Os 4 riscos que fragilizam a gestão de riscos

João Batista Ribas de Moura
Analista Tributário da Receita Federal do Brasil. Chefe da Auditoria Interna e Risco no Conselho Administrativo de Recursos Fiscais (CARF) do Ministério da Fazenda. Mestre em Computação Aplicada. MBA em Administração Estratégica de Sistemas de Informação (FGV). Especialista em Gestão da Segurança da Informação e Comunicações (UnB).

RESUMO

O Decreto nº 9.203, de 22 de novembro de 2017, estabeleceu princípios, diretrizes e mecanismos de governança na administração pública federal direta, autárquica e fundacional, sendo a gestão de riscos imprescindível à integridade e transparência, aspectos basilares à administração. Apesar de todo referencial teórico e metodológico consolidado, observa-se que a prática do processo de gestão de riscos pode ser fragilizada devido a riscos que impactam a completude e exatidão dos relatórios submetidos aos órgãos de controle e à sociedade brasileira. Este artigo objetiva apresentar os riscos que comprometem a própria gestão de riscos e sugere ações preventivas.

Palavras-chave: Palavras-Chave: Governança; Integridade; Gestão de Riscos.

INTRODUÇÃO

O Decreto nº 9.203, de 22 de novembro de 2017, apresenta em seu art. 4º, inciso VI, a diretriz de "implementar controles internos fundamentados na gestão de riscos, que privilegiará ações estratégicas de prevenção antes de processos sancionadores". Também em seu art. 17:

> A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de **gestão de riscos** e controles internos com vistas à **identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica** de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional […] (BRASIL, 2017, grifo nosso)

Há um conjunto de estruturas (*frameworks*), normas ou guias de implementação para auxiliar na operacionalização da gestão de riscos e, dentre eles, destacam-se o *Orange Book: Management of risk – Principles and Concepts*, do Reino Unido; *Comitte of Sponsoring Organizations* (COSO) e *International Organization for Standardization* 31.000 (ISO 31.000) traduzida no Brasil em norma

da Associação Brasileira de Normas Técnicas (ABNT). Enquanto COSO é tradicionalmente voltado às instituições financeiras, a norma ABNT NBR ISO 31.000:2018 traz estrutura aplicável aos mais diversos perfis e, portanto, mais adequada à pluralidade das organizações públicas. Por essa razão este artigo explora as fontes de risco que fragilizam a gestão sob a ótica da norma 31.000.

Esta norma apresenta diretrizes para gerenciar riscos já utilizadas em órgãos de governo, cujo modelo de implementação é dividido em etapas bem definidas, conforme apresentado na Figura 1.

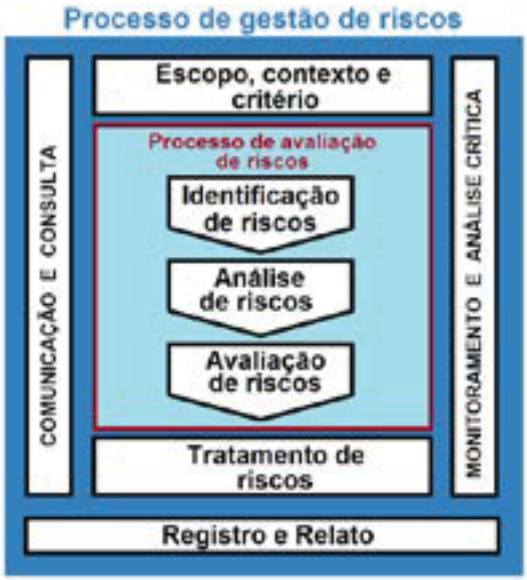

Figura 1: Processo de gestão de riscos.
Fonte: Adaptado de ABNT (2018)

Analogamente a uma construção que, para ser erigida, depende de base sólida obtida com materiais de qualidade, assim também o processo de avaliação de riscos depende da obtenção de informações de qualidade na etapa inicial de "identificação de riscos" para produção de resultados verdadeiramente úteis aos gestores públicos. **A forma de execução das diversas técnicas voltadas ao reconhecimento de riscos pode levar à produção de relatórios incompletos ou fraudulentos.**

ENTENDENDO RISCO

O entendimento do conceito de risco, embora pareça trivial, não raras vezes leva a estratégias errôneas e a retrabalhos quando mal interpretado. A palavra "risco" deriva do italiano antigo *risicare* e significava ousar (BERSTEIN, 1997, p. 8) no sentido de o risco ser uma opção e não um destino cujos acontecimentos dependeriam de sorte ou azar sem possibilidade de ações preventivas.

