
# GLOBAL PERSPECTIVES & INSIGHTS

*Inovação e Tecnologia*

**PARTE I:** O Papel da Auditoria Interna na Avaliação da Tecnologia

**PARTE II:** Ficando por Dentro da Adoção Tecnológica da Organização

**PARTE III:** O Desafio da Auditoria Interna com Talentos de Tech

Wolters Kluwer

The Institute of Internal Auditors

# Conteúdo

# Parte 1: O Papel da Auditoria Interna na Avaliação da Tecnologia

## Sobre o Especialista

### Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, é gerente de produto sênior da TeamMate Audit Solutions, onde trabalha para melhorar continuamente a produtividade da auditoria e, ao mesmo tempo, oferecer insights estratégicos por meio da solução de ponta da TeamMate. Ele tem mais de 20 anos de experiência em auditoria interna nos setores público e privado.

Anteriormente, Jim ocupou vários cargos de liderança no The Institute of Internal Auditors, atuou como Auditor Municipal da cidade de Palo Alto, CA, e foi Chefe de Auditorias do Condado de San Diego, CA. Sua experiência diversificada em auditoria interna inclui cargos no California State University System, PETCO Animal Supplies, Inc., State Street Corporation e General Electric.

# Introdução

**A tecnologia tornou-se o motivador inquestionável da mudança e da inovação empresarial**. Da transformação digital generalizada à inteligência artificial emergente e em evolução, as novas tecnologias estão abrindo oportunidades – e riscos – como nunca. Para compreender os impactos das novas tecnologias, as organizações contam com a auditoria interna para obter avaliação sobre sua adoção e seu uso da tecnologia. Este *Brief* abordará por que a avaliação da tecnologia deveria ser uma parte rotineira de qualquer auditoria. Abrangerá as principais áreas de vulnerabilidade e discutirá oportunidades para a auditoria interna assumir a liderança em obter consistência e coordenação de forma a proporcionar auditorias tecnológicas mais eficazes.

## Um foco central

Como a tecnologia permeia todos os aspectos dos negócios, é natural que a avaliação da tecnologia já seja um foco central para os auditores internos. "Existe um risco tecnológico subjacente em essencialmente tudo que as organizações fazem", disse Jim Pelletier, CIA, CGAP, gerente sênior de produtos da TeamMate Audit Solutions. Não há mais separação entre operações e tecnologia, porque a tecnologia capacita operações e inúmeras outras funções. Avaliar e garantir controles adequados deve, portanto, incluir qualquer tecnologia relacionada que seja subjacente a um processo. Por exemplo, embora os auditores internos possam ter auditado contas a pagar – ou qualquer outra função – e os seus sistemas separadamente, as funções e os sistemas estão agora completamente interligados, disse Pelletier. "Tudo que você audita envolve algum grau de avaliação da tecnologia."

# Questões a Considerar

## Riscos e Governança de Dados de Terceiros

### Reconhecendo as principais áreas de ameaça

**Devido à prevalência da tecnologia, há muitas questões** a serem examinadas na prestação de avaliação da tecnologia. Esta seção discutirá diversas áreas de alto risco.

### Relacionamentos com Terceiros

A pesquisa mostrou que 98% das organizações do mundo todo têm relacionamentos com pelo menos um fornecedor terceiro que sofreu uma violação nos últimos dois anos. As empresas também podem ser afetadas pelas conexões downstream dos fornecedores. Um total de 50% das organizações têm relacionamentos indiretos com pelo menos 200 fornecedores terceirizados com violações recentes.[1]

A extensa dependência e inter-relação das organizações com terceiros é um risco crítico, especialmente quando ocorre um problema. As relações com terceiros podem ser especialmente vulneráveis, porque muitas organizações assumem incorretamente que um fornecedor está abordando todos os riscos relacionados e que não é necessária qualquer revisão adicional dos seus esforços, ou que uma supervisão menos rigorosa seria adequada.

Estes exemplos de empresas que sofreram violações de dados de terceiros mostram que qualquer tipo de organização ou indústria pode ser afetada:  SolarWinds AT&T, Chick-fil-A, LinkedIn, T-Mobile, Uber, Okta e Dollar Tree.[2]

A tecnologia ou serviços relacionados oferecidos por fornecedores terceirizados podem incluir plataformas de hospedagem na web e software como serviço (SaaS), data centers terceirizados ou serviços de segurança de rede. Embora o fornecedor assuma a responsabilidade pelos serviços que oferece, as organizações que utilizam esses serviços devem ainda garantir que tenham os controles e processos de gerenciamento de riscos adequados para conferir que o terceiro está cumprindo com as suas obrigações. “Você não pode basear a segurança da sua organização na esperança de que o terceiro faça a parte dele”, disse Pelletier.

Os auditores internos deveriam considerar se a sua organização avaliou adequadamente o terceiro e os riscos associados. A auditoria interna pode não realizar esta avaliação, mas deveria considerar como a organização está monitorando e gerindo seu relacionamento e os riscos relacionados e verificando se o terceiro tem e está seguindo os controles adequados. Pelletier recomendou incluir uma cláusula de direito de auditoria no contrato com o fornecedor, para que a auditoria interna possa examinar os processos e controles do fornecedor conforme necessário, inclusive após uma violação.

### Governança de Dados

As organizações estão coletando e alavancando volumes de dados em rápida expansão para o uso com tecnologias emergentes, como a inteligência artificial. Os dados podem representar um risco crítico para as organizações, devido à importância de manter a privacidade dos dados. Além disso, se a liderança tomar decisões importantes de negócios com base nos dados disponíveis, a organização deve ter confiança na integridade dos dados e garantir que sejam completos,

[1] “SecurityScorecard Research Shows 98% of Organizations Globally Have Relationships With At Least One Breached Third-Party,” SecurityScorecard release de imprensa baseado em um estudo feito pela SecurityScorecard e The Cyentia Institute, 1º de fevereiro de 2022.
[2] “Top Third-Party Data Breaches in 2023,” FortifyData, atualizado em 4 de dezembro de 2023.

precisos e confiáveis. Isso inclui compreender a confiabilidade da fonte de dados, especialmente quando se trabalha com IA generativa.

As organizações precisarão garantir que os dados não sejam vulneráveis a hackers ou outros usos indevidos. "As organizações precisam avaliar como os dados são processados e armazenados", disse Pelletier, bem como garantir que requisitos legais ou regulatórios específicos tenham sido cumpridos, como aqueles relacionados à privacidade das informações. Se a organização tiver dado garantias aos clientes ou parceiros de negócios sobre como seus dados serão utilizados, terá que garantir que está cumprindo com seu compromisso. Embora a gestão seja responsável pela governança dos dados, a auditoria interna pode oferecer garantia de que os controles de governança dos dados sejam suficientes.

Os dados deveriam ser armazenados pelo menor tempo possível, de acordo com a Comissão Europeia. O armazenamento é caro e, no caso de uma violação, há mais dados para os hackers acessarem. As empresas deveriam ter cronogramas apropriados sobre quando os dados deveriam ser revisados ou excluídos, tendo em mente quaisquer requisitos comerciais, regulatórios ou legislativos que exigiriam períodos de retenção mais longos para alguns materiais. A título de exemplo, de acordo com os princípios do Regulamento Geral de Proteção de Dados da Comissão Europeia, a comissão refere-se a uma situação em que uma empresa mantém os currículos dos candidatos a emprego durante 20 anos, sem tomar medidas para sua atualização.[3] Em muitos casos, esses dados ficarão claramente obsoletos após um curto período, dada a rápida rotatividade em muitos empregos ou indústrias. A pessoa pode perder uma oportunidade de emprego e a empresa pode perder pessoas talentosas se confiar neste conjunto de informações desatualizadas ao procurar trabalhadores para vagas futuras, ou os dados pessoais dos candidatos podem ser roubados se a organização for hackeada.

