Third-Party Risk Management: O papel do Conselho de Administração

KPMG ACI Celebrando 20 anos

KPMG Board Leadership Center
Exploring issues. Delivering insights. Advancing governance.

Novembro de 2023

Nos últimos anos, como resultado de danos reputacionais causados pela falha de terceiros, ao entregar produtos e serviços em desacordo com o esperado, as empresas vêm priorizando e aprimorando cada vez mais o seu programa de gerenciamento de riscos de terceiros (também conhecido pela nomenclatura em inglês *Third-Party Risk Management*-TPRM). Esses terceiros — incluindo fornecedores; prestadores de serviços; armazenadores de informações e dados em nuvem (*cloud*); consultores e *advisors*; canais de vendas e distribuição; parceiros e alianças estratégicas; bem como quartos, quintos e enésimos— enfrentam o mesmo conjunto complexo e em constante evolução de riscos que essas empresas enfrentam.

Em uma recente **pesquisa da KPMG** sobre o gerenciamento de riscos de terceiros, três quartos dos respondentes disseram que nos últimos três anos suas empresas passaram por uma disrupção significativa nos negócios causada por terceiros, e que expuseram suas empresas a riscos reputacionais. Progressivamente, mais organizações estão percebendo, algumas pela primeira vez, que a segurança cibernética e a privacidade de dados; os riscos geopolíticos; o *compliance*; os riscos climáticos e outros riscos ambientais e sociais; e as questões de continuidade dos negócios podem impactar rapidamente as operações da empresa e a sua marca.

Embora, muitas empresas possuam atualmente programas robustos para o gerenciamento de riscos de terceiros como uma necessidade estratégica, garantir que o TPRM acompanhe o ambiente regulatório e de *compliance* e a rápida transformação dos riscos, é um desafio significativo. À medida que os conselhos de administração têm atuado mais próximos da gestão, no propósito de manter um TPRM efetivo e que atenda os propósitos da empresa, alguns dos seguintes componentes devem ser considerados:

Riscos de terceiros em segurança cibernética e de privacidade de dados

De acordo com a pesquisa global 2023: "**Desafios e Prioridades do Comitê de Auditoria"**, lançada pelo ACI Institute Brasil, os riscos relacionados à segurança cibernética e à privacidade de dados estão entre os principais riscos associados a terceiros, e o nível desses riscos aumenta cada vez mais, devido à crescente sofisticação dos hackers, incluindo o uso da inteligência artificial generativa (IA). Conforme observado em um recente relatório do Fórum Econômico Mundial[1], um dos principais desafios para as empresas é manter o monitoramento contínuo e a visibilidade em tempo real, para identificar potenciais riscos e questões relacionados à segurança cibernética de terceiros. Isso requer maximizar o uso da automação, alinhar o monitoramento contínuo dos controles internos da própria empresa e de terceiros, e entender como a gestão vem aprimorando o monitoramento das ameaças contra a segurança cibernética de terceiros, em tempo real.

1 Global Cybersecurity Outlook 2023, Fórum Econômico Mundial, janeiro de 2023.

Dada a importância dos riscos ligados à segurança cibernética, os órgãos reguladores vêm avaliando e criando regras sobre o assunto. Além das divulgações já compulsórias quando um incidente significativo acontece, as empresas serão obrigadas, cada vez mais, a divulgar com detalhes, se possuem processos e controles para supervisionar e identificar riscos de ameaças à sua segurança cibernética, recorrentes do uso de serviços terceirizados.

A segurança cibernética também pode trazer riscos no compliance, caso terceiros tenham acesso a dados pessoais. Muitos países, incluindo o Brasil, com a Lei Geral de Proteção de Dados (LGPD), já estabeleceram leis e regulamentações relacionadas à privacidade e proteção de dados pessoais. Dessa forma, se terceiros tiverem acesso a dados pessoais existentes na empresa, esta precisará assegurar que esses terceiros possuem controles em vigor para utilizar e armazenar esses dados, de acordo com as leis e as regulamentações, bem como com as políticas de privacidade de dados da própria empresa.

Os conselhos de administração deverão manter uma comunicação constante com a gestão, a fim de entender como ela gerencia os riscos relacionados à segurança cibernética e de privacidade de dados de terceiros; a efetividade dos controles internos para assegurar que as políticas corporativas vêm sendo cumpridas; e o processo de comunicação para eventuais incidentes de vazamentos de informações da empresa, que possam ocorrer em terceiros.

