PERSPECTIVAS Y PERCEPCIONES

Innovación y tecnología

PARTE I: El papel de la auditoría interna en el aseguramiento tecnológico

PARTE II: Estar al tanto de la adopción de tecnología por parte de la organización

PARTE III: El reto del talento tecnológico en Auditoría

Wolters Kluwer

Traducción al Español Auspiciada por:
FLAI
Fundación Latinoamericana de Auditores Internos

The Institute of Internal Auditors

Contenido

Parte 1: El papel de la Auditoría Interna en el aseguramiento tecnológico

Sobre el Experto

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, es director sénior de producto en TeamMate Audit Solutions, donde trabaja para mejorar continuamente la productividad de las auditorías al tiempo que proporciona información estratégica a través de la mejor solución de TeamMate. Cuenta con más de 20 años de experiencia en auditoría interna, tanto en el sector público como en el privado.

Anteriormente, Jim ocupó diversos cargos directivos en el Instituto de Auditores Internos, fue auditor municipal de la ciudad de Palo Alto (California) y jefe de auditorías del condado de San Diego (California). Su amplia experiencia en auditoría interna incluye puestos en el Sistema Universitario Estatal de California, PETCO Animal Supplies, Inc. State Street Corporation y General Electric.

Introducción

La tecnología se ha convertido en el motor indiscutible del cambio y la innovación empresarial. Desde la transformación digital generalizada hasta la inteligencia artificial emergente y en evolución, las nuevas tecnologías están abriendo oportunidades -y riesgos- como nunca antes. Para comprender el impacto de las nuevas tecnologías, las organizaciones confían en la auditoría interna para obtener garantías sobre su adopción y uso de la tecnología. En este informe se explica por qué el aseguramiento de la tecnología debe ser una parte rutinaria de cualquier auditoría. Cubrirá las áreas clave de vulnerabilidad y discutirá las oportunidades para que la auditoría interna tome la iniciativa de aportar coherencia y coordinación que proporcionen auditorías tecnológicas más eficaces.

Un enfoque central

Dado que la tecnología impregna todos los aspectos de la empresa, es natural que el aseguramiento tecnológico sea ya un tema central para los auditores internos. "Existe un riesgo tecnológico subyacente en prácticamente todo lo que hacen las organizaciones", afirma Jim Pelletier, CIA, CGAP, director de producto senior de TeamMate Audit Solutions. Ya no hay separación entre operaciones y tecnología, porque la tecnología permite las operaciones y muchas otras funciones. Evaluar y garantizar controles adecuados debe incluir cualquier tecnología relacionada subyacente a un proceso. Por ejemplo, mientras que antes los auditores internos podían auditar las cuentas por pagar -o cualquier otra función- y sus sistemas por separado, ahora las funciones y los sistemas están completamente entrelazados, afirma Pelletier. Todo lo que se audita implica cierto grado de garantía tecnológica."

Cuestiones a tener en cuenta

Riesgos de terceros y gobernanza de datos

Reconocer las principales amenazas

Debido a la prevalencia de la tecnología, hay muchos problemas que hay que examinar al ofrecer garantía tecnológica. En esta sección se analizarán varias áreas de alto riesgo.

Relaciones con terceros

La investigación ha demostrado que el 98% de las organizaciones de todo el mundo tienen relaciones de proveedor con al menos un tercero que ha experimentado una violación en los últimos dos años. Las empresas también pueden verse afectadas por las conexiones indirectas de los proveedores. Un total del 50% de las organizaciones tienen relaciones indirectas con al menos 200 proveedores de cuarta parte que han sufrido una violación recientemente.[1]

La gran dependencia e interrelación de las organizaciones con terceros es un riesgo crítico, sobre todo cuando se produce un problema. Las relaciones con terceros pueden ser especialmente vulnerables porque muchas organizaciones asumen incorrectamente que un proveedor está abordando todos los riesgos relacionados y que no es necesaria una revisión adicional de sus esfuerzos o que una supervisión menos rigurosa es adecuada.

Estos ejemplos de empresas que han sufrido filtraciones de datos de terceros demuestran que cualquier tipo de organización o sector puede verse afectado: SolarWinds AT&T, Chick-fil-A, LinkedIn, T-Mobile, Uber, Okta y Dollar Tree.[2]

Los servicios tecnológicos o relacionados que prestan terceros pueden incluir plataformas de alojamiento web y software como servicio (SaaS), centros de datos subcontratados o servicios de seguridad de redes. Aunque el proveedor asume la responsabilidad de los servicios que ofrece, las organizaciones que los utilizan deben asegurarse de que disponen de los controles y procesos de gestión de riesgos adecuados para comprobar que el tercero cumple sus obligaciones. "No puedes basar la seguridad de tu organización en la esperanza de que el tercero haga su trabajo", afirma Pelletier.

Los auditores internos deben considerar si su organización ha evaluado adecuadamente al tercero y sus riesgos asociados. La auditoría interna no puede llevar a cabo esta evaluación, pero debe considerar cómo la organización está supervisando y gestionando su relación y los riesgos relacionados y verificando que el tercero tiene y sigue los controles adecuados. Pelletier recomendó incluir una cláusula de derecho de auditoría en el contrato con el proveedor para que la auditoría interna pueda examinar los procesos y controles del proveedor cuando sea necesario, incluso después de un incumplimiento.

Gobernanza de datos

Las organizaciones recopilan volúmenes de datos cada vez mayores y los utilizan para tecnologías emergentes como la inteligencia artificial. Los datos pueden representar un riesgo crítico para las organizaciones debido a la importancia de mantener su privacidad. Además, si la dirección va a tomar decisiones empresariales clave basadas en los datos

[1] "SecurityScorecard Research Shows 98% of Organizations Globally Have Relationships With At Least One Breached Third-Party," SecurityScorecard press release based on a study by SecurityScorecard and The Cyentia Institute, February 1, 2022.
[2] "Top Third-Party Data Breaches in 2023," FortifyData, updated December 4, 2023.

disponibles, la organización debe confiar en la integridad de los datos y asegurarse de que son completos, precisos y fiables. Esto incluye conocer la fiabilidad de la fuente de datos, especialmente cuando se trabaja con IA generativa.

Las organizaciones tendrán que garantizar que los datos no son vulnerables a la piratería informática u otros usos indebidos. "Las organizaciones necesitan evaluar cómo se procesan y almacenan los datos", dijo Pelletier, así como asegurarse de que se han cumplido los requisitos legales o reglamentarios específicos, como los relacionados con la privacidad de la información. Si la organización ha dado garantías a sus clientes o socios comerciales sobre cómo se utilizarán sus datos, tendrá que asegurarse de que cumple su compromiso. Aunque la dirección es responsable del gobierno de los datos, la auditoría interna puede ofrecer garantías de que los controles del gobierno de los datos son suficientes.

Según la Comisión Europea, los datos deben almacenarse el menor tiempo posible. No sólo es costoso el almacenamiento, sino que, en caso de violación, los piratas informáticos tienen más datos a los que acceder. Las empresas deben establecer plazos adecuados para la revisión o eliminación de los datos, teniendo en cuenta cualquier requisito empresarial, reglamentario o legislativo que exija periodos de conservación más largos para algunos materiales. Como ejemplo, en virtud de los principios del Reglamento General de Protección de Datos de la Comisión Europea, la Comisión señala una situación en la que una empresa conserva CV de solicitantes de empleo durante 20 años, sin tomar medidas para actualizarlos.[3] Es evidente que estos datos quedarán obsoletos al cabo de poco tiempo en muchos casos, dada la rápida rotación en muchos puestos de trabajo o industrias. La persona puede perder una oportunidad de empleo y la empresa puede perder personas con talento si confía en este conjunto de información obsoleta a la hora de buscar trabajadores para futuras vacantes, o los datos personales de los solicitantes pueden ser robados si la organización es hackeada".

