, las buenas

habilidades blandas y el conocimiento de los procesos y las operaciones son esenciales para explorar el nuevo mundo de los negocios.

La habilidad para gestionar todos los talentos es vital para el éxito de auditoría interna y puede aportar beneficios duraderos (más allá de cubrir la escasez esporádica de personal). Para optimizar los esfuerzos de gestión de talentos, los DEA y la alta dirección deberían desarrollar enfoques bien razonados y bien desarrollados orientados a reestructurar y mejorar su fuerza laboral. En pos de la eficacia y con el fin de desarrollar, involucrar y retener la mejor actividad de auditoría interna posible frente a los riesgos nuevos, los DEA deben desarrollar estrategias que incluyan medir lo que se necesita de los miembros existentes de su personal, lo que se necesita de las adiciones previstas a su personal e, igual de importante, lo que los miembros del personal deben ver y escuchar de sus líderes para crecer y tener éxito.

Una estrategia sólida de gestión de talentos depende de una combinación de enfoques. Los DEA *no* serán capaces de salir de una escasez de talentos mediante las contrataciones. Hay un suministro reducido de candidatos con las habilidades necesarias para abordar los riesgos futuros (lo que incluye aquellos con habilidades en ciencias de los datos, razonamiento innovador, razonamiento analítico o crítico, comunicación y otras). Una estrategia eficaz incluye comprender cuáles habilidades y atributos se necesitan, y los esfuerzos continuos

Objetivo de la auditoría

La Norma 1210 del IIA: Pericia

Los auditores internos deben poseer los conocimientos, las habilidades y demás competencias necesarias para poder cumplir con sus responsabilidades La actividad de auditoría interna, en forma colectiva, debe poseer u obtener los conocimientos, las habilidades y demás competencias necesarias para cumplir con sus responsabilidades.

La Norma 1230 del IIA: Desarrollo profesional continuo

Los auditores internos deben incrementar sus conocimientos, habilidades y demás competencias a través del desarrollo profesional continuo.

para adquirir, desarrollar y retener a los mejores talentos.

Objetivos

- Las competencias colectivas de auditoría interna están impulsadas por los riesgos que conlleva el alcance de auditoría interna.
- Los DEA, el comité de auditoría y la dirección ejecutiva tienen una comprensión sólida de las habilidades necesarias para respaldar los objetivos de la organización y del coste total del personal de auditoría interna.
- Auditoría interna ha implementado un proceso consistente de gestión del desempeño.
- Los líderes de auditoría interna tienen la capacidad de guiar, orientar e involucrar a las nuevas generaciones o a aquellos miembros de cualquier generación que seas nuevos en la profesión de auditoría interna.
- Hay planes profesionales formales implementados para todo el personal de auditoría interna.
- Auditoría interna tiene programas establecidos para integrar a los empleados nuevos y educar continuamente a todos sobre la cultura de la organización, el nivel de aceptación de riesgos y la dirección estratégica.

Acciones

- Revisar la evaluación de riesgos y el plan de auditoría e identificar las habilidades necesarias para llevar a cabo el plan. Realizar un análisis de las brechas entre las habilidades actuales y las habilidades necesarias y desarrollar una estrategia para cubrir las brechas.
- Estructurar o reestructurar las revisiones de desempeño para que incluyan competencias laborales específicas, objetivos viables que estén alineados con el plan estratégico de la organización y estructuras de salarios para profesionales especializados como los analistas de datos.

Objetivo de la auditoría

La Norma 1220 del IIA: Debido cuidado profesional

Los auditores internos deben aplicar el cuidado y la pericia que se espera de un auditor interno razonablemente prudente y competente. El debido cuidado profesional no implica ser infalible.

1220.A2: Al ejercer el debido cuidado profesional, los auditores internos deben considerar el uso de técnicas de auditoría basadas en la tecnología y de otras técnicas de análisis de datos.

- Orientar y desarrollar las habilidades dentro del personal existente, lo cual permite la menor cantidad de disrupción e integra el conocimiento empresarial existente con las habilidades nuevas requeridas.
- Adquirir persistentemente habilidades nuevas en el mercado. Buscar candidatos con diferentes formaciones, no solo aquellos con diplomas en finanzas y contabilidad. Considerar proveedores de servicios externos como recurso para obtener rápidamente las habilidades necesarias para abordar riesgos complejos y especializados.
- Establecer un programa eficaz de integración y transferencia de conocimientos.

Análisis de datos

El análisis de datos es el proceso de reunir y analizar datos, y a continuación usar los resultados para tomar mejores decisiones *(Internal Auditing, 4.ª edición, 11-2,* Fundación de Auditoría Interna, 2017*)*. Las organizaciones están produciendo almacenes crecientes de datos de sus operaciones, lo cual presenta dos desafíos clave para auditoría interna. El primero es cómo ayudar al consejo de administración y a la dirección a comprender cómo se están recopilando, gestionando, protegiendo y aprovechando esos datos. El segundo es cómo explotar los datos crecientes desde la perspectiva de la auditoría interna a la hora de aplicar herramientas analíticas a los procesos de auditoría existentes, y automatizar las auditorías de rutina y enfocarse en las áreas de riesgo emergente (consulte Risk in Focus: Hot Topics for Internal Audit 2018 [Enfoque en el riesgo: principales temas para auditoría interna en 2018]).

Básicamente, el análisis de datos desglosa volúmenes de datos y los reconstruye nuevamente en la forma de pepitas más pequeñas, lo cual proporciona la oportunidad de extraer significados y comprensiones de los datos. Con esa información, auditoría interna puede analizar los riesgos y las posibles correlaciones de la *población total*, proporcionar perspectivas y previsiones e informar acerca de cuestiones que les preocupan a las partes interesadas y que ellas están interesadas en seguir. Gestionar el análisis de datos, y los riesgos asociados con este, puede ser abrumador. A veces derivar perspectivas significativas de esos datos (y convertir el conocimiento en acción) es más fácil de decir que de hacer. Para el análisis de datos sea eficaz, debe estar la gente, los formatos, la tecnología y los procesos correctos en su lugar.

