04

2018
Julho

IBGC Análises & Tendências

Gerenciamento de Riscos

IBGC
Análises
& Tendências

Nº 4 / 2018

Produção e coordenação da publicação

Jornalista responsável: Sandra Nagano (MTB 42425/SP)

Projeto gráfico e diagramação

Atelier de Criação (atelierdecriacao.com.br)

Fotos

Divulgação / Arquivo IBGC

IBGC
Av. das Nações Unidas, 12551
World Trade Center Tower - 21º andar - CEP 04578-903 - São Paulo/SP
tel.: 55 11 3185 4200 / e-mail: ibgc@ibgc.org.br

www.ibgc.org.br

Sumário

Editorial

As organizações deparam-se cada vez mais com temas como sustentabilidade, corrupção, fraude, abuso nos incentivos de curto prazo para executivos e investidores, ética nos negócios e reputação. Cada um destes temas traz embutidos em si a noção de risco, cujo gerenciamento é parte do que as organizações precisam para obter lucros, realizar objetivos importantes, criar valor e, principalmente, ter uma existência longeva. O conceito atual de risco no mundo corporativo envolve a quantificação e a qualificação da incerteza, sendo sua administração um elemento chave para a sobrevivência das companhias e demais entidades [1].

De acordo com o estudo *Norton Cyber Security Report*, em 2017, apenas no Brasil, os crimes cibernéticos causaram prejuízos de cerca de 22 bilhões de dólares. Neste mesmo ano, 62 milhões de brasileiros foram vítimas de cibercrime, o que representa 61% da população adulta conectada no país. O Brasil é o segundo país que mais perdeu financeiramente com ataques cibernéticos, atrás apenas da China.

É nesse sentido que esta edição do Análises e Tendências convida o leitor a entender a importância de prevenir e monitorar adequadamente esses riscos, de forma que estejam incorporados no processo decisório e na cultura da corporação. Somente dessa forma será possível identificar o nível dos riscos que a empresa está disposta a incorrer para atingir seus objetivos estratégicos.

Mais grave do que vivenciar um risco e ter um acidente é não saber quais são os riscos que uma organização pode sofrer e não ter um plano para gerenciá-los. Essa publicação traz artigos que colocam a importância de a organização contar com uma função de gestão de riscos, além de contar com uma estrutura de controles internos e processos de monitoramento e gestão.

Ainda, esta publicação traz a análise de alguns casos de fracassos empresariais nas dimensões ambiental e social, ocasionados por problemas de governança corporativa, tais como a falta de um adequado gerenciamento de riscos, bem como a omissão e negligência da atuação dos conselhos de administração. Além desses casos, também transitamos pelos desafios de instaurar um plano de gerenciamento de riscos na administração pública e que esbarram, muitas vezes, na falta de integração

dos programas das diversas pastas, além da tão questionada "vontade política".

Temas específicos sobre o assunto são tratados, tais como o papel do profissional de riscos na organização, os riscos regulatórios inerentes ao negócio, assim como a especificidade dos riscos inerentes aos projetos de engenharia. Outro ponto abordado está no fato de que a gestão de riscos não atua apenas no incidente, mas avalia o nível do problema trazido, como e quais pessoas e departamentos foram impactados e que tipo de plano de ação pode ser estudado para evitar sua reincidência.

Diante de todos os casos e cenários, também destacamos, nesta edição, processos de fraude e corrupção, gestão de riscos cibernéticos, uma discussão sobre a disposição ao risco e uma pesquisa que apresenta alguns caminhos tomados por profissionais envolvidos em ilícitos.

Aproveito para agradecer e salientar a inestimável colaboração da Comissão de Gerenciamento de Riscos Corporativos para a realização desta edição.

Espero que tenham uma ótima leitura.

Valéria Café
Superintendente de Vocalização e Influência

1. Parágrafo adaptado extraído do caderno 19 de governança corporativa do IBGC – *Gerenciamento de Riscos Corporativos: Evolução em Governança e Estratégia*

Integração da gestão de riscos cibernéticos nas três linhas de defesa

Por Sergio Kogan e Henrique Quaresma

É fato que a preocupação em relação aos riscos cibernéticos ganhou a atenção da alta administração de muitas empresas e dos governos, especialmente com a grande cobertura que a mídia tem dado para o assunto, como por exemplo o caso do WannaCry, ocorrido em maio de 2017.

De acordo com relatório "*The Global Risks Report 2018*"[1], desenvolvido anualmente pelo Fórum Econômico Mundial, os ataques cibernéticos figuram como o 3º risco em termos de probabilidade, seguido por roubos ou fraudes de dados (4ª posição), que também têm relação direta com a segurança cibernética. Em 2016, o risco de ataques cibernéticos não constava no *Top 10*.

Adicionalmente, os órgãos reguladores no mundo todo têm promulgado leis, regulamentos e orientações que endereçam essa preocupação em relação a esse tema. Como exemplo, o Banco Central do Brasil (Bacen) publicou em 26 de abril deste ano a resolução 4.658 que determina que as instituições financeiras brasileiras devem definir e implementar uma política e medidas de proteção cibernética, além de monitorar e gerenciar os incidentes dessa mesma natureza.

Desafio de gerenciar os riscos cibernéticos

Em diversas organizações no Brasil, o tema segurança cibernética é delegado à área de Tecnologia da Informação (TI), uma vez que o componente tecnológico é visto como o principal mecanismo de proteção a ser implementado e gerenciado. Outro fator que contribui para o foco tecnológico da gestão dos riscos cibernéticos é o desconhecimento dos executivos da organização em relação aos riscos envolvidos e seu real impacto no negócio.

O que algumas empresas não levam em consideração é que quando ocorrem incidentes, a organização pode ser impactada de diversas maneiras. Por esse motivo, os riscos cibernéticos devem ser gerenciados como um risco de negócio, com o mesmo nível de atenção e diligência dos outros riscos corporativos.

Integrando riscos cibernéticos nas três linhas de defesa

Estabelecendo como uma premissa fundamental que risco cibernético é um risco de negócio, faria sentido utilizarmos as estruturas, metodologias, práticas e ferramentas de Gestão de Riscos Corporativos para identificar, classificar, analisar, tratar e monitorar os riscos cibernéticos?

A resposta é sim. Uma vez que a forma de gestão - e, principalmente, de apresentação e comunicação - dos riscos corporativos é conhecida pela alta administração, torna-se um pré-requisito a tradução do linguajar técnico, comumente utilizado para comunicar os riscos cibernéticos, para uma linguagem de fácil entendimento de profissionais que não possuem o conhecimento técnico em segurança cibernética, porém conhecem profundamente do negócio da organização, e como riscos podem impactar no atingimento dos objetivos estratégicos ou operacionais.

Do ponto de vista de governança de riscos, a estrutura das Três Linhas de Defesa (3LoD – Line of Defense) está sendo amplamente divulgada e implementada pelas organizações (ver figura).

1. The Global Risks Report 2018", Fórum Econômico Mundial, 17 de janeiro de 2018

Como adotar essa estrutura para gerenciar os riscos cibernéticos de uma forma holística e integrada?

Em primeiro lugar, é importante determinar as atribuições de cada linha de defesa para que não haja sobreposição e retrabalho, especialmente no cenário atual de busca constante de otimização de custos nas empresas brasileiras.

Primeira linha de defesa

A primeira linha de defesa é responsável por implementar e operacionalizar os controles para mitigar os riscos cibernéticos. A tradicional função de segurança de TI se enquadra nesse papel, uma vez que, geralmente, é responsável por implementar e gerenciar processos e soluções tecnológicas relevantes para a segurança cibernética, tais como desenvolvimento e atualização de *software* seguro, gestão de acessos, gestão de vulnerabilidades, monitoramento de eventos de segurança, entre outros.

Entretanto, outras áreas da organização também possuem um papel importante na gestão de riscos cibernéticos:

- Recursos Humanos: geralmente, os colaboradores de uma organização são o elo mais fraco para assegurar uma adequada segurança cibernética, por essa razão, deve-se dar o devido nível de atenção do momento da contratação até o desligamento do funcionário. Para que isso ocorra, o departamento de Recursos Humanos deve estar alinhado e conhecer o seu papel na gestão de riscos cibernéticos;

- Suprimentos e Compras: durante a contratação de um fornecedor, diversas atividades devem ser coordenadas pela área, em conjunto com a área contratante e com o apoio da Segurança da Informação Corporativa (segunda linha de defesa que discutiremos logo a seguir neste artigo), para assegurar que os devidos cuidados foram tomados em relação à seleção do terceiro. Uma adequada gestão de riscos de segurança

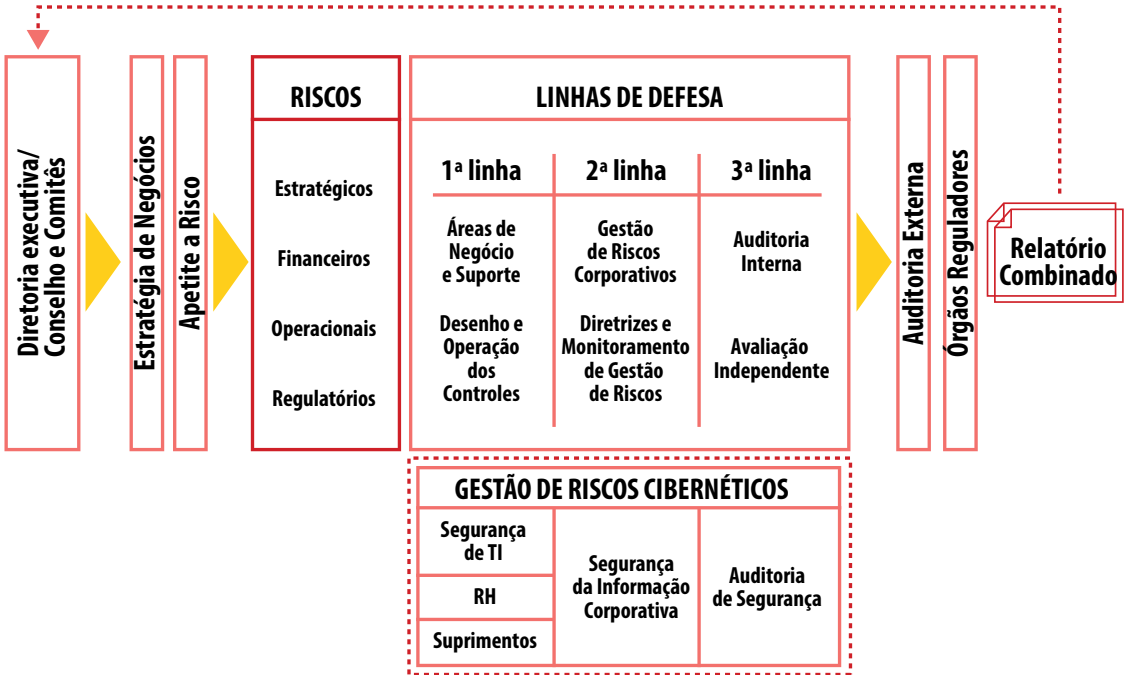


Figura - Modelo de gestão de riscos cibernéticos alinhado às 3 linhas de defesa

da informação em terceiros (fornecedores e parceiros) deve ser definida e implementada pela organização. Para isso, é importante questionar-se se seus fornecedores e parceiros inspiram-lhe confiança e conforto, bem como tratam a sua informação com o mesmo nível de diligência que a sua organização.

Outras áreas também possuem um papel fundamental nessa gestão de riscos cibernéticos corporativos como Segurança Patrimonial/Física, áreas de negócio e de Inovação e Digital.

Entretanto, como atuar de forma integrada e organizada? A resposta é a segunda linha de defesa.

Segunda linha de defesa

É responsável por definir as diretrizes e monitorar o cumprimento pela primeira linha de defesa. Na gestão de riscos cibernéticos, a proposição é a existência de uma função de segurança da informação corporativa independente, cabendo-lhe a responsabilidade por:

- Definir a visão, missão e estratégia para gestão dos riscos cibernéticos na organização alinhada à estratégia do negócio e apetite ao risco;
- Definir as diretrizes e dar suporte à primeira linha de defesa na implementação das políticas, normas e procedimentos, considerando seus papéis e responsabilidades;
- Realizar o treinamento e conscientização dos colaboradores da organização fomentando uma cultura de segurança cibernética;
- Identificar, classificar, analisar, tratar e monitorar os riscos cibernéticos;
- Apoiar na gestão de riscos em fornecedores e parceiros, durante a seleção do terceiro e de todo o ciclo de vida do relacionamento da organização com o mesmo;
- Atuar na resiliência e continuidade de negócios (Plano de Continuidade Operacional, Plano de Recuperação de Desastres de TI e Gestão de Crises);
- Realizar o monitoramento dos indicadores e da conformidade da organização e dos terceiros.

Terceira linha de defesa

Por fim, a auditoria interna necessita de profissionais capacitados e com conhecimento técnico para realizar avaliações independentes que permeiam o ciclo completo de gestão de riscos cibernéticos. É preciso considerar essas ameaças em todas as auditorias de estratégia, governança e processos da organização e não somente das áreas de TI e Segurança.

Conclusão

O risco cibernético é um risco de negócio e sua efetiva gestão permeia as diversas áreas da organização. O conceito de três linhas de defesa auxilia na estruturação e definição clara dos papéis e responsabilidades de forma que a atuação seja integrada.

Não espere sua organização ser impactada por um incidente cibernético para agir. Entenda como os riscos cibernéticos estão evoluindo e afetam a sua organização; mantenha-se à frente das novas regulamentações; integre uma adequada estratégia e cultura de segurança cibernética dentro da organização; trabalhe integradamente junto aos terceiros para proteger todo o ecossistema do negócio, focando nos ativos críticos que não podem ser comprometidos.

Sergio Kogan
Líder em Cybersecurity da EY Brasil

Henrique Quaresma
Gerente senior especialista em gestão de riscos cibernéticos da EY Brasil

Risco de reputação e crise

Por membros da Comissão de Riscos Corporativos

Os pilares de governança de diferentes modelos de organização - pública ou privada, familiar ou profissionalizada, ou quaisquer outros - exigem uma análise cuidadosa para que os objetivos estratégicos da organização possam ser atingidos, sem que os percalços produzidos pelos riscos de imagem e reputação interrompam sua jornada.

Escândalos de corrupção de dimensão nacional e internacional, como as deflagradas na Operação Lava Jato, mostraram que, além das implicações legais, as empresas sofrem impactos devastadores ao serem meramente citadas em denúncias. A recuperação de uma empresa passa a depender de esforços significativos para reconstrução da confiança.

