

## Perspectivas de auditoria interna

### A eficácia da auditoria interna de TI do ponto de vista do CIO

A tecnologia digital se transformou em aspecto-chave de desenvolvimento global por sua capacidade de conectar, informar e facilitar a vida em todos os níveis, desde os indivíduos até as instituições. Para as empresas atuais, o digital é essencial – ele está de tal maneira incorporado a áreas como estratégia, infraestrutura, operações e produtos e serviços, que os negócios e a tecnologia da informação (TI) se tornaram, de fato, uma coisa só. A revolução digital em curso está transformando os negócios de três maneiras bastante importantes: promovendo uma mudança do físico para o virtual, do isolado e não integrado para o conectado e integrado e de entidades fechadas e repletas de barreiras para plataformas abertas e compartilhadas, incentivando a colaboração e o envolvimento com clientes. Além de criar novas oportunidades de crescimento para os negócios, essa rápida expansão digital está modificando empresas e modelos de negócios bastante consolidados e aumentando os riscos cibernéticos, entre outros, ao trazer novas ameaças e vulnerabilidades.

**A Internet das Coisas, as tecnologias cognitivas, a nuvem, os dispositivos móveis e o Big Data estão proporcionando novas oportunidades de negócios, mas as complexidades e os riscos envolvidos estão se agravando.**

Em consequência da transformação de negócios e de TI e da disrupção digital em curso, os diretores de Tecnologia da Informação (CIOs) estão vivenciando um mundo de mudanças e mais pressão para gerar resultados. A necessidade de reduzir custos e a disponibilidade de novos recursos exigem que os CIOs alterem seus principais modelos organizacionais e operacionais. Crescem também as expectativas de que os CIOs usem mais a tecnologia de nuvem, realizem *sourcing* estratégico e criem laboratórios de inovação para testar novos produtos. Os conselhos e a alta administração também estão se envolvendo mais na agenda dos CIOs. Embora queiram que os CIOs adotem novas tecnologias para estar na vanguarda, eles também fazem mais perguntas e avaliam em detalhes a eficácia e as decisões sobre investimentos. Em resumo, espera-se que os CIOs encontrem novos meios de servir as empresas e diminuir os custos da tecnologia – tudo isso enquanto administram os riscos que possam vir a surgir.

Para conseguir fazer isso de forma eficaz, os CIOs estão buscando relacionamentos e o apoio de parceiros de negócios internos e das áreas responsáveis por riscos. As funções de auditoria interna de TI estão especialmente preparadas para gerar valor e apoiar os CIOs na identificação antecipada de riscos e para guiá-los na implementação de suas estratégias.

CIOs eficazes precisam contar com áreas de auditoria interna de TI capazes de reconhecer que a missão delas é ajudar as empresas a reduzir riscos de TI e preparar o negócio para aproveitar as oportunidades criadas pelas novas tecnologias e pela revolução digital.

Muitos *stakeholders* querem que a auditoria interna vá além de seu papel tradicional de asseguaração, prestando, de forma hábil, serviços com valor agregado e assessorando as áreas de TI de forma proativa. Em uma pesquisa recente da PwC, 64% dos membros de conselhos e da administração disseram esperar mais do que recebiam da auditoria interna. As áreas de auditoria interna de TI mais eficientes estão avançando na formação de parcerias com

os CIOs a fim de criar valor para o negócio, oferecendo competências de asseguaração e gestão de riscos, além de suporte especializado, quando necessário. Além de dar aos CIOs condições para que eles concretizem suas estratégias, essas áreas demonstram seis características principais que estão interconectadas e com as quais elas podem oferecer níveis elevados de relevância para os CIOs, além de gerar valor para suas empresas.

Uma área de auditoria interna de TI bem-sucedida:



### 1 Alinha-se à estratégia de negócios e de TI

Executivos, conselhos e comitês de auditoria de grandes empresas esperam que as áreas de auditoria interna de TI voltem sua atenção para os riscos de tecnologia envolvidos na concretização da estratégia de negócios. Por isso, as melhores áreas de auditoria interna de TI são proativas no sentido de eliminar *checklists* tradicionais de auditorias de TI que listam tarefas que elas “deveriam” estar executando. Em vez disso, elas se envolvem com os *stakeholders* para descobrir exatamente o que eles deveriam estar fazendo para apoiar suas empresas e os objetivos do negócio. Com esse tipo de engajamento, essas áreas conseguem ter um panorama dos objetivos estratégicos, operacionais, de comunicação e de *compliance* que estão por trás dos investimentos em TI das empresas. Elas se apoiam nesse entendimento para conduzir a avaliação de riscos de auditoria interna de TI, o plano de auditoria e a alocação de recursos. Essas áreas de auditoria de TI alinham o cronograma e o escopo dos serviços de auditoria e de consultoria às prioridades de TI da empresa, gerando valor de forma proativa. Com o tempo, elas se adaptam, juntamente com suas empresas, aos novos riscos e oportunidades que surgem.