Con más datos que nunca a su inmediata disposición, la dirección y el consejo de administración deben darse cuenta de que las cantidades masivas de datos exponen a la organización a riesgos financieros y no financieros relacionados con los datos. Se deben abordar varias áreas de riesgo en cualquier iniciativa de análisis (consulte Understanding and Managing the Risks of Analytics [Comprender y gestionar los riesgos del análisis]):

- **Riesgo de calidad de la información y los datos**: las personas a cargo de tomar las decisiones necesitan datos que comuniquen y fomenten una

comprensión de lo complejo.
Debe haber definiciones claras y normas de calidad para todos los datos y la información.

- **Riesgo de cumplimiento de la información y los datos**: si se incumplen los requisitos de un agente autorizado y reconocido (por lo general asociado con lo estatal, federal o internacional) puede llevar a un resultado adverso como una multa financiera, trabajo adicional o responsabilidad personal.
- **Riesgo de gobierno de la información y los datos**: los datos y la información deben controlarse minuciosamente a través del uso de procesos y principios de gestión de riesgos en los niveles correspondientes para asegurar la privacidad, seguridad, calidad y capacidad de auditarse.
- **Riesgo de uso inapropiado o prematuro del análisis**: el análisis no será útil si no hay tiempo para reunir, procesar e interpretar datos; cuando no hay historial o precedente relacionado con las decisiones o cuando los datos históricos son confusos; o cuando no se pueden medir las variables clave o estas tienen un alto grado de incertidumbre.
- **Riesgo de impacto contracultural**: imponer iniciativas de análisis en la cultura de una organización que no está orientada hacia los datos puede representar un riesgo significativo para los líderes; las iniciativas de análisis deberían incluir una evaluación del sistema de toma de decisiones de la organización y el grado en el cual la cultura de la organización está orientada hacia la los datos.
- **Riesgos de ética de datos**: las iniciativas de análisis de datos deberían alinearse con los valores fundamentales, la toma de decisiones y los comportamientos de la organización. Deberían estar implementados los controles para asegurar la recopilación y el uso éticos de los datos.

Auditoría interna siempre debería ser consciente de los peligros que podrían enfrentar las organizaciones con los proyectos de macrodatos, específicamente en una situación en la cual el personal carece de alguna habilidad. La demanda de análisis de datos está en alza y pronto será una parte integral de *cada* organización (si es que todavía no lo es). Aunque es importante que las organizaciones participen en proyectos de macrodatos para seguir siendo competitivas y no quedar atrás, hay riesgos que deben considerarse:

- Seguridad de los datos.
- Privacidad de los datos.
- Costes.
- Datos poco fiables, inválidos, insuficientes o irrelevantes.
- Procesos analíticos poco fiables, inválidos, insuficientes o irrelevantes.

La tecnología cambia el mundo en el cual vivimos a un ritmo vertiginoso, y las consecuencias de esa velocidad del cambio es frustrante, como mínimo, si no estamos correctamente preparados. La tecnología genera cantidades mucho mayores de datos, y auditoría interna puede usarlos para evaluar los riesgos de

forma más minuciosa, mejorar la realización de las auditorías y posiblemente incrementar el nivel de aseguramiento proporcionado.

Los resultados de estudios de caso realizados recientemente demuestran que los beneficios clave del análisis de datos para auditoría interna incluyen mayor eficiencia, mayor eficacia, mayor aseguramiento, mayor enfoque en los riesgos estratégicos, mayor cobertura de auditoría y ahorros significativos en términos de tiempo y dinero en el largo plazo. No obstante, para experimentar estos beneficios, auditoría interna debe evaluar qué tan bien el programa de análisis de datos sirve para sus objetivos generales y actividades deseadas.

El análisis de datos es crucial para el conjunto de herramientas de auditoría interna, ya que puede proporcionar revelaciones enterradas en la profundidad de los datos además de permitir pruebas más eficientes y eficaces. Muchos equipos de auditoría interna todavía no han adoptado las tecnologías más sofisticadas de análisis de datos; aún dependen principalmente de herramientas y aplicaciones basadas en hojas de cálculo. El respaldo del comité de auditoría es esencial. Auditoría interna debería asegurarse de que el comité de auditoría esté educado acerca de la importante del análisis de datos (consulte Data Analytics: Is it Time to Take the First Step? [Análisis de datos: ¿es momento de dar el primer paso?]).

Para desarrollar o mejorar un programa de análisis de datos, los DEA deberían debatir con las partes interesadas acerca de los resultados esperados, definir los objetivos del análisis y determinar cuáles *competencias* y tecnologías se necesitarán.

Una de las principales barreras para desarrollar un programa eficiente de análisis de datos (y un riesgo constante para auditoría interna) es el personal cualificado inadecuado para manipular los macrodatos. Debido al déficit en esta especialización, los programas de análisis de auditoría interna podrían ser menos que óptimos; no necesariamente debido al programa en sí, sino porque no se está usando aprovechando su potencial completo. Como sucede con cualquier iniciativa nueva de negocios, los proyectos de macrodatos implican un elemento de riesgo. Si falta el talento para gestionar los macrodatos, aumenta todavía más el elemento de riesgo.

Objetivos

- Auditoría interna tiene una comprensión profunda del análisis de datos y la tecnología y de cómo la tecnología avanzada puede mejorar la eficacia y eficiencia de auditoría interna.
- Auditoría interna evalúa qué tan bien la dirección responde a los nuevos riesgos introducidos a partir del uso ampliado del análisis de datos.
- Auditoría interna hace uso de las habilidades avanzadas de los programas de análisis de datos para el beneficio total de la organización (por ejemplo, validación y supervisión de esquemas y comportamientos de alto riesgo,

evaluación y precisión de procesos de evaluación de riesgos específicos de la organización, etc.).

- Auditoría interna aprovecha la tecnología para la identificación de anomalías y patrones de riesgo de fraude de forma temprana y comunica los hallazgos clave.
- Auditoría interna aprovecha la tecnología para mejorar la cobertura general de riesgo de la organización en menos horas de trabajo y costes de mano de obra.