Desde o caso Enron, em 2001, até o mais recente imbróglio envolvendo o Facebook, gigantes de diversos setores já tiveram a imagem e a reputação comprometidas nos últimos tempos. Estes podem ser, muitas vezes, utilizados como sinônimos, mas há diferenças sutis entre ambos:

- **Reputação** é a percepção coletiva que os *stakeholders* têm das imagens que uma empresa transmite ao longo do tempo, como um somatório de imagens.
- **Imagem**, por sua vez, está ligada à identidade visual, algo momentâneo, mais superficial e raso.

Uma boa analogia para se entender melhor a diferença entre os riscos de imagem e de reputação seria pensar nos elos de uma corrente.

O risco de imagem apresenta-se quando um problema produz um arranhão na forma como a empresa conduz os seus negócios, representando uma pequena rachadura em um dos elos.

Sucessivos arranhões levam a um conjunto de rachaduras no elo, capaz de produzir um dano maior como a ruptura da corrente. Este último seria o risco para a reputação da empresa.

Há situações em que mesmo medidas estruturais, mais planejadas ou até mesmo disruptivas, são insuficientes para reparar a imagem e a reputação. A experiência tem demonstrado que clientes e *stakeholders*, simplesmente, deixam de ter confiança na resistência dessa corrente.

A reputação, uma vez comprometida, pode ter um processo de reconstrução muito caro e moroso. Como reflexão sobre este tema, uma notória frase de Warren Buffet, homem de negócios e filantropo, nascido em 1930, nos Estados Unidos: "Demora-se 20 anos para construir uma reputação e apenas cinco minutos para destruí-la. Se pensássemos sobre isso, faríamos as coisas de maneira diferente...".

Agir com transparência, preservar e manter a boa reputação corporativa, manter sistemas de controles atualizados e gerenciar riscos

permitirá que a marca da organização seja projetada e reconhecida por sua identidade, composta pela sua missão, visão e valores.

Continuamos nossa analogia com a figura da corrente. Se cada elo representa uma área da organização, é preciso que todos entendam suas responsabilidades e seus papéis na jornada. Importante ressaltar que os riscos de imagem e reputação não surgem de si próprios, mas são decorrentes de outros riscos. Se existir um ou mais elos da corrente com problemas, estes poderão encadear um ciclo de erros, que se materializam com causas e consequências, e provocar os indesejáveis danos à imagem e à reputação da organização.

Os pilares da governança devem agir nesses pequenos sinais de ruptura, dirigindo, monitorando e apoiando a forma como são solucionados. Também devem acompanhar a evolução e o tratamento das rupturas, que pode nem sempre estar visíveis.

Se um risco de imagem e reputação não é adequadamente gerenciado, pode levar a empresa a uma crise estratégica muito maior. Uma crise de reputação acontece quando a expectativa e o comportamento dos *stakeholders* mudam.

Diante deste cenário, as empresas precisam reavaliar a sua postura e ações, que podem colocar em xeque a sua imagem e reputação, e implementar as práticas de governança corporativas de maneira efetiva, incorporando indicadores de monitoramento que podem alertá-las a qualquer sinal de ruptura, o qual pode ser observado em três momentos distintos: pré-crise, durante e o pós-crise.

PRÉ-CRISE

Dentre alguns sintomas que podem preceder a ocorrência de um risco de imagem e de reputação, podemos citar:

Existência de discurso diferente da prática: os relatórios de administração demonstram que as empresas, em geral, operam com modelos efetivos e eficientes de governança corporativa, que incluem, dentre outros, a gestão de riscos, *compliance*, segurança da informação, auditoria interna, sustentabilidade, responsabilidade social e demais práticas consideradas referências em gestão. Na realidade, e pela nossa experiência, estas práticas estão explicitadas em políticas e procedimentos, mas podem não ser executadas e conhecidas pelos administradores e colaboradores. Este tipo de divulgação pode transmitir para os *stakeholders* internos e externos a percepção que tudo funciona adequadamente. Por que isto acontece? Faz parte do mundo empresarial ou existe uma grande probabilidade de existir o discurso diferente da prática?

Existência de cultura de governança tóxica: o mundo empresarial pode estar cercado de armadilhas. As empresas buscam os melhores empregados, que trabalham unidos em busca de objetivos comuns, bem como são remunerados conforme resultados alcançados. Estes trabalham com metas e indicadores desafiadores e buscam a rentabilidade para a empresa, investidores e os resultados esperados a fim de cumprir e/ou superar suas metas. Ao mesmo tempo que a pressão pela busca dos resultados é muita alta, as tentações para o ilícito como forma de favorecer a empresa ou a si próprio podem ser constantes. É neste momento que pessoas podem estar determinadas a superar os resultados a qualquer preço e onde fatores como pressão, oportunidade e racionalização podem tomar conta do indivíduo que, com ações impensadas, podem realizar o ilícito. Num ambiente em que fins lucrativos justificam os meios, nem todas as práticas de governança corporativa informadas ao mercado conseguem mitigar improbidades, passando para um estágio de governança tóxica, onde os interesses individuais suplantam os interesses da empresa.

Quebra de confiança: a quebra de confiança é um dos aspectos críticos aos danos à imagem e à reputação e coloca em dúvida a credibilidade da empresa, seu modelo de governança corporativa, assim como o relacionamento com os diversos públicos de *stakeholders*.

Falhas e negligência no modelo de gestão de riscos: a existência do programa de gestão de riscos não garante que o modelo de fato está

implementado e é efetivo. A gestão de riscos somente será efetiva a partir do momento que a liderança considerar a visão de riscos nas discussões estratégicas e naquelas sobre o futuro da empresa. Para tal, deve existir total conexão entre a estratégia, a criação de valor e gestão de riscos, bem como devem estar presentes no processo de tomada de decisões estratégicas. Se esta relação não está acontecendo, então existe muito espaço para aperfeiçoar a efetividade do modelo de gestão de riscos da empresa.

Falhas e negligência no modelo de *compliance*: a existência do programa de *compliance* também não garante que este está implementado e é efetivo. Ele somente será efetivo se cumprir alguns requisitos, entre os quais a saber: comprometimento e apoio da alta direção, instância responsável pelo programa; análise de perfil e riscos (*risk assessment*); estruturação das regras, instrumentos e estratégias de monitoramento contínuo. Se estes componentes não estão implementados, existe espaço para também aperfeiçoar a efetividade do modelo de *compliance*.

Negligência com a responsabilidade corporativa: ignorar que "pequenos deslizes" não provocam os danos à imagem e à reputação, mas representam uma falha importante na responsabilidade corporativa. A boa governança é essencial para atender a pressão nas empresas, cada vez maior, por transparência, prestação de contas e responsabilidade social. Isto significa que qualquer empresa que queira sobreviver, ter sucesso, terá que considerar na sua gestão as novas regulamentações, tecnologias, gerenciar novos riscos e preparar-se para o futuro por meio de um plano robusto de sucessão. Esta demanda por sobrevivência tem como aliada a responsabilidade corporativa que deve imperar em todos os níveis da organização.

O "DURANTE" E O PÓS-CRISE

Não somente com relação aos sintomas da pré-crise mencionados, as empresas podem continuar sentindo fortemente as consequências caso não estejam preparadas para se proteger – durante e após a crise – com robusto plano de comunicação e de gestão de crise a fim de minimizar os impactos nos negócios.

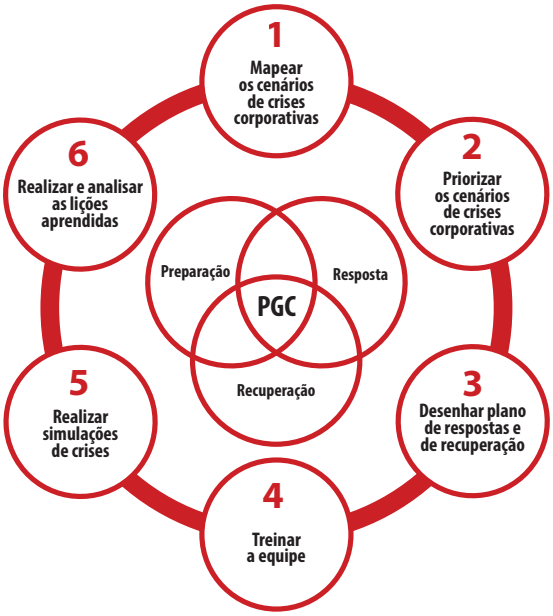
Falta de comunicação objetiva na crise: nos momentos de crise, a pressão por informação é absurda e a assimetria de informações maior ainda. Neste momento, as empresas podem sofrer com os impactos das *fake news* que se dissipam rapidamente. No momento zero da crise, poucos têm a informação correta para compartilhar. Desta forma, a existência do plano de comunicação com os *stakeholders* internos e externos é imprescindível, a fim de divulgar informações confiáveis, padronizadas e atualizadas a estes públicos sobre o detalhamento da crise, assim como a evolução do tratamento por parte da empresa. Se isto não acontece, tanto a empresa como os *stakeholders* podem tomar decisões precipitadas e equivocadas e todos saem perdendo. Falhas na comunicação podem ser o acelerador para o agravamento da crise, que pode não ter volta.

Inexistência de plano de gestão de crise: o plano de gestão de crise é uma ferramenta fundamental para todas as empresas. É apresentada como ferramenta para a elaboração e manutenção de relacionamento com públicos de interesse em momentos de crise, incentiva o planejamento das ações de comunicação para que a organização consiga minimizar os problemas ou mesmo evite as crises. Isso deve ocorrer a partir do envolvimento e treinamento dos funcionários.

As empresas podem ainda não terem percebido a importância de conectar a gestão de riscos, a continuidade e o gerenciamento de crises, atuando como pilares fundamentais a sua perenidade. Isto é algo a ser perseguido e buscado como propulsores do aumento de valor das empresas.

Uma das lições aprendidas diante dos cenários de crises e de impacto reputacional é a preparação das organizações para enfrentar de forma mais estruturada estes cenários. Segundo as boas práticas, o gerenciamento de crises está sustentado por três pilares conforme apresentado a seguir.

Nesse contexto, as empresas devem trabalhar na construção do plano de gestão de crises (PGC) que deve considerar entre outras as seguintes etapas:



Elaborado pelos autores e adaptado de Deloitte e IBRI

Em resumo, enquanto a construção da boa reputação é constante, sua destruição pode acontecer em um piscar de olhos, sendo imperativo para as empresas gerenciar sua imagem e reputação cuidadosamente. Com o crescimento das mídias eletrônicas e sociais, as informações sobre as crises se dissipam rapidamente e capturam a atenção de diferentes públicos, deixando uma impressão indelével sobre a imagem e a reputação da empresa.

Aplicada ao negócio, a reputação representa uma interpretação ou percepção da confiabilidade ou integridade de uma organização. Pode-se basear em falsas percepções no curto prazo. Se for preciso, ao longo do tempo, a reputação fornece um barômetro de como uma organização provavelmente responderá em determinada situação. Importante ressaltar que a reputação é um ativo empresarial precioso e sua reparação é uma tarefa árdua, custosa e, se tardia, por vezes impossível.

As consequências do impacto na imagem e na reputação são extremamente graves, quer com relação aos prejuízos morais, financeiros e, de forma mais drástica, com a sua própria continuidade, que se não gerenciadas podem levar a empresa a sua extinção.

Dada a volatilidade das informações - verdadeiras ou não – que percorrem rapidamente, especialmente por meio das mídias sociais, parece-nos que o risco de imagem e reputação continuará aumentando nos próximos anos, o que significa que as empresas devem continuar seu aprendizado neste tema e agir rapidamente a fim de mitigar essas ameaças e garantir a perenidade de seus negócios.

Andrea Regina de Arruda Ramos Bueno
Profissional da área de Compliance, Controles Internos e Risco Operacional. Membro da Comissão de Riscos do IBGC e da Comissão de Governança nas Instituições Financeiras.

Corinto Arruda
Profissional da área de processos e riscos corporativos, Mestre em Controladoria (Fipecafi) e membro da Comissão de Riscos do IBGC.

Frederico de Campos Ventriglia
Profissional com atuação nas áreas de Governança, Riscos e Compliance, MBA Executivo (FGV), membro da Comissão de Gestão de Riscos e da Comissão de Governança em Instituições Financeiras do IBGC.

Ives Pereira Müller
Consultor e conselheiro formado pelo IBGC, foi sócio da Arthur Andersen e Deloitte Touch & Tohmatsu por quase 30 anos, na divisão de Consultoria em Gestão de Riscos, Governança e Sustentabilidade. MBA Executivo de Sustentabilidade (Stanford University) e "Risk & Brand Management" (Mumbay University). Membro da Comissão de Riscos do IBGC.

Luciana Bacci Costa
Coordenadora da Comissão de Riscos do IBGC. Participou dos grupos redatores do Guia do IBGC de Gerenciamento de Riscos Corporativos lançado em março/2017. MBA Executivo de Finanças, Controladoria e Contabilidade (Fipecafi) . MBA Executivo de Compliance (FGV-SP).

Marcus Vinicius Lanzelotti
Profissional da área de Gestão de Riscos Corporativos. Participou da elaboração do Guia do IBGC de Gerenciamento de Riscos Corporativos lançado em março/2017. Membro da Comissão de Riscos do IBGC.

Natasha Machado Anderáos
Profissional nas áreas de Governança, Riscos e Compliance. MBA Executivo (Insper). Membro da Comissão de Riscos do IBGC.

Tatiana Leite
Profissional da área de Governança Corporativa, Compliance, Auditoria e Gestão de Riscos. MBA – CEAG – FGV. Membro da Comissão de Riscos do IBGC.

Waldemir Bulla
Profissional com mais de 30 anos de experiência apoiando a Alta Administração (Conselho, Comitês e Diretoria) na implantação e gestão de projetos em Governança Corporativa, Auditoria Interna, Gerenciamento de Riscos e Compliance. Experiência profissional consolidada como (Sócio e Diretor) em organizações internacionais de Auditoria e Consultoria (Arthur Andersen, EY, Protiviti e Deloitte) . Membro da Comissão de Riscos do IBGC.

Os desafios do auditor interno na mitigação do risco de fraude

Por Fabio Mendes e Geert Aalbers

Enquanto regras e leis regulamentarem o mundo corporativo, fraudadores oportunistas encontrarão uma forma de violá-las. A Association of Certified Fraud Examiners (ACFE) estima que empresas perdem 5% da sua receita anual para fraudes.