Algumas das outras áreas tecnológicas onde a avaliação da auditoria interna pode identificar a falha de uma organização em implementar monitoramento ou proteções adequadas incluem:

- **Controles de acesso.** A auditoria interna pode examinar se são conduzidas revisões dos acessos dos usuários, para garantir que apenas usuários legítimos tenham acesso ao funcionamento interno da tecnologia da organização. Entre outras coisas, as análises podem identificar se um ex-funcionário ou membro do departamento tem acesso não autorizado a aplicações ou infraestrutura, de acordo com o ISACA Journal. "Essa vulnerabilidade pode ser explorada, resultando em perdas financeiras e/ou de reputação para a empresa", afirmou.[4]
- **Cibersegurança.** "Patchs de segurança, senhas fortes, gestão de ativos e treinamento de segurança para os funcionários contribuem muito para manter a segurança online", de acordo com um artigo da Forbes.[5]
- ***Shadow IT* (TI Sombra).** Este termo refere-se a situações em que os funcionários adquirem e implementam tecnologia sem o conhecimento ou autorização do departamento de TI. A prática está crescendo com o trabalho remoto e o uso crescente de dispositivos pessoais no trabalho. Os riscos incluem não ficar sob a supervisão da equipe de TI ou não seguir os protocolos de cibersegurança e privacidade da organização e outras diretrizes.
- **Riscos relacionados com a IA generativa e outras tecnologias emergentes.** O perigo de os funcionários carregarem dados corporativos, de clientes ou dados pessoais para um sistema público de IA generativa é uma preocupação significativa. (O Framework de Auditoria de IA do Institute of Internal Auditors[6] ajuda os auditores internos a compreender os riscos e a determinar as melhores práticas e controles internos de IA.)
- **Considerações culturais.** Os auditores internos podem considerar se a falta de envolvimento dos funcionários ou a má comunicação das diretrizes ou salvaguardas tecnológicas são uma ameaça.
- **O impacto da legislação ou regulamentação relacionada à tecnologia.** As organizações terão que monitorar as necessidades de conformidade relacionadas às novas leis e normas emitidas em resposta às mudanças significativas que as tecnologias emergentes podem significar para os negócios e a sociedade.

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

# O Valor de Esforços Coordenados

## Alinhando-se com os profissionais de risco da segunda linha

### A auditoria interna pode ajudar a coordenar os esforços de gerenciamento do risco da tecnologia

**Uma das desvantagens da presença e do impacto generalizados da tecnologia** é o risco de que algo será esquecido ao tentar compreender completamente e prestar avaliação nesta área. "Como há muito a cobrir, haverá lacunas", disse Pelletier. Dados os muitos riscos envolvidos, para melhorar a sua eficiência no seu papel como prestador de avaliação sobre a adoção e uso da tecnologia, será do interesse da auditoria interna obter a melhor cobertura possível das áreas de alto risco com os recursos disponíveis.

Para melhorar esses recursos, a função de auditoria interna tem a oportunidade de se alinhar com funções de avaliação da segunda linha, como segurança da informação, controles internos, gerenciamento de riscos e conformidade, de acordo com Pelletier. Para proporcionar à alta administração e ao conselho um maior grau de segurança quanto à identificação dos riscos, a auditoria interna pode coordenar suas atividades com estas funções, para obter uma imagem integrada de como a avaliação da tecnologia — e os principais riscos tecnológicos — estão sendo tratados em toda a organização.

Embora a auditoria interna deva permanecer independente destas funções da segunda linha, a coordenação com elas pode ajudar a auditoria interna a determinar quais riscos já estão cobertos e em que grau. "A auditoria interna não deveria operar isolada", disse Pelletier. Ao minimizar a duplicação de esforços, o alinhamento permite que a auditoria interna concentre seus próprios recursos nos riscos mais importantes. Como parte do esforço, a auditoria interna pode avaliar o trabalho que as funções da segunda linha estão realizando quanto à avaliação da tecnologia.

Esse alinhamento também pode ajudar a minimizar a "fadiga de avaliação", que ocorre quando diversas funções solicitam aos gerentes de departamento relatórios sobre os mesmos dados ou realizam revisões semelhantes. Isso pode ser evitado se a auditoria interna e as funções da segunda linha trabalharem em conjunto para coletar as informações essenciais necessárias.

#### Tech é *top of mind* para auditores internos

A tecnologia foi um foco central no *North American Pulse of Internal Audit* de 2023 do IIA[7], que coleta informações valiosas de benchmarking da liderança da auditoria interna sobre riscos, planos de auditoria, orçamentos, equipe e outros tópicos importantes.

Por exemplo, quando se perguntou aos principais executivos de auditoria como gastariam dinheiro adicional do orçamento se o tivessem, a segunda escolha mais comum foi a tecnologia. (O aumento da equipe interna ficou em primeiro lugar.)

Embora as revisões de conformidade e operações sejam prioridades tradicionais, os auditores internos também despendem muito tempo e esforço em tópicos relacionados com a tecnologia. Na pesquisa Pulse, os entrevistados disseram que 10% dos seus planos de auditoria se concentravam na cibersegurança e 9% na TI em geral. O total de 19% foi superior à quantidade média de planos de auditoria dedicados ao reporte financeiro (incluindo ICFR), operações e conformidade/ regulamentação (excluindo ICFR). Cada um deles foi objeto de 15% dos planos de auditoria.

Por fim, quando foi pedido aos participantes que escolhessem quais questões representavam riscos altos ou muito altos para suas organizações, as três principais escolhas foram ligadas à tecnologia:

- Cibersegurança, escolhida por retumbantes 78%.
- TI em geral, com 57%.
- Relacionamentos com terceiros, frequentemente usados para serviços de TI, com 51%.

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

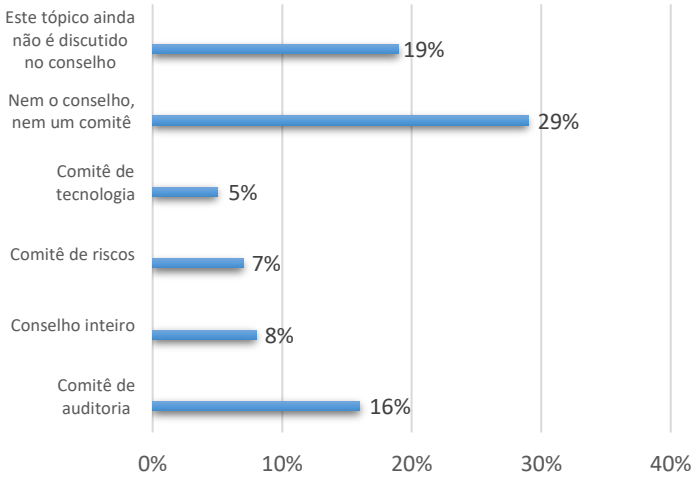
A auditoria interna pode assumir um papel de liderança na coordenação deste alinhamento entre atividades de avaliação de toda a organização e no melhor uso das atividades existentes, disse Pelletier. Para começar, os auditores internos podem promover uma maior consistência nos esforços de avaliação da tecnologia, determinando se as funções de gerenciamento de riscos, conformidade, auditoria interna e outras têm, cada uma, seus próprios sistemas de avaliação e classificação de riscos. Nas discussões com o conselho e a gestão, essas inconsistências entre as funções podem ilustrar um cenário confuso ou talvez aparentemente incompleto. A auditoria interna pode recomendar e liderar um esforço coordenado utilizando uma taxonomia comum de risco. As comunicações sobre riscos ao conselho e à alta administração serão mais compreensíveis se a auditoria interna e as funções da segunda linha falarem a mesma língua. Os resultados ou avaliações dessas funções não precisam necessariamente de concordar, mas os termos e abordagens que utilizam deveriam ser consistentes.