Adaptado parcialmente de: First Steps in Building a Data Analytics Program for Your Internal Audit Team [Primeros pasos en el desarrollo de un programa de análisis de datos para su equipo de auditoría interna]

Acciones

- Determinar cuáles resultados de los análisis sirven mejor para los objetivos de auditoría interna, al decidir cuáles son las necesidades básicas y específicas para el programa de análisis de datos.
- Comprender los beneficios que podrían proporcionar los programas de análisis a la organización y a auditoría interna en términos de innovación y oportunidad. Identificar las habilidades necesarias para implementar de forma óptima los programas y materializar los beneficios.
- Considerar el análisis de datos como un componente de negocios crucial y personalizar el trabajo de auditoría para recibir el mejor enfoque de calidad sostenible posible para gestionar el marco completo de controles y cumplimiento de la organización.
- Involucrar a la dirección en relación con las reglas específicas, puntos de datos, códigos y presunciones en el programa que detectarán correctamente irregularidades o patrones de fraude.

Cibernéticos

Ya sea que se trate de la embestida implacable de las vulneraciones de información en contra de las organizaciones o los infinitos informes de robo de identidad personal, los delincuentes cibernéticos (sofisticados y bien financiados) son rivales poderosos. La interconexión genera un mundo complejo y basado en el riesgo, simplemente propicio para los delincuentes cibernéticos. Las técnicas que utilizan continúan expandiéndose y evolucionando; tanto así que es un fastidio seguirles el ritmo.

Lanzar un plan de defensa contra los ataques cibernéticos y asegurarse de que el plan sea eficaz es un trabajo de 24 horas; no es cuestión de *si* se producirá un ataque, sino *cuándo* lo hará. Hay una gran diferencia entre conciencia del riesgo cibernético y *preparación* para el riesgo cibernético. Todos somos *conscientes* de los riesgos; todos nos enfrentamos a la verdad de estos a diario. No obstante, la preparación incluye la habilidad para *frustrar* totalmente un intento de ataque o *tolerar* un ataque y recuperarse sin daños o con una cantidad relativamente menor. Para que las organizaciones disfruten incluso

una pizca de protección contra la calamidad de una vulneración, deben ser capaces de resistir, reaccionar y recuperarse de los ataques cibernéticos (*resistencia cibernética*).

A medida que aumenta la preocupación por los problemas cibernéticos (por ejemplo, pirateos o intrusiones, ataques de «spear phishing», espionaje económico, etc.), las partes interesadas requieren una mayor visibilidad de los programas de gestión de riesgos de seguridad cibernética de sus organizaciones, y los consejos de administración desean una revisión independiente, objetiva y amplia de los riesgos y programas cibernéticos por parte de auditoría interna. Por lo tanto, auditoría interna también debe conocer los riesgos posibles y desempeñar un rol importante en la resistencia cibernética.

«No es necesario que los directores sean tecnólogos para desarrollar un rol eficaz en la vigilancia del riesgo cibernético; pero cada consejo de administración puede aprovechar la oportunidad para mejorar la eficacia de sus prácticas de vigilancia cibernética».

Manual sobre vigilancia del riesgo cibernético del director de la NACD, Asociación Nacional de Directores Corporativos (NACD), 2017

Fuente: The Value of Visibility: Cybersecurity risk management examination [El valor de la visibilidad: examen de gestión de riesgos de seguridad cibernética]

Desafortunadamente, el riesgo para la seguridad cibernética no está limitado a las amenazas externas; pueden producirse posibles amenazas a partir de las acciones de los empleados o socios de negocios. Por consiguiente, un componente crucial de la resistencia cibernética es la gestión adecuada y eficaz de la cultura de la organización, además de la evaluación de su *riesgo.* A la hora de considerar la cultura, los consejos de administración también están incluyendo la *cultura de riesgo*, porque es la base de todas las decisiones, conducta y asunción de riesgos dentro de toda la organización. Auditoría interna puede auditar la cultura de riesgo dentro de las auditorías financieras y operativas normales al recabar datos y realizar revisiones informales.

Al encabezar las acciones, auditoría interna puede fortalecer la comprensión que tiene la dirección de la eficacia de los controles de seguridad cibernética en todas las áreas, incluso al nivel al cual la cultura de una organización impacta en los requisitos, procesos y capacidades. La cultura impulsa la productividad, los valores, las actitudes y las prácticas dentro de una organización, y recibe su forma y se mantiene gracias a muchos factores diferentes; por lo tanto, auditoría interna puede evaluar la cultura para el riesgo de la misma forma que evalúa otras áreas de una organización (consulte Internal Audit Future Trends [Tendencias futuras de auditoría interna]). Auditoría interna puede maximizar su valor al comprender cómo evaluar la cultura y educar a la dirección acerca de su importancia.

Para superar los riesgos relacionados con lo cibernético, lo que incluye la cultura, es crucial que el equipo de liderazgo desarrolle medidas de precaución, las implemente con programas de formación y concientización, y luego se asegure que se demuestren continuamente en el comportamiento. Por consiguiente, los empleados, proveedores, socios y contratistas por igual deben estar formados y debe procurarse que comprendan exactamente lo que se espera de ellos en relación con las medidas y los protocolos de seguridad cibernética.

Las estrategias de evaluación de riesgos de auditoría interna se deberían desarrollar en relación con todos los riesgos específicos de la seguridad

cibernética, y asegurar el cumplimiento de políticas y controles internos. Auditoría interna debe desarrollar un enfoque de auditoría intenso que satisfaga las necesidades de la organización y de sus partes interesadas en todas las áreas a las que pueden llegar los problemas cibernéticos. En pos de la eficacia, esto requiere la instalación de (como mínimo) actividades de control, un entorno de control, evaluación de riesgos, comunicación y supervisión, además de un marco para evaluar las medidas de seguridad cibernética (consulte Risk in Focus: Hot Topics for Internal Audit 2018 [Enfoque en el riesgo: principales temas para auditoría interna en 2018]).