Há décadas, acionistas e executivos têm se preocupado com as ocorrências de fraudes pelo mundo. No Brasil, após a Lei anticorrupção nº 12.846/13 e a Operação Lava Jato, deflagrada em março 2014 e a qual buscou-se empresas envolvidas em esquemas de corrupção contra erário público, intensificou-se a busca pelo fortalecimento dos mecanismos de controles internos para prevenir e remediar riscos de fraude e conformidade.

O alto número de casos de fraude e corrupção relatados na mídia nos últimos anos indica que o ambiente das empresas está cada vez mais vulnerável à materialização de "risco de fraude", podendo gerar perdas financeiras expressivas, redução das margens de lucros, dano à imagem e reputação e até a falência.

Em detrimento da sofisticação dos fraudadores em subtrair ativos das empresas e pressão dos órgãos fiscalizadores para combater crimes corporativos, tem crescido a preocupação para acionistas e executivos, os quais precisam investir cada vez mais em uma boa defesa dos seus riscos para prevenir e detectar ocorrência de fraude.

Desde pequenas empresas locais a multinacionais, as empresas precisam rapidamente adequar suas estruturas e mecanismos de defesa do risco de fraude. A auditoria interna – considerada a terceira linha

de defesa, precisa atuar com a missão de ser "o melhor goleiro do mundo" para continuar melhorando a sua habilidade de identificar risco ou ocorrência de fraude.

Ou seja, diante deste contexto, o melhor ataque é uma boa defesa. Faz-se necessário que as auditorias internas continuem focando e dedicando suas horas do seu plano em prol da detecção do "risco de fraude". Vale reiterar que segundo Normas Internacionais - Prática Profissional de Auditoria Interna do IIA (Normas), - International Professional Practices Framework (IPPF), o auditor interno deve possuir "conhecimento suficiente para avaliar risco de fraude", apesar de necessariamente não existir um profissional especializado em "detectar e investigar fraude" no time de algumas auditorias internas.

O investimento em tecnologias para análises de dados ("*data analytics*") une investigadores de fraudes corporativas, gestores de *compliance* e auditores internos, e representa uma mudança de paradigma. O objetivo passa a ser a detecção tempestiva da fraude e a redução da probabilidade e do impacto que esta representa.

Segundo a ACFE, as organizações que não possuíam controles internos voltados para a prevenção de fraude sofreram, em média, duas vezes mais perdas quando comparadas com empresas que possuíam programas antifraude, tais como o monitoramento e análise de dados e sistemas, avaliação de gestão e canais de denúncia[1].

Diante do exposto, o auditor interno deve zelar e ter habilidades para o bom exercício da sua função com independência e profissionalismo, visando aumentar a probabilidade de identificar erros significativos, fraudes ou não conformidades, buscando realizar análise de dados no planejamento e execução das auditorias. Cada vez mais, para os executivos que buscam aumentar a competitividade de suas empresas, a prevenção de fraudes executada de forma eficiente e efetiva se mostra uma oportunidade única para melhorar os resultados da empresa e reduzir perdas.

Redução de perdas

O uso da tecnologia para detectar fraudes e apoiar nos programas de auditoria interna, além de reduzir as perdas, requer investimento, mas pode gerar um retorno expressivo.

Por exemplo, uma instituição financeira no Brasil, recentemente, implementou uma solução de análise de dados para monitorar e prevenir fraudes. A solução agrega, analisa e permite a visualização dos dados de sistemas da empresa, o que melhorou significativamente a eficiência e eficácia de sua equipe de investigação de fraudes.

Esta solução inteligente permitiu que a equipe mudasse a forma de combater esses ilícitos. Ou seja, passou a atuar de forma preventiva, ao invés de reativa, proporcionando uma recuperação significativa de perdas financeiras. O retorno sobre investimento realizado com a implementação desta solução foi acima de 1.000%.

A evolução de soluções tecnológicas, como a análise preventiva de dados, pode fazer com que as empresas repensem a ideia de que perdas causadas por fraude são inevitáveis. Avanços na tecnologia continuam reduzindo os custos da detecção de fraudes, ao mesmo tempo em que aumentam sua eficiência.

Recentes evoluções em medidas antifraude favorecem o investigador, reduzem custos de mão de obra e aumentam a eficiência operacional na luta contínua para prevenir fraudes. Tais soluções permitem que o investigador:

- Melhore a identificação de potenciais incidentes gerados por fraudes ao utilizar regras para melhorar a precisão da detecção e reduzir a chance de "informações não confiáveis";
- Elimine o tempo que seria gasto investigando ocorrências não fraudulentas.
- Priorize o foco das investigações ao utilizar uma abordagem baseada nos riscos, direcionando os investigadores a analisarem primeiro as transações

1. http://www.fraudweek.com/uploadedFiles/Fraudweek/2016/content/Staggering-Cost-of-Fraud-infographic%202016%20FW.pdf

potencialmente fraudulentas de maior risco ou de maior valor, otimizando a alocação e o uso dos recursos internos.

- Melhore o processo de avaliação e tomada de decisões por meio da criação de um ambiente acessível e centralizado, e da redução da necessidade de tarefas manuais para coletar, analisar e revisar as informações. Isto aumenta a eficiência e a eficácia dos investigadores.

Papel da auditoria interna

Segundo IPPF The IIA Global, 2120 – Gerenciamento de riscos, a atividade de auditoria interna deve avaliar a eficácia e contribuir para a melhoria dos processos de gerenciamento de riscos, incluindo "avaliar o potencial de ocorrência de fraude, e como a organização gerencia o risco de fraude".

A auditoria interna precisa considerar no seu planejamento dos trabalhos o "risco de fraude", utilizando-se de técnicas de análise de dados para tornar as análises mais abrangentes, efetivas e eficazes. Ou seja, a auditoria interna precisa reduzir a probabilidade ao máximo de "não detectar risco de fraude", afinal, auditor precisa mitigar riscos inerentes a sua atuação.

O verdadeiro custo da fraude

Muitas vezes, a perda atribuída à fraude considera apenas os custos diretos, ou seja, aqueles gerados pelo próprio ilícito. Pouca atenção é dada à gama de outros impactos negativos, tais como a perda de motivação dos colaboradores e os danos reputacionais. Em uma era em que a lealdade do consumidor pode mudar em 140 caracteres, danos reputacionais podem ser desastrosos.

Quando os custos adicionais são considerados no custo total da fraude, o retorno sobre o investimento em um programa de prevenção de fraudes pode ser ainda maior. Inclusive, estudos feitos pela Universidade de Nevada (2014)[2] e pela

Universidade Friedrich-Alexander (2015)[3], identificaram que empresas envolvidas em fraudes implicando seus altos executivos poderiam sofrer uma queda de 30% no preço das suas ações, além da perda causada pelo ato ilícito.

É preciso investir em tecnologias eficazes para realizar análise de dados, auxiliar em investigações internas e apoiar gestores de *compliance*, pois o foco dos trabalhos de auditoria precisa sempre de aprimoramento, visando reduzir a probabilidade e impacto dos atos ilícitos nas empresas.

A "nova" auditoria Interna

O grande desafio não é apenas ser cético e ter uma boa experiência para investigar fraude. É necessário conhecer a cultura, processos, controles e complexidade das operações dos negócios. Além disso, o profissional deve ser especializado em detectar riscos de fraude e ter a habilidade

2. http://www.fox.temple.edu/cms/wp-content/uploads/2012/05/karpoff-KLM-bribery-paper-23Jan2014.pdf
3. http://ssrn.com/abstract=2557270
4. IIA Brasil – Instituto dos Auditores Internos do Brasil

para investigar, atentando para os aspectos legais com objetivo de reduzir a chance de passivos jurídicos e riscos reputacionais para empresa decorrente de uma investigação malconduzida.Desafios operacionais na luta contra fraudes.

Desafios operacionais na luta contra fraudes

Além da perda de receita, empresas também incorrem em custos operacionais (p. ex., custos com mão de obra) ao dedicar recursos e ativos para detectar, remediar e recuperar-se da fraude. Em empresas maiores ou que possuem maior exposição aos riscos de fraude, áreas de negócios têm evoluído consideravelmente, mas nem sempre no mesmo ritmo dos fraudadores.

Para algumas instituições financeiras globais, o programa de detecção de fraudes existente é o mesmo piloto que foi implementado anos atrás. Além disso, os programas não foram atualizados ou aprimorados para considerar a crescente sofisticação das fraudes.

Investigadores costumam ser recursos caros em momentos ineficientes e subjetivos. Em grandes empresas globais, informações críticas para a detecção da fraude estão soterradas sob uma miríade de sistemas inacessíveis. Investigadores, então, são forçados a revisar e agregar as informações necessárias para avaliar os incidentes da potencial fraude de forma manual, cobrando por hora utilizada podendo gerar uma bola de neve de custos operacionais.

Empresas podem aumentar o retorno sobre investimentos ao implementar tecnologias inteligentes para monitoramento de riscos em tempo real, utilizando análises de dados ("*data analytics*") que não apenas reduzem o tempo e os custos de apuração, mas também fazem melhor uso de recursos limitados.

As áreas de compliance e a auditoria interna nas empresas também podem ajudar os gestores a tomarem decisões mais inteligentes, fornecendo informações precisas e sugestões práticas no combate a fraudes e na proteção dos ativos da empresa. Uma solução eficaz de prevenção de fraude não apenas ajuda empresas a reduzir as perdas geradas pela fraude e outros riscos associados, mas também a tomar decisões bem fundamentadas, assim, contribuindo na sua capacidade para apoiar no gerenciamento dos riscos estratégicos, aumentando sua lucratividade e sustentabilidade.

Fabio Mendes

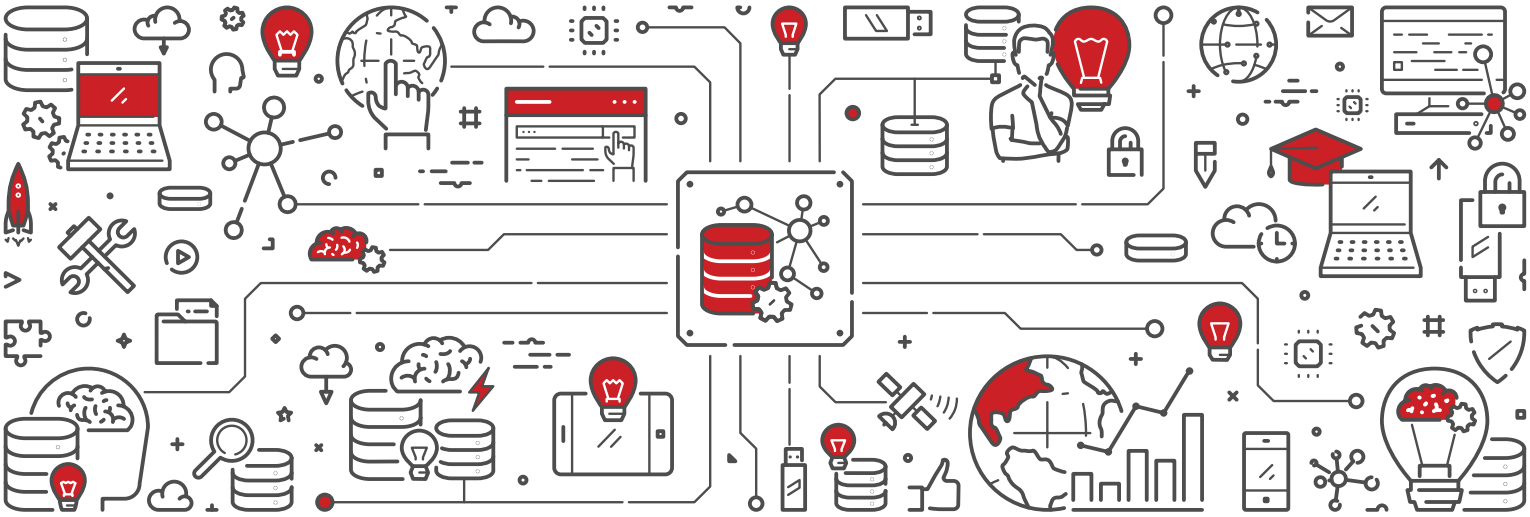
Head de auditoria interna no SBT, membro da Comissão de Gerenciamento de Riscos Corporativos do IBGC, membro voluntário do Instituto dos Auditores Internos (IIA Brasil) - Chefe de Auditoria Interna e professor de cursos de MBA no Brasil e Portugal, nas universidades Trevian - Escola de Negócios, Universidade do Oeste Paulista – UNOESTE e Universidade de Coimbra Business School.

Geert Aalbers

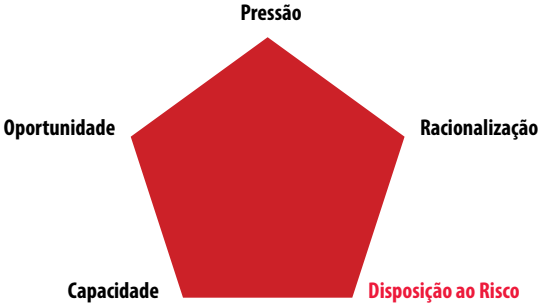
Sócio sênior da Control Risks, membro do comissão de Gerenciamento de Riscos Corporativos do IBGC e professor da Insper no curso Gestão de *Compliance*.

A vida profissional após a fraude

por Gustavo Ebner Melchiori e Renato Santos



Entender as razões que levam os indivíduos a engajarem-se em fraudes é um desafio antigo e explorado por diversos estudiosos do tema. Um dos modelos mais conhecidos e respeitados é o "Triângulo da Fraude", desenvolvido por Cressey (1953), no qual o autor defende que para uma fraude ocorrer, é necessário que três fatores subsistam: racionalização, pressão ou necessidade, e oportunidade. Posteriormente, Wolfe e Hermanson (2004) apresentaram o modelo "Diamante da Fraude" com a inclusão do fator 'capacidade' e, em 2015, Santos propôs uma evolução destes modelos com a inclusão de mais um novo vértice ao modelo: a "Disposição ao Risco", formando o "Pentágono da Fraude" (ver figura)



Antes de se tornar um fraudador, o então colaborador efetua um balanço dos custos *versus* benefícios envolvidos advindos com a fraude e, com isso, precisa estar disposto a "enfrentar" os riscos envolvidos na operação. O vértice de "disposição ao risco" foi decomposto em três tipos de risco: (i) risco perigo, que representa o medo das consequências, (ii) risco probabilidade, que representa o risco de ser identificado e o (iii) risco aventura, que representa a ousadia, o desafio de superação no cometimento do delito.

Nesse novo modelo, o vértice da "Disposição ao Risco", traz à tona a discussão sobre o papel das organizações em poder influenciar a tomada de decisão de seus colaboradores por meio do aumento da percepção sobre os riscos, sobre a severidade das possíveis consequências e probabilidade de identificação da fraude.