Algunas de las otras áreas tecnológicas en las que la garantía de auditoría interna puede identificar el fracaso de una organización a la hora de implementar la supervisión o las protecciones adecuadas incluyen:

- **Controles de acceso.** La auditoría interna puede examinar si se realizan revisiones de acceso de usuarios para garantizar que sólo los usuarios legítimos tienen acceso al funcionamiento interno de la tecnología de la organización. Entre otras cosas, las revisiones pueden identificar si un antiguo empleado o miembro de un departamento tiene acceso no autorizado a aplicaciones o infraestructuras, según el ISACA Journal. "Esta vulnerabilidad puede ser explotada, dando lugar a pérdidas financieras y/o de reputación para la empresa", señaló.[4]
- **Ciberseguridad.** "Los parches de seguridad, las contraseñas seguras, la gestión de activos y la formación en seguridad de los empleados contribuyen en gran medida a la seguridad en Internet", según un artículo de Forbes.[5]
- **Shadow IT.** Este término se refiere a situaciones en las que los empleados compran e implementan tecnología sin el conocimiento o la autorización del departamento de TI. Esta práctica está creciendo con el trabajo a distancia y el uso cada vez mayor de dispositivos personales en el trabajo. Los riesgos incluyen no estar bajo la supervisión del equipo de TI o no seguir los protocolos de ciberseguridad y privacidad de la organización y otras directrices.
- **Riesgos relacionados con la IA generativa y otras tecnologías emergentes.** El peligro de que los empleados puedan cargar datos corporativos, de clientes o personales en un sistema público de IA generativa es una preocupación importante. (Marco de auditoría de la IA del Instituto de Auditores Internos. [6] ayuda a los auditores internos a comprender los riesgos y determinar las mejores prácticas de IA y los controles internos).
- **Consideraciones culturales.** Los auditores internos pueden considerar si la falta de compromiso de los empleados o una comunicación deficiente de las directrices o salvaguardias tecnológicas constituyen una amenaza.

[3] "For how long can data be kept and is it necessary to update it?" European Commission.
[4] "Effective User Access Reviews," Sundaresan Ramaseshan, *ISACA Journal*, August 21, 2019.
[5] "16 Tech-Related Risk Factors Company Executives Often Overlook," *Forbes*, December 21, 2022.
[6] The Institute of Internal Auditors' AI Auditing Framework.

- **El impacto de la legislación o reglamentación relacionada con la tecnología.** Las organizaciones tendrán que supervisar las necesidades de cumplimiento relacionadas con las nuevas leyes y normas promulgadas en respuesta a los importantes cambios que las tecnologías emergentes pueden suponer para las empresas y la sociedad.

El valor de los esfuerzos coordinados

Alinearse con profesionales de riesgos de la segunda línea

La auditoría interna puede contribuir a coordinar la gestión del riesgo tecnológico

Uno de los inconvenientes de la omnipresencia y el impacto de la tecnología es el riesgo de que que algo se pase por alto al intentar comprender plenamente y ofrecer garantías en este ámbito. "Como hay tanto que cubrir, habrá lagunas", dijo Pelletier. Habida cuenta de los numerosos riesgos existentes, para mejorar su eficacia como proveedor de garantías sobre la adopción y el uso de la tecnología, la auditoría interna querrá obtener la mejor cobertura posible de las áreas de alto riesgo con los recursos disponibles.

Para mejorar esos recursos, la función de auditoría interna tiene la oportunidad de alinearse con las funciones de aseguramiento de segunda línea, como la seguridad de la información, los controles internos, la gestión de riesgos y el cumplimiento, según Pelletier. Para proporcionar a la alta dirección y al consejo un mayor grado de seguridad en la identificación de los riesgos, la auditoría interna puede coordinar sus actividades con estas funciones para obtener una visión holística de cómo se gestiona el aseguramiento tecnológico -y los riesgos tecnológicos clave- en toda la organización.

Aunque la auditoría interna debe permanecer independiente de estas funciones de segunda línea, la coordinación con ellas puede ayudar a la auditoría interna a determinar qué riesgos ya están cubiertos y en qué grado. "La auditoría interna no debe funcionar como un silo", afirma Pelletier. Al minimizar la duplicación de esfuerzos, la alineación permite a la auditoría interna centrar sus propios recursos en los riesgos más importantes. Como parte del esfuerzo, la auditoría interna puede evaluar el trabajo que las funciones de segunda línea están haciendo en relación con la garantía tecnológica.

Esta alineación también puede ayudar a minimizar la "fatiga de aseguramiento", que se produce cuando numerosas funciones solicitan a los directores de departamento informes sobre los mismos datos o realizan revisiones similares. Esto

La tecnología es lo más importante para los auditores internos

La tecnología fue uno de los temas centrales del Pulso Norteamericano de la Auditoría Interna 2023 del IIA.[7], que recoge valiosa información de referencia de los responsables de auditoría interna sobre riesgos, planes de auditoría, presupuestos, personal y otros temas candentes.

Por ejemplo, cuando se preguntó a los directores de auditoría cómo gastarían el dinero del presupuesto adicional si lo tuvieran, la segunda opción más común fue la tecnología. (El aumento del personal interno ocupaba el primer lugar).

Aunque las revisiones del cumplimiento y las operaciones son prioridades tradicionales, los auditores internos también dedican mucho tiempo y esfuerzo a temas relacionados con la tecnología. En la encuesta Pulse, los encuestados afirmaron que el 10% de sus planes de auditoría se centraban en la ciberseguridad y el 9% en TI en general. El total del 19% era superior a la cantidad media de planes de auditoría dedicados a la información financiera (incluido el ICFR), las operaciones y el cumplimiento/regulación (excluido el ICFR). Cada uno de ellos fue objeto del 15% de los planes de auditoría.

Por último, cuando se pidió a los encuestados que eligieran los problemas que planteaban riesgos elevados o muy elevados para sus organizaciones, las tres primeras opciones estaban relacionadas con la tecnología:

- Ciberseguridad, que fue elegida por un rotundo 78%.
- TI en general, en 57%.
- Las relaciones con terceros, que suelen utilizarse para los

[7] 2023 North American Pulse of Internal Audit, The Institute of Internal Auditors, March 2023.

puede evitarse si la auditoría interna y las funciones de segunda línea colaboran para recopilar la información básica que necesitan.

La auditoría interna puede asumir un papel de liderazgo en la coordinación de esta alineación en torno a las actividades de aseguramiento en toda la organización y hacer el mejor uso de las actividades existentes, dijo Pelletier. Para empezar, los auditores internos pueden impulsar una mayor coherencia en los esfuerzos de garantía tecnológica determinando si la gestión de riesgos, el cumplimiento, la auditoría interna y otras funciones tienen cada una sus propios sistemas de evaluación y calificación del riesgo. En las discusiones con la junta directiva y la gerencia, estas inconsistencias entre las funciones pueden presentar una imagen confusa o tal vez aparentemente incompleta. La auditoría interna puede recomendar y dirigir un esfuerzo coordinado utilizando una taxonomía de riesgo común. Las comunicaciones sobre riesgos al consejo y a la alta dirección serán más comprensibles si la auditoría interna y las funciones de segunda línea hablan el mismo idioma. Los resultados o evaluaciones de todas estas funciones no tienen por qué coincidir, pero los términos y enfoques que utilicen deben ser coherentes.