## Ficando de Olho na IA

Com muitas empresas ainda tendo dificuldades no uso da IA e da IA generativa, os auditores internos têm a oportunidade de conduzir uma melhor supervisão das tecnologias emergentes e de seu uso por suas organizações.

Em uma pesquisa[8] da Deloitte e da *Society for Corporate Governance* feita em 2023 com empresas de grande e média capitalização, apenas 13% tinham uma estrutura formal de supervisão de IA. Apenas 9% revisavam políticas corporativas relacionadas à cibersegurança, gerenciamento de riscos, retenção de registros e outras para abordar o uso da IA. No entanto, a *National Association of Corporate Directors* observou que, no ano anterior, 94% dos entrevistados corporativos disseram que a IA era crítica para o sucesso da sua empresa a curto prazo.[9]

**Quem faz a principal supervisão da IA no conselho da organização?**




*Fonte:* *Deloitte and Society for Corporate Governance Board Practices Quarterly: Future of tech: Artificial intelligence (AI)*, agosto de 2023.
*Obs.:* Respostas de "outro/não sei" não estão inclusas no gráfico.

Apesar da importância da IA, os conselhos parecem ainda não estar abordando preocupações relacionadas. A pesquisa mostrou que um total de 48% dos conselhos de administração participantes ainda não consideram a IA ou não atribuíram responsabilidade por ela (veja o gráfico). Entre aqueles que atribuíram a responsabilidade pela IA, foi mais provável a supervisão do comitê de auditoria, que é muitas vezes o grupo ao qual o CAE reporta. A auditoria interna pode agregar um valor considerável, ajudando as organizações a reconhecer a importância da IA e a de sua própria resposta a ela.

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

# Conclusão

**A avaliação da tecnologia que identifica riscos e obstáculos já está bem integrada** na função da auditoria interna. Enquanto mantém o foco em algumas das maiores vulnerabilidades relacionadas à tecnologia, a auditoria interna também pode promover uma melhor coordenação de esforços, para garantir um cenário mais completo e preciso para os gestores de risco e os stakeholders. As etapas descritas neste *Brief* podem ajudar a garantir que a abordagem geral da organização ao risco tecnológico e o plano de auditoria abordem adequadamente os riscos tecnológicos potenciais.

# Parte 2: Ficando por Dentro da Adoção Tecnológica da Organização

## Sobre os Especialistas

### Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, é gerente de produto sênior da TeamMate Audit Solutions, onde trabalha para melhorar continuamente a produtividade da auditoria e, ao mesmo tempo, oferecer insights estratégicos por meio da solução de ponta da TeamMate. Ele tem mais de 20 anos de experiência em auditoria interna nos setores público e privado.

Anteriormente, Jim ocupou vários cargos de liderança no The Institute of Internal Auditors, atuou como Auditor Municipal da cidade de Palo Alto, CA, e foi Chefe de Auditorias do Condado de San Diego, CA. Sua experiência diversificada em auditoria interna inclui cargos no California State University System, PETCO Animal Supplies, Inc., State Street Corporation e General Electric.

### Dennis Wong, CIA, CFSA

é diretor administrativo de um banco internacional com sede em Londres. É um profissional experiente em auditoria e riscos, com mais de 20 anos de experiência em bancos internacionais e mercados de capitais. Sua paixão é liderar e impulsionar mudanças por meio da reengenharia de processos e inovação tecnológica. Ele é voluntário na filial de Nova York do IIA e atua no *Exam Development Committee*.

# Introdução

**A tecnologia tornou-se a força vital das organizações,** uma ferramenta vital usada regularmente em essencialmente todas as funções. Mas, embora 60% dos líderes corporativos e de riscos vejam uma nova ferramenta tecnológica, a IA generativa (GenAI), como uma oportunidade, 57% dizem que a preparação para investimentos em novas tecnologias é o maior gatilho para revisar o cenário de risco, de acordo com a *Global Risk Survey* de 2023 da PwC.[10]

A tecnologia oferece novos benefícios, mas a dependência dela também traz ameaças, ameaças que crescem conforme o uso da tecnologia se torna mais crítico e difundido. Eles incluem riscos relacionados com a forma como a tecnologia é adotada. A auditoria interna pode ajudar as organizações a determinar e executar as melhores estratégias de implementação para minimizar riscos e aumentar o valor das novas tecnologias. Este *Brief* discute as etapas que a auditoria interna pode seguir para agregar valor a esse esforço.

[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," *press release* da PwC, 20 de novembro de 2023.

# Desenvolva um Novo Framework de Governança

## Como as novas tecnologias se encaixam?

### A auditoria interna pode ajudar a guiar a adoção de tecnologias

**Novas tecnologias apresentam sempre novas considerações de riscos.** Embora a GenAI, por exemplo, tenha inspirado uma grande variedade de usos inovadores para essa tecnologia transformadora, também apresenta novos perigos em áreas que incluem privacidade, viés incorporado e a transparência e precisão das informações recebidas. Ao mesmo tempo, podem surgir riscos conforme novas tecnologias impulsionam mudanças nas operações comerciais que expõem uma organização a novos riscos operacionais.

Por essas razões, ao adotar novas tecnologias, as organizações deveriam desenvolver um framework robusto de governança de projetos que considere como as novas ferramentas se adaptam ao negócio, se alinham com as estratégias corporativas e ajudam a atingir as metas corporativas, disse Dennis Wong, CIA, CFSA, um profissional experiente de auditoria e riscos, com mais de 20 anos de experiência em bancos internacionais e mercados de capitais. De fato, entre as empresas designadas como "pioneiras em risco" na pesquisa da PwC, 73% apresentaram alta probabilidade de ter uma estratégia e um roteiro tecnológico para toda a empresa, em comparação com 57% das organizações menos avançadas. O framework deveria incluir uma ampla consideração do risco, incluindo uma avaliação abrangente de riscos e controles que possam enfrentar as ameaças representadas por novos riscos, disse Wong.

A auditoria interna pode prestar avaliação sobre a governança do projeto e sobre seu bom funcionamento, e pode prestar consultoria sobre a adoção da tecnologia em geral. De início, a auditoria interna pode realizar uma revisão pré-implementação que considere a adequação da tecnologia, bem como quaisquer riscos relacionados e alterações necessárias nos controles. Uma vez implementadas as novas ferramentas, a auditoria interna também pode fornecer feedback sobre como está funcionando a adoção da tecnologia e o impacto que as novas ferramentas estão tendo em toda a organização, de acordo com Wong. Após a implementação, a auditoria interna pode avaliar se a tecnologia está funcionando conforme previsto e por que não, se não estiver, incluindo se os benefícios esperados foram alcançados.

A auditoria interna também pode detectar obstáculos que possam dificultar a adoção. Empresas fortemente compartimentalizadas podem estar sujeitas a um pensamento de silo, em que profissionais de diferentes funções desconhecem o que se passa nas outras áreas. Uma área pode não saber que outro grupo está explorando a mesma tecnologia, mas descobriu diferentes usos para ela, ou que uma terceira função enfrentou algumas falhas com a tecnologia, mas aprendeu lições valiosas. "Isso poderia criar uma bifurcação, quando se busca sinergia", segundo Wong. Como a auditoria interna tem uma visão holística da organização, está em uma posição única para quebrar esses silos e oferecer insights de ponta a ponta que evitam a duplicação de esforços. "Devido ao seu conhecimento institucional, a auditoria interna pode trazer uma nova perspectiva que pode levar a um uso de tecnologia mais valioso", disse. Também pode prestar avaliação sobre se os controles operacionais estão funcionando adequadamente e se estão garantindo o uso seguro da tecnologia. Como o dinheiro para investimento é sempre escasso, as organizações valorizarão os conselhos sobre se suas despesas com tecnologia estão sendo usadas da melhor forma, disse Wong.