Uma das ferramentas muito discutidas no combate e prevenção a fraudes é o processo educativo, no qual tem por objetivo principal conscientizar os colaboradores e influenciar sua decisão para o não envolvimento com fraudes. Fazendo um paralelo com os modelos preditivos discutidos anteriormente, o objetivo principal é o de influenciar a

decisão dos colaboradores no que tange a sua "racionalização" e "disposição ao risco".

Entretanto, pesquisa realizada pela Association of Certified Fraud Examiners - ACFE (2018) aponta que empresas vítimas de fraudes ocupacionais constantemente optam por não aplicarem sanções severas aos autores dos desvios de conduta, sendo que a razão mais citada pelos empregadores é o medo de uma má publicidade.

Mas, no "país da Lei de Gerson", em que o bordão "tem que levar vantagem em tudo" tem imperado, o desenvolvimento moral nem sempre é trabalhado e, certamente a impunidade não contribui com a moralidade.

Em função destas considerações, o objetivo da pesquisa aqui exposta foi de compreender os possíveis impactos na vida profissional de funcionários que optaram por cometer fraudes contra seus empregadores, lançando luz a uma discussão do quão efetivas são as medidas disciplinares contra atos fraudulentos e, com isso, refletindo o quão capaz elas são de influenciar a percepção de outros colaboradores sobre os riscos envolvidos e severidade das consequências de seus atos.

Resultados da pesquisa

A pesquisa foi elaborada a partir de dados cedidos pela S2 Consultoria, empresa especializada em gestão de risco e apuração de fraudes ocupacionais, a qual forneceu informações secundárias de 95 entrevistados em casos onde foi constatado o envolvimento de profissionais em fraudes ocupacionais, ou seja, fraudes cometidas contra seus empregadores entre os anos de 2016 e 2017. As entrevistas foram realizadas a pedido de 23 empresas sediadas no Brasil, de diferentes segmentos.

A metodologia do estudo foi baseada em pesquisa de mídia e posterior análise qualitativa e quantitativa. A partir da base de dados, foram selecionados intencionalmente dezoito profissionais – de níveis variados – cujas informações públicas disponíveis preenchiam os pré-requisitos necessários para a pesquisa, ou seja, tinham informações públicas disponíveis a respeito de suas atividades profissionais. A amostra se restringiu a apenas 19% do banco de dados por conta da dificuldade em se pesquisar esse segmento da população, que muitas vezes prefere se manter no anonimato em decorrência do delito. As pesquisas foram realizadas entre junho e novembro de 2017 e, para minimizar a possibilidade de desvios na análise, as informações foram confirmadas em diferentes fontes de informações ou em base de dados oficiais. Com base no acordo firmado com a S2 Consultoria, as informações são confidenciais e o nome dos pesquisados, bem como de seus empregadores, foram preservados.

A pesquisa identificou que após terem seus contratos de trabalho rompidos, devido a constatação de seu envolvimento em fraudes ocupacionais, 44% dos pesquisados abriram uma empresa (CNPJ) e pelo menos 28% deles mudaram de estado após o desligamento. Os dois principais motivos para a mudança de estado foram: por conseguirem uma oportunidade profissional em outro estado ou para empreender em sua cidade natal ou na cidade do cônjuge.

Também foi identificado que pelo menos 44% dos fraudadores instauraram uma ação trabalhista contra seus empregadores. O alto índice de ações trabalhistas, considerando que os reclamantes são fraudadores confessos, possivelmente indica a ausência de responsabilização ou custos no caso de registro de ações trabalhistas infundadas ou inidôneas. Esse contexto tende a mudar após a Reforma Trabalhista (Lei 13.467/2017), que entrou em vigor em 11 de novembro de 2017, a qual prevê que reclamantes que perderem ações na Justiça Trabalhista poderão arcar com os custos processuais e tendem a sofrer sanções como multas e/ou indenizações, caso entendido que houve má fé no ingresso da ação.

Os dados apontam que estes profissionais levaram em média 4 meses para iniciar uma nova atividade profissional, sendo dois terços deles recolocados em uma empresa privada e um terço como empreendedor. No que tange a carreira profissional dos fraudadores avaliados, não foi identificado um impacto

expressivo por terem sido demitidos, pois de acordo com pesquisa realizada pela Confederação Nacional de Dirigentes Lojistas e pelo Serviço de Proteção ao Crédito (2017), no Brasil, as pessoas levam em média 12,2 meses para se recolocarem no mercado de trabalho.

A rapidez na recolocação destes profissionais ao mercado de trabalho demonstra a fragilidade das empresas em identificar esse perfil de risco durante o processo seletivo. Uma das soluções que as empresas têm adotado é implantação de testes de integridade, que auxiliam o empregador a identificar o grau de resiliência do colaborador em situações de dilemas éticos.

A pesquisa demonstra ainda que pelo menos um terço destes profissionais receberam promoção em seu novo emprego, ou seja, foram contratados para ocupar posições hierárquicas superiores às ocupadas e, possivelmente, também houve aumento salarial. Em sua maioria (75%), os pesquisados continuam atuando na mesma área. Estes dados indicam que estes profissionais podem estar expostos a uma maior oportunidade para operacionalizar outras fraudes, uma vez que estará exposto a uma maior responsabilidade, poder de decisão e alçadas de aprovações.

Com base nos dados obtidos e, considerando o impacto de fato na carreira dos fraudadores analisados, a fraude no Brasil compensa?

A pesquisa demonstra que o impacto na carreira dos pesquisados é pouco expressivo, deixando a sensação de que a fraude pode compensar, o que traz um alerta para a boa governança corporativa: medidas mais eficazes para seu combate são necessárias.

Nesse sentido, a criação de leis para criminalização da corrupção privada no país é imprescindível. Também é fundamental o reforço de medidas nas próprias empresas para coibirem esse tipo de atitude, tanto na prevenção à fraude com: (i) aplicação de testes de integridade no processo seletivo, (ii) constituição e comunicação de código de conduta e (iii) desenvolvimento e treinamento sobre o tema para os colaboradores, como também por meio da devida reação a atos fraudulentos por meio de: (iv) implantação de canais de denúncias, (v) apurações robustas dos casos identificados e/ou denunciados, (vi) independência da área responsável pela apuração e (vii) aplicação de medidas disciplinares adequadas.

Gustavo Ebner Melchiori

Formado em Administração de Empresas, mestre em Business Economics pela City University of London e MBA em Gestão de Riscos e Compliance pela Trevisan Escola de Negócios. Atuante na área de Combate à Fraude, Compliance e Auditoria há 8 anos e, atualmente, parte da equipe de auditoria da Louis Dreyfus Company responsável pela região da Europa, Oriente Médio e África.

Renato Santos

Advogado, MBA Gestão de Pessoas, mestre e doutor em administração pela PUC-SP, sócio-diretor da S2 Consultoria, membro da comissão de Gerenciamento e Riscos e professor da disciplina Ética e Dimensão do Risco Humano, na Trevisan Escola de Negócios, FECAP e FESP. Autor do livro *Compliance Mitigando Fraudes Corporativas*.

REFERÊNCIAS

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS - ACFE. “Report to the nations on occupational fraud and abuse”, 2018. Disponível em < http://www.acfe.com/report-to-the-nations/2018/. Acesso em 19 mai 2018.

CRESSEY, Donald Ray. Other people’s money: a study in the Social Psychology of embezzlement. New York: Free Press, 1953.

SANTOS, Renato de Almeida. Modelo preditivo de fraude ocupacional nas organizações privadas. Tese (Doutorado). Pontifica Universidade Católica de São Paulo – PUC. São Paulo, 2016.

S2 CONSULTORIA. Disponível em < http://www.s2consultoria.com.br. Acesso em 19 mai 2018.

WOLFE, David T.; HERMANSON, Dana R. “The fraud diamond: considering the four elements of fraud”. CPA Journal, New York, vol. 74, 2004, pp. 38-42.

Gestão de riscos – planejamento estratégico nas organizações públicas

por João Francisco Arcoverde Lopez

O gerenciamento de riscos corporativos nas organizações dos setores privados – indústria, instituição financeira, prestação de serviços, empreendimentos, infraestrutura – está incorporado nos respectivos processos de planejamento estratégico, na medida em que a identificação e mensuração dos riscos (estratégicos e operacionais) inerentes aos negócios, necessitam ser tratados com muita seriedade e comprometimento por parte das administrações.

A sobrevivência dos negócios e a capacidade de geração de valor das organizações que se importam com os seus riscos, são evidentes.

O gerenciamento dos riscos de imagem, de integridade, produto e qualidade de atendimento de clientes, permite a constante inovação das organizações, a partir da construção de planos de ação para a melhoria contínua dos processos, com grande envolvimento dos conselhos de administração, dirigentes e gestores.

Na administração pública, o gerenciamento de riscos tem evoluído consideravelmente nas três esferas de governo, a partir da aplicação de leis e instruções relacionadas à governança para as administrações direta e indireta (municipal, estadual e federal). Os órgãos de regulação e de controle têm fomentado as boas práticas, produzindo o conhecimento por meio de informações, cartilhas e cursos para a formação e desenvolvimento de funcionários e agentes públicos. A Lei nº 13.303, de 30/06/2016 – Estatuto Jurídico da Empresa Pública, da Sociedade de Economia Mista e suas Subsidiárias – e a Instrução Normativa Conjunta nº 1, de 10/05/2016, – Controles Internos, Gestão de Riscos e Governança no Âmbito do Poder Executivo Federal, do Ministério do Planejamento, Orçamento e Gestão e da Controladoria-

Geral da União (CGU) –, foram fundamentais para a introdução da gestão de riscos na administração pública.

Existem esforços importantes de instituições que incorporaram o *compliance*, atentas às questões de transparência, controle interno e social e de integridade. São iniciativas que levam em conta a inserção do processo de gerenciamento de riscos.

Ainda que haja muito a fazer em termos de governança, transparência, gestão de riscos, controle e auditoria no setor público, o fato é que tem havido uma evolução gradativa em sua gestão.

Entretanto, ainda são pouco visíveis as inciativas do gerenciamento de riscos integrado ao planejamento estratégico.

Os reflexos negativos da ausência desta tão importante integração têm sido percebidos quando ocorre a materialização de riscos que poderiam ter sido mitigados, com ações preventivas e de controle, planejados, que pudessem amenizar as perdas dos setores de saúde, educação, segurança pública, habitação e outros.

O planejamento estratégico nos órgãos da administração pública, se associado ao gerenciamento de riscos, poderia mitigar os acontecimentos nefastos que pegam a sociedade de surpresa - de natureza climática, social e econômica – que são reincidentes nos municípios, nos estados e na federação. Bons planejamentos, integrados à gestão de riscos, poderiam minimizar os efeitos de enchentes sazonais, desmoronamentos de encostas, má conservação de vias e estradas públicas, distúrbios sociais, agressões ao meio ambiente, escassez de água e saneamento e inadequado dimensionamento de serviços às demandas sociais.

Agora, não se trata de aplicar o processo de gestão de riscos unicamente sob o ponto de vista corporativo, para mitigar os eventos localizados em um determinado órgão ou empresa pública. Trata-se do processo de gestão de riscos com uma visão mais abrangente, com o norte do atendimento às demandas sociais como um todo.

A identificação, mensuração e tratamento dos riscos dos diversos negócios envolvidos na administração pública, permitem bons planos de ação, programas de integridade e planos de contingência, que podem ser dimensionados, priorizados e equilibrados em termos de recursos humanos, materiais e financeiros.

O caminho a ser seguido para o desenvolvimento da gestão de riscos estratégicos na administração pública parece ser difícil, dado o gigantismo da rede de serviços, da diversidade de organizações e administrações e da falta de sintonia entre os órgãos pertencentes às diferentes esferas de governo, que necessitariam estar integrados no trato das demandas sociais.

Os desafios são os indutores das mudanças de paradigmas. É preciso ser perseverante na busca de políticas e processos organizacionais que, progressivamente, possam elevar a quantidade e a qualidade dos serviços públicos.

Um caminho factível, parece ir na direção do fomento do planejamento estratégico integrado à gestão de riscos.

Não como sendo um caminho exclusivo e independente de uma determinada secretaria municipal, estadual ou de um órgão da federação. É preciso disseminar o conceito e o processo de gestão de riscos de forma integrada, nas unidades da administração direta, nas empresas públicas, nas fundações e nas agências.

Capitaneadas pelo ministério e secretarias de planejamento, nas diferentes esferas da administração pública, as unidades governamentais precisam estar integradas em programas abrangentes de gestão de riscos estratégicos, que tenham bons conteúdos programáticos, incluindo ações para a disseminação de conhecimento dos dirigentes e gestores públicos, capacitação e desenvolvimento dos funcionários e orientação técnica para a implantação dos processos e ferramentas de gestão.

Um programa abrangente de gestão de riscos contribui para a priorização e otimização dos recursos orçamentários, que precisam ser direcionados para projetos e ações relevantes, que não podem ser preteridos na tomada de decisão dos investimentos públicos.

João Francisco Arcoverde Lopez
Administrador de empresas, membro da Comissão de Gerenciamento de Riscos Corporativos do IBGC e consultor independente para assuntos de governança de instituições públicas.

Gestão de Riscos ASG: reflexões sobre crises empresariais

por João Redondo, Paulo Vanca, Amália Sangüeza, Sérgio Mindlin e Carlos Eduardo Lessa Brandão

A análise de casos reais de fracassos em gestão de riscos permite tirar lições sobre como prevenir novos casos, tanto em áreas Ambiental, Social e Governança (ASG), como em quaisquer outras. O fracasso parte da premissa de que a empresa tem uma função de gestão de riscos. Se adequadamente estruturada, com reporte correto na organização e processos definidos, é uma questão de governança corporativa. As melhores práticas recomendam a sua existência. A não existência da função já é um problema na governança.

Portanto, o G do ASG está implícito em qualquer caso de sucesso ou fracasso em gestão de riscos. Assim, focamos na análise de casos de fracassos em que o tema foi ambiental e/ou social, além da governança, já implícita. A gestão de riscos sempre se inicia com o mapeamento de riscos, avaliação de potenciais impactos da sua materialização e análise de probabilidade de ocorrência, principalmente em função da vulnerabilidade de processos e controles.

Tanto na área ambiental como na social, a questão básica para todo conselheiro de administração e todo membro de comitê de auditoria é se assegurar que processos e ações relacionados a essas áreas estão mapeados, avaliados e incluídos no mapeamento de riscos. E que os riscos estão sendo adequadamente gerenciados.