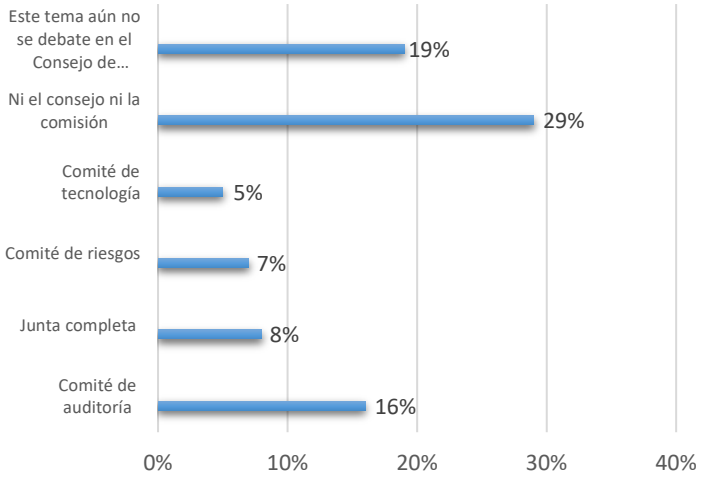
Atentos a la IA

Con muchas empresas todavía lidiando con su uso de la IA y la IA generativa, los auditores internos tienen la oportunidad de impulsar una mejor supervisión de las tecnologías emergentes y el uso que sus organizaciones hacen de ellas.

En una encuesta [8] por Deloitte y la Sociedad para el Gobierno Corporativo de grandes y medianas empresas realizado en 2023, solo el 13% tenía un marco formalizado de supervisión de la IA. Solo el 9% había revisado las políticas corporativas relacionadas con la ciberseguridad, la gestión de riesgos, la conservación de registros y otras para abordar el uso de la IA. Sin embargo, la Asociación Nacional de Directores Corporativos señaló que un año antes, el 94% de las empresas encuestadas afirmaron que la IA era fundamental para el éxito a corto plazo de su empresa.[9]

A pesar de la importancia de la IA, parece que los consejos de administración aún no se han puesto manos a la obra. La encuesta reveló que el 48% de los consejos de administración encuestados o bien aún no estaban considerando la IA o bien no habían asignado responsabilidades al respecto (véase el gráfico). Entre los que habían asignado responsabilidad a la IA, lo más probable era que estuviera bajo la supervisión del comité de auditoría, que suele ser el grupo al que informa el director ejecutivo de auditoría. La auditoría interna puede añadir un valor considerable ayudando a las organizaciones a reconocer y abordar la desconexión entre la importancia de la IA y su propia respuesta a la misma.

¿Quién es el principal responsable de la IA en el consejo de administración de



Fuente: *Deloitte and Society for Corporate Governance Board Practices Quarterly: Future of tech: Artificial intelligence (AI),* Agosto 2023.
Nota: Respuestas "otros/no sé" no incluidas en el gráfico.

[8] *"Deloitte and Society for Corporate Governance Board Practices Quarterly: Future of tech: Artificial intelligence (AI)."* August 2023.
[9] "Artificial Intelligence: An Emerging Oversight Responsibility for Audit Committees?" Brian Cassidy, Ryan Hittner, and Krista Parsons, NACD 2024 Governance Outlook.

Conclusión

La garantía tecnológica que identifica riesgos y obstáculos ya está bien integrada en el papel de la auditoría interna. Al tiempo que se mantiene el enfoque en algunas de las mayores vulnerabilidades relacionadas con la tecnología, la auditoría interna también puede promover una mejor coordinación de los esfuerzos para garantizar una imagen más completa y precisa para los gestores de riesgos y las partes interesadas. Los pasos descritos en este informe pueden ayudar a garantizar que el enfoque general de la organización sobre el riesgo tecnológico y el plan de auditoría aborden adecuadamente los riesgos tecnológicos potenciales.

Parte 2: Estar al tanto de la adopción de tecnología por parte de la organización

Sobre los Expertos

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, es director sénior de producto en TeamMate Audit Solutions, donde trabaja para mejorar continuamente la productividad de las auditorías al tiempo que ofrece perspectivas estratégicas a través de la mejor solución de su clase de TeamMate. Cuenta con más de 20 años de experiencia en auditoría interna tanto en el sector público como en el privado.

Anteriormente, Jim ocupó diversos cargos directivos en el Instituto de Auditores Internos, fue auditor municipal de la ciudad de Palo Alto (California) y jefe de auditorías del condado de San Diego (California). Su amplia experiencia en auditoría interna incluye puestos en el Sistema Universitario Estatal de California, PETCO Animal Supplies, Inc. State Street Corporation y General Electric.

Dennis Wong, CIA, CFSA

Dennis Wong, CIA, CFSA, es director general de un banco internacional con sede en Londres. Es un experimentado profesional de la auditoría y los riesgos con más de 20 años de experiencia en banca internacional y mercados de capitales. Su pasión es liderar e impulsar cambios a través de la reingeniería de procesos y la innovación tecnológica. Trabaja como voluntario en la sección de Nueva York del IIA y forma parte del Comité de Desarrollo de Exámenes.

Introducción

La tecnología se ha convertido en el alma de las organizaciones, una herramienta vital utilizada regularmente en prácticamente todas las funciones. Pero mientras que el 60% de los líderes empresariales y de riesgos ven una nueva herramienta tecnológica, la IA generativa (GenAI), como una oportunidad, el 57% dice que la preparación para las inversiones en nuevas tecnologías es el mayor desencadenante para revisar el panorama de riesgos, según la Encuesta Global de Riesgos 2023 de PwC.[10]

La tecnología ofrece nuevas ventajas, pero la dependencia de ella también conlleva amenazas, unas amenazas que van en aumento a medida que el uso de la tecnología se hace más crítico y omnipresente. Entre ellas se encuentran los riesgos relacionados con las formas en que se adopta la tecnología. La auditoría interna puede ayudar a las organizaciones a determinar y llevar a cabo las mejores estrategias de implementación para minimizar el riesgo y aumentar el valor de las nuevas tecnologías. Este informe analiza los pasos que la auditoría interna puede dar para añadir valor a este esfuerzo.

[10] "Cyber and Digital Technology Risks Are a Key Concern for Businesses and Risk Leaders, Even as 60% See GenAI as an Opportunity: PwC 2023 Global Risk Survey," PwC press release, November 20, 2023.

Desarrollar un nuevo marco de gobernanza

¿Cómo encajan las nuevas tecnologías?

La auditoría interna puede ayudar a orientar la adopción de tecnología

Las nuevas tecnologías siempre plantean nuevos riesgos. Aunque la GenAI, por ejemplo, ha inspirado una gran cantidad de usos innovadores para esta tecnología transformadora, también conlleva nuevos peligros en áreas que incluyen la privacidad, la parcialidad incorporada y la transparencia y exactitud de la información recibida. Al mismo tiempo, pueden surgir riesgos a medida que las nuevas tecnologías impulsan cambios en las operaciones empresariales que exponen a una organización a nuevos riesgos operativos.

Por estas razones, a la hora de adoptar nuevas tecnologías, las organizaciones deben desarrollar un sólido marco de gobernanza de proyectos que tenga en cuenta cómo encajan las nuevas herramientas en el negocio, cómo se alinean con las estrategias corporativas y cómo ayudan a alcanzar los objetivos corporativos, afirma Dennis Wong, CIA, CFSA, un experimentado profesional de auditoría y riesgos con más de 20 años de experiencia en banca internacional y mercados de capitales. De hecho, entre las empresas designadas como "pioneras del riesgo" en la encuesta de PwC, el 73% disponía de una estrategia y una hoja de ruta tecnológica para toda la empresa, frente al 57% de las organizaciones menos avanzadas. El marco debe incluir una amplia consideración del riesgo, incluida una evaluación exhaustiva del riesgo y controles que puedan hacer frente a las amenazas que plantean los nuevos riesgos, dijo Wong.

La auditoría interna puede ofrecer garantías sobre la gobernanza del proyecto y su funcionamiento, así como asesorar sobre la adopción de tecnología en general. Al principio, la auditoría interna puede llevar a cabo una revisión previa a la implantación que considere la idoneidad de la tecnología, así como los riesgos relacionados y los cambios necesarios en los controles. Una vez implantadas las nuevas herramientas, la auditoría interna también puede proporcionar información sobre cómo está funcionando la adopción de la tecnología y el impacto que las nuevas herramientas están teniendo en toda la organización, según Wong. Tras la implantación, la auditoría interna puede opinar sobre si la tecnología está funcionando como se preveía y, en caso contrario, por qué no, y si se han logrado los beneficios esperados.