As organizações terão que abordar a inter-relação entre os riscos estratégicos e operacionais e a tecnologia subjacente. "Um impacta o outro", disse Wong. As novas tecnologias mudam a forma como a organização opera, o que traz novos riscos. Isso, por sua vez, pode gerar mudanças nas operações que podem levar a riscos adicionais. A chave é ter uma

compreensão clara dos objetivos da organização, como são afetados por novos riscos ou como eles acarretam novos riscos, e quais controles podem resolver essas preocupações.

As organizações também se beneficiarão de uma forte cultura de risco, dadas as mudanças trazidas pela nova tecnologia. Mesmo que a organização tenha uma mentalidade e um framework de controle robustos, ainda precisa depender de indivíduos para implementar controles ou tomar as medidas corretas em sua ausência, observou Wong, motivo pelo qual uma forte disciplina de risco e uma compreensão adequada do risco de novas tecnologias são fundamentais. A cultura da empresa deveria identificar e comunicar ameaças potenciais de novas ferramentas e as expectativas corporativas quanto ao seu uso, para que fiquem claras para todos.

# Considere Passos Calculados

## Encontre um equilíbrio entre velocidade e segurança

### Assessorando sobre quando adotar novas tecnologias

**Frequentemente, há uma urgência de implementação assim que uma nova tecnologia é apresentada**, o que foi ilustrado mais recentemente pela pressa em implantar a GenAI. Devido aos riscos potenciais associados às novas ferramentas, "as organizações precisam encontrar o equilíbrio certo entre velocidade e segurança", disse Wong. Ele enfatizou o caso dos automóveis, que não tinham cintos de segurança quando foram lançados pela primeira vez, mas que acrescentaram cada vez mais recursos de segurança ao longo dos anos, conforme os carros começaram a se mover mais rápido. Dado o atual ritmo de mudança tecnológica e a complexidade dos sistemas envolvidos, uma auditoria interna pode ajudar a examinar se a gestão implementou características de segurança adequadas – ou controles. "O risco, identificado ou não, começa no primeiro dia", disse Wong. "Pode não se transformar imediatamente em uma perda ou em uma ameaça, mas quando você começa a usar uma tecnologia, você já está exposto ao risco."

Por exemplo, a GenAI é uma ferramenta sofisticada com camadas de complexidade; é fácil que ela seja explorada por malfeitores para fins maliciosos. Além disso, uma equipe que não tenha sido devidamente treinada sobre os riscos da GenAI pode expor involuntariamente dados confidenciais ou sensíveis, que poderiam ser incorporados no aprendizado do programa e poderiam ser acessíveis a terceiros.

As organizações deveriam considerar se devem ser as primeiras a comercializar e enfrentar riscos provenientes de fontes inesperadas e potenciais danos comerciais ou de reputação, ou se deveriam adotar uma estratégia de *quick follower*, rapidamente seguindo os pioneiros e aprendendo com as experiências e erros dos outros.

# Entendendo a Dívida Técnica

## Infraestrutura, equipe e cultura podem não ser capazes de lidar com as tecnologias mais recentes

### Identificando a dívida técnica e os passos para corrigir

**As organizações também precisarão determinar se a infraestrutura existente** pode lidar com novas ferramentas tecnológicas. Quando a tecnologia é adotada, as pressões de tempo, considerações de custo ou outros obstáculos muitas vezes forçam as organizações a economizar para cumprir um prazo, ou outros desafios podem fazer com que não consigam atingir a implementação ideal. Essa dívida técnica pode aumentar ao longo do tempo, se a organização não conseguir atualizar para novas versões de software ou novo hardware, implementar patches ou tomar outras medidas importantes de manutenção, disse Jim Pelletier, CIA, CGAP, gestor de produto sênior da TeamMate Audit Solutions. Conforme a organização constantemente adota novas soluções alternativas para manter o sistema funcionando, sua agilidade técnica fica cada vez mais para trás.

A dívida técnica pode impedir a organização de fazer o melhor uso do software existente ou até mesmo impossibilitar a adoção eficaz de novas tecnologias, disse Pelletier. O problema pode não ser bem comunicado pela equipe de TI, porque ela não tem conhecimento dele, reluta em discutir as falhas do sistema ou considera a tecnologia muito complexa para ser explicada a profissionais não-tecnológicos. Como resultado, os auditores internos podem não estar cientes dessa dívida técnica ou do seu impacto na capacidade da organização de adotar novas tecnologias.

Embora a auditoria interna não precise dos mesmos conhecimentos que a equipe de tecnologia da organização, ela pode resolver o problema da dívida técnica tomando medidas para garantir que sua equipe mantenha habilidades suficientes para ter diálogos produtivos com a equipe de TI, de modo que possam revelar o estado atual dos sistemas da organização, disse Pelletier. Armados com esse conhecimento, os membros da equipe de auditoria interna podem ter conversas frutíferas que respeitem o tempo e a experiência dos membros da equipe de TI.

### Perguntas a Fazer sobre Novas Tecnologias

Ao prestar avaliação ou consultoria, algumas das perguntas que a auditoria interna pode fazer incluem:

- Qual impacto a nova tecnologia terá na organização e nos seus processos de negócio, incluindo riscos, benefícios e novas oportunidades?
- Como a tecnologia se enquadra nas abordagens de gerenciamento de riscos corporativos, governança, risco e conformidade da organização?
- Como a tecnologia deveria ser integrada aos controles existentes? Houve uma avaliação do impacto nos controles internos? Se sim, quais mudanças deveriam ser feitas nos controles e processos? A auditoria interna deveria trabalhar com cada unidade de negócios para reavaliar seus riscos e controles, e preparar-se para documentar novos riscos e controles?
- Precisamos fazer atualizações tecnológicas, mudanças nos processos de negócios ou aprimorar as habilidades de nossa equipe?
- Quais novos riscos ela apresenta, incluindo ameaças à privacidade, aos dados dos clientes, às informações proprietárias e outros?
- Onde é utilizado o novo sistema e por quem?
- O que acontece com os dados que a tecnologia coleta ou produz? Onde são armazenados e como são protegidos?
- A organização estará agora compartilhando dados que não deveria ou expondo-se de outra forma a novos riscos de privacidade de dados?

Em outros casos, mesmo que a infraestrutura tecnológica de uma organização seja adequada, a tecnologia pode ultrapassar a empresa e seus colaboradores. Isso pode acontecer quando as organizações modernizam sua tecnologia sem atualizar suas forças de trabalho ou processos de negócio. A empresa pode estar implementando a tecnologia para aumentar a eficiência, mas não dedica tempo para alinhar e compreender como os processos serão afetados ou precisarão ser alterados. "As pessoas não sabem como usar a tecnologia, o que desperdiça tempo, energia e dinheiro", disse Pelletier. "É uma oportunidade perdida de fazer melhorias significativas." Mais uma vez, a auditoria interna possui o conhecimento institucional necessário para fazer as perguntas certas e garantir que a tecnologia e os objetivos e ativos do negócio sejam igualmente correspondidos.