Nas duas áreas há riscos decorrentes de ações internas fora das regras e códigos de ética internos, como fraudes em informações e/ou processos.

Dado que a atuação do conselho de administração deve atentar, entre outras atividades, para o gerenciamento dos riscos, deve-se discutir quais perguntas deveriam ser feitas aos executivos das organizações. Da mesma forma, como poderiam se certificar com certo nível de conforto, de que as vulnerabilidades são conhecidas e que controles existem.

A organização, muitas vezes, sofre pressões por resultados de curto prazo, até mesmo em função da cultura dominante. Porém, no extremo e diante de situações críticas, os valores internos serão testados e, se houver possibilidade de uma ação discricionária dos executivos, estes poderão tomar decisões nem sempre em consonância com os valores da organização, privilegiando seus interesses pessoais em detrimento dos da organização.

É comum que temas ligados a ASG atraiam pouca atenção do conselho, por desconhecimento dos riscos, complexidade ou pelo pouco tempo que esses temas demandam do colegiado. Dependendo do setor de atuação, estes temas podem ter impacto relevante na organização. Dado que riscos associados a temas ASG têm tido maior relevância nas avaliações por parte do mercado, manter estrutura de governança que considere boa gestão do mapa de riscos pode significar melhor posicionamento das ações e, portanto, atração de investimentos menos especulativos. Além disso, a forma como a empresa gerencia esses riscos pode reduzir significativamente o custo de capital e, em alguns casos, habilitar a organização para acesso a fundos de investimentos específicos.

O caso abaixo traz a reflexão em torno da aparente dicotomia entre lucro e atuação ética. A questão em pauta é qual é o preço que a empresa está disposta a pagar para auferir mais lucro?

Fraude na manipulação de resultados de emissões de poluentes para carros

É fato que tem aumentado a pressão para que montadoras de veículos migrem a tecnologia para uma que seja mais limpa e que utilize matriz energética mais eficiente e menos dependente da cadeia do petróleo. Enquanto essa mudança não ocorre, montadoras europeias passaram a equipar automóveis com motores a diesel que consomem menos e são mais eficientes. Mas, por outro lado, emitem poluentes mais nocivos à saúde do que os motores a gasolina, o que fez as autoridades na Europa e nos EUA exigirem níveis de emissões de poluentes cada vez mais baixos.

Em 2015, após a revelação do escândalo da manipulação dos dados de emissões de poluentes nos motores a diesel de várias montadoras europeias e japonesas, o caso de uma grande montadora de veículos teve enorme destaque na mídia internacional. A empresa passou por uma crise reputacional sem precedentes. Os dados levantados pelas autoridades americanas (EPA e a California Air Resources Board - CARB) revelam que os testes de emissões de poluentes para veículos movidos a diesel eram fraudados e apontavam para uma emissão até 40 vezes menor que a real[1]. Tal fraude ocorreu entre maio de 2006 a novembro de 2015. Segundo o ex-CEO da empresa, apenas gestores da média gerência das fábricas sabiam da fraude. Mesmo assumindo que, em 2014, tomou conhecimento do fato, o executivo tornou-se leniente com a prática, já que não agiu para que a ilegalidade deixasse de existir. Não se sabe se o conselho de administração tinha conhecimento do procedimento fraudulento. Mas sua prática por tantos anos indica que ou o conselho era conivente, o que é difícil de imaginar, ou não exerceu adequadamente sua função de supervisão.

Os impactos causados à empresa foram significativos. Apenas nos EUA foram US$ 26 bilhões em multas. Em setembro de 2015 as ações chegaram a despencar 22% na Bolsa de Frankfurt[2].

Relacionada ao tema ambiental, com graves impactos, essa fraude deve ser encarada como severa falha de governança. O caso demonstra um grave caso de leniência/conivência da liderança que, ao tomar conhecimento da prática não atuou para impedir a continuidade, assim como não veio a público para esclarecimentos. Tal atitude estaria ligada ao receio de perdas de grande monta, assim como a danos à imagem? Ter permitido a continuidade da prática poderia ser uma forma de não comprometer o modelo de remuneração baseado nos resultados de curto prazo da empresa? De onde veio a orientação para burlar o sistema de medição de poluentes? Como isso deveria ter sido acompanhado pelo conselho de administração da empresa? No plano estratégico, como equilibrar o apetite para crescimento no mercado e a adesão aos rigorosos níveis de emissão? Não cabia ao comitê de auditoria, que frequentemente se concentra em aspectos financeiros, dar atenção aos temas ASG e ter verificado se os motores se enquadravam nos parâmetros de emissão exigidos pelas autoridades? E, especialmente, que os testes reproduziam reais condições de uso?

O conselho de administração tinha em seu mapa de riscos as externalidades que seriam transferidas à sociedade ao permitir a emissão de partículas poluentes acima do permitido?

Mão de obra em condições degradantes e análoga ao trabalho escravo

É natural empresas procurarem reduzir os custos de aquisição, tanto de matéria-prima quanto de produtos acabados. Para isso, uma prática utilizada é a terceirização de parte da produção utilizando cadeias consolidadas com maiores volumes, logística consolidada etc. e evitar a verticalização de atividades na operação. Esse processo exige da empresa a mudança do modelo mental de decisão, assim como a revisão do mapa de riscos, já que não terá supervisão direta das atividades e também trabalhará com diferentes culturas e prioridades.

Ao terceirizar, a empresa deve compreender que o risco reputacional aumenta exponencialmente, pois haverá em sua cadeia de valor, atores que não necessariamente compartilham dos mesmos valores. Desta forma, a organização deve estabelecer rigoroso processo de governança e controle, além de revisitar o mapa de riscos para considerar outros fatores antes pouco expressivos.

Diante de problemas advindos desse modelo, a empresa jamais deve-se eximir da sua responsabilidade sobre o que acontece no ambiente das empresas contratadas para execução de serviços em seu nome.

Em julho de 2011, uma equipe de fiscalização do Ministério do Trabalho brasileiro encontrou em uma casa, em São Paulo, 16 pessoas estrangeiras (bolivianos e paraguaios) que viviam e trabalhavam em condições análogas ao trabalho escravo. Eles produziam peças para um fornecedor de uma empresa detentora de uma marca de roupas que faz parte de um grupo espanhol.

O flagrante, objeto da denúncia, expôs uma prática que, infelizmente, tem sido utilizada por diversas empresas do setor da moda, não só no Brasil como em outros mercados. Essas empresas operam com estratégia de preços baixos e buscam reduzir os custos de fabricação gerando externalidades sociais. Utilizam-se da terceirização e quarteirização e esperam não colocar em risco a reputação da empresa.

A empresa veio a público e informou que se tratava de uma "terceirização não autorizada", que "atenta contra seu Código de Conduta e a qual o Grupo repudia absolutamente". De acordo com nota emitida pela empresa na época dos fatos, cerca de 50 fornecedores no Brasil produziam peças para a marca e contavam com mais de 7 mil trabalhadores.

Em 2012, como parte das negociações junto aos órgãos de fiscalização do governo, a rede de varejo concordou em pagar R$ 3,150 milhões num termo de ajuste de conduta (TAC). Esse valor seria usado em projetos com organizações não governamentais para estabelecer ações que impedissem a ocorrência desse tipo de prática em sua cadeia de fornecimento.

No mesmo ano, ao relatar as atividades e desempenho nos negócios referente ao ano de 2011, o relatório anual[3] destacou o caso e informou sobre os entendimentos com o Ministério do Trabalho.

O fato em si parece não ter afetado significativamente os resultados da empresa, que em 2013 registrou um lucro de € 2,4 bilhões, para um faturamento global de € 16,7 bilhões, montante 5% acima do obtido no ano anterior. O número demonstrou na época que a empresa continuava sendo preferida dos investidores e analistas globais, bem como de consumidores, que tinham pouca informação para avaliar as práticas de responsabilidade social da empresa.

Quatro anos após o ocorrido, a empresa foi novamente alvo de denúncias por descumprir o Termo de Ajuste de Conduta, o que gerou obrigações adicionais para a empresa, além do pagamento de R$ 5 milhões como "investimento social".

Em novembro de 2017 a justiça do país decidiu que a empresa é a responsável pelo caso de trabalho análogo à escravidão registrado na cadeia produtiva da marca em 2011. No acórdão divulgado, o relator do caso considerou que seria "impossível" a empresa não conhecer as condições de trabalho nas oficinas subcontratadas. O juiz informa em seu parecer a existência de uma espécie de "cegueira conveniente".

Esse caso contribui para alertar líderes organizacionais quanto ao papel social da empresa e o imperativo de uma atuação responsável pautada por princípios éticos.

Fica evidente que a decisão de terceirizar ou quarteirizar parte do processo produtivo foi para não verticalizar processos fabris e garantir menor custo unitário por peça produzida. Dado que a decisão foi tomada, algumas perguntas fazem sentido para buscar compreender o processo de análise de riscos.

Se esse modelo é o comumente utilizado no setor de moda, a empresa mantinha estrutura com profissionais especializados na gestão de terceiros, assim como promovia auditoria própria ou por meio de empresa especializada para acompanhar os contratados?

O mapa de riscos da empresa alertava para o risco reputacional, assim como os estudos financeiros apontavam para a decisão de menor custo? A decisão de terceirizar sem o devido suporte de auditoria e acompanhamento considerou os riscos atrelados ao modelo a ser adotado?

Qual a responsabilidade do conselho de administração da empresa? A filial brasileira é de capital fechado, mas a controladora é de capital aberto. Quanta atenção o conselho dedica a riscos socioambientais? Na busca de resultados, os sistemas de remuneração variável incluem metas sociais e ambientais? Há uma estrutura independente dedicada a esses assuntos com poder de interferir junto à alta administração?

Em que medida a decisão tomada sob olhar estritamente financeiro considerou os riscos reputacionais?

Fraudes em certificados de qualidade de alimentos

Nosso último caso contribui para uma reflexão em torno da atuação não ética de uma reconhecida empresa no segmento de alimentação. A incapacidade de gerenciar adequadamente processos fitossanitários na manipulação de alimentos permitiu que certificados de qualidade fossem adulterados por muitos anos, comprometendo a segurança alimentar dos consumidores.

O caso se tornou público após investigação da Polícia Federal, em março de 2017, quando dezenas de empresas do setor de alimentos foram indiciadas por fraudes em resultados de laudos de qualidade de seus produtos. A empresa em questão foi investigada por supostas irregularidades por uso de material impróprio na fabricação de alimentos em um frigorífico de carnes de aves. [4].

Em relação às acusações, a empresa informou na época que estava colaborando com as autoridades para o esclarecimento dos fatos e afirmou que cumpria as normas e regulamentos referentes à produção e à comercialização de seus produtos e que não compactuava com práticas ilícitas. Menos de um ano após o primeiro episódio a empresa voltou a ser alvo de nova denúncia, agora com origem em um ex-funcionário que informou à justiça que era obrigado a fraudar documentos que atestavam a qualidade dos alimentos. A investigação apontou que cinco laboratórios e setores de análises da empresa fraudavam resultados de laudos. As irregularidades teriam sido cometidas entre 2012 e 2015, com conhecimento de executivos da empresa.

A exposição negativa do episódio, que teve também a prisão de executivos da empresa, foi determinante para que fundos de pensão, que estão entre os principais investidores da empresa, defendessem a troca dos executivos do conselho, incluindo o presidente do conselho de administração. [5]

Novamente, temos aqui uma grave falha de governança, seja por leniência ou por incapacidade de detectar a fraude, com graves consequências sociais e ambientais para o público consumidor. Caberia ao comitê de auditoria ter detectado a fraude.

O caso ainda em curso pode comprometer os executivos, que têm o dever fiduciário para com a organização e, no extremo, a empresa pode ser enquadrada na Lei Anticorrupção, em que a multa pode variar de 0,1 a 20% do faturamento bruto do ano anterior, que foi de 33,5 bilhões de reais em 2017.

Assim como nos casos anteriores, o fator agravante é que, segundo dados tornados públicos pelos órgãos de governo, os administradores tinham conhecimento da fraude e aparentemente nada fizeram até que o caso viesse a público.

Aqui ficam mais uma vez perguntas sobre a gestão de riscos, a estrutura de governança e o nível de consciência organizacional. O caminho escolhido pelos gestores da companhia

beneficiaria quem em última instância? Sob que ótica a decisão foi endereçada? Dos interesses dos executivos, remunerados com base em resultados de curto prazo, dos acionistas controladores que buscam remuneração sobre o capital investido ou com base nos valores e princípios da empresa?

O caso ainda está longe de ter um desfecho junto à justiça e aos mercados onde a empresa atua. Como corrigir e recuperar confiança dos mercados e dos stakeholders? Quem tomou a decisão e quem aprovou tal prática internamente tinha clara noção das consequências para os negócios ou entendia que tudo ocorria num ambiente razoavelmente controlado?

Se as organizações não estiverem atentas aos riscos ASG, enfrentarão dificuldades na captação de recursos financeiros, assim como no acesso a determinados mercados onde as exigências são mais severas. As instituições financeiras buscam capturar de forma precisa os riscos e impactos das questões socioambientais nas empresas e nos projetos que financiam ou nos quais investem. Fazem isto com o objetivo de gerir seus riscos e capturar oportunidades de negócio.

Assim, é imperativo que as organizações considerem a gestão de riscos de ASG em seu planejamento estratégico e que o conselho de administração estabeleça a governança necessária que permita melhor acompanhamento da gestão. Seja por conveniência ou por convicção, as organizações buscarão meios para reduzir o risco de compliance num primeiro estágio e perceberão que a atuação pautada por princípios éticos promove um ambiente interno e de relacionamento favorável à longevidade dos negócios.

É de responsabilidade dos agentes de governança criar e aprimorar a gestão de riscos relacionados a ASG.

Finalmente, destacamos que a boa prática recomenda a elaboração anual de um relatório de sustentabilidade, com matriz de materialidade segundo as normas da GRI, que é uma fonte importante para a identificação de fatores de risco a considerar no mapeamento de riscos corporativos.

João Redondo

Consultor nas áreas de governança corporativa, sustentabilidade, compliance, relações institucional e governamental.

Paulo Vanca

Sócio aposentado e consultor da PwC, onde por mais de 10 anos foi responsável, no Brasil e na América do Sul, por serviços nas áreas de Gestão de Riscos, Auditoria Interna e Sustentabilidade.

Amalia Sangüeza

Subcoordenadora da Comissão de Sustentabilidade do IBGG e presidente do Comitê de Sustentabilidade da Câmara Espanhola.

