

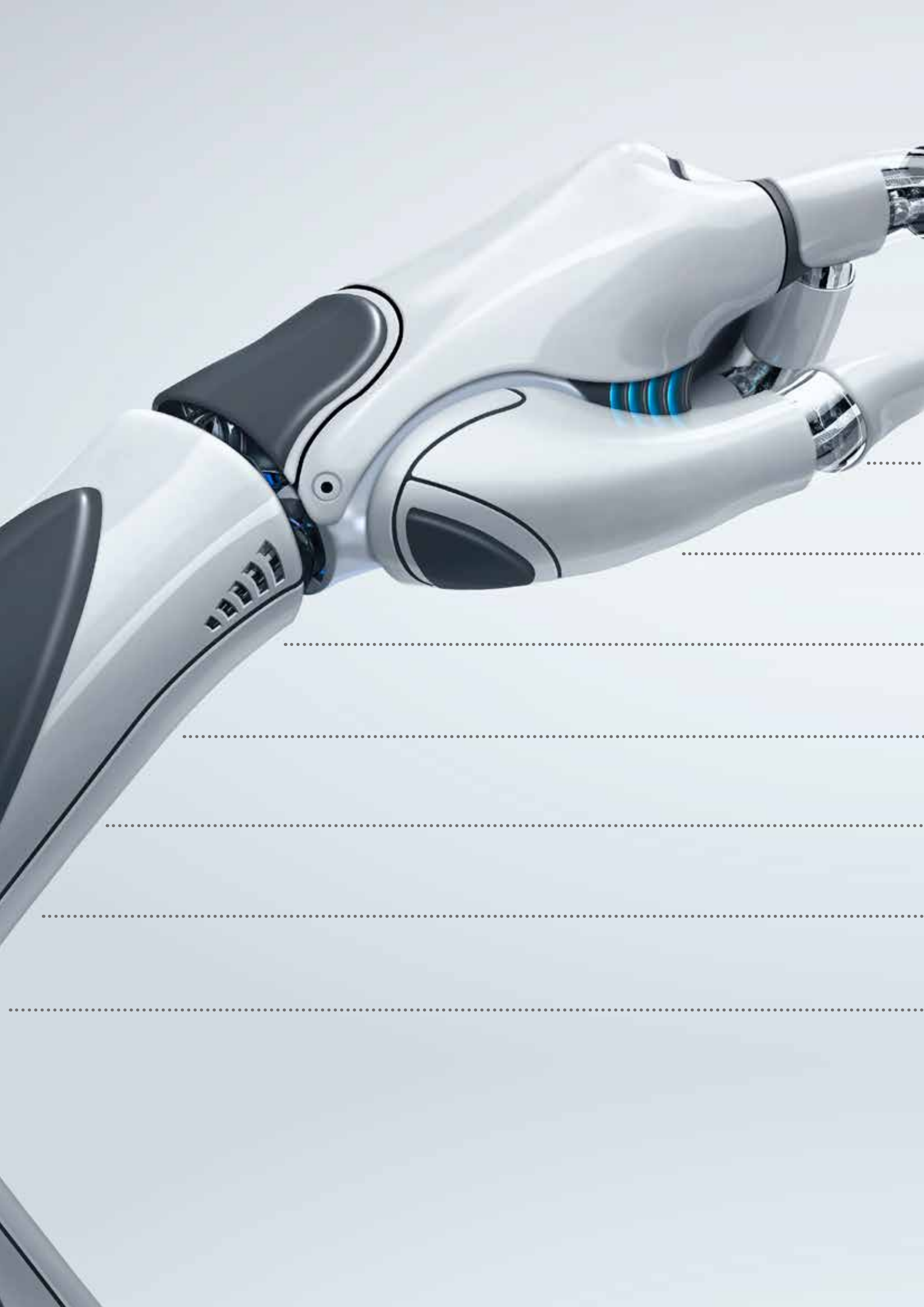


# Mudança do panorama das tecnologias emergentes

**Pesquisa acerca dos riscos associados  
às tecnologias emergentes que  
impulsionarão a transformação dos  
negócios no futuro.**

[kpmg.com.br](https://www.kpmg.com.br)







# SUMÁRIO

04 Prefácio: a ruptura é a nova norma para risco tecnológico?

---

06 As tecnologias emergentes continuam emergindo?

---

10 Garantindo ao risco tecnológico um lugar à mesa

---

14 Rebatendo o mito em torno das métricas

---

18 Provas de talentos

---

20 Repensando dados de risco e relatórios

---

24 Considerações finais: criação de gerenciamento de risco tecnológico da próxima geração

---

26 Metodologia da pesquisa e dados demográficos

---

29 Como a KPMG pode ajudar

# Prefácio: a ruptura é a nova norma para risco tecnológico?

**“Temos o prazer de compartilhar os resultados da nossa pesquisa de gerenciamento de risco das tecnologias emergentes. Com a análise dos dados, um fator ficou absolutamente claro: os métodos tradicionais de avaliação de risco tecnológico evaporaram e as empresas precisam criar uma organização de riscos de tecnologia ágil e dinâmica, para acompanhar o ritmo da mudança. A pergunta é: “Como?” Por meio desta pesquisa, tentamos lançar luz sobre algumas perspectivas que as organizações líderes estão tomando para construir uma tecnologia voltada para o futuro.”**

– Vivek Mehta, Sócio

**“Empresas e executivos estão enfrentando o desafio da transformação digital, que inclui, mas não se limita às diversas tecnologias emergentes. A transformação digital deve ocorrer em ciclos de inovação nos próximos anos e exigirá das empresas e executivos não apenas atualização tecnológica, mas, também, uma mudança de cultura e habilidades. Dentre as principais adaptações, se destaca a necessidade de uma estrutura de gestão de riscos robusta e ao mesmo tempo dinâmica. Por meio desta pesquisa sobre a mudança do panorama das tecnologias emergentes, buscamos trazer ao mercado informações que auxiliem a jornada de transformação digital.”**

– Marcelo de Angelo, Sócio

Bem-vindo à quarta revolução industrial. Em meio a ela, o controle sobre o ambiente de tecnologia é absolutamente vital, mas consistentemente indescritível.

Em bancos, hospitais, indústrias e empresas de tecnologia, essa é a realidade que as organizações enfrentam hoje em quase todos os setores. Por quê?

Por um lado, softwares e sistemas alimentam cada vez mais as principais atividades do negócio. A tecnologia é incorporada aos processos operacionais mais críticos, suportando o trabalho de funções de *back end* e *front end*. Isso significa que as implicações de erros, falhas ou violações podem ser graves do ponto de vista operacional, financeiro e de reputação.

Uma pesquisa com mais de 4.000 CIOs globais, da KPMG International e Harvey Nash, descobriu que os líderes de TI estão totalmente focados em navegar na incerteza à luz das mudanças políticas, comerciais e sociais. Somando-se à incerteza, há o aumento implacável de organizações que estão sujeitas a “grandes” ataques cibernéticos. De fato, a vulnerabilidade da segurança cibernética está na maior alta de todos os tempos.

Em segundo lugar, vivemos em um mundo disruptivo. Os dados proliferam e a tecnologia está se tornando mais complexa. Da automação à inteligência artificial (IA), à Internet das coisas (IoT), ao *big data* e aos aplicativos e serviços digitais voltados ao cliente, o ritmo acelerado das mudanças tecnológicas representa uma das maiores ameaças às empresas.

A pesquisa de 2018 da KPMG sobre o cenário em mudança das tecnologias emergentes descobriu que as maiores barreiras à comercialização são as seguintes:

47% Gerenciamento de riscos e segurança cibernética

25% Conformidade e regularização

28% Governança de privacidade

Além disso, observou-se que a inteligência artificial, a computação cognitiva, a IoT e a robótica são as quatro principais tecnologias que impulsionarão a transformação dos negócios nos próximos quatro anos. Dentro das organizações, essa rápida evolução da tecnologia está colocando o risco tecnológico no centro das atenções e ampliando o perfil da função de gerenciamento de risco tecnológico, de salas de servidores a salas de reuniões.

À luz desse cenário desafiador, a KPMG decidiu explorar a situação atual do risco tecnológico em diversos setores, pesquisando sobre como os líderes de risco em tecnologia das empresas estão:

**Lidando com tecnologias emergentes e complexidade tecnológica**

**Identificando, gerenciando e medindo de forma proativa os riscos de tecnologia**

**Transformando riscos tecnológicos baseados em custos em direcionadores estratégicos de valor**

O presente relatório apresenta as principais descobertas da pesquisa realizada pela KPMG para desvendar percepções sobre as abordagens da próxima geração em relação ao risco tecnológico – melhores práticas que permitem às organizações que operam na era digital recuperar o controle sobre seus ativos de tecnologia, processos e pessoas.

Esperamos que este relatório contenha as orientações de que você precisa para começar a criar uma função de risco tecnológico mais eficaz.

## O que falam os CIOs?



**20%**

dos CIOs dizem que o ambiente político, comercial e econômico está se tornando mais imprevisível.



**35%**

dos CIOs estão focados na criação de uma plataforma de tecnologia mais ágil para responder.



**43%**

dos CIOs estão investindo em segurança cibernética.



**21%**

das organizações foram vítimas de um grande ataque cibernético em 2018.