Riscos decorrentes do uso de ferramentas de inteligência artificial (IA) de terceiros

As empresas estão reconhecendo rapidamente a necessidade de abordar os crescentes riscos associados ao uso ou à integração de ferramentas de IA de terceiros. Conforme um artigo do *MIT Sloan Management Review*, de abril de 2023: "Ferramentas de IA de terceiros, incluindo modelos de código-fonte aberto (*open-source models*), plataformas de fornecedores e programas de interface comerciais (*Application Programming Interface-API*), tornaram-se uma parte essencial da estratégia de IA de todas as organizações, de uma forma ou de outra, tanto que geralmente é difícil separar os componentes internos dos externos."[2]

2 Elizabeth M. Renieris et al., "Responsible AI at Risk: Understanding and Overcoming the Risks of Third-Party AI," MIT Sloan Management Review, 20 de abril de 2023.

Como resultado, as empresas precisam reavaliar a governança da sua estrutura e dos seus processos envolvendo o desenvolvimento, uso e proteção dos sistemas e dos modelos de IA, assim como e quando um sistema ou modelo de IA — incluindo o uso de ferramentas de IA de terceiros — deve ser desenvolvido e implementado e quem toma essas decisões. Quais riscos relacionados ao *compliance* regulatório e à reputação da empresa — incluindo vieses — podem afetar a empresa pela utilização de ferramentas de IA de terceiros? Como a gestão está mitigando ou endereçando esses riscos? (Veja também: "***Assessing the risks and opportunities of generative AI***" - "**Avaliando os riscos e oportunidades da IA generativa**", publicado pelo BLC dos EUA).

Riscos de terceiros relacionados ao clima, à sustentabilidade e a outros fatores ESG

O ativismo crescente dos *stakeholders* por mais e melhores divulgações relacionadas às mudanças climáticas e questões ambientais, sociais e de governança (ESG), obriga os conselhos de administração a aumentar seu foco em iniciativas e esforços para gerenciar uma ampla gama de riscos associados ao clima e sustentabilidade na sua cadeia de suprimentos. Nesse contexto, os conselhos de administração devem monitorar de forma contínua a legislação e regras regulatórias sobre o assunto e como elas vêm sendo cumpridas pela empresa, incluindo suas divulgações e informações fornecidas publicamente.

As regras atuais da CVM, sobre a divulgação obrigatória nos formulários de referência dos riscos sociais e ambientais, bem como do ESG (a CVM utiliza a denominação ASG), e as regras da B3, sobre diversidade, deverão rapidamente ser complementadas com divulgações sobre o impacto das mudanças climáticas na cadeia de suprimentos; divulgações sobre emissões de gases de efeito estufa do Escopo 3; e divulgações relativas a uma série de riscos de sustentabilidade e social na cadeia de suprimentos, tais como direitos humanos e trabalho forçado.

Iniciativas incluindo as normas globais de divulgação de sustentabilidade do *International Sustainability Standards Board* (ISSB) e as normas europeias do *European Sustainability Reporting Standards* (ESRS) já estão nas fases finais de conclusão e emissão.

Se obrigatória, a coleta e o cálculo dos dados do Escopo 3, sobre emissões de gases de efeito estufa, representará um desafio significativo, considerando o número de terceiros na cadeia de suprimentos e o fato de esses dados estarem fora do controle das empresas.

O conselho de administração deve discutir com a gestão sobre a existência de controles internos que assegurem consistência e precisão nas informações divulgadas publicamente, sejam elas regulatórias e mandatórias ou voluntárias, tais como os relatórios de sustentabilidade (até esse momento) e relatórios de divulgação ao mercado.

Projetos da gestão para abordar as vulnerabilidades dos negócios e aumentar a resiliência e a sustentabilidade

Nos últimos anos, as empresas vêm lidando com disrupções, tensões e incidentes operacionais sem precedentes nos negócios, cujos fracassos ou falhas estão vindo a público. Na 8ª edição do "**Estudo Gerenciamento de Riscos**," elaborado pelo ACI Institute Brasil em 2023, 63% das empresas abertas brasileiras divulgaram o risco associado a sua marca e reputação, como um dos riscos significativos dos seus negócios. Muitas empresas vêm tomando iniciativas importantes para diminuir os riscos na sua cadeia de suprimentos, entre elas: entender o papel que terceiros desempenham na entrega de seus bens e serviços; identificar e abordar as vulnerabilidades nessa dependência operacional; e aumentar a resiliência e a sustentabilidade do negócio, adotando uma abordagem baseada em riscos. Essa abordagem varia de acordo com a empresa e pode incluir: atualização do plano de continuidade do negócio e de recuperação de desastres; diversificação da base de fornecedores; reavaliação da estrutura das operações da cadeia de suprimentos; redução da dependência de alguns fornecedores ou países e o desenvolvimento de fornecedores locais e regionais; desenvolvimento de tecnologias para melhorar a visibilidade das operações e gerenciamento dos seus riscos, melhorando a segurança cibernética para reduzir o risco de violação de dados e desenvolvendo planos para enfrentar possíveis futuras disrupções.