Como la tercera línea de defensa, auditoría interna debería trabajar con la dirección y con el consejo de administración a medida que desarrollan las estrategias y políticas de seguridad cibernética para mejorar la habilidad que tiene la organización para identificar y mitigar los riesgos de seguridad cibernética; aprovechar las relaciones con el comité de auditoría y el consejo de administración, asegurándose de que continúen participando; y asegurarse de que el riesgo de seguridad cibernética esté *formalmente* integrado en el plan de auditoría, con las habilidades necesarias (internas o mediante la inclusión de tercerizados) para llevar a cabo el plan. Las tecnologías y tendencias emergentes afectan el perfil de riesgo de seguridad cibernética de una organización; en consecuencia, auditoría interna también debería mantenerse al tanto de las tecnologías emergentes y evaluar el nivel de vulnerabilidad de la organización, y sus actividades de riesgo en comparación con el plan de seguridad cibernética preferido.

Objetivos

- La organización tiene una cultura cibernéticamente resistente.
- Auditoría interna aporta componentes clave cruciales para la examinación y preparación de la seguridad cibernética:
  - Protección y detección: auditoría interna proporciona un enfoque holístico para identificar dónde podría ser vulnerable una organización e incorpora análisis de datos en su ámbito de responsabilidad, lo cual dará una alerta de que algo está mal.
  - Continuidad del negocio: auditoría interna proporciona asesoramiento, involucrando a la dirección a medida que planifica enfrentar o superar los escenarios de riesgo que podrían impactar las operaciones continuas, lo cual incluye ataques cibernéticos, desastres naturales o sucesión.
  - Comunicaciones o gestiónde crisis: Auditoría interna ayuda con la planificación de la gestión de crisis y la preparación de las comunicaciones al proporcionar comprobaciones de aseguramiento de eficacia y puntualidad y realizar análisis y críticas de los planes ejecutados.
  - Mejoras continuas: Auditoría interna añade valor al proporcionar perspectivas y mejorar las estrategias y los protocolos para tener una

mejor
preparación para los ataques cibernéticos.

Acciones

- Evaluar la cultura de la organización en relación con la resistencia cibernética.
- Realizar evaluaciones de riesgo de modelos de seguridad y procesos de seguridad cibernética y realizar recomendaciones para mejoras.
- Realizar pruebas de penetración de datos con contratistas externos y de TI para evaluar la habilidad que tiene el tercero de cumplir con los protocolos establecidos.
- Realizar análisis de lagunas en la resistencia cibernética, recomendar subsanaciones y realizar un seguimiento de las actividades de subsanación.
- Influenciar la cultura al enfatizar la supervisión y la respuesta de la seguridad cibernética como principales prioridades.
- Asegurarse de que se pruebe periódicamente el plan de continuidad del negocio y que se realice la acción correctiva para cualquier deficiencia identificada.
- Implementar y fomentar una cultura cibernética y cultura del riesgo sólidas en toda la organización, lo cual, con el transcurso del tiempo, influenciará e incrementará las medidas y los protocolos de seguridad cibernética.

Normas

A nivel global, las organizaciones enfrentan requisitos normativos nuevos o modificados, diseñados en parte para proteger a los consumidores o a los intereses del público. Las normas de mayor perfil se concentran en los riesgos y controles financieros y en la privacidad y seguridad de los datos e impactan a las organizaciones de todos los sectores económicos.

Criptomonedas

Según CNBC, las criptomonedas podrían pasar la marca del billón de dólares estadounidenses en términos de valor, tras una reciente e intensa venta en todas las monedas digitales. El valor de la Bitcoin es volatil: A principios de 2018, fluctuó entre 6000 USD y 10 000 USD. Thomas Glucksmann, director de desarrollo de negocios de Asia Pacífico en la bolsa de criptomonedas Gatecoin, indicó, «El aumento del reconocimiento normativo de las bolsas de criptomonedas, el ingreso de capital institucional y los grandes desarrollos tecnológicos contribuirán al rebote del mercado y empujarán los precios de las criptomonedas a nuevos máximos este año. No hay razón por la cual no podríamos ver a la Bitcoin llegar a un valor de 50 000 USD en diciembre (2018)».

A nivel global, a medida que las principales instituciones financieras se involucran cada vez más en la tecnología de la cadena de bloques y en las transacciones con criptomonedas, deben determinar cómo manejar los conflictos que podrían surgir cuando los empleados realicen transacciones con monedas digitales en sus cuentas personales. Los precios en alza de las

Objetivo de la auditoría

La Norma 2130 del IIA: Control

La actividad de auditoría interna debe ayudar a la organización a mantener controles eficaces mediante la evaluación de tal eficacia y eficiencia y la promoción de mejoras continuas.

2130.A1: La actividad de auditoría interna debe evaluar la suficiencia y eficacia de los controles en respuesta a los riesgos de los sectores de gobierno, operaciones y sistemas de información de la organización en relación con:

- El logro de los objetivos estratégicos de la organización.
- La confiabilidad e integridad de la información financiera y operativa.
- La eficacia y eficiencia de las operaciones y programas.
- La protección de activos.
- El cumplimiento de las leyes, regulaciones, políticas, procedimientos y contratos.

«La RGPD y sus implicaciones están ganando prominencia. Desde la perspectiva del aseguramiento, el comité de auditoría querrá que inicialmente evaluemos el programa en sí, pero después desarrollemos nuestro propio programa de forma continua para asegurarnos de que la empresa tiene los procesos correctos implementados con el fin de continuar cumpliendo».

DEA de un grupo bancario multinacional

Fuente: Risk in Focus: Hot Topics for Internal Audit 2018 [Enfoque en el riesgo: principales temas para auditoría interna en 2018].

monedas digitales no solo han suscitado el interés de los inversores y los bancos, sino que los departamentos de cumplimiento también les están prestando suma atención. Podrían surgir conflictos si los empleados involucrados en la criptomoneda (o aquellos que desean invertir en ella) realizan apuestas con una ventaja desleal. En general, los empleados deben obtener una autorización antes de poder realizar transacciones en cualquier valor que represente un conflicto de intereses; no obstante, las políticas son mucho más difíciles de aplicar con las criptomonedas, ya que las transacciones se realizan a través de una red fragmentada de bolsas (a veces de forma anónima) y es complicado realizarles un seguimiento. Además está la ausencia de reglas claras de los organismos globales de control, lo cual hace que para las organizaciones financieras sea difícil establecer las propias. Algunos consideran que las criptomonedas son materias primas y otros dicen que algunas criptomonedas podrían ser valores, pero no especifican cuáles. Los organismos globales de control han estado ansioso debido a la reciente volatilidad explosiva en el valor de la Bitcoin y de otras monedas digitales, y podrían implementarse normas contundentes (consulte Compliance Officers Sweat as Cryptocurrency Trades Go Mainstream [Los directores de cumplimiento se estresan a medida que el mercado de las criptomonedas pasa a ser masivo]).