Por fim, conforme a tecnologia avança, pode ser fácil esquecer o valor do toque humano, mas a revisão e avaliação humanas continuarão sendo críticas para o processo, observou Wong. Uma ferramenta como a GenAI não apenas comete erros ou inventa coisas às vezes, se usada com o cliente ou em outras interações humanas, mas também pode deixar passar sinais que uma pessoa teria captado ou fornecer respostas impraticáveis que um ser humano familiarizado com o cliente saberia que são inadequadas.

## Abordando Algumas Limitações da GenAI

A GenAI foi recebida com grande entusiasmo quando foi apresentada pela primeira vez, mas suas deficiências, discutidas neste relatório, suscitaram preocupação. Pode ser uma ferramenta valiosa para abordar a adoção da tecnologia em uma organização, se usada corretamente. Jim Pelletier identifica duas opções para auditores internos que desejam aprimorar seu uso de GenAI.

- Em alguns casos, a GenAI inventa respostas, ou tem alucinações, se não consegue responder a uma pergunta, ou comete erros porque só sabe aquilo que a ensinaram. Para resolver isso, a *Retrieval-Augmented Generation* (RAG) é uma técnica que disponibiliza dados precisos e tempestivos para aumentar o que está em um sistema de GenAI. A RAG otimiza a saída de grandes modelos de linguagem, como a GenAI, referenciando uma base de conhecimento confiável fora das fontes de dados de treinamento da GenAI antes que uma resposta seja gerada. E embora as fontes de GenAI não sejam transparentes, a RAG torna possível identificar os materiais de origem.
- Obter o melhor resultado da GenAI depende, em parte, de fornecer as instruções corretas, conhecidas como prompts. Os prompts deveriam especificar detalhes como a duração da resposta, o público-alvo para casos em que vá ser compartilhada com outras pessoas, o estilo e o tom. Pelletier fornece um exemplo:

  Você é um gerente de auditoria interna experiente, com experiência em gerenciamento de riscos tecnológicos no setor de serviços financeiros. Você avalia o risco tecnológico com base no impacto sobre as operações comerciais e sobre a probabilidade de ocorrência do risco.

  - Em formato de tabela, identifique os 10 principais riscos relacionados à adoção de novas tecnologias em um grande banco.
  - Inclua colunas para Nome do Risco, Descrição do Risco e Justificativa, descrevendo por que o risco é uma prioridade máxima.
  - Priorize as linhas da tabela de alto risco para baixo risco.

# Conclusão

**Embora a adoção de novas tecnologias possa trazer riscos**, também é importante se lembrar dos perigos de não se manter atualizado sobre as novas ferramentas. As muitas desvantagens de fazer isso incluem:

- Desperdiçar os benefícios que as novas tecnologias podem oferecer.
- Não conseguir acompanhar os concorrentes, devido às vantagens que eles obtêm com a transformação digital.
- Deixar de contar com eficiência e produtividade melhoradas, ou não conseguir inovar em novos produtos e serviços.
- Perder clientes potenciais ou existentes, parceiros de negócios valiosos ou funcionários talentosos que preferem trabalhar com organizações tecnologicamente mais avançadas.

"A tecnologia está na base de tudo que fazemos todos os dias", disse Pelletier. A auditoria interna pode desempenhar um papel para garantir que as novas ferramentas tenham o máximo impacto positivo.

# Parte 3: O Desafio da Auditoria Interna com Talentos de Tech

## Sobre os Especialistas

### Jim Pelletier, CIA, CGAP

Jim Pelletier, CIA, CGAP, é gerente de produto sênior da TeamMate Audit Solutions, onde trabalha para melhorar continuamente a produtividade da auditoria e, ao mesmo tempo, oferecer insights estratégicos por meio da solução de ponta da TeamMate. Ele tem mais de 20 anos de experiência em auditoria interna nos setores público e privado.

Anteriormente, Jim ocupou vários cargos de liderança no The Institute of Internal Auditors, atuou como Auditor Municipal da cidade de Palo Alto, CA, e foi Chefe de Auditorias do Condado de San Diego, CA. Sua experiência diversificada em auditoria interna inclui cargos no *California State University System*, PETCO Animal Supplies, Inc., State Street Corporation e General Electric.

### Dennis Wong, CIA, CFSA

Dennis Wong, CIA, CFSA, é diretor administrativo de um banco internacional com sede em Londres. É um profissional experiente em auditoria e riscos, com mais de 20 anos de experiência em bancos internacionais e mercados de capitais. Sua paixão é liderar e impulsionar mudanças por meio da reengenharia de processos e inovação tecnológica. Ele é voluntário na filial de Nova York do IIA e atua no *Exam Development Committee*.

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

Nisha Nair trabalha como especialista em auditoria interna para a Autoridade Federal de Regulamentação Nuclear dos Emirados Árabes Unidos. Ela acumulou mais de 10 anos de experiência como profissional de consultoria de risco financeiro e empresarial, o que inclui trabalhar na prática de consultoria de riscos de uma empresa de consultoria das 'Big 4'. Ela é membro de diversos órgãos de qualificação profissional e é apaixonada por promover e revelar o verdadeiro valor da profissão de auditoria interna. Além disso, atua como especialista no *Global Professional Knowledge Group* do IIA Global, com sua expertise que se estende por vários assuntos relacionados à auditoria interna, incluindo gerenciamento de riscos, análise de dados, governança, gerenciamento do risco de fraude, ética e auditoria externa.

# Introdução

## A rachadura na armadura da auditoria interna

De acordo com o *North American Pulse of Internal Audit* de 2024, a cibersegurança e a TI foram selecionadas pelos líderes de auditoria interna como as duas áreas de maior risco em suas organizações, com 78% e 58% dos entrevistados, respectivamente, classificando-as como de risco alto ou muito alto. Isso não deveria ser uma surpresa; na verdade, a tecnologia dominou o cenário de risco nos últimos anos. No entanto, ano após ano, torna-se mais evidente que a auditoria interna enfrenta sérios desafios nesta área, que só irão piorar se não forem abordados.

Os esforços combinados de cibersegurança e TI representam quase 20% dos planos de auditoria, de acordo com os entrevistados da pesquisa Pulse, que são principalmente líderes de auditoria norte-americanos. Juntos, eles criam uma porcentagem maior do que qualquer outra área de risco, mas os dados do Pulse também indicam que tanto a cibersegurança quanto a segurança de dados e a TI foram as áreas em que mais se usa terceirização ou equipe compartilhada. Além disso, embora cerca de 2 em cada 10 participantes da pesquisa indiquem que a tecnologia seria a principal prioridade, quase metade das funções de auditoria prioriza o aumento da equipe interna. Isso ocorre apesar de as funções de auditoria continuarem enfrentando uma variedade de problemas com o recrutamento, com 29% dos entrevistados da Pulse citando as expectativas de remuneração como o desafio mais significativo, seguidos por 17% que afirmam que os candidatos a empregos não possuem as competências necessárias.

Tomadas em conjunto, essas conclusões retratam um cenário que mostra que a própria auditoria interna, embora aborde os riscos tecnológicos da melhor forma possível através da terceirização e do cosourcing (compartilhamento de talentos), não está, em geral, em uma posição ideal para incorporar as competências tecnológicas à equipe interna. A longo prazo, essa abordagem pode ter repercussões significativas não apenas na cobertura de riscos, mas também nas capacidades das funções de auditoria de aproveitar a tecnologia para melhorar todos os aspectos do seu papel.

Como parte final desta série de três partes sobre inovação e tecnologia patrocinada pela TeamMate, este Brief de Conhecimento examina uma série de facetas do que pode ser chamado de "desafio tecnológico" da auditoria interna, como a luta para construir equipes com experiência em tecnologia. Também irá, através da contribuição de especialistas selecionados da indústria, fornecer algumas melhores práticas e estratégias que as equipes, independentemente da indústria, do orçamento ou do porte da função, podem usar para prestar serviços de avaliação e consultoria que possam acompanhar o ritmo acelerado e implacável da tecnologia.