A ideia de risco evoluiu com a estatística que permitiu análise dos acontecimentos passados calculando a probabilidade de eventos se repetirem no futuro sob determinadas condições. Assim, por exemplo, se existe um histórico de elevada quantidade de assaltos em determinado local e horário da cidade, é possível reduzir o risco, ou, em outras palavras, reduzir a probabilidade de um evento de risco ocorrer simplesmente evitando-se aquela região naqueles

horários. Não se trata, portanto, de prever o futuro, mas de analisar cientificamente as ameaças existentes frente às vulnerabilidades. Risco não é material ou real, mas uma medida probabilística de algo acontecer: ao passar por uma área registrada com altos índices de assalto em certo horário, por exemplo, o "risco de incidente é de 90%".

Os dois elementos constituintes das **fontes de risco** – ameaça e vulnerabilidade (fragilidade) – podem aumentar a chance de materialização de eventos – **consequência** – capazes de prejudicar o alcance dos objetivos estratégicos organizacionais.

> […] Convém que risco seja descrito como a combinação da probabilidade de um evento (ou perigo ou **fonte de risco**) e a sua **consequência**.
>
> O entendimento de que risco pode ter consequências positivas ou negativas é um conceito central e vital a ser compreendido pela direção. O risco pode expor a organização tanto a uma oportunidade quanto a uma ameaça ou a ambos. (ABNT, 2015, p. 8, grifos nossos)

A compreensão de que a gestão de riscos depende fortemente da precisão com que é feita a identificação de riscos, portanto de suas vulnerabilidades e ameaças, é fundamental para o sucesso da técnica de captura dessa informação no meio organizacional. Normalmente, o registro de vulnerabilidades recebe maior detalhamento do que o registro de ameaças porque sobre aquele pode-se executar mais facilmente ações preventivas ou corretivas. Por exemplo, o risco de derrapagem em dias de chuva pode ser reduzido com mais facilidade tratando-se a vulnerabilidade de pneus carecas do que tentando-se reduzir a ameaça de chuva.

Há inúmeras técnicas utilizáveis para se identificar riscos. Muitas delas estão descritas na Norma ABNT ISO/IEC 31.010. Muitas organizações trabalham com *brainstorming*, atividade em que as pessoas são convidadas a relatarem em grupo, ou preenchendo formulários com as fragilidades – normalmente internas – e ameaças – normalmente externas – que acreditam existir relacionadas aos seus ambientes laborais ou processos de trabalho no qual estão inseridas.

Muitas fragilidades existentes nas organizações são conhecidas apenas pelas pessoas que lá trabalham há anos e dificilmente apareceriam com a utilização de técnicas estatísticas. Esse conhecimento ou sabedoria guardado apenas na mente desses colaboradores é denominado **conhecimento tácito** e necessita ser transformado em **conhecimento explícito** para ser útil à gestão. A explicitação ou documentação das fragilidades que levam a riscos é a matéria-prima mais valiosa porque documenta as percepções individuais das "coisas erradas" existentes na organização pública. O processo de transformação desse conhecimento encontra-se esquematizado na Figura 2.

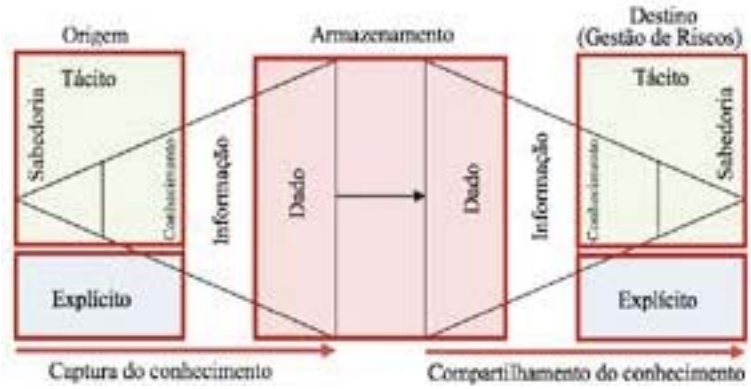

Figura 2: Transformação do conhecimento tácito em conhecimento explícito.
Fonte: Adaptado de Kirsch, Hine, Maybury (2015, p. 66)

RISCO E INTEGRIDADE

A gestão de riscos deve ser utilizada como componente dos programas de integridade porque tem o poder de revelar não apenas os ilícitos previamente categorizados pela legislação, mas também outras ameaças com capacidade para prejudicar o alcance dos objetivos estratégicos. Integridade é definida no Decreto nº 9.203/2017 como um dos princípios da governança pública e sua relação com a avaliação de riscos é apresentada na Figura 3.