Normas globales de protección de datos

Un serie de gobiernos está implementando mayores normas sobre la privacidad de los datos. Dos ejemplos son la Unión Europea (UE) y China.

Tras cuatro años de preparación y debate, la Regulación General de Protección de Datos (RGPD) de la UE, que reemplaza la Directiva 95/46/CE sobre protección de datos, fue aprobada por el Parlamento europeo en abril de 2016. La RGPD entrará en vigor en mayo de 2018, a la vez que año tras año, las vulneraciones de datos resultan ser mayores, más intrusivas y más costosas. Las vulneraciones de datos aumentaron sustancialmente en 2017 por encima del aumento de datos informado del 40 por ciento desde 2015 a 2016. (Para obtener más información, consulte «Vulneraciones de datos en 2017» en la siguiente página).

Aunque muchas empresas tienen políticas de privacidad consistentes con la antigua directiva, la nueva RGPD contiene una serie de protecciones nuevas para los datos de la UE y promete multar y sancionar a los controladores y procesadores de datos si incumplen con ella una vez que entre en vigor. En términos simples, cualquier organización (local o internacional) que realice negocios en Europa o manipule datos personales de residentes de la UE debe cumplir con las nuevas reglas.

Para las infracciones más dañinas de incumplimiento de las disposiciones clave, los organismos de control tienen la autoridad de imponer una multa por una suma que alcance los 20 millones de euros o un 4 por ciento de la facturación global anual del año previo, la que sea mayor. Hay un enfoque escalonado

hacia las multas (por ejemplo, una empresa puede recibir una multa del 2 por ciento si no tiene sus registros en orden [Artículo 28], no notifica a la autoridad supervisora y al sujeto de los datos acerca de la vulneración o no realiza una evaluación del impacto). Es importante destacar que estas reglas se aplican tanto a los controladores como a los procesadores. Esto significa que los servidores en la nube no quedarían exentos del cumplimiento de la RGPD. Otros ejemplos que caen dentro de esta categoría son la falta de observancia de los principios fundamentales del procesamiento de datos personales, la violación de los derechos de los sujetos de los datos y la transferencia de datos personales a países terceros u organizaciones internacionales que no garanticen un nivel adecuado de protección de datos (consulte The EU General Data Protection Regulation [La Regulación General de Protección de Datos de la UE]).

Vulneraciones de datos en 2017

Mes	Organización	Violación o vulneración
8 de enero de 2017	E-Sports Entertainment Association (ESEA)	1 503 707 registros añadidos a su base de datos información personal o privada.
2 de febrero de 2017	Xbox 360 ISO y PSP ISO	1,2 millones de usuarios de Xbox 360 ISO y 1,3 ISO afectados; robo de información personal o
15 de marzo de 2017	Dun & Bradstreet	Más de 33 millones de contactos empresariales web, incluso el Departamento de Defensa de lo de los EE. UU.; filtración de información person
6 de abril de 2017	FAFSA: Herramienta de recopilación de datos del IRS	Es posible que se haya robado información pers 000 contribuyentes o estudiantes.
10 de mayo de 2017	Bronx Lebanon Hospital Center	Es posible que se haya comprometido informac personal de al menos 7000 pacientes entre 201 adicciones, diagnósticos de salud médica y men denuncias de agresiones.
20 de junio de 2017	Deep Root Analytics	Aproximadamente 198 millones ciudadanos est cuando Deep Root Analytics, contratada por el Republicano, almacenó información privada o p nube sin protección de datos, expuesta durante
13 de julio de 2017	Verizon	Información de 14 millones de suscriptores exp guardaron en un servidor no seguro; los datos registro, generados cuando los clientes contact
30 de agosto de 2017	Online Spambot	Se recolectaron 711 millones de direcciones de contraseñas de un servidor no seguro.
7 de septiembre de 2017	Equifax	Es posible que 143 millones de clientes se haya que piratas informáticos explotaron un punto d web; se expuso información personal o privada seguro social y números de tarjetas de crédito.
12 de octubre de 2017	Hyatt Hotels	Acceso no autorizado a información de pago pa crédito, lo cual incluyó números de tarjetas de verificación y nombres de titulares de tarjetas q propiedad en 11 países.
21 de noviembre de 2017	Uber	Se expuso información personal de 57 millones incluidos nombres, direcciones de correo electr

10 de diciembre de 2017	TIO Networks (PayPal)	Se comprometieron las identidades de más de 1,6 millones que incluyó información de cuentas bancarias, información pago, contraseñas, nombres de usuario y números del segu

Adaptado de: 2017 Data Breaches – The Worst So Far [Vulneraciones de datos en 2017: las peores hasta ah

Objetivo de la auditoría

La Norma 2120 del IIA: Gestión de riesgos

La actividad de auditoría interna debe evaluar la eficacia y contribuir a la mejora de los procesos de gestión de riesgos.

2120.A1: la actividad de auditoría interna debe evaluar las exposiciones al riesgo referentes a gobierno, operaciones y sistemas de información de la organización, en relación con lo siguiente:

- El logro de los objetivos estratégicos de la organización.
- La confiabilidad e integridad de la información financiera y operativa.
- La eficacia y eficiencia de las operaciones y programas.
- La protección de activos.
- El cumplimiento de las leyes, regulaciones, políticas, procedimientos y contratos.