# Construindo a Equipe de Tech

## Prepare-se Agora para um Futuro Tech

## A questão do financiamento

A auditoria interna não está sozinha na corrida para adquirir talentos com conhecimento de tecnologia. Na verdade, quase todos os departamentos de todas as organizações e de todas as indústrias estão enfrentando o mesmo desafio, criando uma concorrência feroz para contratar pessoas que já eram um grupo limitado. Após as demissões em massa nos setores tecnológicos durante a pandemia da COVID-19, muitos analistas esperavam que os cerca de 20.000 trabalhadores da indústria tecnológica que procuravam trabalho satisfizessem de alguma forma esta necessidade. No entanto, como testemunho da rápida evolução da tecnologia, a lacuna entre os cargos necessários e os talentos devidamente qualificados aumentou – e os talentos disponíveis para contratação não são baratos. Com 51% das funções de auditoria, de acordo com dados da pesquisa Pulse, vendo seus orçamentos permanecerem praticamente os mesmos do ano anterior, claramente, qualquer função de auditoria que queira contratar talentos de tech tem um grande desafio pela frente.

"O tema mais recorrente que sempre surge quando vários líderes de AI falam sobre as dificuldades na implantação da tecnologia é a necessidade de financiamento adequado", afirma Nisha Nair, especialista em auditoria interna da Autoridade Federal de Regulamentação Nuclear nos Emirados Árabes Unidos. "Isso inclui financiamento para ferramentas de TI, financiamento para treinamento de tecnologia para a equipe do departamento de auditoria interna e financiamento para a contratação dos recursos tecnológicos certos dentro da equipe. Muitas vezes, quando você tenta recrutar um indivíduo de, digamos, uma área específica, como a indústria cibernética, suas expectativas do ponto de vista do pacote de remuneração serão muito maiores do que um pacote de remuneração típico de AI, e muitos deles também preferem trabalhar e crescer em seu nicho de trabalho especializado que lhes remunera mais, em vez de serem empregados em um cargo de auditoria interna generalista."

Enfrentando esta dura realidade, para talvez chegar perto de acompanhar o cenário de risco impulsionado pela tecnologia, a auditoria interna teve de ser criativa para preencher estas lacunas de competências necessárias. "A estratégia do conjunto de competências não é única", afirma Dennis Wong, diretor administrativo e chefe global de auditoria de risco de crimes financeiros do HSBC. "A combinação certa é diferente para cada departamento de auditoria. É uma combinação de crescimento/*upskilling* (aprimoramento) orgânico, cosourcing com empresas de consultoria e, quando possível, contratação externa."

Cada elemento dessa estratégia tripartida é digno de discussão:

### *Contratando de Fora*

Conforme mencionado anteriormente, dados os atuais níveis orçamentais e a falta de financiamento adicional, a implementação dessa estratégia pode parecer um pensamento tanto quanto irrealista e pode até ser totalmente descartada. No entanto, embora seja certamente um desafio, o avanço nesta área é possível – e começa com o comitê de auditoria.

Como o Conselho e/ou o Comitê de Auditoria têm um papel importante a desempenhar na aprovação do orçamento anual da auditoria interna, a meta para um líder de auditoria interna deveria ser apresentar um forte argumento comercial sobre por que o financiamento adicional para contratação de equipe técnica é necessário à luz da implantação e inovação tecnológica. Isso vai além de citar dados; em vez disso, a meta deveria ser "contar uma história convincente" que seja difícil de recusar, diz Nair. "Os líderes de AI precisam obter o apoio do Comitê de Auditoria e da alta administração quanto à

necessidade de talentos tecnológicos dentro do departamento de AI, quanto ao valor que isso deve proporcionar à organização e precisam explicar a necessidade de um pacote de remuneração e plano de carreira adequados para atrair tais talentos para o departamento de AI", diz Nair.

"Temos que conseguir a adesão do comitê de auditoria e fazê-los perceber que esse talento é um nicho e que o pacote de remuneração que se aplica à equipe de auditoria interna pode não ser suficiente para alguém na área cibernética", diz ela.

Isso também pode exigir que o comitê de auditoria reconsidere a eficácia da estruturação das equipes de auditoria interna para o ambiente de risco atual. O que é exigido hoje da equipe de auditoria é muito diferente do que era há 15 anos. "Olhando para o panorama geral, precisamos pensar sobre a composição de nossas equipes", diz Jim Pelletier, gerente sênior de produtos da TeamMate Audit Solutions. "Hoje, você não está contratando um auditor interno tradicional, mas sim um especialista em cibersegurança – então, talvez esse seja o cargo que você precisa ter. Os líderes de auditoria precisam explicar aos seus comitês que não podem oferecer salários de auditoria interna, porque não estão contratando um auditor interno. Eles podem nem ter 'auditoria' no cargo."

Como parte do argumento de venda, esse especialista em cibersegurança não precisa ser explicitamente reservado para a auditoria interna. "Eles podem ser usados onde quer que seu conjunto de habilidades se encaixe", diz Pelletier. "Quando fosse fazer uma auditoria de cibersegurança, eu a faria de forma abrangente, mas talvez não precise fazê-la continuamente, então, talvez eu precisasse de habilidades de cibersegurança apenas algumas vezes por ano. É hora de a auditoria interna ser criativa. Talvez eu não precise trazer um especialista cibernético para minha equipe em tempo integral, mas se eu puder usar um especialista cibernético que normalmente trabalha na segunda linha como auditor quando necessário, isso será incrivelmente valioso e eficiente, desde que eu possa gerenciar quaisquer preocupações com independência e objetividade."

Essas conversas não deveriam estar reservadas ao Comitê de Auditoria ou ao Conselho; o líder de auditoria interna deveria usar sua posição como conselheiro confiável para comunicar o valor do talento tecnológico qualificado. "Os líderes do departamento de auditoria podem tornar-se os porta-vozes da mudança", continua Nair. "Eles precisam ter uma comunicação orientada para a tecnologia com a equipe de gestão e facilitar a navegação de toda a organização em direção a um futuro mais capacitado pela tecnologia." Essas comunicações do topo, diz ela, se espalharão para outros departamentos da organização. Isso ajudará a criar um ambiente que incentive a colaboração para desenvolver ou permitir que soluções tecnológicas atinjam um objetivo comum. Com apoio organizacional suficiente, o financiamento inevitavelmente vem.

Igualmente importante na busca por talentos externos é aproveitar todas as possibilidades para ampliar o talento disponível, se e quando possível. Isso pode ser feito de algumas maneiras. Por exemplo, manter o foco nas iniciativas de diversidade, equidade e inclusão (DEI) não só promove a inteligência cognitiva dentro do departamento e da organização, mas também torna as organizações mais atraentes para as gerações mais jovens de talentos qualificados. Além disso, os departamentos que publicam vagas deveriam considerar fortemente a ampliação do leque para incluir opções de trabalho remoto. De acordo com a pesquisa Pulse, surpreendentes 95% dos líderes de auditoria interna da geração Millennial (1981-1996) esperam que os níveis de trabalho remoto permaneçam os mesmos, o que implica que há uma expectativa de que talentos em busca de futuras contratações procurarão por essas opções.