La auditoría interna también puede detectar los obstáculos que dificultan la adopción. Las empresas que están muy compartimentadas pueden estar sujetas al pensamiento de silo, en el que los profesionales de diferentes funciones no son conscientes de lo que ocurre en otras áreas. Un área puede no saber que otro grupo está explorando la misma tecnología, pero ha descubierto usos diferentes para ella, o que una tercera función se ha enfrentado a algunos fracasos con la tecnología, pero ha aprendido valiosas lecciones. “Eso podría crear bifurcaciones cuando lo que se busca son sinergias", según Wong. Como la auditoría interna tiene una visión holística de la organización, está en una posición única para romper esos compartimentos y ofrecer una visión integral que evite la duplicación de esfuerzos. Debido a su conocimiento institucional, la auditoría interna puede aportar una nueva perspectiva que puede conducir a un uso más valioso de la tecnología,” dijo. También puede ofrecer garantías de que los controles operativos funcionan adecuadamente y garantizan un uso seguro de la tecnología. Dado que el dinero para inversiones es siempre escaso, las organizaciones valorarán el asesoramiento sobre si sus gastos en tecnología se están aprovechando al máximo, dijo Wong.

Las organizaciones tendrán que abordar la interrelación entre los riesgos estratégicos y operativos y la tecnología subyacente. "Uno afecta al otro", afirma Wong. La nueva tecnología cambia el funcionamiento de la organización, lo que conlleva nuevos riesgos. Eso, a su vez, puede impulsar cambios en las operaciones que pueden dar lugar a riesgos

adicionales. La clave está en comprender claramente los objetivos de la organización, cómo se ven afectados o conllevan nuevos riesgos, y qué controles pueden resolver estos problemas.

Las organizaciones también se beneficiarán de una sólida cultura del riesgo, dados los cambios que trae consigo la nueva tecnología. Aunque la organización tenga una mentalidad y un marco de control sólidos, seguirá dependiendo de las personas para aplicar los controles o tomar las medidas adecuadas en su ausencia, señaló Wong, por lo que es fundamental una disciplina de riesgo sólida y una comprensión adecuada del riesgo de las nuevas tecnologías. La cultura de la empresa debe identificar y comunicar las amenazas potenciales de las nuevas herramientas y las expectativas corporativas para su uso, de modo que estén claras para todos.

Considerar Pasos Medidos

Encontrar el equilibrio entre velocidad y seguridad

Asesoramiento sobre cuándo adoptar nuevas tecnologías

Cuando se introduce una nueva tecnología, suele ser urgente implantarla, ilustrado más recientemente por la prisa por desplegar GenAI. Debido a los riesgos potenciales asociados a las nuevas herramientas, "las organizaciones tienen que encontrar el equilibrio adecuado entre velocidad y seguridad", dijo Wong. Señaló el ejemplo de los automóviles, que no tenían cinturones de seguridad cuando se introdujeron por primera vez, pero que fueron añadiendo más y más características de seguridad a lo largo de los años a medida que los coches empezaban a moverse más rápido. Dado el ritmo actual de cambio de la tecnología y la complejidad de los sistemas implicados, una auditoría interna puede ayudar a examinar si la dirección ha implantado las medidas de seguridad o los controles adecuados. "El riesgo, se identifique o no, empieza el primer día", afirma Wong. "Puede que no cristalice en una pérdida o amenaza inmediata, pero una vez que empiezas a utilizar una tecnología, ya estás expuesto al riesgo."

Por ejemplo, GenAI es una herramienta sofisticada con capas de complejidad; es fácil para los malos actores explotarla con fines maliciosos. Además, un personal que no haya recibido la formación adecuada sobre los riesgos de GenAI puede cargar involuntariamente datos confidenciales o sensibles, que podrían incorporarse a la formación del programa y a los que podrían acceder personas ajenas.

Las organizaciones deben plantearse si ser las primeras en llegar al mercado y afrontar riesgos de fuentes inesperadas y posibles daños empresariales o de reputación, o si deben adoptar una estrategia de seguidor rápido para aprender de las experiencias y los errores de los demás.

Entender la deuda técnica

Es posible que la infraestructura, el personal y la cultura no sean capaces de manejar la última tecnología.

Identificación de la deuda tecnológica y medidas para corregirla

Las organizaciones también tendrán que determinar si sus actuales infraestructuras puedan manejar las nuevas herramientas tecnológicas. Cuando se adopta una tecnología, las presiones de tiempo, las consideraciones de coste u otros obstáculos obligan a menudo a las organizaciones a recortar gastos para cumplir un plazo, u otros retos pueden hacer que no alcancen una implantación óptima. Esta deuda técnica puede acumularse con el tiempo si la organización no actualiza a nuevas versiones de software o nuevo hardware, no aplica parches o no toma otras medidas clave de mantenimiento, dijo Jim Pelletier, CIA, CGAP, director senior de producto de TeamMate Audit Solutions. A medida que la organización adopta constantemente nuevas soluciones para mantener el sistema en funcionamiento, su agilidad técnica se va quedando atrás.

La deuda técnica puede impedir que la organización aproveche al máximo el software existente o incluso imposibilitar la adopción efectiva de nuevas tecnologías, explica Pelletier. Es posible que el equipo informático no comunique bien el problema porque lo desconoce, es reacio a hablar de los fallos del sistema o considera que la tecnología es demasiado compleja para explicársela a quienes no son profesionales de la tecnología.

Preguntas sobre nuevas tecnologías

A la hora de ofrecer garantías o asesoramiento, algunas de las preguntas que puede plantear la auditoría interna son las siguientes:

- ¿Qué impacto tendrá la nueva tecnología en la organización y sus procesos empresariales, incluidos riesgos, beneficios y nuevas oportunidades?
- ¿Cómo encaja la tecnología en la gestión del riesgo empresarial de la organización y en los enfoques de gobernanza, riesgo y cumplimiento?
- ¿Cómo debe integrarse la tecnología con los controles existentes? ¿Se ha evaluado el impacto en los controles internos? En caso afirmativo, ¿qué cambios deberían introducirse en los controles y procesos? ¿Debería la auditoría interna trabajar con cada unidad de negocio para reevaluar sus riesgos y controles y prepararse para documentar los nuevos riesgos y controles?
- ¿Necesitamos actualizar la tecnología, cambiar los procesos empresariales o mejorar la cualificación de nuestro personal?
- ¿Qué nuevos riesgos introduce, incluidas las amenazas a la privacidad, los datos de los clientes, la información privilegiada y otros?
- ¿Dónde se utiliza el nuevo sistema y quién lo utiliza?
- ¿Qué ocurre con los datos que recoge o produce la tecnología? ¿Dónde se almacenan y cómo se protegen?
- ¿Compartirá ahora la organización datos que no debería o se expondrá a nuevos riesgos para la privacidad de los

Como resultado, los auditores internos pueden no ser conscientes de esta deuda técnica o de su impacto en la capacidad de la organización para adoptar nuevas tecnologías.

Aunque la auditoría interna no necesita la misma experiencia que el equipo de tecnología de la organización, puede abordar el problema de la deuda técnica tomando medidas para garantizar que su personal mantiene las habilidades suficientes para mantener diálogos productivos con el equipo de TI que puedan revelar el estado actual de los sistemas de la organización, dijo Pelletier. Armados con este conocimiento, los miembros del equipo de auditoría interna pueden mantener conversaciones fructíferas que respeten el tiempo y la experiencia de los miembros del equipo de TI.