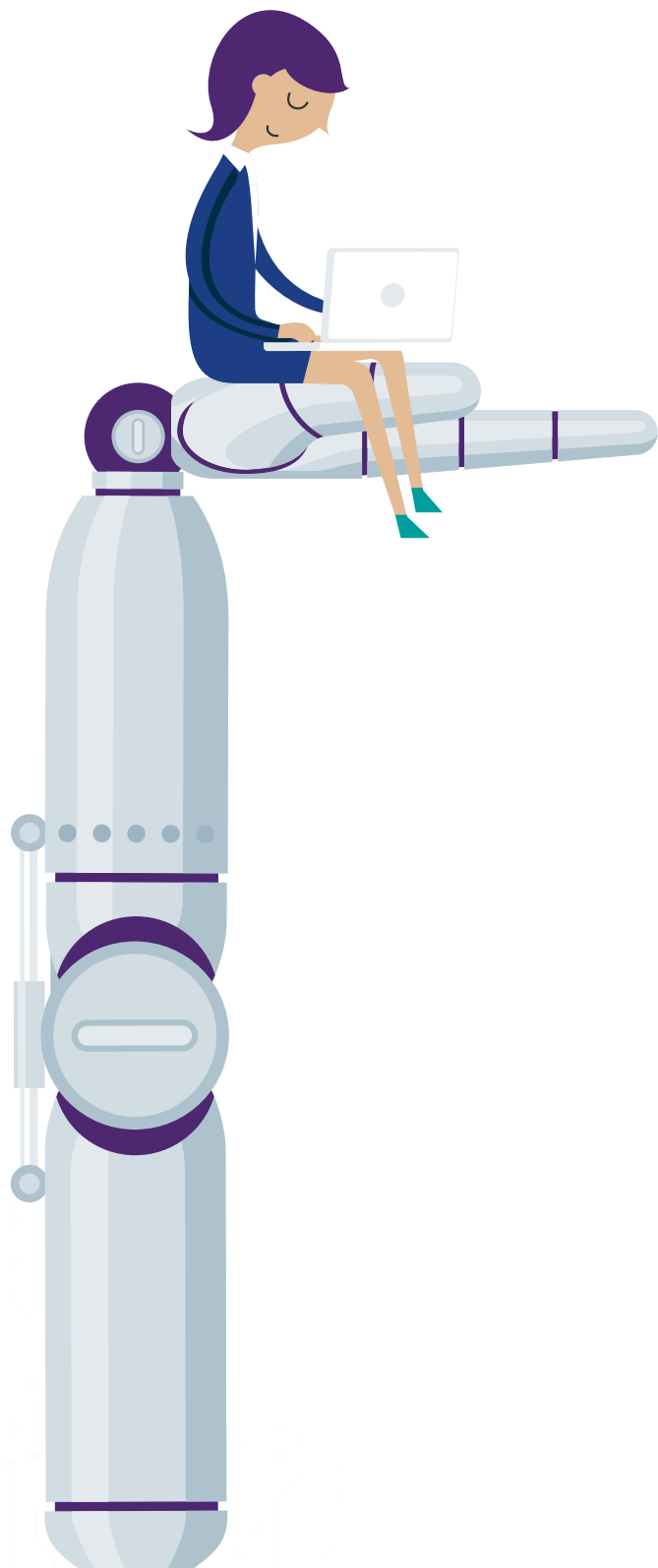
# As tecnologias emergentes continuam emergindo?

Computação em nuvem. Dispositivos conectados. *Going digital* e *Going mobile*. Robótica. *Blockchain*. A quarta revolução industrial chegou. Na verdade, essas tecnologias antes emergentes já existem há algum tempo. Adotá-las não é mais uma opção; é mandatório para competir no século 21.

A velocidade da mudança tecnológica nunca foi mais rápida do que é agora.

Para as empresas, a velocidade de implantação da tecnologia é fundamental para o seu sucesso e a sua sobrevivência, mas não pode ser à custa da saúde da organização ou de seus *stakeholders* e clientes.

Nos departamentos de TI de muitas organizações, tem havido um forte foco em permitir rapidamente tecnologias emergentes para que a empresa possa aproveitar os benefícios prometidos – de melhor experiência do cliente e maior eficiência operacional para impulsionar os lucros. No entanto, nossos dados mostram que, quando se trata de inovação tecnológica, muitas empresas lutam para equilibrar a necessidade de velocidade e agilidade com a necessidade de controle.



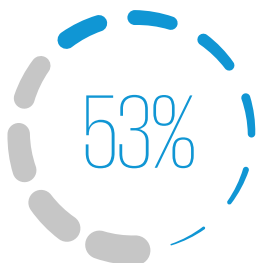
## Sua organização está investindo ou investiu no último ano em tecnologias emergentes?



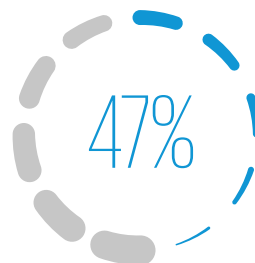
**85%** das empresas estão investindo ou investiram em tecnologias emergentes no último ano.



**Fatores que causariam  
uma expansão do escopo  
do gerenciamento de  
riscos de tecnologia:**



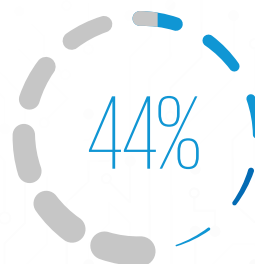
Tecnologias emergentes tornam-se predominantes no setor de nossa organização.



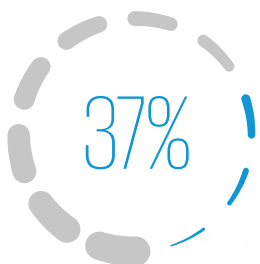
Novas tecnologias são identificadas com um grande potencial de adoção organizacional.



Novas tecnologias são implantadas em nossa organização.



Nossa organização tem pontos de falha no gerenciamento de riscos, controle ou conformidade.



Uma mudança de regulamentação exige que nossa organização aplique uma nova perspectiva em relação ao risco de TI.

**“A gestão do risco tecnológico precisa evoluir para estar preparada para o novo mundo no qual a interrupção é normal. Isso significa que os líderes de risco de TI devem parar de olhar para o volante e olhar para onde a organização está caminhando.”**

– Phil Lageschulte, Sócio

# Risco tecnológico ágil

O futuro profissional de risco tecnológico precisará desmistificar os riscos da nova tecnologia emergente e desenvolver uma estrutura de tecnologia ágil, com flexibilidade suficiente para responder a novos riscos. Essa estrutura incluirá uma avaliação de risco dinâmica que combine o apetite de risco da organização com a adoção de novas tecnologias.

Algumas empresas estão tomando medidas para cumprir essa promessa. Por exemplo, vemos clientes aproveitando a análise de dados e o monitoramento contínuo para mudar a maneira como gerenciam o risco tecnológico.

A razão pode ser que apenas uma parte das organizações possua *know-how* para identificar e gerenciar os riscos associados. Mas esse é o papel da função de risco tecnológico.

É claro que a inovação e o controle tecnológico devem andar de mãos dadas. Afinal, quando os riscos relacionados às novas tecnologias são gerenciados com habilidade, as organizações podem se sentir muito mais confiantes em liberá-las em escala.

**Dentre 85% das empresas que estão investindo ou investiram em tecnologias emergentes no último ano, as seguintes tecnologias estão sendo adotadas:**



32%

Aplicativos e dispositivos móveis



20%

Internet das coisas



38%

Cloud computing



8%

Inteligência artificial



4%

Robótica e processos automáticos



0%

Computação cognitiva



4%

Blockchain



0%

Impressoras 3D



## Como as organizações que estão passando pelo impacto da transformação digital equilibram cuidadosamente os temas inovação e controle?

Começa com o envolvimento do risco de tecnologia no planejamento estratégico, com investimentos e esforços em capacitação.

A função de risco de TI deve conectar-se e entender a estratégia de negócios mais ampla, e concentrar-se em incorporar antecipadamente

algum gerenciamento básico de riscos nos esforços de adoção de tecnologia e não no *back end*.

Em nossa experiência, o sucesso na incorporação do risco de TI à estratégia inicial de mudança de tecnologia geralmente se resume a vários fatores-chave:

### 1 A cultura de liderança no topo da organização de tecnologia.

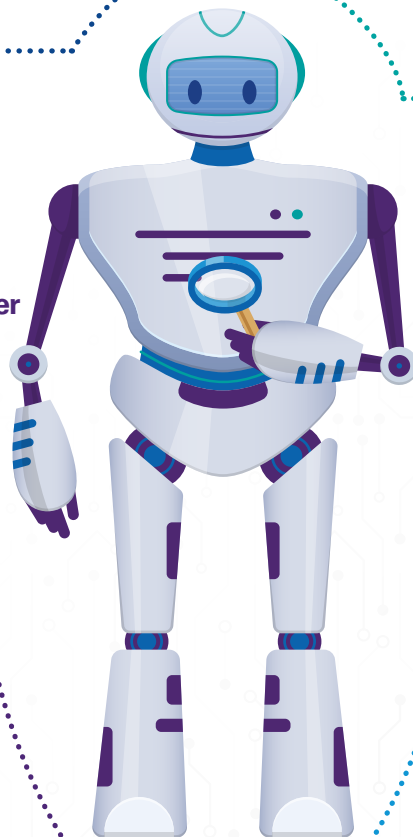
Como os líderes de tecnologia adotam, apoiam e orientam uma cultura de gerenciamento de riscos? Onde o risco tecnológico está posicionado? Para quem ele se reporta? O que isso traz de benefícios?