Incluso la definición y las condiciones de «consentimiento» quedan restringidas significativamente. Anteriormente, los controladores de datos tenían permitido depender del consentimiento implícito y de «exclusión» en algunas circunstancias. A partir del 25 de mayo de 2018, la RGPD fortalece las condiciones para el consentimiento, y las empresas ya no podrán usar textos de términos y condiciones largos e ilegibles repletos de terminología legal, ya que la solicitud de consentimiento debe darse de una forma fácilmente accesible, con el objetivo del procesamiento de los datos adjunto a ese consentimiento. El consentimiento debe ser claro y distinguible de otras cuestiones y debe proporcionarse en un lenguaje claro y simple. Retirar el consentimiento debe ser igual de fácil que prestarlo. Además, una vez que se retira el consentimiento, los sujetos de esos datos tienen el derecho a que se *borren* sus datos personales y que ya no se usen para el procesamiento (consulte The Top 10 Operational Impacts of the EU's General Data Protection Regulation [Los principales 10 impactos operativos de la Regulación General de Protección de Datos de la UE]).

La RGPD afectará significativamente los esfuerzos de seguridad cibernética de Alemania. En mayo de 2017 la legislatura adoptó una versión modificada de la Ley Federal de Protección de Datos, la cual entrará en vigor a la par de la RGPD de la UE el 25 de mayo de 2018. Alemania, conocida por sus fuertes leyes nacionales de protección de datos, con multas que alcanzan los 300 000 EUR, ahora está avanzando hacia normas de seguridad cibernética estrictas y asignando la responsabilidad de proteger a los usuarios y asegurar la información cibernética a los proveedores de servicios y operadores de infraestructura crítica. La nueva ley contiene 85 disposiciones, varias de las cuales hacen referencia a la RGPD de la UE. Los operadores de infraestructura crítica deben implementar protecciones organizativas y técnicas adecuadas y otras medidas de conformidad con *la última tecnología* en el plazo de dos años tras la entrada en vigor de la legislación secundaria que especifique esas protecciones. Además, los operadores de la infraestructura crítica deben demostrar regularmente que cumplen con los requisitos de seguridad y notificar al *Bundesamt für Sicherheit in der Informationstechnik* (BSI) de inmediato si hubieran disrupciones significativas de la disponibilidad, integridad, autenticidad y confidencialidad de sus sistemas, componentes o procesos de TI, las cuales podrían generar o haber generado el fallo o una limitación en el funcionamiento de la infraestructura crítica operada por ellos (consulte What You Need to Know About Germany's Cybersecurity Law [Lo que debe saber acerca de la ley de seguridad cibernética de Alemania]).

Aunque China ya tenía leyes, reglas y normas estrictas relacionadas con la seguridad de la información, presentó una ley amplia que cubre la brecha entre la seguridad cibernética y la protección de los datos (en vigor desde junio de 2017), la cual fusiona las disposiciones de la RGPD de la UE. En muchos sentidos, la Ley de Seguridad Cibernética de la República Popular de China (CSL, en inglés) concuerda con la RGPD (consulte Risk in Focus: Hot Topics for Internal Audit 2018 [Enfoque en el riesgo: principales temas para auditoría interna en 2018]). La CSL realizó modificaciones que prestan mayor atención a

la protección de la información personal y privacidad individual, y normaliza la recopilación y el uso de la información personal. Por ejemplo, en el pasado, las empresas extranjeras transferían información hacia el exterior de China; ahora, la ley estipula que los datos delicados deben almacenarse a nivel local, y hay graves sanciones para aquellos que infrinjan la ley, lo cual incluye la suspensión de las actividades de la empresa. Las multas podrían alcanzar la suma de 1 000 000 CNY. (Para obtener más información, consulte «Modificaciones a la CSL» en la siguiente página).

Modificaciones a la CSL

Artículo	Versión final	Modificación significativa
31	En relación con la protección de la seguridad cibernética, el estado enfatiza la protección de la infraestructura de información crítica en ***servicios de información y comunicaciones públicas, energía, finanzas, transporte, conservación del agua, servicios públicos y gobierno electrónico***, además de otra infraestructura de información crítica que podría causar un daño a la seguridad nacional, la economía nacional y el interés público si fuera destruida, se perdiera su funcionamiento o se filtraran datos.	Este artículo aclara los sectores económicos y las áreas en las cuales recibirá prioridad la protección de la infraestructura de información crítica.
43	Las personas tienen derecho a solicitar a los operadores de la red que corrijan errores en la información personal reunida o almacenada por ellos. ***Los operadores de la red deberían tomar las medidas para eliminar o corregir los errores.***	Este artículo les otorga a los ciudadanos mayores derechos para proteger su información personal e incrementa la obligación de los operadores de la red de corregir errores con rapidez.
46	Las personas o las organizaciones ***son responsables del uso de sus redes*** y no podrán crear sitios web o grupos de comunicaciones con fines fraudulentos o para otras actividades ilegales.	Este artículo enfatiza que las personas y las organizaciones acarrean la responsabilidad del uso de sus redes.
76(5)	«Información personal» hace referencia a todo tipo de información, registrada de forma electrónico o por otro medio, que pueda determinar la identidad de personas físicas de forma independiente o en combinación con otra información, la cual incluye, entre otros datos, el nombre de una ***persona física***, su fecha de nacimiento, número de identificación, información biométrica personal, dirección y número de teléfono.	Este artículo amplía el alcance de la protección de la información personal de «ciudadanos» a «personas físicas».
63	Las personas que infrinjan el Artículo 27 de la ley y participen en actividades que puedan poner en riesgo la seguridad cibernética podrían quedar detenidas entre 5 y 15 días y podrían sufrir multas de entre ***100 000 CNY*** y ***1 000 000 CNY***, según la gravedad del caso.	La sanción máxima por infringir la Ley de Seguridad Cibernética ha aumentado a 1 000 000 CNY.

Fuente: Overview of China's Cybersecurity Law [Resumen de la Ley de Seguridad Cibernética de China]

Pero la CSL no carece de opositores. Como informó The New York Times en mayo de 2017, «una coalición de grupos de intereses empresariales que representan a empresas europeas, estadounidenses y asiáticas exhortaron a China a que demorara la implementación de la ley, mientras que la Cámara de Comercio de la Unión Europea en China solicitó tiempo adicional para permitir que las empresas cumplan debido a las "obligaciones de cumplimiento sustancial"».