Figura 3: Relação entre compliance, integridade e avaliação de riscos.
Fonte: Elaborada pelo autor.

O termo *compliance* é utilizado para designar ações para mitigar riscos e prevenir corrupção e fraude nas organizações, independentemente do ramo de atividade (SANTOS et al., 2012, p. 1). Nesse sentido, observa-se um esforço contínuo e mundial dos governos no combate à corrupção. A primeira lei de *compliance* anticorrupção surgiu nos EUA em 1977 e foi chamada de "Lei sobre Práticas de Corrupção no Exterior (FCPA)". Em 2011, a lei antissuborno foi aprovada no Reino Unido. No Brasil, diversas leis foram criadas nessa linha:

- Lei nº 7.492/1986 – Crimes contra o sistema financeiro nacional;
- Lei nº 8.137/1990 – Crimes contra a ordem tributária, econômica e as relações de consumo;
- Lei nº 8.429/1992 – Lei de Improbidade Administrativa;
- Lei nº 8.666/1993 – Lei de Licitações;
- Lei nº 9.613/1998 – Crimes de "lavagem" ou ocultação de bens, direitos e valores;
- Lei nº 12.846/2013 – Lei Anticorrupção.

Programa de Integridade é definido na Portaria nº 1.089, de 25 de abril de 2018, do Ministério da Transparência e Controladoria-Geral da União (CGU), na qual são estabelecidas orientações aos órgãos e entidades da administração pública federal:

> Art. 2º Para os efeitos do disposto nesta Portaria, considera-se:
>
> I – Programa de Integridade: conjunto estruturado de medidas institucionais voltadas para a prevenção, detecção, punição e remediação de fraudes e atos de corrupção, em apoio à boa governança; e
>
> II – Riscos para a integridade: riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.
> […] (BRASIL, 2018).

Evidencia-se na Figura 4 a **relação entre gestão de riscos e Programa de Integridade** pela dependência da segunda em receber da primeira o rol de eventos de risco com potencial para materialização de atos de corrupção. Dessa forma, as possíveis ações lesivas ao erário e ainda não detectadas em ações rotineiras de controle ou auditoria – o "radar" da integridade – são descortinadas pela capacidade que a gestão de riscos tem em trazer à tona fontes de risco ainda não explicitadas em nenhum documento organizacional.

Figura 4: O radar da integridade e a gestão de riscos.
Fonte: Elaborada pelo autor

RISCOS À GESTÃO DE RISCOS

Como já dito, a matéria-prima para o processo de avaliação de riscos é extraída na etapa de identificação e dela dependem as fases seguintes de análise, avaliação e tratamento. Há um conjunto de fontes de riscos que tornam a identificação deles menos eficiente e contribuem para **geração de riscos à própria gestão.** Para a norma 31.000 (ABNT, 2018, p. 2), "fonte de risco é o elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco".

A **primeira fonte de risco** surge quando somente chefes são ouvidos no processo de identificação. Além da tendência natural de não deixar transparecer problemas ou fragilidades existentes sob sua responsabilidade, a rotatividade nos cargos de chefia – fenômeno denominado *turnover* – faz com que eles nem sempre conheçam os detalhes de sua área de atuação tanto quanto seus subordinados.

Basta abrir o Diário Oficial em qualquer dia para se ver a quantidade de cargos em comissão que sofrem exonerações e novas nomeações antes, durante e após trocas de governo. O excessivo *turnover* gerencial não somente destrói o valor da organização como também fere a outros. Os relacionamentos eficazes de longo prazo que foram conquistados erradicam-se, após a rotatividade, por toda a rede de contatos, diminuindo a lealdade, a produtividade e destruindo o valor para todo o sistema. (REICHHELD; TEAL, 2001, p. 157).

Para evitar que esse primeiro fator se transforme em risco à própria gestão, sugere-se que todo "chão de fábrica" seja ouvido sem qualquer tipo de limitação, crítica ou interferência porque é ele o grande conhecedor das vulnerabilidades e ameaças existentes nas atividades laborais.

A consequência da utilização de técnicas de identificação de riscos que não escutam todos os subordinados ou que limitam sua participação é o aumento da probabilidade de a gestão de riscos tornar-se incompleta e ineficiente. Osborn (1963 apud Chapman, 2011, p. 175) vai ao encontro desse pensamento ao dizer que durante a exposição de ideias a "crítica deve ser descartada" e o "pensar livremente" encorajado.