### 2 Onde os profissionais de risco tecnológico estão posicionados na estrutura organizacional e com quem eles colaboram

Os profissionais de risco tecnológico devem colaborar estreitamente com as equipes de planejamento estratégico, incluindo equipes de planejamento de negócios, inovação e capacitação de tecnologia.

### 3 A disposição dos líderes de risco tecnológico para mudar sua visão de “não deveria ser feito” para “como isso pode ser feito com menos riscos”

Algumas equipes de risco tecnológico são muito rígidas em relação aos riscos associados à tecnologia emergente e, portanto, são marginalizadas ou mantidas afastadas do processo de planejamento estratégico, o que acaba impedindo o processo de inovação por causa da resistência e da negatividade. Em vez disso, elas devem ajudar a possibilitar e apoiar o crescimento dos negócios.



### 4 O talento certo.

Embora a lacuna de habilidades seja uma questão de risco tecnológico, a questão do talento é mais sobre conscientização do que sobre capacidades. Responsáveis de risco de TI devem educar a si próprios e seus profissionais sobre questões de macronegócios, portanto, a função de risco tecnológico tem o conhecimento e a compreensão necessários para efetivamente incorporar *insights* de risco nas discussões e decisões estratégicas.

# Garantindo ao risco tecnológico um lugar à mesa

Com a tecnologia cada vez mais presente em quase todos os aspectos do negócio, mais líderes de nível C agora reconhecem a conexão direta entre risco de TI e risco corporativo - e mais amplamente a estratégia corporativa. Como tal, muitas organizações estão começando a ver o risco tecnológico como um centro de valor que ajuda a atingir objetivos críticos de negócios.

**“Quando se trata de tecnologia, o risco é sempre um potencial. Esse potencial pode entrar em erupção, causando uma questão regulatória, de cliente ou de segurança que pode ter enormes consequências financeiras ou de reputação. Ou ainda pode nunca se manifestar em um evento real. Se o gerenciamento de risco não for incorporado no início, as empresas estarão apostando na sorte. É como comprar uma apólice de seguro que você talvez nunca acabe usando, mas, se for preciso, ficará muito agradecido por tê-la comprado.”**

– Phil Lageschulte, Sócio



O risco tecnológico é percebido como fator que gera valor para a empresa.

85% dos líderes de risco tecnológico acreditam que esse risco está gerando valor para a organização.



Risco tecnológico e colaboração de negócios estão em alta.

91% dos líderes de risco tecnológico relatam comunicação proativa entre funções.



Os gastos com o risco tecnológico devem acelerar.

84% dos líderes de risco tecnológico dizem que os investimentos nessa área aumentarão nos próximos três anos.

# Além da conformidade

Apesar do perfil crescente da função do risco tecnológico, os resultados da pesquisa indicam que os profissionais de risco de negócios e de tecnologia ainda não se envolvem ativamente o suficiente para gerenciar riscos de maneira proativa. A função do risco tecnológico pode maximizar o impacto apenas quando incluída no limiar das iniciativas do projeto.

De acordo com os dados de nossa pesquisa, a maioria das organizações não considera o risco tecnológico isoladamente. Em vez disso, veem o risco tecnológico como um braço de conformidade ou segurança cibernética.

Consideram o risco tecnológico parte da gestão de conformidade

50%  
das organizações



Veem o risco tecnológico isoladamente

14%  
das organizações



Consideram o risco tecnológico parte da gestão de segurança cibernética

36%  
das organizações



Também descobrimos que, muitas vezes, as equipes de risco tecnológico só são incluídas nos projetos após o surgimento de problemas. Nesta fase, o impacto que eles são capazes de gerar é mínimo.

Como resultado, o negócio está exposto a mais riscos.

Equipes de risco tecnológico incluídas em projetos após o surgimento de problemas

43%



Outras pesquisas da KPMG reforçam o fato de que o risco tecnológico tem maior papel a desempenhar quando se trata de proteger a organização do risco - especialmente em relação à segurança cibernética.

De acordo com pesquisa realizada pela KPMG em 2017, apenas 40% dos CEOs diziam que suas organizações estavam bem preparadas para um evento cibernético.

Além disso, a KPMG descobriu que uma parte significativa dos incidentes de tecnologia são evitáveis, com as precauções corretas.

Ao envolver os profissionais de risco tecnológico desde o início, exercendo rigor ao testar sistemas, e construindo o nível certo de resiliência para permitir a implementação de ações mitigatórias, a maioria dos incidentes poderia ser evitada.



● Apenas  
**77%**  
das empresas estão bem preparadas para o evento cibernético.



● Mais de  
**20%**  
de incidentes são causados por falhas no software.

## **Violações de *blockchain* são mais prevenidas com uma robusta gestão de riscos tecnológicos**

Sejam sistemas legados ou novas tecnologias, uma das principais causas subjacentes da maioria das falhas tecnológicas é a mesma: não incluir o risco tecnológico em conversas estratégicas iniciais e de alto nível.

A KPMG estudou dois recentes incidentes cibernéticos relacionados à tecnologia *blockchain*.

As vulnerabilidades e falhas de design poderiam ter sido identificadas e corrigidas antes das violações, se as empresas afetadas tivessem contratado profissionais de risco tecnológico para realizar revisões de segurança completas e formais, de ponta a ponta.

## Como a gestão de riscos tecnológicos pode ganhar relevância e aumentar seu valor ao negócio?

**1** Por um lado, os líderes de risco tecnológico devem estabelecer um plano de atividade e um menu de serviços que se alinhem com as atividades diárias e que sejam baseados em projetos do grupo de TI que suportam diretamente os negócios. Por exemplo, o risco tecnológico poderia alinhar suas atividades com os projetos prioritários no ciclo orçamentário anual de TI, tornando-se um fluxo de trabalho direto desses projetos.

**2** Também é importante que os profissionais de risco tecnológico participem de comitês e grupos focais que estejam buscando novos produtos ou serviços, com foco em esclarecer os riscos potenciais.

**3** Além disso, os profissionais de risco de alto nível da tecnologia devem interagir regularmente com o CIO, o CISO, o CRO e o COO. Anualmente, o risco tecnológico também deve reportar-se ao comitê de risco do conselho.

É claro que, em reuniões de status e outros pontos de contato com as lideranças operacional e de TI, os responsáveis pelo risco tecnológico devem ser muito claros sobre qual valor a função traz e qual autoridade eles têm nessas discussões.

Na verdade, em conversas com executivos, os líderes de risco tecnológico devem assumir o papel de “desafiantes” amigáveis - usando sua perspectiva de risco para ajudar a pensar em assuntos de negócios e questionar decisões que possam aumentar o perfil de risco da organização, seja a introdução de uma nova tecnologia ou a entrada em um novo mercado. Para serem desafiadores e eficazes, profissionais de risco tecnológico precisam de amplo conhecimento da estratégia e dos processos de negócios, bem como da experiência e seriedade para falar com confiança. Isso exigirá que o risco tecnológico preencha a lacuna de habilidades e alavanque os dados de forma mais eficaz, o que discutiremos mais adiante no relatório.

**4** Por fim, estabelecer uma mensagem clara da liderança fará com que a empresa deseje colaborar ativamente com o risco tecnológico. Isso exige um duplo esforço tanto pelos profissionais de risco tecnológico como de sua liderança de negócios. Eles devem trabalhar juntos para mostrar à organização inteira que o risco tecnológico merece ser uma parte crítica do processo de tomada de decisões estratégicas, seja sobre adoção de uma nova tecnologia ou qualquer iniciativa de transformação de negócios.

**“Para elevar o papel do risco tecnológico, o profissional deve ter uma compreensão mais ampla dos objetivos organizacionais da estratégia de tecnologia e servir como consultor de risco.**

**O conjunto de habilidades e capacidades é crítico.**

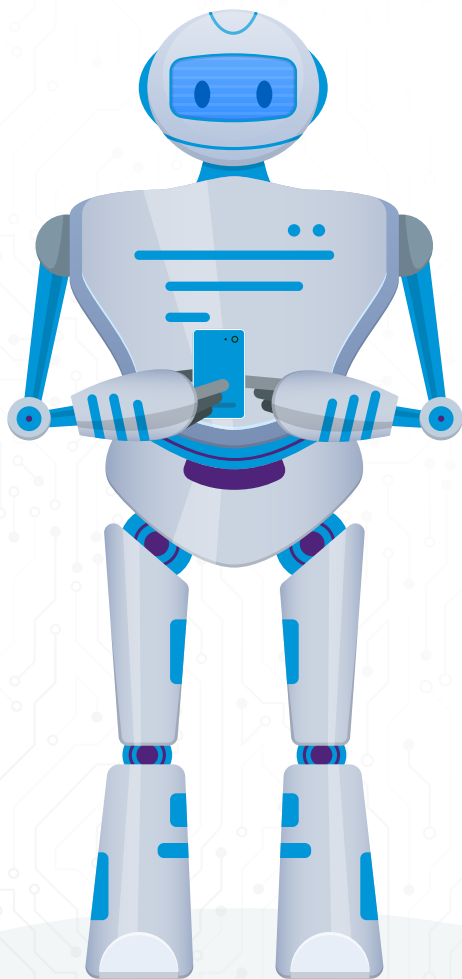
**Quando a área de risco tecnológico tem as pessoas certas fazendo as perguntas certas, o negócio, a tecnologia e as partes interessadas virão naturalmente.”**

– Kiran Nagaraj, Managing Director

# Rebatendo o mito em torno das métricas

As organizações definem o universo de risco de TI como todos os riscos tecnológicos que poderiam impactar os negócios. Geralmente, é um grande número. Para entender e gerenciar esses riscos, a maioria das organizações pesquisadas usam indicadores de risco (KRIs) – medidas para aferir a probabilidade de que eventos de risco individuais prejudiquem a organização.