Ya sea que realicen negocios en la UE, China o en cualquiera de una serie de otros países con crecientes normas relacionadas con la privacidad de los datos, las organizaciones están sintiendo los efectos. Los consejos de administración están presionando para tener mejores marcos de gobierno dentro de sus organizaciones, y los organismos de control, los inversores y otras partes interesadas están presionando a los consejos de administración, haciéndolos responsables de la eficacia de sus procesos globales (consulte Of Corporate Governance, Risk Management, and Internal Audit [Acerca del gobierno

empresarial, la gestión de riesgos y auditoría interna]). Las nuevas normas incrementan los costes y ejercen presión sobre las organizaciones al sumar complejidad a los procesos de gestión de riesgos, gobierno.

A medida que aumenta la presión ejercida sobre los consejos de administración, también se presiona a auditoría interna. Las organizaciones observan a auditoría interna con grandes expectativas. Reconocen la necesidad de que auditoría interna proporcione asesoramiento y aseguramiento a medida que

Objetivo de la auditoría

La Norma 2210 del IIA: Objetivos del trabajo

Para cada trabajo, se deben establecer los objetivos.

2210.A3: se necesitan criterios adecuados para evaluar los controles, la gestión de riesgos y el gobierno. Los auditores internos deben verificar hasta qué punto la dirección o el consejo de administración ha establecido criterios adecuados para determinar si se han cumplido los objetivos y las metas. Si son adecuados, los auditores internos deben usar dichos criterios en su evaluación. Si no lo son, deben identificar los criterios adecuados de evaluación a través de un debate con la dirección o el consejo de administración.

La Norma 2050 del IIA: Coordinación y fiabilidad

El director ejecutivo de auditoría debería compartir la información, coordinar las actividades y considerar depender del trabajo de otros prestadores internos y externos de servicios aseguramiento y consultoría para asegurar una cobertura adecuada y minimizar la duplicación de tareas.

redirigen las fuerzas disruptivas hacia las oportunidades, mientras se mantienen a la vez en cumplimiento del constante cambio en las normas (consulte KPMG Internal Audit: Top 10 Key Risks in 2016 [Auditoría interna: 10 riesgos clave principales en 2016 de KPMG]).

La clave para sobrevivir a las fuerzas disruptivas es alcanzar el cumplimiento normativo, la gestión de riesgos y el gobierno y un equilibrio en el desempeño. Superar estos desafíos puede proteger e incrementar el valor de la empresa e impulsar
la eficiencia operativa.

Objetivos

- Aclaración del nivel de aceptación de riesgo a la hora de evaluar proyectos y estrategias.
- Concientización en toda la organización sobre las normas nacionales e internacionales.
- Establecimiento de medidas para el cumplimiento de normas nacionales e internacionales vigentes.
- Coordinación de prestadores internos y externos de aseguramiento.

Acciones

- Comprender los marcos internacionales de cumplimiento y las normas de aseguramiento.
- Realizar un inventario sobre los organismos de control existentes y sus requisitos.
- Evaluar el enfoque de la organización hacia la gestión de sus actividades globales de cumplimiento, lo cual incluye la integración de organizaciones nuevas adquiridas.
- Evaluar la respuesta de la organización a instancias notorias de incumplimiento.
- Revisar los programas de formación sobre cumplimiento y evaluar la adecuación para los respectivos roles.
- Coordinar con prestadores internos y externos para asegurar la cobertura adecuada y minimizar la duplicación de tareas.
- Elaborar comunicaciones personalizadas según los intereses y las prioridades de la organización para fomentar una cultura del cumplimiento.
- Evaluar la asignación de responsabilidades de la organización para el cumplimiento de las normas.

Cómo responder a la disrupción

Día nuevo (nueva campana, nuevo denunciante). La tecnología actual cambia constantemente; es más rápida, más grande (y más pequeña); llega más lejos y

es más intensa. Es como nunca ha sido. Los auditores internos se enfrentan cada día con nuevas oportunidades para proporcionar perspectivas y previsiones a las partes interesadas, pero podrían no tener habilidades desarrolladas relacionadas con la innovación, como razonamiento crítico y creatividad. En consecuencia, sin innovación, se dan cuenta de que son incapaces de manejar lo inesperado y vulnerable satisfactoriamente. Los auditores internos deben adaptar sus metodologías para utilizar la tecnología (para hacerse ágiles y proactivos y cambiar rápidamente la dirección para seguirle el ritmo a la innovación).

Aunque las innovaciones, como las nuevas tecnologías, ofrecen excelentes oportunidades para que auditoría interna realice trabajos de auditoría, en muchos casos, la innovación está acompañada por nuevos riesgos, amenazas y *disrupciones*, las cuales se suman a las preocupaciones de auditoría interna. Por ejemplo, en lugar de concentrarse (tradicionalmente) solo en los riesgos, los auditores internos ahora deben ser capaces de *identificar* rápidamente las posibles disrupciones y determinar cuáles requieren atención inmediata o adicional.

Una de las principales razones por las cuales una organización debería innovar es separarse de la competencia (y auditoría interna puede liderar el camino). Según la encuesta 2018 North American Pulse of Internal Audit (El ritmo de auditoría interna en América del Norte en 2018), la innovación le presenta dos opciones a auditoría interna: rever sus capacidades para ocupar un rol cada vez más importante en la organización o asumir prácticas del pasado y llevarlas hacia el futuro. La última opción es una garantía casi total de fracaso en el futuro; por lo tanto, auditoría interna debe estar abierta a las ideas creativas (o incluso radicales) y debe estar lista y dispuesta a concentrarse en la gestión eficaz de los riesgos relacionados.

Habrá desafíos. La dirección podría sentirse incómoda ante la idea de hacer las cosas de forma diferente; los presupuestos podrían estar limitados por el entorno de negocios y la reserva de candidatos podría ser pobre en lo que se refiere a las habilidades necesarias. Pero la buena noticia es que auditoría interna no está sola. Auditoría interna puede aprender de otras unidades de la empresa, organizaciones o actividades de auditoría interna que ya hayan desarrollado técnicas específicas para gestionar el proceso de innovación.