Por fim, ao contratar, esteja ciente de que a tecnologia está avançando tão rapidamente que muitas das competências que alguém pode incluir em uma descrição de cargo podem ficar desatualizadas em questão de anos ou até meses. Portanto, os gerentes de contratação não deveriam ser tão categóricos ao escolher as qualificações dos candidatos. O que é fundamental não é o quanto alguém domina uma habilidade tecnológica específica, mas sim sua capacidade de desenvolver continuamente novas habilidades. "Não sugerimos que você contrate um indivíduo para uma tecnologia específica, mas sim alguém que possa compreender facilmente novas tecnologias", diz Nair. "As funções de AI precisam de pessoas que sejam adaptáveis, em termos de serem capazes de absorver novas competências como uma esponja."

Esses são os tipos de indivíduos que mais se beneficiarão da formação de equipes que os coloque em posição de aprender e ter sucesso. “É muito raro encontrar um indivíduo unicórnio que ‘singularmente’ tenha todas as habilidades de riscos, conhecimento de negócios, auditoria, ciência de dados e tecnologia. Não é impossível, mas é raro”, diz Wong. “Portanto, a prioridade deveria ser criar uma equipe que tenha pessoas trabalhando juntas, como cientistas de dados trabalhando ao lado de auditores internos que podem aprender e crescer através do processo de auditoria.”

## *Terceirização e Cosourcing para Upskilling*

Conforme mencionado anteriormente, muitas funções de auditoria hoje optam por terceirizar e compartilhar suas responsabilidades de auditoria cibernética e de TI. Esta tendência decorre obviamente de uma necessidade, dados os desafios e restrições de contratação, mas especialmente em áreas tecnológicas como a cibersegurança também é uma necessidade.

“Internamente, é muito difícil obter conhecimento da melhor e mais recente tecnologia”, diz Wong. “Você tem que sair da sua empresa para buscar esse conhecimento. É aí que entram consultorias e especialistas.”

No entanto, ao contratar essas empresas externas, pode-se por vezes ignorar como esse talento terceirizado pode ter um impacto na função de auditoria para além da duração do seu contrato.

“O que funciona muito bem é quando os departamentos de AI utilizam seus fornecedores de AI, parceiros de AI e/ou empresas de consultoria existentes para o *upskilling* (aprimoramento) das habilidades de sua própria equipe de AI departamental, enquanto os talentos terceirizados/compartilhados executam o trabalho de auditoria prescrito”, diz Nair. “É bom combinar talentos/parceiros/consultores externos terceirizados/compartilhados com a equipe interna de AI, para permitir a transferência de conhecimento enquanto o trabalho está sendo executado. A aprendizagem prática definitivamente prova ser a mais eficaz.”

Pelletier concorda.

“Se estamos terceirizando ou compartilhando, tudo bem, mas você está melhorando?” ele pergunta. “Você está incorporando sua equipe nos projetos para que eles aprendam? Você está aproveitando ao máximo o tempo que tem para desenvolver um pouco mais os conjuntos de habilidades internas?”

Também é uma ideia útil difundir as competências tecnológicas básicas de talentos terceirizados e compartilhados de uma forma mais estruturada. Isso pode assumir a forma de workshops ou sessões de grupo, onde indivíduos de todos os departamentos podem ver em primeira mão as possibilidades da tecnologia e, em seguida, podem trazer o conhecimento recém-adquirido de volta às suas respectivas áreas.

No entanto, uma vez que a equipe estiver qualificada ou a expertise for incorporada em tempo integral, o *cosourcing* deveria sempre fazer parte da estratégia de conjunto de competências da organização. “Quando talentos altamente qualificados são contratados como funcionários em tempo integral, inevitavelmente eles perdem a vantagem”, diz Wong. “Na cibersegurança, por exemplo, digamos que você contrate um hacker *white hat* com o conhecimento técnico mais recente para fazer coisas como testes de penetração. Mas se eles não estiverem mais ‘hackeando’, eles não estarão mais na vanguarda do campo. Portanto, não importa o nível de habilidade da equipe interna, você sempre vai querer contratar uma empresa externa, até certo ponto, porque ela sempre conhecerá as vulnerabilidades mais recentes.”

## *Upskilling de Dentro para Fora*

Embora muitas das discussões sobre tecnologia girem em torno da captação de talentos, é fundamental não ignorar os talentos que já estão internos à organização. Através de relações positivas e da colaboração entre a auditoria interna, a alta administração e a equipe de TI, a auditoria interna deveria trabalhar para desenvolver uma compreensão clara das competências e ferramentas que os outros departamentos possuem. A análise de dados ou o software de monitoramento contínuo, por exemplo, podem ter aplicações amplas que, com um pouco de treinamento, poderiam se encaixar perfeitamente em tarefas de auditoria.

“Você deveria trabalhar em conjunto com outras equipes e explorar os vários caminhos onde você pode colaborar – e se o relacionamento for bom, eles poderão dizer algo como: 'Ok, temos essas ferramentas em funcionamento, então, por que não as usamos para fins de auditoria interna?'”, diz Wong.

Isso também se aplica à alta administração. Como segunda linha, ela pode ter acesso a ferramentas de análise de dados, ferramentas de monitoramento contínuo de auditoria contínua *(continuous auditing continuous monitoring* – CACM) e ferramentas que lidam com ISOs e procedimentos — todas as quais podem ser úteis em um contexto de auditoria interna.

Claro, a necessidade de aprimorar competências vai muito além da simples auditoria interna. Com certeza, o esforço para aumentar as competências tecnológicas básicas em toda a organização precisa ser onipresente no ambiente atual. Novamente, alavancando seu papel como porta-vozes da mudança, os líderes de auditoria interna deveriam defender, em todas as interações entre os seus departamentos, treinamento obrigatório sobre tendências e técnicas tecnológicas atuais. “Uma abordagem eficaz seria definir o nível mínimo de conhecimento e habilidades relacionados à tecnologia ou aos dados, juntamente com níveis de progresso/especialização para cada cargo dentro do framework de competências de AI”, diz Nair. “Precisamos incentivar cada profissional de AI a passar pelo treinamento mínimo exigido, para aprender pelo menos as habilidades básicas de TI para seu cargo e progredir nele.”

Wong expressa um sentimento semelhante. “Há uma necessidade constante de qualificação em todas as funções”, diz ele. “É fundamental permanecer relevante e acompanhar o ritmo dos mercados. Sempre há novas ferramentas e técnicas que você deve conhecer.”

Obter essas competências nem sempre implica o aumento dos orçamentos de treinamento. Muitas dessas habilidades podem ser aprendidas individualmente por meio de cursos online gratuitos ou sessões interdepartamentais de conhecimento – de preferência, ambos. “Muitas vezes, quando uma pessoa não técnica lê artigos técnicos online, o jargão técnico tende a desanimá-la”, diz Nair. “Ter pessoas dentro do departamento ou da organização apenas para ajudar a equipe de AI a entender tais jargões e conceitos tecnológicos é bastante útil em termos de criar um desejo de explorar várias facetas da tecnologia.”

Tenha em mente, no entanto, que uma vez estabelecido um “mínimo”, esse nível logo terá que ser elevado. Ao avaliar esses frameworks através de uma auditoria, os auditores internos precisam se concentrar não apenas em saber se as competências estão sendo ensinadas, mas também em ver como essas competências são implementadas de forma contínua e eficaz e desenvolvidas conforme a base de conhecimento cresce.

“Uma estratégia eficaz de upskilling deveria incluir alguma mensuração da ‘aptidão digital’”, afirma Nair. “As métricas de desempenho departamental não deveriam se restringir à implementação de tecnologia; também deveriam incluir KPIs que mensurem como o departamento evolui continuamente em relação ao uso daquela tecnologia específica. Portanto, os líderes de auditoria interna precisam defender a atualização dos KPIs que indicam como os departamentos estão se transformando, em vez de apenas implantar uma tecnologia específica. Sem evolução ou transformação contínua, todos correm o risco de ficar estagnados.”