**As empresas estão aproveitando a análise de dados para desenvolver os principais indicadores de risco?**



## Métricas significativas

Embora os clientes estejam cada vez mais conscientes do conceito e do valor dos KRIs, e a adoção e implementação de KRIs sejam amplamente difundidas em alguns setores, os KRIs nem sempre correspondem aos riscos tecnológicos reais enfrentados pela organização.

## Os riscos não são óbvios .....

Às vezes, os riscos não são óbvios. Pode haver inúmeras razões pelas quais as empresas não têm total transparência no escopo dos riscos tecnológicos que podem afetá-las.

## KRIs são vistos apenas ..... individualmente.

Talvez os KRIs sejam vistos apenas individualmente, em vez de coletivamente. Ver os KRIs juntos, em vez de individualmente, leva a uma compreensão mais profunda do risco e ao apelo a uma ação mais forte. No entanto, muitas organizações estão lutando para racionalizar e consolidar vários sistemas corporativos em toda a tecnologia e suas funções. Quando não há uma fonte única de dados, é difícil ter uma boa noção de quais dados você possui, mais ainda classificá-los, categorizá-los e compreendê-los.

## KRIs emergem de partes desconhecidas do negócio. ....

Os KRIs podem emergir de partes do negócio que tradicionalmente não estão familiarizadas com a função de risco tecnológico.

Por exemplo, as organizações podem se concentrar excessivamente na conformidade e nos controles, em vez de no gerenciamento de riscos. Por isso, não definem os KRIs para riscos que estão fora do escopo dessas áreas, como auditoria, regulamentação e conformidade. Como tal, os riscos emergentes, como aqueles associados à segurança cibernética, automação, computação em nuvem ou inteligência artificial, podem ser negligenciados.

## Má qualidade dos dados. ....

A qualidade dos dados também pode afetar a eficácia dos KRIs. Se os KRIs forem baseados em dados de baixa qualidade, os líderes empresariais podem hesitar em agir com base nesses KRIs.



# Usando os KRIs

## Como as organizações podem usar os KRIs de maneira mais eficaz para avaliar os seus riscos tecnológicos mais relevantes

Descobrimos que os KRIs eficazes possuem as seguintes características:

- Um conjunto menor de métricas, que geralmente é mais fácil de manter, monitorar e gerenciar.
- Eles servem como uma medida de risco. Suas definições são acordadas pelas principais partes interessadas para servir como uma medida de risco, em vez de uma questão única, erro ou evento.
- Eles têm dados de suporte subjacentes, normalmente armazenados em um dicionário de dados que inclui uma fórmula métrica, elementos de dados e taxonomia de risco, que permite que a área de risco tecnológico mapeie e rastreie riscos do nível de unidade de negócios para a empresa.
- Eles são mensuráveis e acionáveis. Eles se vinculam diretamente ao impacto nos negócios, permitindo que o risco tecnológico esteja alinhado com o negócio em termos significativos.
- Eles são regularmente mantidos, monitorados e atualizados. Quando uma métrica apresenta variação relevante, alguém presta atenção, toma uma decisão e executa uma ação.

**“As limitações para alavancar os KRIs no espaço de risco de TI incluem:**

- **Um foco em conformidade e controles, em vez de gerenciamento de riscos.**
- **Pressão contra o investimento em risco de TI.**
- **Fontes de dados não confiáveis, correlação de dados e risco.**
- **Dificuldade em determinar os critérios de medição de risco e a subjetividade desses critérios.**
- **Falta de confiança nas ações tomadas com base nas medições do KRI.**
- **Falta de clareza sobre quem escala os resultados do KRI para autorização final da ação.”**

– Joshua Galvan, Principal

**“Com o crescente impacto da tecnologia emergente na maioria das indústrias, a velocidade do risco passa a ser critério absolutamente necessário na fórmula de gerenciamento de risco tecnológico.”**

– Vivek Mehta, Partner

## Melhores práticas de risco tecnológico para superar os desafios de alavancar os KRIs:



### DESENVOLVER UMA MENTALIDADE DE RISCO PARA TODA A ORGANIZAÇÃO

Quando o risco de TI é prioridade em toda a organização, ele ajuda a tecnologia a criar confiança e suporte ao desenvolvimento de KRI. Há muitas maneiras criativas de desenvolver uma mentalidade de risco para toda a organização, como recompensar atividade de gerenciamento de risco, especialmente em equipes de desenvolvimento e entrega de soluções de tecnologia.



### INCORPORAR FERRAMENTAS E PRÁTICAS DE CORREÇÃO DE RISCO EM TI

Muitos líderes de negócios acham que, cada vez que identificam um risco, precisam recomeçar a maneira de corrigi-lo. Na realidade, pode haver boas práticas que já existem no ambiente.



### Aproveitar os recursos de medição de risco existentes

As funções de risco não relacionadas à tecnologia têm KRIs predefinidos e próprios, com os quais a empresa já está familiarizada. Se o risco tecnológico adotar esses KRIs, o tempo de implementação poderá ser reduzido.



### Vincular identificação de risco a objetivos estratégicos de negócios

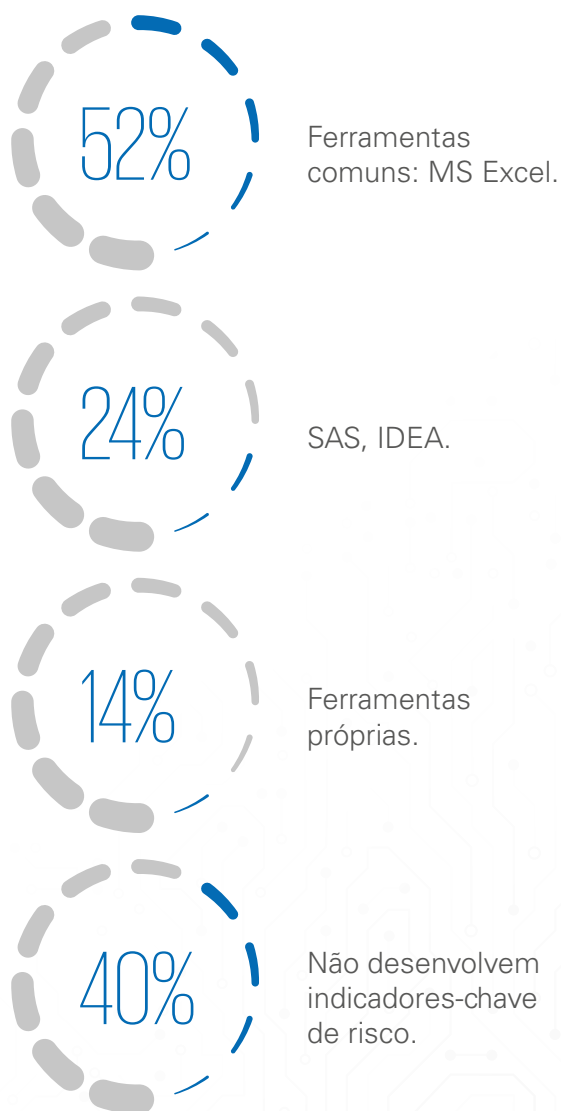
Para identificar e avaliar adequadamente os verdadeiros riscos tecnológicos da organização, os profissionais de risco da tecnologia precisam se envolver e se integrar de forma proativa com as unidades de negócios. Isso não apenas permite que o risco tecnológico traga mais valor, mas ajuda as organizações a evitar esforços duplicados com outras equipes, como o gerenciamento de riscos corporativos.

# KRIs preditivos

Em toda essa conversa sobre métricas de risco, ainda não mencionamos o que talvez seja o tipo mais importante: KRIs preditivos. Dados sobre riscos tecnológicos podem ser empregados para estabelecer padrões que podem ajudar a prever potenciais problemas antes que eles aconteçam. E KRIs preditivos são ideais para um gerenciamento proativo de riscos tecnológicos. Entretanto, apenas 29% das empresas pesquisadas alavancam consistentemente o risco preditivo.

**Muitas organizações ainda estão usando ferramentas comuns, como o MS Excel, para desenvolver indicadores-chave de risco ou KRIs:**

**Quais ferramentas as organizações utilizam para o desenvolvimento de indicadores-chave de risco:**



**“Para aumentar sua capacidade de prever o risco tecnológico, as empresas devem investir em recursos analíticos e cognitivos, relatórios efetivos de painel e melhor confiabilidade e acesso a dados.”**

– Joshua Galvan, Principal

Muitas organizações não adotaram os KRIs preditivos, em parte devido a questões de viabilidade e praticidade. Desafios de recursos desempenham um papel importante. Embora os KRIs preditivos possam ser valorizados, eles podem não ser totalmente aceitos pelas partes interessadas do negócio, que preferem usar os recursos em outro lugar, inibindo assim o gerenciamento de risco. Por exemplo, se o KRI indicar uma necessidade de reorientar pessoas, sistemas ou investimentos para antecipar um problema, isso pode surgir como um sacrifício para outras prioridades operacionais, de conformidade e de gerenciamento de riscos.

Os resultados da pesquisa também indicam que algumas organizações utilizam ferramentas de terceiros, como SAS e IDEA, para desenvolver indicadores preditivos de risco. No entanto, não está claro se eles estão usando os resultados das ferramentas em seus relatórios de risco ou para gerenciamento proativo de riscos.