2



### 2 Atua como consultora estratégica e confiável

As áreas de auditoria interna de TI estão especialmente preparadas para ajudar na avaliação e gestão dos riscos crescentes de TI. As áreas mais eficazes prestam serviços com valor agregado e oferecem consultoria proativa que vai muito além da execução do plano anual de auditoria de TI. Para isso, elas fornecem *insights* mais aprofundados sobre aspectos emergentes de TI e, assim, ajudam as empresas a entender e administrar de forma proativa os riscos associados à evolução digital. Por exemplo, a área de auditoria interna de TI de uma empresa de gestão de ativos desenvolveu relacionamentos baseados em confiança com o seu CIO e o diretor de Segurança da Informação (CISO). Todos contribuem regularmente para as discussões sobre segurança cibernética e para a implementação de novas soluções empresariais capazes de gerenciar com eficácia os riscos do negócio.

3



### 3 Inova por meio de análises e tecnologia

Investir em análises de dados e ferramentas tecnológicas para inovar em processos é uma prioridade para as áreas de auditoria interna de TI eficazes. O objetivo da análise de dados não é apenas automatizar procedimentos isolados de auditoria, mas transformar a atuação da auditoria interna. A análise de dados faz parte da avaliação de riscos e de todo o processo de planejamento, execução e elaboração de relatórios da auditoria. É importante também perceber e aceitar que a inovação não se limita à análise de dados. As modernas áreas de auditoria interna de TI precisam considerar várias ações, como implementar auditorias contínuas ou em tempo real, adotar práticas avançadas de avaliação de segurança cibernética e fazer as alterações necessárias para enfrentar os desafios impostos pelas tecnologias de *blockchain* ou de robótica. As áreas de auditoria de TI eficazes estão ajudando a auditoria interna, de modo geral, a evoluir aproveitando os recursos da análise de dados e das novas tecnologias.

4

#### Comunica-se com o conselho e a administração

Os conselhos de administração estão dedicando cada vez mais tempo para entender riscos, oportunidades e desafios competitivos criados pela tecnologia. Por exemplo, conselheiros de grandes empresas estão dedicando mais de 10% do tempo das reuniões a discutir sobre segurança cibernética e a entender os esforços da administração envolvendo os riscos cibernéticos. Sendo assim, as melhores áreas de auditoria interna de TI se comunicam com o conselho e com a administração fora do contexto dos projetos de auditoria interna de TI e fornecem mais do que relatórios sobre um projeto específico de auditoria interna. As áreas de auditoria interna de TI eficazes oferecem visões fundamentadas sobre novos riscos de TI, além de ideias sobre as causas-raízes de questões temáticas. Essas áreas também colaboram com as mensagens de CIOs e CISOs ao informar, regularmente, sobre riscos relacionados à TI e sobre o progresso das iniciativas de tecnologia e de segurança cibernética, a fim de aumentar a confiança do conselho na TI. Essas comunicações geralmente envolvem esclarecimentos ao conselho ou outras formas de comunicação de caráter informativo ou consultivo.

5

#### Envolve os talentos certos

As áreas de auditoria interna de TI eficazes empregam várias estratégias para alocar as pessoas certas, com as competências certas, nos locais certos e na hora certa. Elas fazem isso usando recursos externos e talentos internos para atender às necessidades de TI e dos negócios. Elas não restringem o escopo do plano de auditoria de TI ou de uma auditoria específica de acordo com o conjunto de competências disponíveis no momento. Por exemplo, as áreas de auditoria de TI eficazes contratam recursos com conjuntos novos e diferentes de habilidades, buscam talentos da TI corporativa e se relacionam com fornecedores de *co-sourcing* a fim de desenvolver as competências de que precisam para lidar com novos riscos e gerar cada vez mais valor. As áreas de auditoria de TI, em geral, buscam recursos com um conjunto não tradicional de habilidades, como segurança cibernética, nuvem, análise de *Big Data* e grandes projetos de integração de sistemas, como ERPs e gestão de terceiros.

