Gestão de Riscos: o principal pilar para a governança da sua estratégia de negócio

"Não se gerencia o que não se mede, não se mede o que não se define, não se define o que não se entende e não há sucesso no que não se gerencia". Essa conhecida frase de William Edwards Deming resume dois importantes pontos da gestão de riscos: é preciso conhecer os riscos de uma empresa e é preciso ter gestão sobre esses riscos para alcançar o sucesso.

Quando perguntamos aos executivos de uma empresa o que são riscos, a resposta é rápida e conhecida. "É o que pode dar errado". "É um potencial de perda ou prejuízo". "É algo incerto". "'É uma ameaça ao negócio". Mas quando perguntamos se um risco pode ser eliminado, as respostas são divergentes. Alguns dizem que sim, outros que não e alguns dizem talvez. Ao ouvirem a resposta correta, ainda existe discordância e muito debate: a resposta é não, um risco não pode ser eliminado. Ele pode ser gerenciado.

A gestão de riscos tem sido o principal pilar de diversos temas que estão na pauta das empresas atualmente, como, por exemplo: programas de compliance, programas de prevenção à lavagem de dinheiro e planos de auditoria interna.

Segundo as diretrizes da CGU para empresas privadas, "a empresa deve conhecer seus processos e sua estrutura organizacional, identificar sua área de atuação e principais parceiros de negócio, seu nível de interação com o setor público – nacional ou estrangeiro – e consequentemente avaliar os riscos para o cometimento dos atos lesivos da Lei nº 12.846/2013". Ou seja, o entendimento dos riscos do negócio é que direciona o código de conduta, as políticas e os procedimentos, as comunicações, o plano de treinamento e o monitoramento de todo o programa.

Recentemente, os principais órgãos reguladores do Brasil (CVM – Resolução n. 50/2021, BACEN – Circular n. 3978/2020, SUSEP – Circular n. 612/2020, PREVIC – Instrução n. 34/2020) lançaram novas versões de suas regulamentações referentes aos programas de prevenção à lavagem de dinheiro, onde a grande evolução frente às versões anteriores foi a determinação de que as empresas devem realizar uma análise dos riscos do seu negócio para estruturar as políticas e os alertas de prevenção à lavagem de dinheiro, a chamada David Hillsonabordagem baseada em risco.

A ISO 19011:2018 – "Diretrizes para auditoria de sistemas de gestão" incluiu o princípio da Mentalidade de Risco, abrangendo a orientação de que a auditoria deve considerar

os riscos e oportunidades, que derivam do contexto da organização, para planejar sua abordagem e para verificar o gerenciamento da organização.

Porém, a implementação da gestão de riscos envolve mudança de comportamento e atitude em uma organização. É necessário "mexer" na cultura da organização. Um especialista em gestão de riscos conhecido internacionalmente, escreveu os "Top 10 Mitos de Risco", que devem ser bem esclarecidos antes de se iniciar a implementação da gestão de riscos em uma empresa. São eles:

- Todo risco é ruim. – Nem todo risco é ruim. Alguns riscos são oportunidades de negócio.
- Perda de tempo. – A gestão de riscos pode ajudar a prever incertezas do futuro e ajudar as empresas a estarem preparadas para enfrentá-las.
- O que não conhecemos não irá nos afetar. – Achar que a ignorância é uma benção não é a melhor forma de lidar com incertezas, pois elas existem e podem afetar, e muito, o negócio.
- Gestor de riscos gerencia os seus riscos. – O papel da gestão de riscos é de todos dentro da empresa. Os riscos devem ser gerenciados pelos donos dos riscos.
- Todos os riscos podem ser evitados. – Nem sempre conseguimos evitar todos os riscos. Seja porque é custoso ou porque o controle pode levar muito tempo para ser implementado. Sendo assim, outras opções como transferência do risco, diminuição do risco ou até mesmo aceitação do risco são estratégias a serem consideradas.
- Nosso negócio não é arriscado. – Não existe empresa sem risco. É preciso assumir riscos para gerar valor.
- Gestão de riscos requer números. – Muitos riscos não são quantificáveis e requerem uma avaliação qualitativa.
- Os riscos são cobertos pelos processos existentes. – Nem todos os riscos são cobertos pelos processos existentes na empresa. Alguns riscos são específicos e precisam de uma avaliação profunda para desenvolver planos de mitigação.
- Contingência é para os fracos. – Nem o melhor gestor de projetos pode prever o futuro. Ter um plano de contingência para imprevistos é um sinal de sabedoria e não de fraqueza.
- A gestão de riscos não funciona. – Dizer que os riscos identificados não acontecem e que as situações não refletem o que o estava no mapa de riscos, não é a melhor explicação para abandonar a gestão de riscos. Quando identificamos os riscos reais e implementamos respostas efetivas, as chances de sucesso são maximizadas.

Existem duas importantes referências para estruturar um processo de gestão de riscos nas empresas: COSO ERM 2017 e ISO 31000:2018. Ambos possuem princípios e etapas que servem como um passo a passo de implementação nas empresas:

1. Identificação dos riscos: A empresa deve analisar o ambiente de negócio tanto interno quanto externo, fatores organizacionais e objetivos estratégicos. Análise

SWOT (forças, fraquezas, oportunidades e ameaças) ou análise PESTEL (político, econômico, social, tecnológico, ambiental e legal) podem ser realizadas nessa etapa, assim como análise de políticas, relatórios e entrevistas com executivos da empresa.

2. Avaliação dos riscos: Identificar as causas e as consequências dos riscos, categorizar os riscos (risco operacional, risco estratégico, risco financeiro, risco cibernético, risco regulatório) e avaliar os controles existentes são essenciais para avaliar os riscos identificados na etapa anterior.
3. Priorização dos riscos: As atividades dessa etapa passam tanto pela classificação dos riscos em uma escala de probabilidade e impacto, quanto pela definição dos níveis de risco (baixo, médio, alto) e pela definição das respostas aos riscos (aceitar, reduzir, mitigar, compartilhar, evitar). Nessa etapa, a Alta Administração também deve definir o apetite aos riscos da empresa, ou seja, qual o nível de risco a empresa está disposta a correr para atingir seus objetivos.
4. Monitoramento dos riscos: Essa etapa final compreende a indicação de eventuais melhorias a serem feitas nos processos para responder aos riscos priorizados na etapa anterior.

É recomendado que esse ciclo seja repetido periodicamente, de forma a manter os controles e processos alinhados à atualidade da empresa.

Concluindo, é importante ter em mente que não existe “receita de bolo” ou mapa de riscos “de prateleira”. Cada empresa é única, possui particularidades que devem ser conhecidas e tratadas para que seus processos sejam robustos, com controles bem implementados, evitando que a materialização de riscos impeçam a continuidade do negócio e a empresa possa ter uma vida duradoura e de sucesso.

Que tal começar a construir um Programa de Gestão de Riscos da sua empresa num curso da FDC? Clique aqui e saiba todos os detalhes o curso Governança, Risco e Compliance!

Autora: Vivian Fluminense, professora convidada da Fundação Dom Cabral