# Provas de talentos

De acordo com os dados da pesquisa, em todos os setores, o maior desafio do risco tecnológico é a dificuldade em encontrar recursos com capacitação adequada. Isso reflete um problema comum a toda a TI.

Em cada um dos últimos quatro anos, 60% dos entrevistados na CIO Survey, realizada pela KPMG International em conjunto com a Harvey Nash, relataram escassez de habilidades, com *big data* / *analytics* no topo da lista de habilidades mais demandadas.

A dificuldade em encontrar recursos com capacitação adequada é responsável por muitos dos desafios para demonstrar a capacidade do risco tecnológico em agregar valor.

## Novos conjuntos de habilidades

Como mencionado anteriormente, para que os profissionais de risco tecnológico realmente agreguem valor, eles devem participar de discussões de estratégia de *front end*, especialmente à medida que novas tecnologias disruptivas entram na organização. Os profissionais de risco tecnológico precisam ficar ativamente à frente do que está acontecendo no negócio em relação às tecnologias disruptivas, realizando avaliação dos riscos, antes que elas sejam adotadas. Ao mesmo tempo, muitas funções de risco tecnológico buscam se tornar mais enxutas e colaborativas com outras equipes de risco para reduzir a redundância e a ineficiência de processos, especialmente no que diz respeito a avaliações e relatórios de risco e conformidade.

Ambas as realidades exigem um novo conjunto de habilidades fundamentais. Os profissionais de risco tecnológico de hoje, em todos os níveis, precisam de:

- Compreensão de negócios
- Compreensão de tecnologia
- Gestão de riscos e compreensão de controles
- Capacidade de compreender os dados de risco de um contexto de negócios



Percepção de que o risco tecnológico afeta o tempo de comercialização.

55%



Recursos / orçamento limitados para risco tecnológico.

45%



**“É difícil desenvolver habilidades para gerenciar os riscos de uma tecnologia nova e desconhecida que ainda não chegou. Entretanto, existem alguns gatilhos que podem ajudar a identificar antecipadamente esta necessidade: um ano ou dois antes que a tecnologia chegue a uma fase piloto em uma grande empresa ou quando está sendo decidido se deve ou não investir ou adotar uma tecnologia específica.**

– Kiran Nagaraj, Managing Director



# Como a tecnologia deve arriscar transformar a força de trabalho para atender às demandas de amanhã?

Algumas organizações estão focadas em treinar profissionais de risco tecnológico com o conhecimento e a mentalidade do negócio necessários para contribuir com importantes discussões de alto nível sobre riscos corporativos. Mas o treinamento é apenas uma parte disso.

Para que a empresa realmente aceite e respeite a função de risco tecnológico, outras mudanças são provavelmente necessárias, como maiores

benefícios e remunerações aos profissionais de risco da tecnologia, localização física perto das principais partes interessadas do negócio e inclusão mais regular nas reuniões da diretoria e da administração.

## Trabalho digital

As funções de risco tecnológico também são desafiadas pelos impactos secundários da automação na força de trabalho e nos negócios. Algumas organizações estão reconhecendo que ferramentas de *big data*, automação, inteligência cognitiva e inteligência artificial podem ser aceleradoras de risco tecnológico.

Portanto, enquanto a rápida adoção de tecnologias de ponta traz uma série de economias de custo e aprimoramentos no modelo de negócios, tais iniciativas de transformação de negócios podem levar a riscos significativos sem que seja dada igual atenção aos impactos sobre a força de trabalho, às implicações sociais e ao alinhamento com os valores centrais de uma organização.

## Como as funções de risco tecnológico devem gerenciar o impacto da automação na força de trabalho?

À luz da mudança do cenário da força de trabalho, as tendências indicam que muitas organizações estão mudando de consumidores de trabalho para construtores de talentos, concentrando-se na criação de oportunidades de carreira resilientes e de longo prazo para os funcionários.



**“As organizações não precisam de mil pessoas fazendo reconciliações se tiverem um sistema que reconcilia com apenas dez pessoas fazendo a supervisão. Esse é o potencial de automação e inteligência artificial e cognitiva.”**

– David DiCristofaro, Sócio

**Executivos entrevistados nessa pesquisa informaram que suas organizações estão aumentando investimentos nas seguintes áreas:**

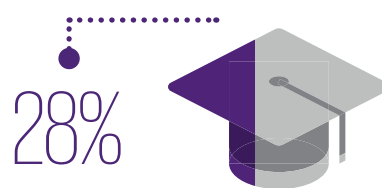
**Recrutamento**



**Infraestrutura digital**



**Treinamento e capacitação**



## Repensando dados de risco e relatórios

Embora 60% dos executivos de risco tecnológico pesquisados relatem que as principais partes interessadas de sua organização confiam em seus dados, as discussões com líderes e clientes da indústria seniores - bem como outras pesquisas da KPMG - nos dizem o contrário.

### INTEGRIDADE DOS DADOS

Os resultados da pesquisa mostram:

#### Executivos de risco tecnológico estão confiantes

60% dos executivos de risco tecnológico relatam que os principais partes interessadas têm alta confiança em seus dados de risco.



No entanto, de acordo com a recente Pesquisa CEO Outlook, da KPMG:

#### CEOs preocupados

Quase a metade dos CEOs questionaram a integridade dos dados sobre os quais baseiam suas decisões.

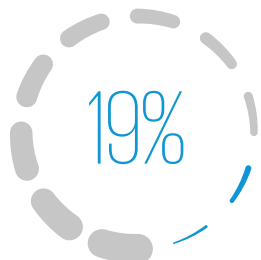


## Método de coleta de dados

Os resultados da pesquisa mostram que apenas a minoria das empresas ainda não formalizou o processo de coleta de dados. A maior parte da coleta de dados para relatórios de risco já é feita por *assessments* de risco ou processos automáticos.

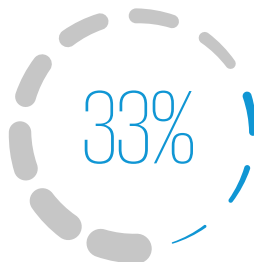
### Processo informal

#### Consultas *ad hoc*



Atividades informais em que dados de risco de TI são coletados por meio de conversas e exemplos.

### Processo automático



#### Dados de risco online

Capacidade automatizada em que dados de risco de TI são coletados por meio de fontes sistêmicas.

### Processo formal

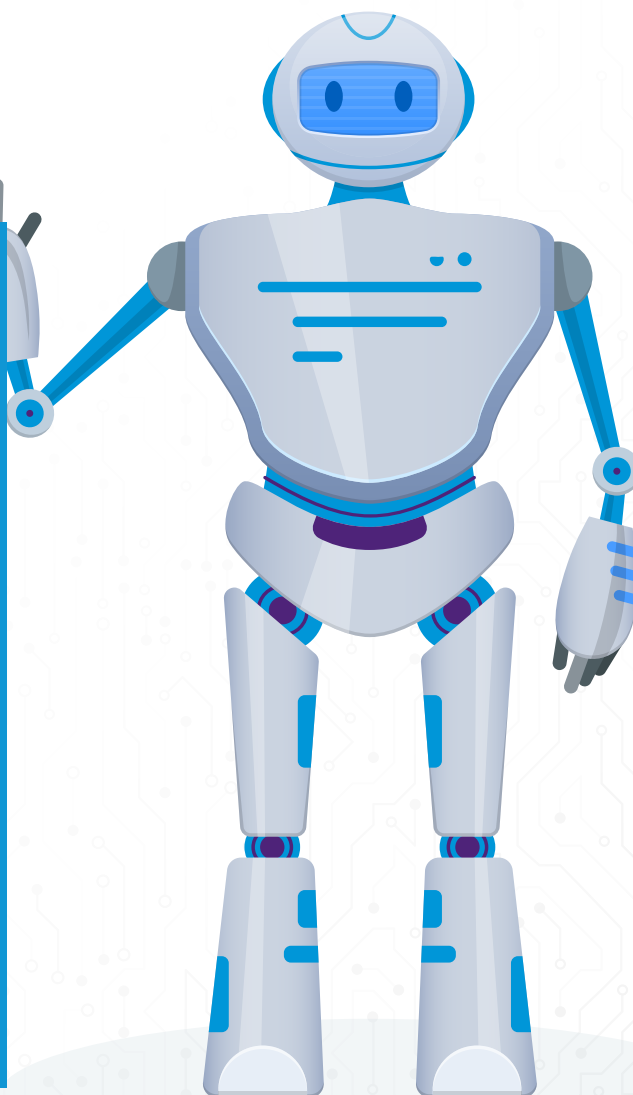
#### Assessments de risco



Atividades formalmente agendadas em que os dados de risco de TI são coletados por meio de um processo padrão e de técnicas rigorosas.