En otros casos, aunque la infraestructura tecnológica de una organización sea adecuada, la tecnología puede adelantarse a la empresa y a su personal. Esto puede ocurrir cuando las organizaciones modernizan su tecnología sin actualizar su personal o sus procesos empresariales. Puede que la empresa esté implantando la tecnología para mejorar la eficiencia, pero no se toma el tiempo necesario para alinear y comprender cómo se verán afectados los procesos o cómo tendrán que cambiar. "La gente no sabe cómo utilizarla, lo que supone una pérdida de tiempo, energía y dinero", afirma Pelletier. "Se pierde la oportunidad de hacer mejoras significativas". Una vez más, la auditoría interna cuenta con los conocimientos institucionales necesarios para formular las preguntas adecuadas que garanticen que la tecnología y los objetivos y activos de la empresa se corresponden por igual.

Por último, a medida que avanza la tecnología, puede resultar fácil olvidar el valor del toque humano, pero la revisión y evaluación humanas seguirán siendo fundamentales para el proceso, señaló Wong. Una herramienta como GenAI no solo comete a veces errores o se inventa cosas, sino que, si se utiliza en interacciones con clientes u otras personas, puede pasar por alto señales que una persona habría entendido o dar respuestas inviables que una persona familiarizada con el cliente habría sabido que eran inapropiadas.

Algunas limitaciones de GenAI

La GenAI fue recibida con un entusiasmo desenfrenado cuando se presentó por primera vez, pero sus deficiencias, como se analiza en este informe, han suscitado preocupación. Puede ser una herramienta valiosa para abordar la adopción de tecnología en una organización, si se utiliza adecuadamente. Jim Pelletier identifica dos opciones para los auditores internos que deseen mejorar el uso de GenAI.

- En algunos casos, la GenAI inventa respuestas, o alucina, si no puede responder a una consulta, o comete errores porque sólo conoce aquello para lo que ha sido entrenada. Para solucionar este problema, la Generación Mejorada por Recuperación (RAG) es una técnica que pone a disposición datos precisos y oportunos para aumentar lo que hay en un sistema GenAI. La RAG optimiza los resultados de grandes modelos lingüísticos, como GenAI, consultando una base de conocimientos autorizada fuera de las fuentes de datos de entrenamiento de GenAI antes de generar una respuesta. Y aunque las fuentes de GenAI no han sido transparentes, RAG permite identificar los materiales de origen
- Obtener los mejores resultados de GenAI depende en parte de dar las indicaciones correctas, conocidas como instrucciones. Las instrucciones deben especificar detalles como la longitud de la respuesta, el público al que va dirigida si se va a compartir con otras personas, el estilo y el tono. Pelletier ofrece un ejemplo:

  Usted es un director de auditoría interna con experiencia en la gestión de riesgos tecnológicos en el sector de los servicios financieros. Evalúa los riesgos tecnológicos en función de su impacto en las operaciones empresariales y de la probabilidad de que se produzcan.

  - En formato de tabla, identifique los 10 principales riesgos relacionados con la adopción de nuevas tecnologías en un gran banco.
  - Incluya columnas para Nombre del riesgo, Descripción del riesgo y Justificación, describiendo por qué el riesgo es de máxima prioridad.
  - Ordene las filas de la tabla de mayor a menor riesgo.

Conclusión

Aunque la adopción de nuevas tecnologías puede entrañar riesgos, también es importante recordar los peligros de no mantenerse al día sobre las nuevas herramientas. Entre las muchas desventajas de hacerlo se incluyen:

- Perder las ventajas que ofrecen las nuevas tecnologías
- No poder seguir el ritmo de los competidores por las ventajas que obtienen de la transformación digital.
- Perder la oportunidad de mejorar la eficiencia y la productividad o no innovar en nuevos productos y servicios..
- Perder clientes potenciales o existentes, socios comerciales valiosos o empleados con talento que prefieren trabajar con organizaciones más avanzadas tecnológicamente.

“La tecnología es la base de todo lo que hacemos cada día", afirma Pelletier. La auditoría interna puede contribuir a garantizar que las nuevas herramientas tengan el máximo impacto positivo.

Parte 3: El reto del talento tecnológico de la auditoría interna

Sobre los expertos

Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, es director sénior de productos de TeamMate Audit Solutions, donde trabaja para mejorar continuamente la productividad de las auditorías al tiempo que proporciona información estratégica a través de la mejor solución de TeamMate. Cuenta con más de 20 años de experiencia en auditoría interna, tanto en el sector público como en el privado.

Anteriormente, Jim ocupó diversos cargos directivos en el Instituto de Auditores Internos, fue auditor municipal de la ciudad de Palo Alto (California) y jefe de auditorías del condado de San Diego (California). Su amplia experiencia en auditoría interna incluye puestos en el Sistema Universitario Estatal de California, PETCO Animal Supplies, Inc. State Street Corporation y General Electric.

Dennis Wong, CIA, CFSA

Dennis Wong, CIA, CFSA, es director general de un banco internacional con sede en Londres. Es un experimentado profesional de la auditoría y los riesgos con más de 20 años de experiencia en banca internacional y mercados de capitales. Su pasión es liderar e impulsar cambios a través de la reingeniería de procesos y la innovación tecnológica. Trabaja como voluntario en la sección de Nueva York del IIA y forma parte del Comité de Desarrollo de Exámenes.

Nisha Nair, CIA, FCCA, UAECA, CFE, ACMA, CGMA

Nisha Nair trabaja como especialista en auditoría interna para la Autoridad Federal de Regulación Nuclear de los Emiratos Árabes Unidos. Ha acumulado más de 10 años de experiencia como profesional del asesoramiento sobre riesgos financieros y empresariales, lo que incluye su trabajo en la práctica de consultoría de riesgos de una consultora "Big 4". Es miembro de varios organismos de cualificación profesional y le apasiona promover y liberar el verdadero valor de la profesión de auditoría interna. Además, es experta en la materia en el Grupo de Conocimiento Profesional Global para IIA Global, con conocimientos que abarcan diversos temas relacionados con la auditoría interna, incluida la gestión de riesgos, análisis de datos, gobernanza, gestión del riesgo de fraude, ética y auditoría externa.

Introducción

El punto débil de la auditoría interna

Según el 2024 North American Pulse of Internal Audit, a ciberseguridad y la TI fueron seleccionadas por los líderes de auditoría interna como las dos áreas de mayor riesgo en sus organizaciones, con un 78% y un 58% de los encuestados respectivamente calificándolas como de riesgo alto o muy alto. Esto no debería sorprender; de hecho, la tecnología ha dominado el panorama del riesgo durante los últimos años. Sin embargo, año tras año se hace más evidente que la auditoría interna se enfrenta a serios retos en este ámbito que no harán más que empeorar si no se abordan.

Los esfuerzos en ciberseguridad y TI combinados representan casi el 20% de los planes de auditoría, según los encuestados de Pulse, que son principalmente líderes de auditoría norteamericanos. Juntas suponen el porcentaje más alto de cualquier otra área de riesgo, pero los datos de Pulse también indican que tanto la ciberseguridad y la seguridad de los datos como las TI fueron las áreas más subcontratadas o co-contratadas. Además, aunque aproximadamente 2 de cada 10 encuestados indican que la tecnología sería la principal prioridad, casi la mitad de las funciones de auditoría dan prioridad al aumento del personal interno. El 29% de los encuestados de Pulse citaron las expectativas de remuneración como el reto más importante, seguido de un 17% que afirma que los candidatos carecen de las competencias necesarias.

En conjunto, estas conclusiones dibujan un panorama que muestra que la propia auditoría interna, aunque aborda los riesgos tecnológicos en la medida de sus posibilidades a través de la externalización y la subcontratación, en general no se encuentra en una situación ideal para incorporar las competencias tecnológicas internamente. A largo plazo, este enfoque puede tener repercusiones significativas no sólo para la cobertura de riesgos, sino también para la capacidad de las funciones de auditoría de aprovechar la tecnología para mejorar todos los aspectos de su función.