Sérgio Mindlin

Consultor, Conselheiro Certificado pelo IBGC, professor do IBGC e do GIFE, membro das comissões de Sustentabilidade e de Ética na Governança, e do Colegiado de Apoio ao Conselho - Conduta do IBGC.

Carlos Eduardo Lessa Brandão

Consultor, professor de programas de educação executiva e conselheiro de empresas e de entidades ligadas à sustentabilidade e negócios no Brasil e exterior.

1. De acordo com análise divulgada no jornal britânico The Guardian, o impacto dos 11 milhões de veículos adulterados pela montadora em todo o mundo pode significar a emissão de 237 mil a 948 mil toneladas de gases poluentes por ano. Segundo a revista científica Nature, o "excesso" de emissões poluentes de veículos a diesel teria contribuído para provocar 38.000 mortes prematuras em todo o mundo em 2015.
2. Na Alemanha, onde o Ministério Público de Brunswick recebeu mais de 1.400 queixas, acionistas que se estimaram prejudicados pela comunicação tardia do grupo pediram mais de 8 bilhões de euros por perdas e danos. Segundo levantamento da época, mais de 600 mil veículos foram afetados nos EUA e 300mil foram recomprados pela empresa, num mercado onde aproximadamente 2% das vendas são de veículos movidos a Diesel. Na Europa, 53% dos veículos vendidos eram movidos a diesel e na Espanha em torno de 66% do mercado.
3. No Relatório Anual, também destacou ações iniciais como a realização de 25 visitas a fornecedores para avaliação de compliance com o código de conduta do grupo, promoção de três seminários de formação sobre trabalho para 57 fornecedores e a realização de 365 auditorias sociais. Essas foram algumas das iniciativas que visaram engajar os fornecedores diretos no Pacto Nacional pela Erradicação do Trabalho Escravo. Na publicação do relatório anual de 2016, a empresa destacou as ações da empresa para maior transparência na gestão da cadeia de fornecedores, que chamou de "TRANSPARENCY OF OUR SUPPLY CHAIN".
4. As consequências do episódio foram desastrosas para a organização, que apurou um prejuízo líquido de R$ 286 milhões no primeiro trimestre e viu o lucro antes de juros, impostos, depreciação e amortização (Ebitda) derreter em 50% se comparado com o mesmo período do ano anterior. No ano de 2017 a empresa apurou um prejuízo de R$1,1 bilhão, resultado de problemas internos somados ao impacto negativo à reputação que comprometeu exportações e criou um ambiente de desconfiança.
5. Os sucessivos episódios de escândalos agravaram o cenário de desconfiança e a empresa perdeu em um único dia, em março de 2018, o equivalente a R$ 5 bilhões de valor de mercado, numa queda de mais de 19% no valor das ações.

Desmistificando o apetite a riscos

por Corinto Lucca Arruda e Isaac Lee Demoner

Decisões tomadas corriqueiramente, envolvendo as mais variadas naturezas e os diversos assuntos nas organizações, possuem algum grau de risco associado. Essa afirmação, comumente aceita, oferece pouca margem de contestação. Em geral, as dúvidas relacionadas a esse tema voltam-se para os seguintes questionamentos: o nível de risco decorrente das decisões tomadas pelos administradores está alianhado à quantidade de riscos em que a organização está disposta a incorrer? A empresa está correndo risco demasiado ou estamos sendo excessivamente conservadores? Deseja incorrer em riscos em troca de algum ganho futuro ou uma postura conservadora é a adequada aos nossos negócios? Pode ter uma postura arrojada em alguns assuntos e ser cautelosa em outros ou o limite de risco deve ser uniforme para toda organização?

Da mesma forma, ao transpor tais questões para o ambiente dinâmico e multidisciplinar inerente às organizações, é possível notar o quanto estas fazem parte do cotidiano das empresas, e ainda surgem outras perguntas: devemos associar a nossa marca a um parceiro externo para desenvolvimento de um novo mercado ou produto? Quão resilientes devem ser os nossos sistemas críticos? Em quais produtos financeiros devemos investir o caixa livre da empresa? Qual deve ser o nível de prontidão das respostas da organização para alterações regulatórias?

Para responder a cada uma dessas questões, é necessário analisar o ambiente interno da organização, determinar o quão a empresa está disposta a incorrer em riscos para alcançar um objetivo, verificar o quão restritivos devem ser os controles internos para cada processo vinculado às perguntas e definir o nível de flexibilidade adequado para cada processo, produto ou serviço oferecido pela empresa.

O resultado dessa análise demonstrará por quais decisões – vinculadas a aspectos que exigem menor nível de controle, maior flexibilidade, ou àquelas relacionadas ao alto grau de incerteza e grande potencial de retorno – a organização está propensa a correr riscos. Por outro lado, processos que demandam alto nível de controle e assertividade, margem reduzida para erros, menor necessidade de flexibilidade e poucos ganhos associados a mudanças são aqueles pelos quais usualmente as emrpesas possuem menor apetite de correr riscos. Diante desse resultado, uma nova questão emerge: é possível estabelecer uma diretriz única válida para toda a organização e que defina as diferentes medidas de risco em que se está disposto a incorrer?

A resposta é sim. Em setembro de 2004, o *Committee of Sponsoring Organizations of Treadway Commission* (Coso) publicou o primeiro documento que estabelece os componentes e os princípios do gerenciamento de riscos corporativos. E essa diretriz única é o que esse documento denominou de apetite e tolerância a riscos da organização.

A documentação formal de apetite e tolerância a riscos é a orientação do conselho de administração aos administradores e executivos de quanto de riscos a empresa está disposta a incorrer para atingir seus objetivos estratégicos.

No entanto, o apetite a riscos não vem sendo utilizado pelas organizações, conforme apontam pesquisas realizadas nos últimos anos. Esses estudos mostram que, embora se tenham registrados alguns progressos e entenda-se que o conceito é de grande utilidade, as organizações terão de aumentar os seus esforços no sentido de desenvolver ferramentas criativas para a tomada de decisões, que incluem o desenvolvimento de formas de medir e reportar o apetite a riscos.

No âmbito internacional, em novembro de 2013, o *Financial Stability Board* (FSB), entidade responsável por promover reformas na regulamentação financeira internacional, emitiu princípios para

construção de um *framework* efetivo de apetite a riscos. Em 2015, o Comitê de Basileia divulgou orientações que enfatizaram o papel do conselho de administração no estabelecimento juntamente com a alta administração e o *Chief Risk Officer* (CRO) no apetite a riscos da instituição.

No âmbito nacional, como uma forma de estender a regulamentação sobre a declaração de apetite a riscos para as instituições financeiras, o Banco Central do Brasil (Bacen) publicou, em fevereiro de 2017, a Resolução 4.557, que dispõe sobre as estruturas de gerenciamento de riscos e de gerenciamento de capital das instituições financeiras e estabelece que as instituições devem documentar a declaração em questão.

Ainda faltam, porém, informações objetivas sobre como as empresas podem realizar esse registro. Essa ausência de clareza reflete-se na dificuldade da definição do que deve ser discutido para formalização do apetite a riscos entre os executivos e no conselho de administração.

Aplicando o apetite a riscos nas organizações

A implementação dos conceitos de apetite a riscos requer exaustivas análises e discussões em diferentes camadas de aprovação. O quadro a seguir apresenta um *framework* simplificado das macroetapas a serem percorridas no processo de implantação do conceito nas organizações:

Etapas para implementação do apetite a riscos

1. Defina os principais tópicos que trazem riscos à organização	2. Defina uma escala de apetite a riscos	3. Avalie o apetite de cada subcategoria	4. Aprove o apetite a riscos da companhia	5. Acompanhe a aderência ao apetite a riscos
Mapeie os assuntos que geram riscos para a organização e agrupe-os em categorias de riscos, que devem ser o elemento seminal de discussão de riscos na organização. **Implemente essa etapa** Inicie a categorização no nível macro (o Coso sugere quatro macrocategorias: estratégica , operacional, financeira e regulamentar) e, em seguida, estruture subcategorias que devem cobrir os processos, elementos e produtos que permeiam a organização. **Dica:** Quanto maior a quantidade de categorias, maior a dificuldade para a sua gestão.	Elabore uma escala para padronizar as medidas de riscos em que a companhia pretende incorrer em cada categoria, desde as categorias mais propensas a correr riscos até aquelas mais restritivas. **Implemente essa etapa** Determine os parâmetros que devem categorizar cada nível da escala. O nível mais restritivo é uma declaração que a companhia envidará todos os esforços para mitigar riscos na subcategoria em questão. **Dica:** O Coso sugere uma escala de três níveis de apetite a risco, mas isso não é uma regra.	Discuta com os responsáveis de cada categoria, com o comitê de riscos e com os executivos o quanto a companhia está disposta a incorrer em riscos. **Implemente essa etapa** Estabeleça um método de coleta e mensuração objetiva do apetite a riscos de cada subcategoria em cada fórum de discussão. **Dica:** Utilize um apetite restritivo a riscos para categorias que necessitam de uma abordagem conservadora e um apetite propenso a tomar riscos para categorias que representam oportunidades de negócio.	Aprove o apetite a riscos na mesma instância responsável por aprovar os objetivos e as estratégias de negócio. Certifique-se de que a proposta de apetite esteja alinhada aos objetivos estratégicos. **Implemente essa etapa** A segunda linha de defesa é a responsável por levar às instâncias de aprovação a proposta do apetite a riscos da organização. Usualmente, os membros desses fóruns possuem pouca familiaridade com o tema; uma introdução conceitual, portanto, é fundamental. **Dica:** O processo de aprovação pode ser moroso e os debates, intensos. Traga elementos das etapas anteriores para embasar as discussões.	Acompanhe se a companhia, em seu dia a dia, está seguindo ou tomando mais ou menos risco do que o declarado em seu apetite. Para isso, estruture indicadores de monitoramento. **Implemente essa etapa** Evite indicadores que possuem propósito estritamente operacional. Utilize indicadores-chave de risco, de escopo macro, que sejam capazes de demonstrar se a subcategoria está gerando risco além do apetite aprovado para a organização. **Dica:** Quanto maior a quantidade de indicadores, maior a dificuldade para a sua gestão. Utilize indicadores-chave!

Benefícios

Para as organizações, a definição e o acompanhamento do apetite a riscos, alinhados aos objetivos estratégicos, trazem transparência quanto ao nível de risco que a empresa está disposta a incorrer para atingir seus objetivos estratégicos; alinhamento da organização quanto aos recursos que serão requeridos ou alocados para suportar o nível de apetite a riscos desejado; direcionamento da atuação das áreas de segunda e terceira linha de defesa, as quais passam a contar com um parâmetro claro dos limites de risco da organização; e priorização de esforços para mitigação e tratamento a riscos. A lógica é simples: não faz sentido investir tempo, recursos e dinheiro em planos de ação para mitigação de riscos em que já se aceitou incorrer.

Corinto Lucca Arruda

Superintendente de Processos e Riscos Corporativos da B3, membro da Comissão de Gerenciamento de Riscos Corporativos do IBGC e mestrando em Controladoria pela Fipecafi.

Isaac Lee Demoner

Gerente de Riscos Corporativos da B3 e mestrando em Administração pelo Insper.

Gerenciamento de riscos e o papel do profissional de riscos

por Alvaro Trilho

As incertezas dos últimos anos, como crise econômica global, escalada terrorista, ataques cibernéticos, pandemias, têm provocado um grande efeito sobre como as empresas trabalham. Empresas que costumavam operar com a ajuda de previsões e projeções, agora se abstêm de tomar decisões de negócios sem antes analisar os riscos envolvidos.

O risco é a principal causa de incerteza em qualquer organização. Assim, é necessário identificá-lo e gerenciá-lo antes mesmo que afete o negócio, ajudando empresas a agir com mais confiança em futuras decisões. Conhecendo os riscos inerentes às suas atividades, haverá mais opções sobre como lidar com problemas em potencial.

O risco pode vir de fontes internas e externas. Os riscos externos são aqueles que não estão no controle direto da administração. Incluem questões políticas, taxas de câmbio, taxas de juros, catástrofes naturais e assim por diante. Os riscos internos, por outro lado, incluem não conformidade, vazamento de informações, acidentes numa planta, entre vários outros.

O gerenciamento de riscos é importante em uma organização, porque, sem ele, não se pode definir objetivos de forma adequada. Se uma empresa define objetivos sem os considerar, e caso ocorra a materialização de algum risco, as chances de perder o controle da situação é imensamente maior, do que se levados em consideração desde o princípio.

O gerenciamento de riscos é composto por três linhas de defesa: A primeira Linha de Defesa é a área de negócio, responsável por identificar, mensurar, avaliar e mitigar os riscos de seu negócio. A segunda inclui funções de gerenciamento de risco e conformidade, e deve trabalhar em conjunto com a área de negócios para garantir que a primeira linha de defesa tenha identificado, avaliado e reportado corretamente os riscos do seu negócio. A

terceira é representada pela auditoria interna. Portanto, o papel do profissional de riscos é trabalhar em cooperação com a área de negócio (dona do risco) para identificar riscos, elaborar estratégias e executá-las. Na identificação é determinada a importância de cada risco, analisando quais são críticos para o negócio. Por críticos, entendemos ser aqueles que podem ter um impacto negativo sobre o negócio; estes devem então ser priorizados. O objetivo do gerenciamento de riscos é garantir que a empresa priorize os riscos que a ajudarão a atingir seus objetivos, mantendo todos os outros sob controle.

Tão importante quanto o trabalho interno do profissional de riscos está o seu trabalho externo, que consiste na busca de solução para alguns dos riscos da empresa, sendo o seguro a mais relevante. Este profissional traduzirá para o mercado (corretoras, seguradoras e resseguradoras) as informações da empresa e seus riscos.

As empresas que não contam com um profissional de riscos tendem a cometer erros que, às vezes, não são identificados pelas corretoras no momento da contratação do seguro. Alguns exemplos são: contratar limites insuficientes, coberturas inadequadas, subavaliar o patrimônio da empresa, dentre outros equívocos. Na ocorrência de um sinistro, vem a surpresa – indenização menor do que a perda, aplicação de um rateio, ou, o pior, a perda fica sem indenização. Constantemente, vemos nos jornais exemplos de regulações malsucedidas.