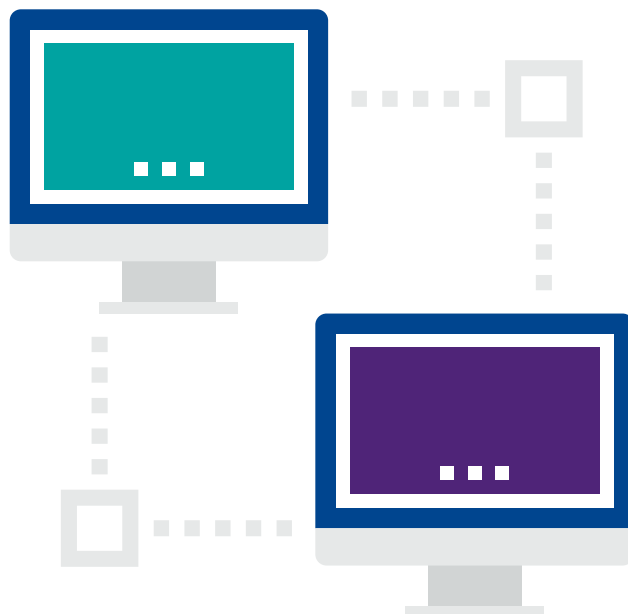
**“Muitas organizações estão considerando o racional entre volume versus qualidade de dados. Embora muitas questões de risco tecnológico sejam colocadas nos dados, o verdadeiro desafio é a falta de consistência sobre quais dados devem ser usados e como. Por exemplo, aplicar os filtros e os critérios corretos na seleção das informações. Ferramentas devem auxiliar na seleção e análise dos dados de maneira significativa e consistente, de modo que seja possível comunicar eficientemente como os resultados das análises afetam os negócios.”**

– Vivek Mehta, Partner



“A maioria dos dados de risco está sendo produzida com base no que está disponível, sem análise prévia do que é necessário saber para a tomada de decisões.”

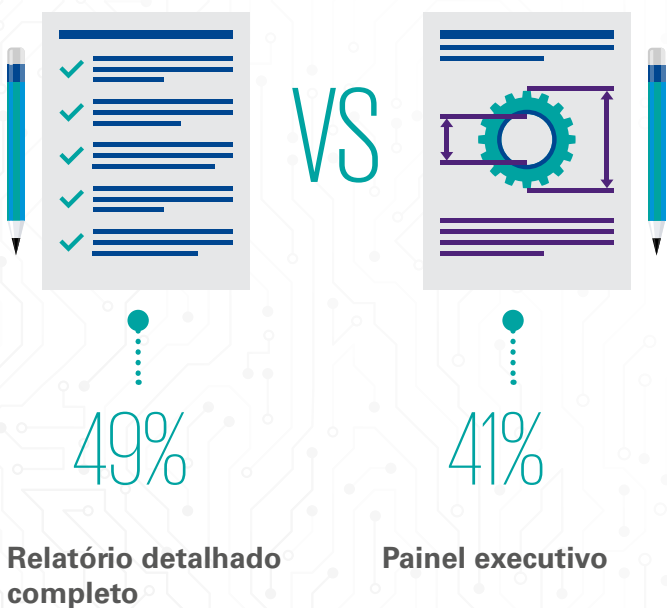
– Robert Westbrook, Principal



## Transformando dados em *insights*

Muitos líderes de risco tecnológico estão claramente fazendo um grande esforço para manter os líderes de negócios seniores informados. Os dados da pesquisa mostram que:

**Os executivos de nível C têm mais probabilidade de receber relatórios detalhados do que painéis com *insights* de alto nível.**



Os detalhes são ótimos, mas também é crítico que o relatório de riscos para a gerência sênior seja compreensível, acionável e impactante.

Um problema comum que os profissionais de risco tecnológico encontram ao relatar seus dados é o escopo, o que pode dificultar a extração de *insights* significativos a partir dele. Os detalhes do relatório devem ser compatíveis com o tipo e o nível de público-alvo.

Além disso, atualmente é muito demorado criar relatórios de risco, especialmente quando os dados são coletados por meio de mecanismos *ad hoc* em vez de sistemas automatizados, sem a devida normatização.

**Uma grande quantidade de volume de dados, com pouca análise e entrega de forma lenta, pode acarretar problemas de entendimento e tomada de ação tardia.**

Quando volumes de dados granulares não estão sendo sintetizados em nível executivo e traduzindo qual é o verdadeiro impacto nos negócios - em tempo real - é difícil para as partes interessadas compreenderem, e, muito mais, agirem a partir das informações que recebem. Como resultado, líderes e diretorias tendem a ignorar os dados.

Muitos líderes de risco tecnológico descobrem que precisam simplificar os problemas e a conversa, além de aprender a falar a mesma língua que as partes interessadas nos negócios.

As funções de risco tecnológico podem abordar os dados de risco e relatar os desafios de várias maneiras.

1

### ESTABELEÇA PADRÕES

Primeiro, a área de risco tecnológico deve estabelecer padrões claros em torno de relatórios de risco e dados de risco, como um dicionário que define fontes e usos de dados. Também é essencial estabelecer processos sólidos de governança de dados para garantir que estes sejam classificados e armazenados corretamente, alocados no grupo apropriado e verificados e testados quanto à qualidade.

2

### CRIE PAINÉIS PERSONALIZADOS

Segundo, para se comunicar de maneira mais eficaz com os negócios, os grupos de risco tecnológico precisam criar *dashboards* e formatos de relatórios personalizados para diferentes públicos, contendo o nível de detalhes apropriado para cada um. Aplicativos digitais e móveis, que permitem que os líderes de negócios visualizem e analisem os dados com facilidade, oferecem potencial para substituir os relatórios de riscos convencionais e, ao mesmo tempo, ajudam a área de risco tecnológico a se tornar muito mais rápida ao relatar alterações nos dados de risco.

3

### FORNEÇA *INSIGHTS* QUALITATIVOS

Em terceiro lugar, também é importante lembrar que os *insights* qualitativos sempre terão um lugar no gerenciamento de riscos de TI. As decisões de negócios geralmente não são conduzidas apenas por uma pontuação de risco, mas sim coletivamente, a partir de tudo que o risco tecnológico proporciona.

**“Criar uma fonte de dados confiável é importante, mas o mais importante é criar parâmetros, restrições e filtros adequados para classificar os dados, para que os responsáveis pelo negócio possam tomar as decisões certas a partir deles.”**

– Vivek Mehta, Sócio

# Considerações finais: criação de gerenciamento de risco tecnológico da próxima geração

À medida que a tecnologia se torna cada vez mais complexa, aberta e onipresente, os executivos de negócios e de TI estão se tornando mais sensíveis ao risco da tecnologia. Eles também estão se tornando mais cautelosos. Nesse ambiente, o risco tecnológico tem muito a contribuir.

As funções de risco tecnológico da próxima geração entenderão melhor os negócios, preverão riscos associados a novas tecnologias ou sistemas legados, gerenciarão riscos de maneira proativa e melhorarão a resiliência da organização caso ocorra um incidente. Esperamos que este relatório ajude você a chegar lá.

**“O risco tecnológico não deve ser um custo adicional para se fazer negócios sem valor agregado. Se existe uma maneira de o risco tecnológico ser um gerador de dinheiro para o negócio – por exemplo, se as empresas puderem obter percepções do comportamento da empresa, cliente ou fornecedor reunidas durante o processo de risco tecnológico – isso seria importante.”**

– Constance Hunter, Principal



## CONTRIBUIÇÕES PARA DISCUSSÕES DE ESTRATÉGIA:

À medida que o ritmo e a complexidade da tecnologia aumentam - e aumenta o perfil de risco da organização - as organizações de ponta passam a integrar o gerenciamento de riscos desde o início, preparando e gerenciando os riscos de acordo com a estratégia de negócios



## VISÃO FORTE DE NEGÓCIO

Os melhores profissionais de risco tecnológico de amanhã terão o conhecimento empresarial para traduzir o risco e seu impacto em linguagem compreensível para os tomadores de decisão. Eles terão o entendimento e a visibilidade para encontrar o meio termo ideal, no qual o risco é mitigado antecipadamente e o crescimento dos negócios é mantido.



## UM LUGAR NA MESA DE NEGÓCIOS, INCLUINDO MAIS COLABORAÇÃO COM AS PARTES INTERESSADAS

Organizações de ponta encontrarão o foco e aumentarão o risco da tecnologia nas direções apropriadas.



## AUMENTO NO RECONHECIMENTO DA MARCA

Organizações de ponta elevarão o perfil de risco tecnológico interno e o perceberão como “mais do que apenas conformidade.”



## RELATÓRIO FOCADO EM RESULTADOS

Os líderes de negócios precisam de informações significativas para tomar as decisões certas. Organizações de ponta sintetizam dados de risco no nível executivo e vinculam os dados diretamente ao impacto nos negócios.



## ORÇAMENTO E NÚMERO DE FUNCIONÁRIOS PROPORCIONAIS AO ORÇAMENTO GERAL

Organizações de ponta deixarão de medir os gastos com gerenciamento de riscos de TI apenas como uma porcentagem de conformidade.



## UM PAPEL FUNDAMENTAL EM TODAS AS ETAPAS DA ADOÇÃO DE TECNOLOGIA, IMPLEMENTAÇÃO E MUDANÇA

A futura função de risco tecnológico desmistificará os riscos da nova tecnologia emergente e desenvolverá uma estrutura com flexibilidade suficiente para responder a novos riscos. Durante e após a adoção, a equipe enfatiza continuamente os processos de teste, monitora o desempenho, monitora as métricas e relata à gestão.



## MODELOS DE DADOS ÁGEIS

Em vez de se concentrar em aumentar o volume geral de dados e métricas de risco ou o número de métricas de categorias de risco, as organizações de ponta enfatizarão confiança e agilidade, aperfeiçoando modelos de dados que podem absorver novos riscos e definir novos controles, como mudanças no ambiente externo que possam impactar a exposição ao risco da organização.