O conselho de administração pode contribuir com a gestão ao repensar, revisar e ajustar seu modelo de negócio e a sua relação com a cadeia de suprimentos, assegurando que a relação comercial com terceiros, seja avaliada de forma estratégica e de continuidade dos negócios, com intuito de mitigar ou endereçar os seus riscos relacionados.

Conclusões:

Assim como sugerem as questões e dilemas acima, a crescente complexidade e magnitude dos riscos de terceiros impõem um desafio significativo para os conselhos de administração na condução das suas atividades. Os investidores, os órgãos reguladores, as agências de *rating* (e especificamente as de classificação ESG) e demais *stakeholders* estão exigindo divulgações cada vez mais detalhadas e claras sobre os riscos de terceiros e como os conselhos de administração vêm supervisionando o gerenciamento desses riscos. Nesse ambiente desafiador, muitos conselhos de administração estão reavaliando como podem supervisionar de forma eficaz os riscos relacionados a terceiros, com o auxílio dos seus comitês de assessoramento.

Dessa forma, a seguir, algumas questões que os conselhos de administração e os seus comitês poderiam considerar para abordar o assunto:

- Os responsáveis pela condução dos negócios com terceiros entendem o escopo e a magnitude dos riscos de terceiros e se esses riscos são gerenciados e controlados de maneira apropriada, de acordo com as políticas da empresa (TPRM)?
- A gestão possui um inventário completo, incluindo uma classificação dos riscos, dos serviços e produtos críticos prestados/fornecidos por terceiros, incluindo subcontratados?
- Com que frequência o conselho de administração interage com a gestão sobre atualizações relativas aos riscos de terceiros? Como as informações são fornecidas e com qual frequência? Os dados estão disponíveis em tempo real?
- O monitoramento dos riscos de terceiros deve ser responsabilidade do conselho de administração, do comitê de auditoria ou de outro comitê? O comitê de auditoria monitora os riscos da cadeia de suprimentos de forma geral ou de forma detalhada?
- O processo de gerenciamento de riscos de terceiros (TPRM) é abordado de maneira holística, como uma atividade que engloba toda a empresa, ou de forma isolada? Ele é integrado ao processo de gerenciamento de riscos (ERM) e ao *compliance* da empresa?
- Os responsáveis pela gestão de riscos de terceiros, bem como pela realização das atividades com terceiros possuem habilidades/talentos, recursos financeiros e tecnologia suficientes para acompanhar o ritmo de mudanças e os desafios relacionados ao TPRM?
- Quando o conselho de administração deve ser incluído na supervisão e/ou na aprovação de serviços ou produtos a serem fornecidos ou que envolvam terceiros?

Fale com nosso time

Sidney Ito

CEO do ACI Institute Brasil e Sócio em Riscos e Governança Corporativa da KPMG no Brasil

Diogo Dias

Sócio-líder de Risk Advisory Solutions da KPMG no Brasil

KPMG ACI Celebrando 20 anos

O ACI Institute (ACI) e o Board Leadership Center são iniciativas globais da KPMG voltadas a membros de conselhos de administração, conselhos fiscais e comitês de auditoria. O ACI chegou ao Brasil em 2004 e, deste então, já promoveu mais de 80 Mesas de Debate para tratar de temas relacionados à governança corporativa.

Ao incentivar a troca de experiências entre seus membros e propiciar um espaço para interlocução de alta qualidade, o ACI Institute Brasil, o Board Leadership Center e a KPMG contribuem para discussões sobre desafios e oportunidades relevantes para os negócios, oferecendo análises exclusivas baseadas em publicações desenvolvidas especialmente para conselheiros e membros de comitês de auditoria.

As expectativas dos stakeholders nunca estiveram tão altas e o escrutínio dos reguladores e investidores tão rigorosos. Participar das atividades do ACI Institute e do Board Leadership Center Brasil contribui para a atualização constante dos profissionais, crucial para o desenvolvimento e o fortalecimento das boas práticas de governança corporativa, gerenciamento de riscos, ESG, novas tecnologias, auditoria, entre muitos outros temas.

Saiba mais em **https://home.kpmg/br/pt/home/services/aci-institute-brasil.html**

kpmg.com.br

/kpmgbrasil