A **segunda fonte de risco** decorre da utilização de um conjunto de perguntas prontas e fechadas em formulários, ou em entrevistas, sobre as ameaças e vulnerabilidades que devam ser relatadas no processo de identificação de riscos. Isso traz como consequência a redução da transparência da organização para a sociedade porque gera possibilidade de incompletude ao próprio processo de avaliação de riscos. Perguntas não deveriam direcionar o pensamento de quem deve apontar fragilidades ou falhas. Se, por exemplo, na identificação de riscos em um hangar de aeroporto, forem realizadas perguntas aos funcionários, como:

- As aeronaves são entregues revisadas e limpas?
- Os pneus encontram-se em bom estado?

Essas perguntas direcionam as respostas e não dão liberdade para que um mecânico possa, por exemplo, relatar o risco de determinada companhia frequentemente apresentar sua aeronave com os tanques de combustíveis praticamente vazios após viagens, indicando uma provável

desconformidade com a legislação que obriga a manutenção de níveis mínimos de combustível para evitar incidentes por pane seca.

Sugere-se que as **perguntas criadas para a captura do conhecimento tácito sejam genéricas** (ver Figura 2), não limitadoras das respostas dos colaboradores e que preferencialmente sigam uma divisão de riscos em categorias (taxonomia) para estimular o pensamento nas mais diversas áreas nas quais os riscos podem surgir: tecnologia, pessoas, financeiro-orçamentário, operacional, ética, ambiental interno e eventos externos. Para Gupta (2016, p. 5) é essencial a compreensão das fontes de riscos corretamente identificadas sob o suporte de uma taxonomia de riscos que auxilie na mensuração dos impactos causados caso eles se materializem.

A **terceira fonte de risco** que põe em xeque a própria gestão surge quando não há suficiente apoio da alta administração ou quando ocorrem sabotagens psicológicas em forma de críticas abertas ao trabalho de identificação de riscos. Resistências são esperadas durante a implantação de qualquer novo procedimento porque reuniões, treinamentos, preenchimento de formulários ou aprendizagem de novos sistemas demandam tempo antes destinados a outras atividades laborais. Se críticas aos novos procedimentos forem externalizadas por chefes diante dos subordinados, desacreditando a importância do trabalho sendo feito, então consequentemente os ouvintes dessas críticas não se sentirão compelidos a colaborarem na identificação de fragilidades nunca antes explicitadas.

Para redução proativa dessa fonte de risco sugere-se o apoio da alta administração na criação e manutenção da cultura de riscos na qual chefes e subordinados sejam conscientizados dos benefícios que essa gestão trará para a melhoria da qualidade e segurança de seus próprios ambientes de trabalho. Nesse sentido, Hillson (2016, p. 36) confirma que as reais barreiras à implementação da gestão de riscos estão relacionadas às pessoas e não necessariamente à metodologia ou *software*. Diz ainda em relação ao frequente tom de apoio da alta administração (*top-down*): **"muito mais do que palavras vazias seja respaldado por ações de reforço consistentes e vigorosas".**

A **quarta fonte de risco** pode surgir quando a política de gestão de riscos do órgão determina que as equipes responsáveis por apontá-los também devam indicar solução para mitigá-los. De acordo com a Instrução Normativa Conjunta nº 1, de 10 de maio de 2016 (BRASIL, 2016) os órgãos e entidades devem instituir política de gestão de riscos:

> […]
>
> Art. 17. A política de gestão de riscos, a ser instituída pelos órgãos e entidades do Poder Executivo federal em até doze meses a contar da publicação desta Instrução Normativa, deve especificar ao menos:
>
> I - princípios e objetivos organizacionais;
>
> II - diretrizes sobre:

> a) como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização;
>
> b) como e com qual periodicidade serão identificados, avaliados, tratados e monitorados os riscos;
>
> c) como será medido o desempenho da gestão de riscos;
>
> d) como serão integradas as instâncias do órgão ou entidade responsáveis pela gestão de riscos;
>
> e) a utilização de metodologia e ferramentas para o apoio à gestão de riscos; e
>
> f) o desenvolvimento contínuo dos agentes públicos em gestão de riscos;
>
> [...]

A política de gestão de riscos é o primeiro e mais importante passo no caminho da institucionalização dessa gestão porque oferece respaldo aos profissionais que trabalharão na área de riscos para executarem todas as ações necessárias ao ciclo dessa gestão.