**“Empresas e executivos que possuem uma visão digital para a abordagem de gestão de riscos de tecnologias emergentes buscam investir cada vez mais na formação de recursos que conheçam não apenas tecnologia, mas também metodologia de riscos e o negócio, e em ferramentas que acelerem o processo de coleta e processamento dos dados, deixando a cargo dos líderes a tarefa de análise e interpretação dos mesmos para tomada de decisão.”**

– Marcelo de Angelo, Sócio

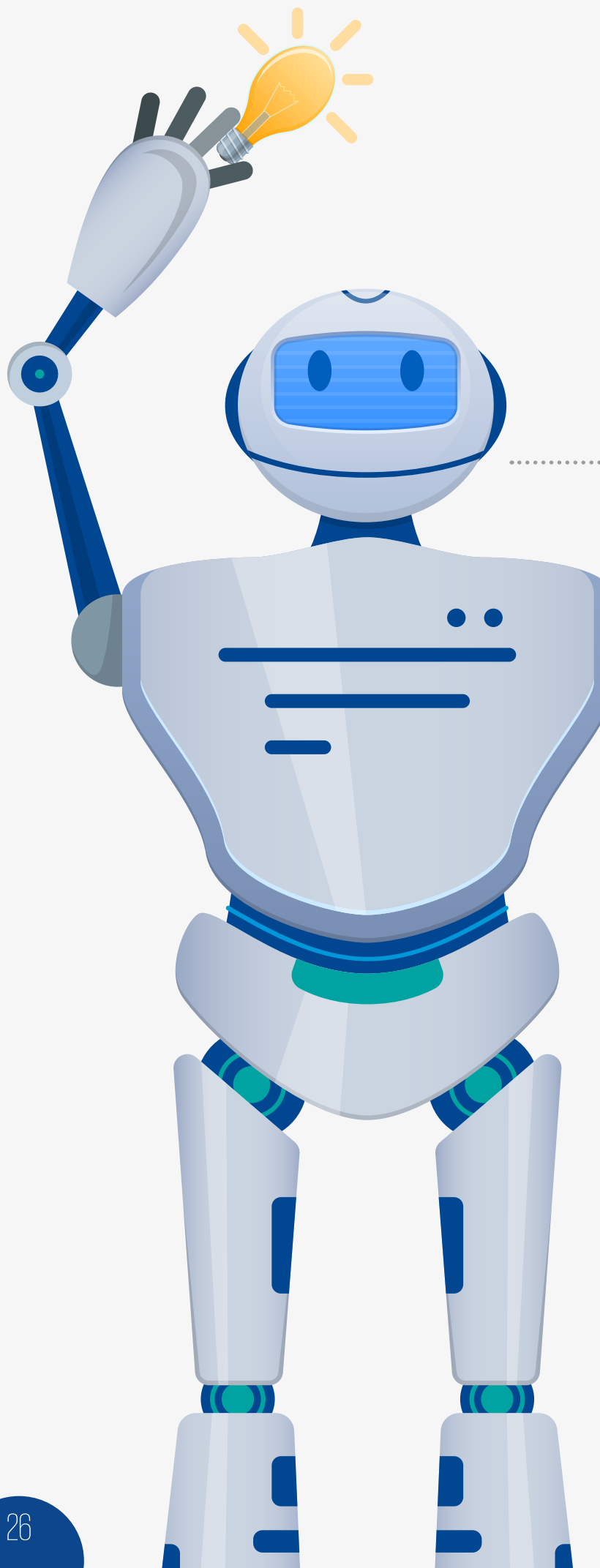
# Metodologia da pesquisa e dados demográficos

No segundo semestre de 2018, a KPMG realizou uma pesquisa com executivos de diversas empresas, de distintos segmentos, que possuem atuação no território nacional.

Inicialmente, desenvolvemos o conjunto de perguntas do questionário relacionado ao tema de riscos das tecnologias emergentes e como as empresas estão tratando este assunto em suas organizações.

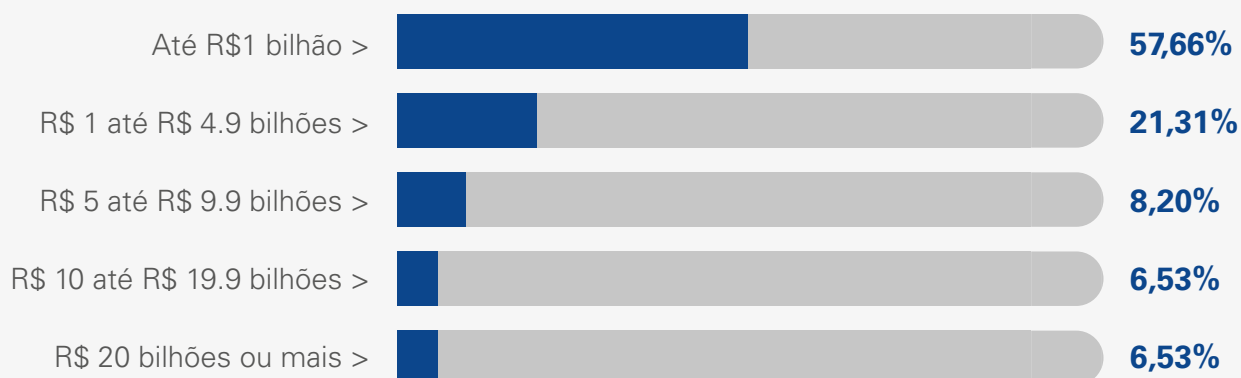
Em seguida, aplicamos a pesquisa por meio de entrevistas ou formulário digital junto aos executivos participantes.

Com base nas respostas que recebemos, analisamos os dados e extraímos os principais temas e *insights* incluídos neste relatório.

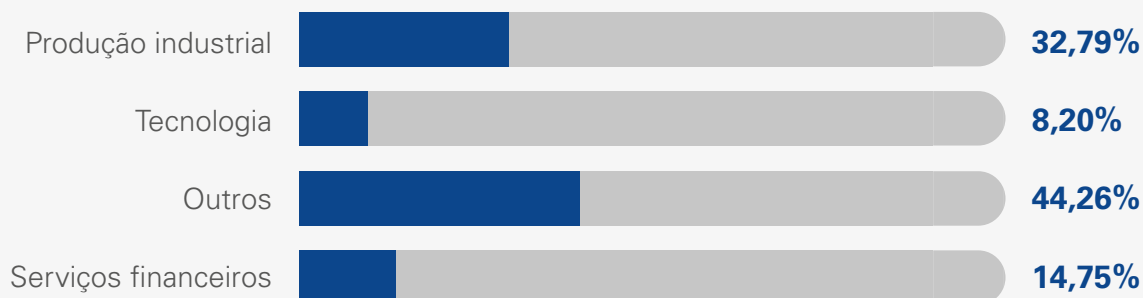




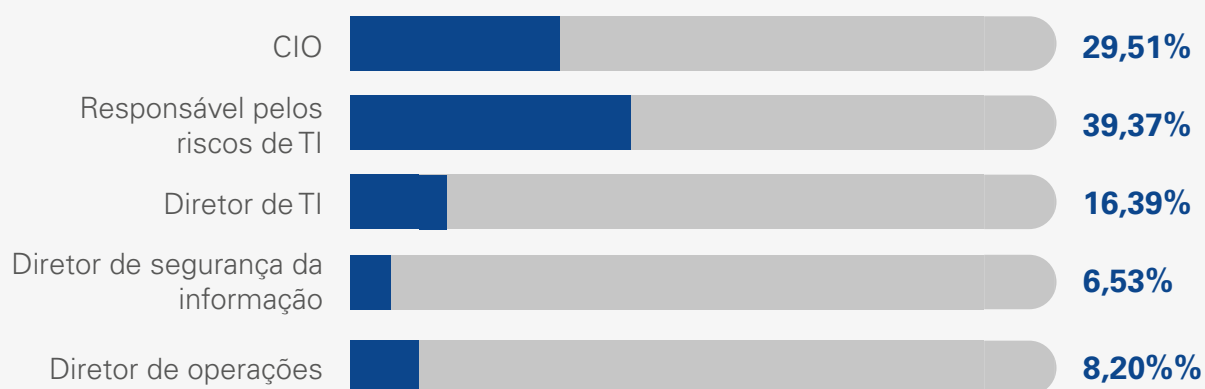
## Faturamento



## Segmento



## Função



# Perguntas adicionais:

**Sua organização tem conhecimento sobre os riscos de TI e sobre este mercado, de uma forma integrada?**

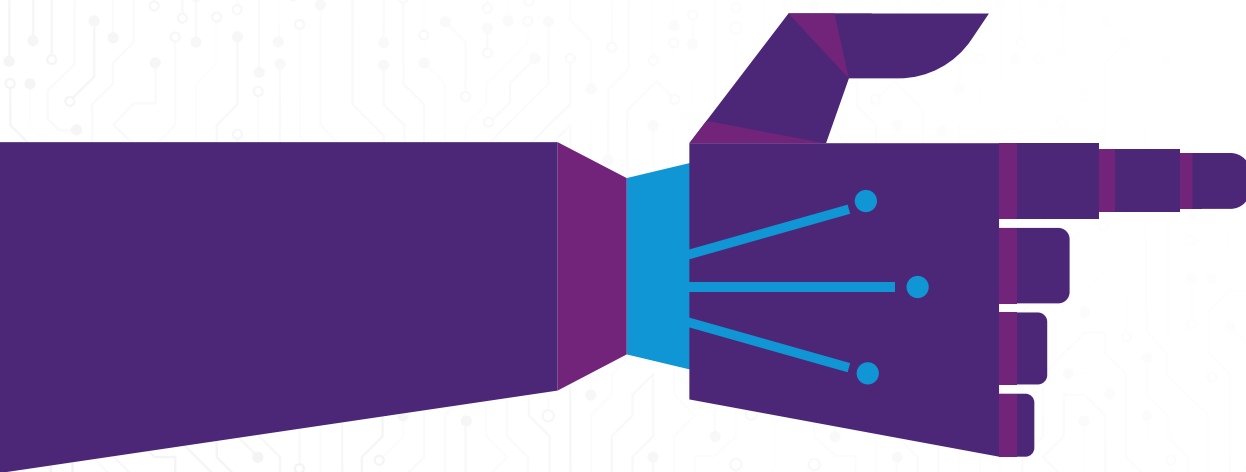


**67%** das empresas entrevistadas têm conhecimento sobre os riscos de TI e o mercado, de uma forma integrada.

**Sua organização possui ou pretende adotar no próximo ano iniciativas que gerenciem de forma integrada os riscos associados à estrutura de TI?**