Como última entrega de esta serie de tres partes sobre innovación y tecnología patrocinada por TeamMate, este resumen de conocimientos examina una serie de facetas de lo que podría llamarse el "reto tecnológico" de la auditoría interna, como la lucha por crear equipos expertos en tecnología. También, a través de las aportaciones de expertos seleccionados del sector, se ofrecen algunas mejores prácticas y estrategias que los equipos, independientemente del sector, el presupuesto o el tamaño de la función, pueden utilizar para prestar servicios de aseguramiento y asesoramiento que puedan seguir el ritmo de la acelerada e incesante marcha de la tecnología.

Formación de equipos tecnológicos

Prepárese ahora para un futuro tecnológico

El problema de la financiación

La auditoría interna no está sola en la carrera por adquirir talentos con conocimientos tecnológicos. De hecho, casi todos los departamentos de todas las organizaciones de todos los sectores están experimentando el mismo reto, lo que está creando una feroz competencia para contratar de lo que ya era un grupo de contratación limitado. Tras los despidos masivos en los sectores tecnológicos durante la pandemia del COVID-19, muchos analistas esperaban que aproximadamente los 20.000 trabajadores de la industria tecnológica en busca de empleo saciaran un poco esta necesidad. Sin embargo, como testimonio de la rápida evolución de la tecnología, la brecha entre los puestos necesarios y el talento adecuadamente cualificado se ha ampliado, y el talento disponible para contratar no es barato. Según los datos de Pulse, el 51% de las funciones de auditoría han visto cómo sus presupuestos se mantenían más o menos igual que el año anterior, por lo que está claro que cualquier función de auditoría que quiera meterse en la piscina de la contratación tecnológica tiene un gran reto por delante.

“El tema más recurrente que siempre surge cuando varios responsables de IA hablan de las dificultades para implantar la tecnología es la necesidad de una financiación adecuada", afirma Nisha Nair, especialista en auditoría interna de la Autoridad Federal de Regulación Nuclear de los Emiratos Árabes Unidos. "Esto incluye financiación para herramientas informáticas, financiación para formación tecnológica del personal del departamento de auditoría interna y financiación para contratar los recursos tecnológicos adecuados dentro del equipo. Muy a menudo, cuando se intenta contratar a una persona de un campo concreto, como el sector cibernético, sus expectativas desde el punto de vista del paquete de remuneración van a ser mucho más elevadas que el paquete de remuneración típico de un auditor interno, muchos de los cuales también prefieren trabajar y crecer en su campo de trabajo especializado, que les paga más, en lugar de ser contratados en un puesto de auditoría interna generalista.”

Ante esta dura realidad, para acercarse siquiera a mantener el ritmo del panorama de riesgos impulsado por la tecnología, la auditoría interna ha tenido que ser creativa a la hora de suplir estas carencias de competencias necesarias. "La estrategia de competencias no es única", afirma Dennis Wong, director general y responsable global de auditoría de riesgos de delitos financieros de HSBC. "La combinación adecuada es diferente para cada departamento de auditoría. Se trata de una combinación de crecimiento y mejora de las competencias de forma orgánica, subcontratación con consultoras y, cuando sea posible, contratación externa.”

Cada uno de los elementos de esta triple estrategia es digno de debate:

Contratación externa

Como ya se ha mencionado, dados los niveles presupuestarios actuales y la falta de financiación adicional, la aplicación de esta estrategia podría parecer poco realista e incluso descartarse por completo. Sin embargo, aunque no cabe duda de que se trata de un reto, es posible avanzar en este ámbito, y todo empieza por el comité de auditoría.

Dado que el Consejo de Administración y/o el Comité de Auditoría desempeñan un papel importante en la aprobación del presupuesto anual de auditoría interna, el objetivo de un responsable de auditoría interna debe ser justificar con argumentos empresariales sólidos por qué es necesaria una financiación adicional para la contratación de personal técnico a la luz del despliegue y la innovación tecnológicos. Esto va más allá de citar datos; más bien, el objetivo debe ser "ofrecer una historia convincente" que sea difícil de rechazar, dice Nair. "Los responsables de IA tienen que conseguir que el Comité

de Auditoría y la Alta Dirección acepten la necesidad de talento técnico en el departamento de IA, el valor que aportará a la organización, y explicar la necesidad de un paquete de remuneración adecuado y una carrera profesional para atraer a ese talento al departamento de AI", dice Nair.

“Tenemos que conseguir que el comité de auditoría se implique y hacer que se den cuenta de que ese talento es un nicho, y que el paquete de remuneración que se aplica al equipo de auditoría interna puede no ser suficiente para alguien del ámbito cibernético", afirma.

Esto también podría requerir que el comité de auditoría reconsidere cómo se estructuran los equipos de auditoría interna eficaces para el entorno de riesgo actual. Lo que se exige hoy al personal de auditoría es muy diferente de lo que era hace 15 años. "Mirando el panorama general, tenemos que pensar en cómo tienen que ser nuestros equipos", dice Jim Pelletier, director senior de producto de TeamMate Audit Solutions. "Hoy en día, no se contrata a un auditor interno tradicional, sino a un experto en ciberseguridad, así que tal vez ese sea el papel que hay que tener". Los responsables de auditoría tienen que explicar a sus comités que no pueden ofrecer tarifas de auditoría interna, porque no están contratando a un auditor interno. Puede que ni siquiera tengan la palabra "auditoría" en el título de su puesto.”

Como parte del lanzamiento, un experto en ciberseguridad de este tipo no tiene por qué reservarse explícitamente para la auditoría interna. "Pueden utilizarse allí donde encajen sus aptitudes", afirma Pelletier. "Cuando hago una auditoría de ciberseguridad, la haría de forma exhaustiva, pero puede que no necesite hacerla continuamente, así que puede que sólo necesite conocimientos de ciberseguridad quizá un par de veces al año. Es hora de que la auditoría interna sea creativa. Puede que no necesite incorporar a un especialista en ciberseguridad a mi equipo a tiempo completo, pero si puedo utilizar a un especialista en ciberseguridad que normalmente trabaja en segunda línea como auditor cuando sea necesario, eso es increíblemente valioso y eficiente, siempre que pueda gestionar cualquier preocupación con independencia y objetividad.”

Sin embargo, estas conversaciones no deben terminar en el Comité de Auditoría o el Consejo de Administración, sino que el responsable de auditoría interna debe utilizar su posición como asesor de confianza para comunicar el valor del talento tecnológico cualificado. "Los líderes del departamento de auditoría pueden convertirse en los portadores del cambio", continúa Nair. "Necesitan tener una comunicación orientada a la tecnología con el equipo directivo y facilitar la navegación de toda la organización hacia un futuro más tecnológico". Una comunicación de este tipo en la cúpula directiva, afirma, repercutirá en otros departamentos de la organización. Esto ayudará a crear un entorno que fomente la colaboración para desarrollar o habilitar soluciones tecnológicas que permitan alcanzar un objetivo común. Si la organización se compromete lo suficiente, la financiación llegará inevitablemente.

Igualmente importante en la búsqueda externa de talentos es aprovechar todas las vías para ampliar la reserva, siempre y cuando sea posible. Esto puede lograrse de varias maneras. Por ejemplo, centrarse en las iniciativas de diversidad, equidad e inclusión (DEI) no sólo fomenta la inteligencia cognitiva dentro del departamento y la organización, sino que también hace que las organizaciones sean más atractivas para las generaciones más jóvenes de talentos cualificados. Además, los departamentos que publican puestos vacantes deberían considerar seriamente la posibilidad de ampliar la oferta para incluir opciones de trabajo a distancia. Según Pulse, un asombroso 95% de los líderes de auditoría interna de la generación del milenio (1981-1996) esperan que los niveles de trabajo remoto se mantengan, lo que implica que existe la expectativa de que las futuras contrataciones busquen estas opciones.