Nos últimos anos, na América Latina algumas empresas adicionaram departamentos de gerenciamento de riscos à sua estrutura. Este trabalho pode ocorrer tanto internamente quanto externamente, sendo um profissional de risco interno, com vínculo empregatício direto com a empresa, ou, um consultor de riscos terceirizado. Na terceirização, o mencionado trabalho de gerenciamento pode ser contratado diretamente pela empresa ou por seu corretor de seguros. Esta é uma tendência em mercados mais maduros, como o norte-americano e o europeu. Apesar da atenção que as empresas latinas vêm dando ao tema, ainda estamos muito longe da estrutura e importância dos departamentos em gestão de riscos das companhias em mercados maduros.

Recentemente, realizei pesquisa com 23 corporações globais (10 norte-americanas, 9 europeias, 2 australianas e 2 latinas) sobre a composição do seu departamento de gestão de riscos. No resultado, ficou muito claro como ainda temos muito a desenvolver na América Latina. O resultado foi o seguinte: 23 corporações: receita total em 2016 – USD 1,215 trilhão; funcionários – 3,14 milhões

> 2 Latinas – os gerentes de riscos reportam ao CFO

- Empresa I: 7 funcionários (atuando em TI, Benefícios, administração de cativa e suporte a expatriados, além das atividades comuns à área);
- Empresa II: 3 funcionários (atuando somente nas atividades comuns à área)

Organograma:

> Demais regiões: em todas as empresas os gerentes de riscos reportam ao CEO ou Conselho de Administração

- 3 empresas: mais de 65 funcionários na área, com responsabilidade inclusive nas áreas de Saúde & Segurança e Engenharia de Riscos;
- Demais empresas: média de 11 funcionários (variando entre 7 e 21)

Organograma:

Vejo este *gap* com otimismo. Afinal, sabemos qual o *benchmark* – buscar a mesma maturidade da estrutura de gestão de riscos das empresas de mercados mais maduros (norte-americano, europeu e australiano).

De algum tempo para cá, falamos e evoluímos muito em governança e *compliance*, mas esquecemos, ou não damos a mesma importância à gestão de riscos. Em tempos de rápidas e grandes mudanças, o gerente de risco é peça fundamental nas corporações. Mesmo em momento de crise econômica, as empresas necessitam compreender os benefícios da contratação deste profissional, pois, uma gestão adequada pode trazer; (i) maior conformidade e confiabilidade nos seus processos internos, desde gerenciais até operacionais; (ii) subsídio nas decisões estratégicas; (iii) coberturas de seguros mais adequadas e, consequentemente, (iv) menores prêmios de seguros, focando no necessário e imprescindível, influenciando na redução de gastos desnecessários.

Alvaro Trilho

Diretor da Associação Brasileira de Gerência de Riscos (ABGR) e sócio-fundador da Atrilho Consultoria em Riscos Ltda, especializada na consultoria em gestão de riscos e seguros para empresas de diversos ramos de atividade.

Tendências da Regulação e seus impactos na discussão de riscos

por Ana Kalil e Sandra Gonoretske

A natureza dos negócios globais e a expansão dos grandes conglomerados nacionais têm exposto as companhias brasileiras a jurisdições de diversos países. Executivos e conselheiros precisam, cada vez mais, considerar os impactos trazidos por normas estrangeiras na formulação de suas estratégias e até mesmo na operação regular da empresa.

Avaliar o risco regulatório ao qual uma companhia está exposta não requer mais apenas um departamento jurídico ou a consulta a advogados externos. Hoje é necessário que os profissionais envolvidos compreendam profundamente o negócio e os relacionamentos com clientes, mercados e fornecedores.

Nesta linha, apresentamos a seguir, duas importantes regras internacionais, que merecem destaque e atenção imediata, dada a sua relevância e aplicabilidade para as companhias brasileiras. A primeira é a *General Data Protection Regulation* (GDPR), regra europeia sobre proteção de dados e privacidade de cidadãos europeus. Em seguida, contamos um pouco sobre as últimas decisões e novidades do Departamento de Justiça dos Estados Unidos (o DOJ) no que se refere ao combate internacional à corrupção.

General Data Protection Regulation (GDPR)

Neste mês de maio, entrou em vigor a GDPR. Esta norma é aplicável aos 28 países do bloco europeu e amplia uma diretriz publicada há 20 anos. Ela estabelece regras rígidas para assegurar que as informações pessoais e a privacidade dos cidadãos europeus sejam preservadas em todo o mundo. As subsidiárias de empresas europeias também estão obrigadas a cumprir esta norma, da mesma forma que qualquer companhia que armazene ou processe dados de clientes do bloco. As empresas que não se adequarem serão proibidas de oferecerem serviços e produtos ao bloco, sob pena de multas severas. Destacamos, a seguir, os principais pontos da norma, que devem estar nas agendas dos conselhos de administração:

- **Consentimento expresso do cliente para uso dos dados:** atualmente, os *websites* utilizam formulários genéricos que coletam algumas informações dos usuários ou clientes. A coleta dos dados acontece quando os usuários assinam algum *newsletter* ou concordam em receber e-mails de algum *e-commerce*. É o chamado *"Soft Consent"*. Com a vigência do GDPR, este tipo de acordo não é mais permitido e deve ser substituído por um consentimento expresso e detalhado conhecido como *"Hard Consent"*.

- **Motivação para a coleta de dados:** no passado, as empresas se aproveitavam

do relacionamento com os clientes para coletar um grande volume de dados. Agora, com a GDPR, apenas os dados realmente necessários poderão ser coletados. Neste quesito, as redes sociais e os navegadores são campeões, eles monitoram a atividade e a localização dos clientes, servindo-se de tal estratagema para direcionar publicidade. Um exemplo são perguntas sugestivas recebidas por consumidores nas proximidades de uma loja. Como, por exemplo, a mãe que recebe uma mensagem perguntando se prefere fraldas Pampers ou Huggies, no exato momento em que passa por uma loja para bebês.

- **Transparência no relacionamento:** os sites devem deixar claro o propósito de coletar os dados do cliente, bem como onde e como eles poderão ser usados. Certamente, em muitos websites já existem uma série de provisões a este respeito na política de privacidade do site ou no documento de Termos e Condições de Uso, mas estes materiais precisam ser reformulados e a linguagem jurídica deverá ser substituída por uma comunicação objetiva de fácil entendimento que estimule o cliente a ler e questionar em caso de dúvidas.

- **Direito de remover seus dados:** o usuário deve ter o direito de retirar a autorização do uso de suas informações pessoais, isto pode torna-se um pesadelo para sites que coletam dados para compartilhar com terceiros e oferecer produtos. Ainda hoje é bastante comum receber um pop-up dizendo: "ao usar este site você está de acordo com a nossa política de cookies". Muitos não sabem que tais cookies podem ser perpétuos. O direito de uso de dados deve ter prazo de validade e ser renovado de tempos em tempos.

- **Obrigação de reportar vazamento de dados:** vazamentos ou suspeitas de vazamento de dados devem ser reportados no prazo de 72 horas. Informar quebras na segurança de dados deve ser o maior desafio das empresas na adequação à norma. Na maioria dos casos conhecidos, as empresas levaram meses para fazer um reporte público. A Equifax, reportou o vazamento de dados 2 meses após a detecção; no caso do Facebook com a Cambridge Analytica, passaram-se anos até que o assunto ganhasse publicidade. No Brasil, o incidente de roubo seguida de extorsão de dados de 20 mil clientes da XP foi reportado apenas 3 anos depois.

Desenvolver a habilidade de detectar e reportar rapidamente os eventos pode exigir vultosos investimentos em tecnologia, pessoas e canais de reporte. O corpo diretivo também deve ser sensibilizado para reformular os atuais planos de gerenciamento de crises, ainda bastante morosos e verticalizados.

As multas para o descumprimento da GDPR vão de 4% do faturamento ou 20 milhões de dólares, o que for maior.

O Brasil acaba de aprovar na câmara o projeto de lei PL 5278/2016. A votação ocorreu no dia 29 de maio em meio a uma corrida entre Câmara e Senado, onde já tramitava outro projeto de lei sobre o mesmo assunto (PL 330/2013). O PL 5278 é mais abrangente e semelhante à norma europeia, estabelecendo regras inclusive para as entidades governamentais. A aprovação da lei de proteção de dados vem de encontro com a ambição do governo federal de incluir o Brasil na Organização para Cooperação e Desenvolvimento Econômico (OCDE). O projeto vai agora para votação no senado.

O programa piloto de combate a corrupção do Departamento de Justiça americano (DOJ)

Desde 2016, quando o DOJ publicou um programa piloto que consiste em dar certos benefícios para as empresas que se auto delatarem por terem violado a lei de anticorrupção (*Foreign Corrupt Practices Act* - FCPA), o número de empresas que voluntariamente aderiram o programa foi consideravelmente alto (30 em 18 meses de vigência do programa) e, consequentemente, aumentou de forma proporcional a cooperação internacional entre os governos. Isto porque, como é sabido, o FCPA é uma

legislação que envolve necessariamente a participação da empresa em algum outro país (ou seja, além dos EUA). Desta forma, aumentando o número de casos, aumentou a necessidade do DOJ obter informações de autoridades internacionais. E estas autoridades vêm, na medida do possível e do permitido por lei, cooperando.

A responsabilidade dos executivos

Também bastante relevante e já altamente anunciado que assim o seria pelo DOJ, aumentou o número de pessoas físicas – condenadas ou em fase de julgamento – por terem violado o FCPA: em 2017, foram 19 condenações de executivos e 16 acusados aguardando julgamento. O foco em investigações para apurar responsabilidade individual dos envolvidos deve continuar a ser tendência nos próximos anos. Um dos motivos é que em geral, os executivos não costumam fazer acordo (diferente das empresas, os executivos tendem a prolongar os litígios), assim, as regras e decisões relacionadas a penalizações de pessoas físicas tardarão para se consolidarem.

A tendência é que o DOJ inclua nas investigações os executivos da sede da empresa investigada e não apenas os executivos do país investigado como tem sido feito até agora. Conforme a linha de comando a companhia, se houver uma investigação por algo que se passou na África com uma subsidiária de empresa brasileira, tal investigação deverá chegar até os executivos responsáveis pela subsidiaria no Brasil.

Aumento da Cooperação internacional

O combate à corrupção tem sido uma das grandes prioridades em diversos países. Desta forma, a colaboração entre os governos tem aumentado significantemente. A cooperação de países como a Suíça, que era conhecida por seu rigoroso sigilo, ou mesmo o Brasil, recentemente classificado em 96º lugar no ranking de corrupção da Transparência Internacional, têm contribuído para a realização de muitos acordos. Casos como o acordo de pagamento de USD 800 milhões pela inglesa Rolls Royce, que envolveu os governos da Inglaterra, Brasil e EUA, ou da SMB Offshore, investigada no escândalo da Petrobras, que contou com a cooperação entre os governos do Brasil, EUA e Holanda e resultou em um acordo de pagamento de USD 238 milhões, têm sido possíveis devido a esta cooperação intergovernamental que até poucos anos atrás, não ocorria.

Nossa recomendação

Como podemos perceber, o GDPR e as recentes decisões do DoJ têm alcance global e têm gerado impactos inclusive na regulação brasileira. As implicações não abrangem apenas as organizações, mas também os indivíduos envolvidos e suas responsabilidades como dirigentes das empresas.

Torna-se urgente que os conselhos de administração e executivos das companhias, considerem normas e tendências regulatórias transnacionais na discussão de riscos. Desta compreensão, poderão sair alterações na estratégia e no plano de investimentos para os próximos anos. Isto sem esquecer da responsabilidade do conselho em certificar-se que o ambiente de controles internos esteja preparado para evitar multas milionárias e prejuízos na imagem das empresas.

Ana Kalil

Economista, membro da Comissão de Gerenciamento de Riscos do IBGC, consultora e professora sobre temas de compliance, riscos e prevenção a Lavagem de dinheiro.

Sandra Gonoretske

Advogada, professora, palestrante e consultora de Compliance e Prevenção à Crimes Financeiros

Riscos em projetos de engenharia

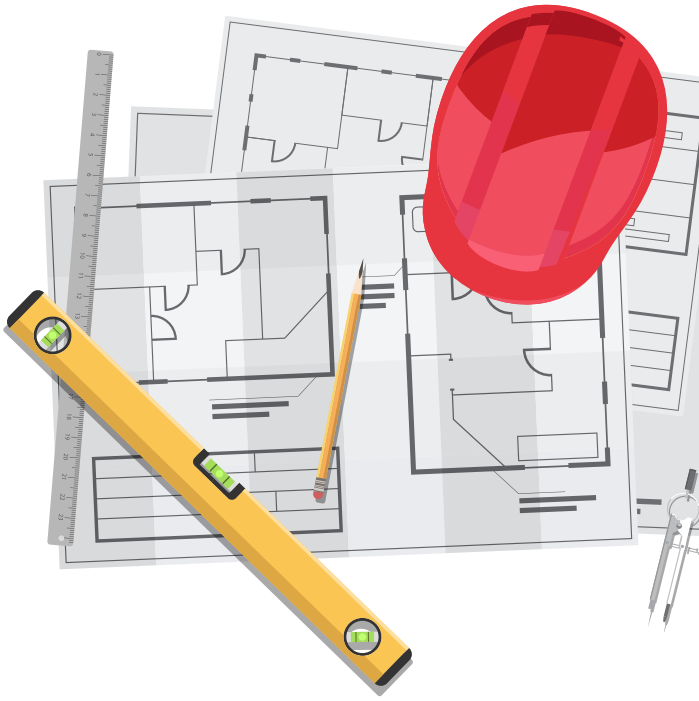
por Erico da Gama Torres e Ricardo Lemos

O objetivo principal desse artigo não é explicar como se gerencia riscos em projetos de engenharia, tarefa impossível para um breve texto como este, mas dar ao leitor uma visão geral da problemática existente na gestão e governança desse tipo de risco focando em alguns tópicos mais críticos.

De início, vamos nos privar das definições de risco e gestão de risco, fartamente encontradas na literatura sobre o tema. Tentaremos abordar a governança da gestão de riscos, que é o elemento que realmente faz a diferença quando se busca garantir a efetividade da gestão de riscos. Assim, quando falamos em riscos de projetos de engenharia, temos que levar em consideração uma abordagem que permita a governança e consequentemente a gestão tanto no próprio projeto, quanto na organização, em especial se for uma organização cujos negócios sejam essencialmente projetos de engenharia, como as projetistas, construtoras e outras organizações como concessionárias de serviços públicos, empresas de consultoria, órgãos públicos que cuidam de infraestrutura, entre outros. É importante observar que a governança da gestão de riscos, quando o tema é projetos de engenharia, pelas características dessa atividade, pode ser uma matéria mais crítica do que em outros tipos de atividade.