La innovación (cuando se adopta de la forma correcta) es extremadamente valiosa para auditoría interna y para toda la organización:

- Se reducen los costes.
- Se incrementa el valor.
- Se consigue un crecimiento y desempeño mayor.
- Se lanzan productos y servicios antes.
- Se mejoran la experiencia y la satisfacción de los clientes.
- Se amplifican la agilidad y la flexibilidad de la organización.

«Creo firmemente que auditoría interna tiene un papel fundamental en el éxito de nuestras organizaciones. Pero también creo que para estar a la altura de la tarea encomendada, necesitamos renovar nuestro compromiso con la innovación en auditoría interna. La innovación debe ser el pilar sobre el que se alza el trabajo de auditoría interna si queremos seguir el ritmo de los avances que se producen en nuestras organizaciones y fuera de ellas».

Shannon Urban, Presidente del Consejo de administración del IIA de América del Norte (2017 – 2018)

Fuente: Internal Auditor

- Se aumenta la satisfacción de las partes interesadas.

La innovación no solo conduce a una auditoría mejor y más eficiente, sino que la innovación respalda directamente la agilidad cuando permite una respuesta más rápida, inteligente y enfocada a la disrupción (consulte 2018 North American Pulse of Internal Audit: The Internal Audit Transformation Imperative [El ritmo de auditoría interna en América del Norte en 2018: la obligación de transformación de auditoría interna]). La presidente del Consejo de Administración Norteamericano del IIA, Shannon, Urban, fomenta la innovación en auditoría interna como algo fundamental para que pueda crecer y necesaria para satisfacer las necesidades cambiantes de las partes interesadas. Podría ser un poco incómodo y frustrante, pero es continua, y requiere de compromiso y valentía. La innovación también puede ser muy gratificante. Si auditoría interna desea comprender a sus partes interesadas y brindarles un buen servicio en el futuro, aceptar la innovación es la única opción (consulte The Innovative Internal Auditor [El auditor interno innovador]).

Objetivos

- Auditoría interna reconoce los cambios en el entorno de negocios.
- Auditoría interna apunta a desarrollar una cultura de innovación y fortalece las capacidades y el desempeño.
- Auditoría interna apunta a las buenas prácticas y a las mejoras alcanzables mediante la innovación.
- Auditoría interna se esfuerza por mayor eficiencia mediante la innovación.

Acciones

- Diseñar e implementar ideas nuevas, al hacer que la innovación sea una base fundamental de la práctica de la auditoría de la auditoría interna.
- Asumir un rol de liderazgo, prever las disrupciones de los negocios, supervisar los cambios en el entorno y ofrecer un rango más amplio de respuestas.
- Desarrollar relaciones e invertir en ellas. Permanecer conectada con la empresa y ser consciente de la innovación que se produce.
- Aclarar el panorama de riesgo cambiante al determinar cuáles disrupciones exigen una atención adicional.
- Proporcionar perspectivas y un punto de vista en torno a los riesgos emergentes asociados con los eventos disruptivos.
- Encontrar y atraer candidatos con las competencias correctas para responder con rapidez y firmeza a los riesgos nuevos o emergentes.
- Colaborar con otras funciones de cumplimiento y gestión de riesgos.

Reflexiones finales

Los riesgos destacados en este informe (aunque las organizaciones afiliadas del IIA los han reconocido como áreas principales de preocupación) no representan todos los riesgos para las organizaciones o para auditoría interna. Además de estas áreas, las organizaciones afiliadas también identificaron riesgos inherentes al comité de auditoría, el presupuesto, las líneas de defensa y la estrategia (todas áreas esenciales del gobierno de la organización que deben reconocerse y examinarse). El riesgo abre la puerta para el fracaso en el logro de la misión y los objetivos estratégicos de la organización y amenaza el valor global de la organización. Por lo tanto, la responsabilidad de auditoría interna (como asesor de confianza para asistir en los procesos de gestión de riesgos, control y gobierno) requiere la consideración de todas las oportunidades de riesgo y la realización de las recomendaciones correctas.

A nivel global, las organizaciones dependen de auditoría interna y de sus evaluaciones. Para seguir siendo relevante y tener el reconocimiento como asesor de confianza, auditoría interna tiene la obligación de considerar los riesgos para el logro de sus propios objetivos, además de los objetivos de la organización. Debido a esto, auditoría interna debe enfocarse en los resultados y comprometerse con mejorar sus habilidades en pos del beneficio de la organización como un todo. Esto requiere la habilidad de superar los desafíos y obstáculos, lo que incluye realizar un razonamiento crítico; mantenerse independiente y objetiva; ser ágil; concentrarse en el *liderazgo* contra el riesgo (real o imaginado); sortear los «tiempos» al operar como consultor cuando sea necesario; proporcionar aseguramiento cuando sea necesario; y comprender la interdependencia de todos los sistemas, los procesos, las normas y las operaciones.

Organizaciones afiliadas del IIA

Las organizaciones afiliadas del IIA son los ladrillos del IIA. El IIA se asocia con las organizaciones afiliadas del IIA en más de 170 países y territorios para cumplir con su misión de hacer avanzar la profesión de auditoría interna y prestar servicio a sus más de 190 000 miembros a nivel global. Las organizaciones afiliadas del IIA sirven como los representantes exclusivos del IIA que colectivamente llevan la voz de la profesión de auditoría interna, fomentando las normas de ética y práctica profesional en sus comunidades de auditoría interna.

Acerca del IIA

El Instituto de Auditores Internos (IIA) es el defensor, educador y proveedor de normas, lineamientos y certificaciones de mayor reconocimiento para la profesión de auditor interno. Fundado en 1941, el IIA asiste en la actualidad a más de 190 000 miembros de más de 170 países y territorios. La sede principal global de la asociación está en Lake Mary, Fla. EE. UU. Para más información, visite www.globaliia.org.

Exención de responsabilidad

Las opiniones expresadas en Percepciones y perspectivas globales no son necesariamente las de los contribuyentes individuales o de los empleadores de los contribuyentes.

Derechos de autor

The Institute of
Internal Auditors

globaliia.org