Por último, a la hora de contratar, hay que tener en cuenta que la tecnología avanza tan rápidamente que muchas de las competencias que uno podría incluir en la descripción de un puesto podrían quedar obsoletas en cuestión de años o incluso meses. Por lo tanto, los responsables de contratación no deben ser tan rígidos a la hora de marcar las casillas de competencias de los candidatos. La clave no está en lo bien que se conozca una habilidad tecnológica concreta, sino en su capacidad para desarrollar continuamente nuevas habilidades. "No sugerimos que se contrate a una persona para una tecnología concreta, sino a alguien que pueda captar nuevas tecnologías con facilidad", dice Nair. Las funciones de AI necesitan personas adaptables, capaces de absorber nuevos conocimientos como una esponja.”

Estos son los tipos de individuos que más se beneficiarán de los emparejamientos de equipos que les pongan en situación de aprender y tener éxito. "Es muy raro encontrar una persona unicornio que 'singularmente' tenga todo el riesgo, el conocimiento del negocio, la auditoría y las habilidades tecnológicas y de ciencia de datos. No es imposible, pero es raro", dice Wong. "Por lo tanto, la prioridad debería ser realmente la creación del equipo que tenga personas que trabajen juntas colectivamente, como científicos de datos que trabajen junto a auditores internos que puedan aprender y crecer a través del proceso de auditoría."

Subcontratación y externalización para mejorar las cualificaciones

Como se ha mencionado anteriormente, muchas funciones de auditoría están optando por externalizar y subcontratar sus responsabilidades de auditoría informática y cibernética. Obviamente, esta tendencia surge de la necesidad, dados los retos y las limitaciones de la contratación, pero especialmente en áreas tecnológicas como la ciberseguridad, también es una necesidad.

"Internamente, es muy difícil adquirir conocimientos sobre la última y mejor tecnología", afirma Wong. "Hay que salir de la empresa para buscar esos conocimientos. Ahí es donde entran las consultorías y los especialistas."

Sin embargo, cuando se contrata a estas empresas externas, a veces se pasa por alto el impacto que el talento subcontratado puede tener en la función de auditoría más allá de la duración de su contrato.

"Lo que funciona realmente bien es cuando los departamentos de IA recurren a sus proveedores de IA, socios de IA y/o empresas de consultoría existentes para mejorar las competencias de su propio personal de IA departamental, mientras que el talento subcontratado/co-subcontratado ejecuta el trabajo de auditoría prescrito", dice Nair. "Es bueno emparejar a los talentos/socios/consultores externos subcontratados/contratados con el personal interno de auditoría interna para permitir la transferencia de conocimientos mientras se ejecuta el encargo. El aprendizaje en el trabajo resulta sin duda más eficaz."

Pelletier está de acuerdo.

"Si subcontratamos o co-contratamos, está bien, pero ¿estamos mejorando?", pregunta. "¿Integra a sus empleados en los proyectos para que aprendan? ¿Aprovechas el tiempo que tienes para desarrollar un poco más las capacidades internas?

También es una idea útil difundir las competencias tecnológicas básicas de los talentos subcontratados y subcontratados de forma más estructurada. Esto puede hacerse en forma de talleres o sesiones de grupo en las que personas de todos los departamentos puedan ver de primera mano las posibilidades de la tecnología, y luego puedan llevar los nuevos conocimientos a sus respectivas áreas.

Sin embargo, una vez que el equipo está más cualificado o la experiencia se incorpora a tiempo completo, la subcontratación debe formar siempre parte de la estrategia de competencias de una organización. "Una vez que el talento altamente cualificado se incorpora como empleado a tiempo completo, inevitablemente pierde su ventaja", afirma Wong. "En ciberseguridad, por ejemplo, digamos que traes a un hacker de sombrero blanco con los últimos conocimientos tecnológicos para hacer cosas como pruebas de penetración. Pero si deja de ser un 'hacker', ya no estará en la vanguardia de este campo. Por lo tanto, no importa el nivel de habilidad del equipo interno, siempre vas a querer contratar a una empresa externa hasta cierto punto, porque siempre van a conocer las últimas vulnerabilidades."

Incrementando las habilidades desde dentro

Aunque gran parte de los debates sobre tecnología giran en torno a la incorporación de talento, es fundamental no pasar por alto el talento que ya existe en la empresa. A través de relaciones positivas y la colaboración entre auditoría interna, la alta dirección y el equipo de TI, auditoría interna debe trabajar para desarrollar una comprensión clara tanto de las habilidades como de las herramientas que poseen otros departamentos. El análisis de datos o el software de supervisión continua, por ejemplo, pueden tener amplias aplicaciones que podrían encajar perfectamente en las tareas de auditoría con un poco de formación.

“Hay que trabajar con otros equipos y explorar las distintas vías de colaboración, y si la relación es buena, puede que nos digan algo así como: "Vale, tenemos estas herramientas, ¿por qué no las utilizamos para una auditoría interna?", dice Wong.

Esto también es cierto para la alta dirección. Como segunda línea, pueden tener acceso a herramientas de análisis de datos, herramientas de auditoría continua y supervisión continua (CACM) y herramientas que se ocupan de las ISO y los procedimientos, todas las cuales pueden ser útiles en un contexto de auditoría interna.

Por supuesto, la necesidad de mejorar las competencias va mucho más allá de la auditoría interna. Sin duda, el impulso para aumentar las competencias tecnológicas básicas en toda la organización debe ser omnipresente en el entorno actual. Una vez más, aprovechando su papel como portadores del cambio, los líderes de auditoría interna deberían abogar en todas las interacciones de sus departamentos por una formación obligatoria sobre las tendencias y técnicas tecnológicas actuales. "Un enfoque eficaz sería definir el nivel mínimo de conocimientos y habilidades relacionados con la tecnología o los datos, junto con los niveles de progreso/experiencia para cada puesto dentro del marco de competencias de IA", afirma Nair. Tenemos que animar a todos los profesionales de la IA a que reciban la formación mínima necesaria para adquirir al menos los conocimientos informáticos básicos para su puesto de trabajo y progresar a partir de ahí.”

Wong expresa un sentimiento similar. "Hay una necesidad constante de actualización de conocimientos en todas las funciones", afirma. "Es imprescindible para seguir siendo relevante y mantener el ritmo de los mercados. Siempre hay nuevas herramientas y técnicas que hay que conocer.”

Conseguir estas habilidades no siempre tiene por qué implicar aumentar los presupuestos de formación. Muchas de estas habilidades pueden aprenderse individualmente a través de cursos gratuitos en línea o de sesiones de conocimiento interdepartamentales, e idealmente ambas cosas. "Muy a menudo, cuando una persona no técnica lee artículos técnicos en línea, la jerga técnica tiende a desanimarla", dice Nair. Contar con personas en el departamento o la organización que ayuden al personal de IA a comprender la jerga y los conceptos técnicos es muy útil para crear el deseo de explorar las distintas facetas de la tecnología.”

Hay que tener en cuenta, sin embargo, que una vez que se establece un "mínimo", el listón tendrá que elevarse en poco tiempo. Al evaluar estos marcos a través de una auditoría, los auditores internos deben centrarse no sólo en si se están enseñando las habilidades, sino también en ver cómo esas habilidades se aplican de forma continua y eficaz y se desarrollan a medida que crece la base de conocimientos.

“Una estrategia eficaz de mejora de las competencias debe incluir algún tipo de medición de la "aptitud digital"", afirma Nair. "Las medidas de rendimiento de los departamentos no deben limitarse a la implantación de la tecnología, sino que también deben incluir KPI que midan cómo evoluciona continuamente el departamento con respecto al uso de esa tecnología concreta. Por lo tanto, los responsables de auditoría interna deben abogar por mejorar los KPI que indican cómo se están transformando los departamentos en lugar de limitarse a implantar una tecnología concreta. Sin una evolución o transformación continuas, todos corren el riesgo de quedarse estancados.”