Da mesma forma que um *cheff* de cozinha, ao perceber o risco de vazamento de uma torneira, talvez não tenha as competências necessárias para corretamente avaliar as causas e o respectivo tratamento do risco, também é provável que os servidores de uma organização pública não se sintam confortáveis em registrar riscos se forem conjuntamente obrigados a darem direcionamento ao tratamento de algo além de sua expertise, trazendo a consequência nefasta ao processo de identificação de riscos de omissão da explicitação de ameaças ou vulnerabilidades que os geram.

Sugere-se, durante a criação ou atualização da política de riscos de cada órgão ou entidade pública, o devido **cuidado para que sua redação não crie desestímulos ao processo de identificação de riscos,** ou seja, para que aqueles responsáveis por identificá-los também não sejam automaticamente responsabilizados por sua correção que, não raras vezes, demanda conhecimentos multidisciplinares.

CONCLUSÃO

A gestão de riscos tornou-se imprescindível às organizações públicas pela capacidade de identificar ameaças e fragilidades antes de se materializarem em incidentes capazes de prejudicar o alcance dos objetivos estratégicos, trazendo danos ao erário e à sociedade brasileira. Apesar de toda recente legislação e todo esforço para operacionalização da gestão de riscos e programas de integridade, há margem para riscos à própria gestão que trazem consequências danosas em cadeia: reduzem a transparência, fragilizam a integridade e, obrigatoriamente, tornam a governança menos eficaz.

Relatórios de gestão entregues aos órgãos de controle normalmente produzem uma visão genérica da atuação da gestão de riscos, abstraindo detalhes de implementação do processo de identificação, etapa crítica ao ciclo de gestão e de onde emergem os riscos documentados. As quatro fontes de risco apresentadas podem ser reduzidas pelos administrados públicos a partir das sugestões expostas neste artigo.

Finalmente, futuros estudos para criação de normativos que orientem às melhores práticas de operacionalização da gestão de riscos podem contribuir com órgãos de controle para muito além da análise do conteúdo, mas principalmente da forma como a identificação de riscos é executada como fator principal de redução de riscos à própria gestão.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – **ABNT NBR ISO 31.000:** Gestão de riscos – Diretrizes. 2. ed. Rio de Janeiro, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO/TR 31.004:** Gestão de riscos – Guia para implementação da ABNT NBR ISO 31.000, Rio de Janeiro, 2015.

BERSTEIN, Peter L**. Desafio aos deuses:** a fascinante história do risco. 23. ed. Rio de Janeiro: Gulf Professional Publishing, 1997. 369 p.

BRASIL. Decreto n. 9.203, de 22 nov. 2017. **Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.** Brasília, DF: Diário Oficial, 23 nov. 2017. Seção I, p. 3.

_____. Instrução Normativa n. 1, de 10 de mai. 2016. **Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.** Brasília, DF: Diário Oficial, n. 89, seção I, p. 14-17, 11 mai. 2016.

_____. Portaria n. 1.089, de 25 de abril de 2018. **Estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências.** Ministério da Transparência e Controladoria-Geral da União (CGU), Brasília, DF, 2018.

CHAPMAN, Robert J. **Simple Tools and Tecniques for Enterprise Risk Management.** 2. ed. Croydon: John Wiley & Sons Ltd, 2011. 494 p.

GUPTA, Aparna. **Risk Management and Simulation.** New York: CRC Press, 2016. 523 p.

HILLSON, David. **The Risk Management Handbook:** A practical guide to managing the multiple dimensions of risk. Croydon: Kongan Page Publishers, 2016. 336 p.

KIRSCH, Philipp; HINE, Amelia; MAYBURY, Terry. A model for the implementation of industry-wide knowledge sharing to improve risk management practice. **Safety Science,** Amsterdam, vol. 80, p. 66-76, 2015.

REICHHELD, Frederick F.; TEAL, Thomas. **The loyalty effect:** the hidden force behind growth, profits, and lasting value. Boston: Harvard Business School Press, 2001. 323 p.

SANTOS, Renato Almeida dos; GUEVARA, Arnoldo José de Hoyos; AMORIM, Maria Cristina Sanches; FERRAZ-NETO, Ben Hur. **Compliance e liderança: a suscetibilidade dos líderes ao risco de corrupção nas organizações,** Einstein, São Paulo, v. 10, n. 1, 10p., 2012.

Recebido em 15/01/2018

Aprovado em 17/05/2018