A gestão efetiva dos riscos exige identificar e mitigar os riscos conhecidos e antecipar os riscos futuros. Como resultado, espera-se que os gestores de projetos tenham uma visão dos riscos emergentes, especialmente em novas tecnologias e das obrigações de conformidade da empresa com as respectivas legislações.

Além da área específica de projetos a área de gestão de riscos deve mapear os riscos inerentes das operações (inclusive os de



projetos), e os classificar na matriz de risco segundo critérios de vulnerabilidade de ocorrência, magnitude de possível impacto e identificar o risco residual máximo admitido.

O Project Management Institute (PMI)[1] dos EUA define projeto como "esforço temporário empreendido para criar um produto, serviço ou resultado único". Deve-se observar que o termo projeto pode, muitas vezes, ser entendido de maneiras diferentes. A definição do PMI é considerada uma definição mais abrangente. No jargão da indústria da construção, o termo projeto refere-se, normalmente, ao conjunto de desenhos e especificações necessários à execução dos serviços de construção. Contudo, a ideia de projeto está associada ao de empreendimento, que é uma atividade com início e fim bem definidos e visa à realização de algo que nunca havia sido feito antes,

1. Referência internacional em gestão de projetos e emissora do GUIA PMBOK – Quinta Edição (Um Guia do Conhecimento em Gerenciamento de Projetos), procedimento padrão para o gerenciamento de projetos adotado por muitas organizações mundo afora, inclusive no Brasil.Toward a Value-creatingBboard, McKinsey&Company, 2016.

enquadrando-se perfeitamente no conceito de projeto do PMI. É importante frisar que, no caso da indústria da construção, o chamado projeto de engenharia está contido no processo de projeto ou simplesmente no projeto, ou seja, no empreendimento, que com ele se confunde.

Aqui chamamos projeto de engenharia[2] o projeto do empreendimento como um todo, pois seja esse empreendimento grande como uma hidrelétrica ou pequeno como a reforma de um banheiro, ele é dividido em fases sequenciais que precisam ser obedecidas e corretamente concluídas para que o empreendimento seja entregue e entre em operação. É daí que se origina a complexidade de se gerenciar riscos em projetos de engenharia e a sua governança: os riscos mudam de acordo com a fase do ciclo de vida e também com a etapa em que se encontra cada atividade ou macroprocesso que o compõe. Além disso, como o projeto não é uma atividade contínua, é necessário que se organize a sua governança e gestão toda vez que se inicia um novo projeto, o que exige mais atenção e disciplina dos administradores.

Nesse sentido, é importante frisar ainda que os projetos de engenharia são feitos, normalmente, em locais sempre diferentes, o que implica na possibilidade do surgimento de novos tipos de riscos ou variações significativas sobre riscos já identificados previamente. Por isso, um tratamento de lições aprendidas, ou seja, a incorporação do conhecimento adquirido na execução de um projeto para melhorar o desempenho dos próximos projetos, é um tema da maior relevância na gestão de riscos, em especial no processo de identificação de riscos de projeto.

Para se ter ideia do ciclo de vida de um projeto genérico de engenharia, no caso um empreendimento típico que tem como objetivo uma construção, portanto um projeto de construção, veja a figura a seguir:

6. Operações existentes	Ciclo de Vida de um Projeto de Construção					6. Operações novas
	1. Planejamento Estratégico	**2. Estudos preliminares**	**3. Projeto de Engenharia**	**4. Concorrência**	**5. Construção**	
	1.1 Formulação de objetivos **1.2** Engenharia conceitual **1.3** Avaliação de alternativas **1.4** Pré-viabilidade **1.5** Obtenção do Termo de Referência para Licenciamento Ambiental	**2.1** Viabilidade **2.2** Definição do escopo do projeto **2.3** Contratação do projeto de eneharia e do EIA/RIMA **2.4** Estudos para equacionamento financeiro	**3.1** Licenciamento Ambiental **3.2** Projeto básico **3.3** Processos e equipamentos **3.4** Projeto dos processos executivos e especificação de materiais **3.5** Orçamento inicial (planejamento) **3.6** Plano inicial de construção **3.7** Equacionamento financeiro	**4.1** Plano final de concorrência/ contratação **4.2** Concorrência **4.3** Definições de contratação **4.4** Orçamento e planejamento final da construção **4.5** Licença de instalação	**5.1** Mobilização **5.2** Projetos executivos (detalhamento) **5.3** Execução dos serviços **5.4** Pré-operação e operação assistida **5.5** Encerramento **5.6** Licença de operação	

Fases do ciclo de vida genérico de um projeto de engenharia. Fonte: Torres, Erico G., (2001, p.100)[3]

2. No Brasil, devido a definição dada pela Lei 8.666/93, a engenharia é explicitada nos chamados projetos básicos, aqueles no qual o conceito está formulado, e projeto detalhado ou executivo, onde são especificados todos os detalhes construtivos.
3. Uma Discussão sobre a Cadeia de Valor na Indústria da Construção. Dissertação de Mestrado EEUFMG.

Como pode ser visto, num projeto de engenharia as atividades normalmente sofrem uma divisão devido a sua complexidade e tempo de duração, sendo obrigatório que se respeite uma sequência lógica, sob pena de grandes contratempos. Em função disso, os riscos também vão se alterando ao longo do ciclo de vida e precisam ser muito bem gerenciados desde o início para que não haja solução de continuidade, comum principalmente nos empreendimentos públicos no Brasil. Nesse sentido, um dos riscos mais comuns é o associado a prazos de execução, muitas vezes decorrentes da falta de entendimento de que cada fase precisa ser muito bem feita e concluída para avançar na fase seguinte. Além disso, é do nosso entendimento que o sucesso de um projeto de engenharia depende fundamentalmente da sua fase de planejamento estratégico, sendo que as estratégias devem estar associadas e ser avaliadas sempre em relação ao risco existente.

Tanto os projetos de construção quanto os demais tipos de projeto estão normalmente inseridos em ambientes bem mais amplos do que o do próprio projeto. Nesse sentido, é importante observar que as operações continuadas de qualquer organização estão fora do escopo de um projeto havendo, entretanto, pontos de interseção. Observe-se que as operações são esforços contínuos, que geram saídas repetitivas, em oposição aos projetos, que são esforços temporários. Contudo, o trabalho do projeto deve ser integrado com as operações continuadas da organização executora. As partes interessadas operacionais devem ser engajadas e as suas necessidades e influência devem ser levadas em consideração na gestão de riscos.

Um empreendimento de engenharia somente será bem-sucedido se conseguir conciliar o "mundo" da construção com o "mundo" da operação. O essencial nesse ponto é entender que para fazer bem a parte da construção é preciso entender bem a parte operacional, observando partes comuns e interfaces do projeto na operação. Essa é uma questão muito importante, tanto para empresas de construção quanto para empresas cuja atividade central está concentrada em operações continuadas e que contratam projetos de engenharia. O risco de eventos negativos para ambas pode aumentar consideravelmente sem essa sintonia.

Adicionalmente, não podemos esquecer que a fase do ciclo de vida onde a maioria dos riscos do projeto se materializam é na fase de construção, a mais cara e a última, para a qual convergem todos os estudos e o trabalho que foi desenvolvido nas fases anteriores. Novamente, se o trabalho desenvolvido nas fases anteriores não tiver sido de boa qualidade e não estiver concluído, a probabilidade de vários riscos se materializarem na fase de construção aumenta significativamente. Em outras palavras, o desenvolvimento das quatro primeiras fases do ciclo de vida do projeto de engenharia é essencial para que a quinta e última, a construção, fique dentro do prazo, do custo e atenda outros parâmetros especificados. Tudo isso deve levar em conta o conhecimento e a experiência em construção na engenharia do projeto. Portanto, há muito trabalho a ser feito antes de se iniciar uma obra.

É importante chamar a atenção para a identificação dos riscos, um dos pontos mais problemáticos da gestão de riscos em projetos. O propósito final da identificação de riscos é definir uma lista e caracterizar quais riscos podem afetar os objetivos em cada fase do projeto. Este processo de identificação pode também revelar oportunidades ao projeto. Uma gestão eficaz de riscos depende fundamentalmente da identificação dos riscos, portanto, é vital que este processo esteja sistematizado.

A identificação dos riscos é um processo interativo que poderá incluir além da equipe do projeto, consultores, clientes, usuários finais, outros gerentes de projeto e outras partes interessadas. Esse processo começa junto com a primeira atividade do projeto e deverá ser constante durante todo o ciclo de vida do projeto, ou seja, à medida que o grau de conhecimento do projeto vai aumentando novos riscos podem ser identificados pela equipe do projeto. Isto significa que a identificação de riscos começa na fase de planejamento estratégico, é ampliada e consolidada nas demais fases e deve ser

levada em consideração no orçamento dos projetos com muita acuidade, inclusive com a definição de reservas de contingência, e atualizada constantemente durante a fase de construção. Atividade que deve ser englobada pela Governança da Gestão de Riscos.

A identificação dos riscos é baseada na avaliação da criticidade, complexidade e resultados de estudos e análise. Os elementos de identificação dos riscos são baseados em parâmetros, tais como, entre outros: estratégia para execução do projeto, tamanho do projeto, tipo de contrato, cláusulas contratuais desfavoráveis, características regionais, localização do canteiro, clima e meio ambiente, condições financeiras do contrato (penalidades, pagamentos, retenções, incentivos), metodologia executiva, aspectos da operação, criticidade do cronograma, regulamentações, questões trabalhistas, tipo de cliente, sem deixar de considerar novas tecnologias, novos produtos, novos processos, novos fornecedores e subcontratados.

Recomenda-se que a organização agrupe os riscos por categorias de risco, que é uma maneira de se ordenar possíveis causas de riscos. Pode ser usada uma estrutura de categorização previamente preparada, podendo ser uma simples lista de categorias ou uma EAR – Estrutura Analítica de Riscos, que é uma representação hierárquica dos riscos de acordo com as suas respectivas categorias (PMBOK). Deve-se ter em mente que no decorrer da construção temos várias etapas nas quais os riscos podem variar significativamente e até mesmo deixar de existir. Daí também a importância da priorização e da avaliação dos riscos por fase do ciclo de vida e em especial na fase da construção onde devem ser muito bem detalhados. A priorização irá permitir à equipe do projeto concentrar seus esforços nos riscos com probabilidade de impactos mais significativos para os resultados planejados

Como mencionado na publicação do IBGC (*Gerenciamento de riscos corporativos: evolução em governança e estratégia*), também em projetos de engenharia "a gestão de riscos deve ser associada ao processo decisório e ao processo de estabelecimento da estratégia" de implementação do empreendimento para o qual se pretende desenvolver um projeto de engenharia. Recomenda-se fortemente a preparação de uma EAR que deve apoiar todo o processo de gestão, a qual deve ser atualizada frequentemente com a incorporação das lições aprendidas. Esse, talvez, seja o grande segredo para uma boa gestão de riscos em projetos de engenharia.

Erico da Gama Torres

Engenheiro civil, advogado, mestre em engenharia da produção (MSc), chefe do Centro Regional de Minas Gerais da Fundacentro e membro da Comissão de Riscos do IBGC.

Ricardo Lemos

Mestre em Administração de Empresas (FGV), MBA em Controladoria (Fipecafi-USP) e graduado em Administração de Empresas (FGV). É membro da Comissão de Gerenciamento de Riscos Corporativos do IBGC e professor em cursos de pós-graduação/MBA, lecionando governança corporativa, gestão de riscos, compliance e controles internos.

Cultura organizacional e gestão de riscos

Conteúdo patrocinado por:

pwc

Saber com clareza a relação entre a cultura e as metas de negócios e considerá-la na formulação da estratégia é uma característica comum das empresas de alta performance. Esse é um aspecto fundamental para definir o grau de apetite ao risco, que irá determinar se a organização adotará uma postura agressiva ou conservadora.

A falta de alinhamento entre a cultura e o nível de risco necessário para a execução da estratégia pode limitar a capacidade de obter os resultados esperados. Se uma empresa com perfil agressivo e inovador adotar uma estratégia conservadora, sua performance ficará abaixo do seu potencial pleno. No outro extremo, uma empresa com cultura conservadora terá dificuldade para executar uma estratégia que exija alto grau de risco e provavelmente, abandonará a estratégia ao primeiro sinal de queda nos resultados e antes de colher os benefícios pelo risco assumido.

Assim, é importante garantir que o apetite ao risco da empresa, ou seja, sua vontade, capacidade e tolerância para assumi-los seja adequado à cultura. Este alinhamento visa manter a consistência na definição e execução das estratégias do negócio, permitindo inclusive revisar a estratégia e/ou a cultura corporativa se necessário.

Para obter o alinhamento adequado é imprescindível envolver as pessoas, que são a base da cultura organizacional. A consolidação da cultura depende das pessoas e elas precisam estar motivadas e ser incentivadas a adotar e partilhar o conjunto de crenças, valores e princípios desejados. Parte dos incentivos está na remuneração. Recompensar executivos por assumir riscos sem ultrapassar– os limites estabelecidos é um aspecto importante de qualquer estrutura de remuneração. Comissões sobre vendas, bônus e opções de ações são alternativas utilizadas em muitos setores, pois, além do efeito motivacional, têm clara influência no comportamento.

Para que a cultura seja consistente em todos os níveis, desde os cargos mais seniores até os operacionais, é necessário engajar os funcionários em torno da visão, missão e valores da empresa.

"A cultura adequada possibilita ao conselho, à diretoria e aos membros da liderança ter a confiança de que os funcionários farão a coisa certa em situações difíceis."

A cultura é considerada muitas vezes um aspecto "soft", importante, mas difícil de gerenciar. Atualmente, os acionistas, os reguladores, a mídia e até mesmo os clientes questionam cada vez mais para entender melhor como a cultura influencia a tomada de decisões e os riscos assumidos.

ris·co

(substantivo masculino)

mcgarrybowen

1 Do francês ***RISQUE.*** Evento que pode ou não ocorrer, com possíveis consequências para pessoas ou organizações caso se concretize.

2 Evento que pode ser transformado em vantagem competitiva. Gestão integrada ao negócio, fazendo parte do processo de definição da estratégia, da cultura organizacional e das atividades do dia a dia. Com isso, sua empresa ficará mais preparada para antecipar mudanças, identificar oportunidades e obter diferenciação em estratégia e performance.

Termos relacionados: gestão de riscos; olhar estratégico; vantagem competitiva; COSO — Gerenciamento de Riscos Corporativos — Integrado com Estratégia e Performance.

pwc

O mundo pede novas leituras.

www.pwc.com.br/imperativos-negocios

PwC Brasil @PwCBrasil @pwcbrasil PwC Brasil PwCBrasil