6

#### Estabelece um posicionamento executivo

As áreas de auditoria interna de TI eficazes promovem discussões proativas sobre riscos estratégicos enfrentados por suas organizações. Elas criam uma plataforma na qual os líderes podem influenciar outras pessoas e construir uma cultura eficaz de controles de TI por toda a empresa. A liderança dá autonomia a essas áreas para gerar valor e mudanças. Por exemplo, a área de auditoria interna de TI de uma grande instituição financeira realizou vários *workshops* com *stakeholders* de TI e de outras importantes unidades de negócios, como finanças, gestão de riscos, compras e jurídico, com o objetivo de discutir, de forma proativa, riscos e oportunidades envolvendo a adoção da tecnologia de nuvem. Ao influenciar mudanças e decisões sobre a adoção de soluções em nuvem, a área de auditoria de TI da instituição conseguiu usar sua posição para contribuir de forma mais significativa para a área de TI e para os negócios.

# Colaboração com o negócio

A colaboração e a parceria estreitas entre todas as áreas do negócio são necessárias para ampliar o valor das áreas de auditoria interna de TI. Ao desenvolver relacionamentos baseados em confiança com o CIO e a liderança de TI da empresa, as áreas de auditoria interna de TI conseguem entender melhor o que está acontecendo no negócio e nos ambientes de TI, adaptar-se melhor às transformações e se antecipar melhor aos riscos, conseguindo manter a objetividade. A colaboração entre todas as linhas de defesa permite que as áreas de auditoria interna de TI desempenhem um papel ainda mais importante na adoção de novas tecnologias. Por meio da coordenação da gestão de riscos de TI entre os diversos departamentos, as áreas de auditoria interna de TI podem ajudar a garantir que os riscos estejam

sendo tratados de forma eficiente e eficaz, ao mesmo tempo em que mantêm sua objetividade.

Mesmo assumindo funções mais amplas no apoio ao CIO, as áreas de auditoria interna de TI devem continuar a focar questões essenciais. Em vez de apenas fornecer relatórios sobre problemas não identificados durante uma auditoria, elas também devem fazer uma análise de causas-raízes que gere visões mais amplas e que resulte em *insights* mais aprofundados sobre negócios e tecnologia, identificar questões temáticas e avaliar benefícios esperados e custos de remediação. As áreas de auditoria interna de TI também devem indicar aspectos a serem mudados pela administração a fim de acelerar a implementação

de melhorias e, em última instância, reduzir os riscos a níveis aceitáveis. As áreas de auditoria interna de TI devem perceber que é importante conseguir a ajuda necessária para entender as tendências tecnológicas atuais e, só então, ajudar a organização a se antecipar a tais tendências.

Ao trabalhar de forma eficaz com o CIO, as áreas de auditoria interna de TI de alta performance conseguem ir além da mera identificação e comunicação de riscos: elas também são capazes de ajudar proativamente o CIO a reduzir os riscos de negócio que a organização enfrenta em seu processo de transformação tecnológica para evoluir em meio à revolução digital.

## Informações adicionais

Para mais informações sobre esta Perspectiva de Auditoria Interna ou outros assuntos de auditoria de tecnologia, entre em contato com:

**André Pannunzio**  
Sócio e líder de auditoria  
interna da PwC Brasil  
andre.pannunzio@pwc.com  
(11) 3674-3850

**Rosana Napoli**  
Sócia de auditoria  
interna da PwC Brasil  
rosana.napoli@pwc.com  
(11) 3674-3753



 PwC Brasil  @PwCBrasil  @PwCBrasil  PwC Brasil  PwC Brasil  PwC Brasil

Neste documento, "PwC" refere-se à PricewaterhouseCoopers Brasil Ltda., firma membro do network da PricewaterhouseCoopers, ou conforme o contexto sugerir, ao próprio network. Cada firma membro da rede PwC constitui uma pessoa jurídica separada e independente. Para mais detalhes acerca do network PwC, acesse: [www.pwc.com/structure](http://www.pwc.com/structure)

© 2017 PricewaterhouseCoopers Brasil Ltda. Todos os direitos reservados

(DC0) Informação Pública

Versão: Novembro/2017 [F239]