Pelletier acrescenta: “A tecnologia está integrada em tudo que fazemos, por isso, temos que defender constantemente que o aumento do nível de exigência. A tecnologia está em constante mudança, então, na verdade, já estamos tentando alcançá-la. Se não nos mexermos, a lacuna continuará crescendo. Como líder de auditoria, seu objetivo é gerenciar o tamanho da lacuna que você e seu conselho estão dispostos a permitir.”

# Os Dados Estão no Comando

## As Bases para Todo o Progresso Tecnológico

### Encontrando dados de qualidade e entendendo o que significam

Os dados "estão com tudo", e cada dia mais. Não importa a estratégia usada para criar equipes digitais eficazes, nenhuma delas terá qualquer tipo de efeito sem acesso a dados de qualidade.

“Os dados são fundamentais para o trabalho de auditoria, especialmente com o uso predominante de sistemas e controles automatizados”, diz Wong. “Dada a abundância de dados da atualidade, as oportunidades de alavancá-los na auditoria interna são imensas – desde que se saiba como usá-los, o que torna a falta deles ainda mais problemática.”

Embora se reconheça que a falta de dados é problemática, ainda hoje o acesso a dados de qualidade não é garantido. E igualmente preocupante, diz Nair, é quando os departamentos de AI usam a sua aparente incapacidade de adquirir dados como desculpa para não avançar na implementação tecnológica nas atividades de AI. Isso não pode acontecer. Em vez disso, a jornada para obter e alavancar dados deveria ser usada como uma parte crítica do argumento comercial da auditoria interna para o avanço tecnológico. “Quando se trata de integridade de dados, as funções de AI não deveriam se restringir à mera identificação ou categorização de dados como bons ou ruins”, diz ela. “Em vez disso, as funções de AI deveriam aproveitar esta oportunidade para chamar a atenção da gestão executiva, fornecer recomendações para melhorar a qualidade dos dados e dar o pontapé inicial. Travar o uso da tecnologia em auditorias por preocupações assim pode fazer com que as funções de AI nunca avancem em seus esforços tecnológicos.”

Não pode ser assim. Na realidade, a jornada para obter e alavancar dados deveria ser vista como uma peça fundamental do discurso da auditoria interna em prol do avanço tecnológico. “O que vemos é que nem sempre deveríamos nos restringir apenas a identificar se os dados são bons ou ruins”, diz ela. “Deveríamos realmente buscar o progresso, destacando e usando os dados como uma forma de identificar áreas de melhoria e de comunicação com a gestão, e manter as coisas fluindo. Porque se pararmos em qualquer ponto, correremos o risco de ficar estagnados para sempre.”

Dados não requerem necessariamente investimento para coleta. Muitas vezes, pode ser apenas uma questão de ter o conhecimento necessário para aproveitar os dados que já estão disponíveis. Mesmo as informações rastreadas em uma planilha do Excel podem ser consideradas dados de qualidade dependendo da situação. As chaves para desbloquear os dados são simples: a habilidade certa para percebê-los, destacá-los e alavancá-los, e a cultura certa para promover o desenvolvimento de tal habilidade. Em outras palavras, onde o talento é cultivado e desenvolvido, os dados também são.

No ambiente certo, os dados nem precisam ser perfeitamente ideais para serem considerados valiosos. “Minha opinião é que ter dados é sempre melhor do que não ter dados”, diz Wong. “Mesmo um conjunto incompleto de dados ainda é melhor do que não ter dado algum. O que é mais importante do que a integridade dos dados é ter a mentalidade de aproveitar todas as oportunidades de análise de dados do que você tem. Digamos que eu lhe dê $ 10, mas dou em centavos. Você ainda aceitará com base no fato de que ainda são US$ 10, mesmo que seja de um jeito relativamente trabalhoso.”

Contudo, a auditoria interna deve fazer mais do que apenas compreender como os dados são utilizados. Segundo Pelletier, o conhecimento dos dados se resume a responder quatro perguntas:

- De onde estão vindo?
- Onde estão armazenados?
- O que está sendo feito com eles?

- Como estão sendo descartados?

Na maior parte dos casos, responder a estas perguntas não requer um grau particularmente elevado de conhecimento técnico.

"A governança de dados é algo em que acredito que todo auditor deveria se tornar especialista", diz Pelletier. "Alguns aspectos podem exigir conhecimento técnico mais profundo, mas cada auditor deveria estar preparado para fazer perguntas desafiadoras, entender processos subjacentes e obter conhecimento técnico apenas sobre o que você precisa."

# Conclusão

## A tecnologia é uma oportunidade, não uma perda

Apesar de toda a conversa sobre os incríveis benefícios que a tecnologia pode trazer, ela pode trazer a mesma quantidade de ansiedade. É natural considerá-la algo desgastante – inclusive ao ponto em que alguém pode até começar a questionar a sua própria segurança no emprego. Em algum momento, conforme a tecnologia evoluir, haverá lugar para o trabalho humano?

Esta é uma preocupação compreensível, mas é uma preocupação que decorre do tipo errado de cultura organizacional. A tecnologia não deveria ser encarada como um concorrente ou uma ameaça – deveria ser vista com entusiasmo como uma oportunidade para conquistar mais, de proporcionar mais valor à organização e, na verdade, até melhorar a rotina de cada trabalhador.

"Embora não seja a maioria, ainda pode haver um número de pessoas que podem acreditar que a automação tiraria seu trabalho ou aqueles que estão comportamentalmente ancorados na manutenção de suas formas estabelecidas de execução de auditorias, tais como fazer da forma que você se sinta confortável, digamos, usando as boas e velhas planilhas", diz Nair. "Os líderes de AI deveriam encorajar discussões sobre a necessidade de permanecer ágil nesta era dinâmica impulsionada pela tecnologia, adotando uma mentalidade de aprendizagem e os potenciais benefícios da tecnologia, enquadrada especialmente como um meio de reduzir a carga de trabalho do departamento ou aumentar a eficiência, não como um meio de substituir auditores."

A auditoria interna pode e deve ser a maior defensora da tecnologia na organização. É a porta-voz da mudança, a parceira, a mensageira que traz boas notícias. Conforme o desafio tecnológico continua, as organizações poderiam se beneficiar ainda mais destes papéis.

## Sobre o The IIA

O Institute of Internal Auditors (IIA) é uma associação profissional internacional sem fins lucrativos que atende mais de 235.000 membros globais e concedeu mais de 190.000 certificações Certified Internal Auditor (CIA) no mundo todo. Fundado em 1941, o IIA é reconhecido globalmente como líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para mais informações, visite theiia.org.

## Sobre a Wolters Kluwer TeamMate

A Wolters Kluwer TeamMate Audit Management Solutions é uma solução líder mundial especializada em auditoria interna e avaliação, com mais de 25 anos dedicados ao avanço de auditores corporativos, comerciais e do setor público. Conforme as equipes de auditoria interna evoluem para oferecer insights mais profundos, uma melhor avaliação de riscos e uma maior eficiência, elas precisam de soluções específicas e prontas para o futuro. A TeamMate fornece soluções especializadas nas quais os auditores internos confiam para agregar valor às suas organizações. Para obter mais informações, visite www.teammatesolutions.com.

## Isenção de Responsabilidade

The IIA publica este documento para fins informativos e educacionais. Este material não se destina a fornecer respostas definitivas a circunstâncias individuais específicas e, como tal, destina-se apenas a ser usado como guia. The IIA recomenda buscar assessoria especializada independente relacionada diretamente a qualquer situação específica. The IIA não aceita qualquer responsabilidade por qualquer pessoa que confie exclusivamente neste material.

## Copyright



Maio de 2024

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