Pelletier añade: "La tecnología está integrada en todo lo que hacemos, así que tenemos que abogar constantemente por subir el listón. La tecnología cambia constantemente, así que ya estamos poniéndonos al día. Si no avanzamos, la brecha seguirá creciendo". Como líder de auditoría, su objetivo es gestionar lo amplia o estrecha que usted y su consejo están dispuestos a que sea esa brecha.”

Viva el Rey Datos

La base de todo progreso tecnológico

Encontrar datos de calidad y comprenderlos

El dato es el rey, dice el tópico, y cada día es más cierto. Independientemente de la estrategia utilizada para crear equipos digitales eficaces, ninguna de ellas tendrá ningún tipo de efecto sin acceso a datos de calidad.

“Los datos son imprescindibles para el trabajo de auditoría, especialmente con el uso predominante de controles automatizados y de sistemas", afirma Wong. "Dada la abundancia de datos en la actualidad, las oportunidades de aprovecharlos en auditoría interna son inmensas, siempre que se sepa cómo utilizarlos, lo que hace que la falta de ellos sea aún más problemática.”

Aunque reconoce que la falta de datos es problemática, incluso hoy en día el acceso a datos de calidad no es un hecho. E igualmente preocupante, dice Nair, es cuando los departamentos de IA utilizan su incapacidad percibida para adquirir datos como excusa para no avanzar hacia el despliegue tecnológico dentro de las actividades de IA. Esto no puede ser así. Por el contrario, el viaje para adquirir y aprovechar los datos debe utilizarse como una parte crítica del caso de negocio de la auditoría interna para el avance tecnológico. "Cuando se trata de la integridad de los datos, las funciones de IA no deben limitarse a la mera identificación o categorización de los datos como buenos o malos", afirma. En su lugar, las funciones de IA deben aprovechar esta oportunidad para llamar la atención de la dirección ejecutiva, ofrecer recomendaciones para mejorar la calidad de los datos y poner la pelota en movimiento". Detener el uso de la tecnología en las auditorías por este tipo de preocupaciones puede dar lugar a que las funciones de IA nunca avancen en sus esfuerzos tecnológicos.”

Este no puede ser el caso. Por el contrario, el viaje para adquirir y aprovechar los datos debe utilizarse como una parte fundamental del argumento comercial de la auditoría interna para el avance tecnológico. "Lo que vemos es que no siempre debemos limitarnos a identificar si los datos son buenos o malos", afirma. "En lugar de eso, deberíamos avanzar, destacarlos y utilizarlos como una forma de identificar áreas de mejora, comunicarnos con la dirección y mantener la pelota en movimiento. Porque si nos detenemos en algún punto, corremos el riesgo de estancarnos para siempre.”

Los datos no requieren necesariamente una inversión para su recopilación. Muy a menudo, puede ser sólo cuestión de tener los conocimientos necesarios para aprovechar los datos que ya se tienen a mano. Incluso la información registrada en una hoja de cálculo de Excel puede considerarse datos de calidad en función de la situación. Las claves para desbloquearlos son sencillas: la habilidad adecuada para detectarlos, destacarlos y aprovecharlos, y la cultura adecuada para fomentar el desarrollo de dicha habilidad. Dicho de otro modo, cuando se cultiva y desarrolla el talento, los datos llegan solos.

En el entorno adecuado, los datos ni siquiera tienen que ser perfectamente ideales para considerarse valiosos. "Mi opinión es que tener datos siempre es mejor que no tener ninguno", afirma Wong. "Incluso un conjunto incompleto de datos es mejor que no tener ninguno. Lo que es más importante que la exhaustividad de los datos es tener la mentalidad de aprovechar todas las oportunidades de análisis de datos de las que disponemos. Digamos que le doy 10 dólares, pero se los doy en céntimos. Lo aceptarás porque siguen siendo 10 dólares, aunque sea algo engorroso.”

Sin embargo, la auditoría interna debe hacer algo más que comprender cómo se utilizan los datos. Según Pelletier, el conocimiento de los datos se reduce a responder a cuatro preguntas:

- ¿De dónde procede?

- - ¿Dónde se almacena?
- - ¿Qué se hace con ella?
- - ¿Cómo se elimina?

En la mayoría de los casos, para responder a estas preguntas no se requiere un alto grado de conocimientos técnicos.

“La gobernanza de datos es algo en lo que creo que todos los auditores deberían convertirse en expertos", afirma Pelletier. Algunos aspectos pueden requerir conocimientos técnicos más profundos, pero todos los auditores deben estar equipados para hacer preguntas difíciles y comprender los procesos subyacentes y recurrir a los conocimientos técnicos sólo en las partes que se necesitan.”

Conclusión

La tecnología es una oportunidad, no una pérdida

Por mucho que se hable de los increíbles beneficios que puede aportar la tecnología, también puede generar ansiedad. Es natural considerarla abrumadora, hasta el punto de que uno puede llegar a cuestionarse su propia seguridad laboral. En algún momento, a medida que evolucione la tecnología, ¿habrá lugar para el trabajo humano?

Se trata de una preocupación comprensible, pero derivada de una cultura organizativa equivocada. La tecnología no debe verse como un competidor o una amenaza, sino con entusiasmo, como una oportunidad para lograr más, aportar más valor a la organización e incluso mejorar el día a día de los trabajadores.

“Aunque no es una mayoría, puede que todavía haya personas que crean que la automatización les quitaría el trabajo o que tengan un comportamiento anclado en el mantenimiento de sus métodos fijos de ejecución de auditorías, como hacer aquello con lo que se sienten cómodos, por ejemplo, utilizar las viejas hojas de cálculo", afirma Nair. Los responsables de auditoría interna deben fomentar el debate sobre la necesidad de seguir siendo ágiles en esta era dinámica impulsada por la tecnología, adoptando una mentalidad de aprendizaje y los beneficios potenciales de la tecnología, sobre todo si se presenta como un medio para reducir la carga de trabajo del departamento o aumentar la eficiencia, y no como un medio para sustituir a los auditores.”

La auditoría interna puede y debe ser el mayor defensor de la tecnología en la organización. Es el portador del cambio, el socio, el portador de buenas noticias. A medida que avanza el desafío tecnológico, a las organizaciones les vendrían bien unos cuantos más de esos.

Sobre el IIA

El Instituto de Auditores Internos (IIA) es una asociación profesional internacional sin ánimo de lucro que cuenta con más de 235.000 miembros en todo el mundo y ha concedido más de 190.000 certificaciones de Auditor Interno Certificado (CIA) en todo el mundo. Fundado en 1941, el IIA es reconocido en todo el mundo como el líder de la profesión de auditoría interna en normas, certificaciones, educación, investigación y orientación técnica. Para más información, visite theiia.org.

Sobre Wolters Kluwer TeamMate

Wolters Kluwer TeamMate Audit Management Solutions es una solución experta en auditoría interna y aseguramiento líder en el mundo con más de 25 años dedicados al avance de los auditores corporativos, comerciales y del sector público. A medida que los equipos de auditoría interna evolucionan para ofrecer conocimientos más profundos, una mayor garantía de los riesgos y mejorar la eficiencia, necesitan soluciones específicas y preparadas para el futuro. TeamMate proporciona soluciones expertas en las que confían los auditores internos para aportar valor a sus organizaciones. Para más información, visite www.teammatesolutions.com.

Disclaimer

Copyright

Mayo 2024

Traducción al Español Auspiciada por:

FLAI
Fundación Latinoamericana de Auditores Internos

Traductora: Andrea Correa (servicios contratados), revisor: Roberto Loo, control de calidad

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101