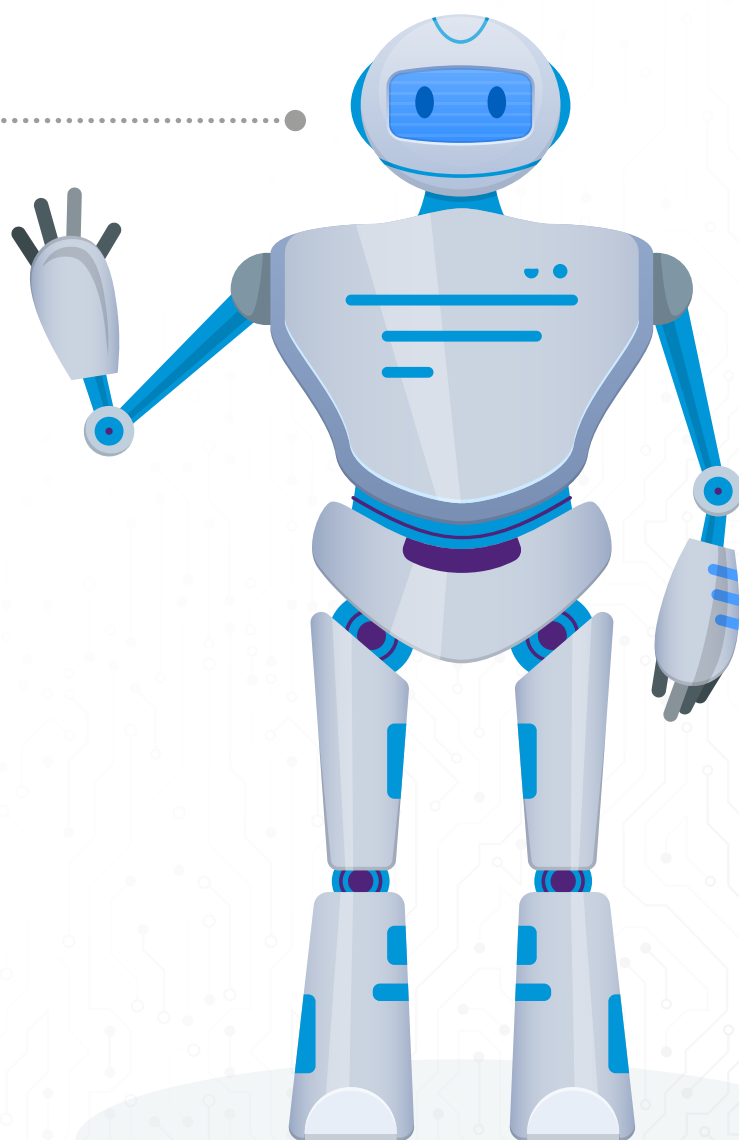


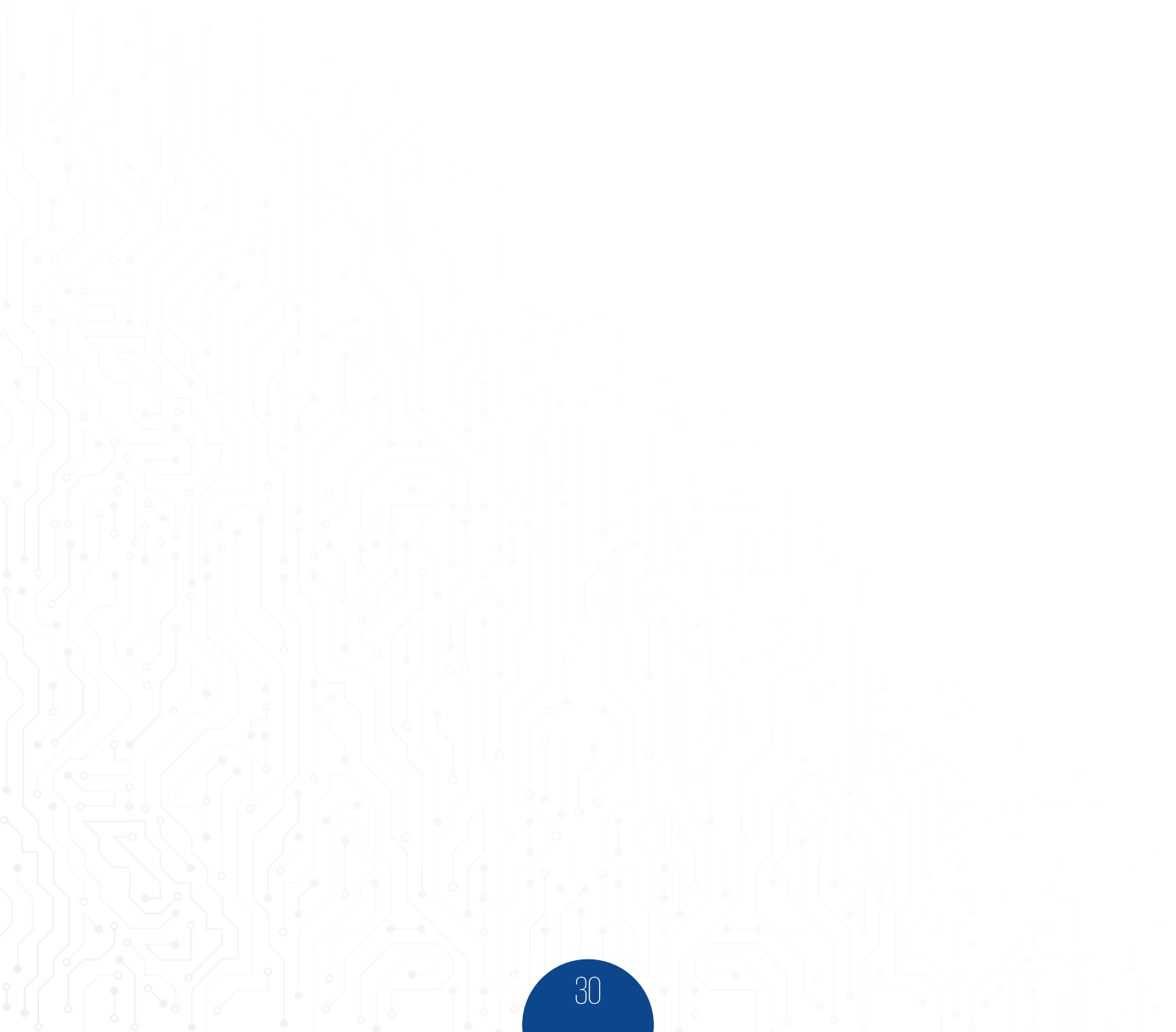
**52%** das empresas entrevistadas pretendem iniciar gerenciamento de riscos de tecnologia de forma integrada.



# Como a KPMG pode ajudar

Hoje, mais do que nunca, a tecnologia é um facilitador crítico dos negócios. Ajudamos os clientes a reconhecerem e gerenciarem com responsabilidade o universo completo de riscos associados ao seu ambiente de tecnologia, para que eles possam obter os benefícios da era digital. Com serviços respaldados por metodologias e processos-chave do setor, combinados a profissionais experientes com profundo conhecimento técnico e *know-how* estratégico, ajudamos várias organizações a transformarem o gerenciamento de riscos de TI e de tecnologias emergentes em atividades que agreguem valor para o negócio.







# Fale com o nosso time

**Marcelo de Angelo**  
**Sócio, Advisory**  
**Risk Consulting, IT Advisory Services**

Tel.: (11) 3940-4402  
mangelo@kpmg.com

Alguns ou todos os serviços descritos nesse material podem não ser permissíveis para clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.



Baixe o APP  
**KPMG Brasil**

[kpmg.com.br](https://kpmg.com.br)



© 2019 KPMG Consultoria Ltda. uma sociedade simples brasileira, de responsabilidade limitada, e firma-membro da rede KPMG de firmas-membro independentes e afiliadas à KPMG International Cooperative ("KPMG International"), uma entidade suíça. Todos os direitos reservados. Impresso no Brasil

O nome KPMG e o logotipo são marcas registradas ou comerciais da KPMG International.

Todas as informações apresentadas neste documento são de natureza genérica e não têm por finalidade abordar as circunstâncias de uma pessoa ou entidade específica.

Embora tenhamos nos empenhado em prestar informações precisas e atualizadas, não há garantia de sua exatidão na data em que forem recebidas nem de que tal exatidão permanecerá no futuro. Essas informações não devem servir de base para se empreenderem ações sem orientação profissional qualificada, precedida de um exame minucioso da situação em pauta.

Projeto Gráfico e diagramação: Gaudí Creative Thinking.