2017

Governança e Gestão de Riscos em Organizações Públicas

APOSTILA

FERNANDO FRANCO

Governança e Gestão de Riscos em Organizações Públicas

Sumário

Governança e Gestão de Riscos em Organizações Públicas

1 Riscos, Decisão e Incerteza

O risco está presente em todas as atividades humanas. Riscos é o resultado de uma decisão. Sempre que tomamos uma decisão ou deixamos de tomá-la, estamos de alguma forma assumindo riscos. Pessoas e organizações, sejam públicas ou privadas, enfrentam algum tipo de risco em suas atividades diárias. Riscos estão relacionados a investimentos, fusões, fraudes, incêndios, terremotos, resultados de um processo ou projeto, ou, simplesmente, à decisão de atravessar uma rua.

O risco está associado à incerteza, ou mais precisamente ao "efeito da incerteza sobre os objetivos" (NBR ISO 31000, 2011, p 1), sendo que o efeito é definido como um desvio em relação ao planejado.

A incerteza e, portanto, o risco associado, decorre da impossibilidade de prever o futuro no momento da tomada de decisão. Mesmo que seja possível obter informações completas sobre o comportamento das variáveis chaves e identificar as estratégias dos atores relevantes a um determinado fenômeno, ainda assim, ficará a incerteza sobre as ações que serão, de fato, tomadas por esses atores e seus impactos sobre o futuro. Esse aspecto foi pontuado por Gaston Berger, em 1958, quando cita que "prever uma catástrofe é condicional, pois significa prever algo que aconteceria se nada fosse feito para alterar o curso das coisas, e não aquilo que acontecerá de qualquer maneira" (BERGER, 2004, p. 317).

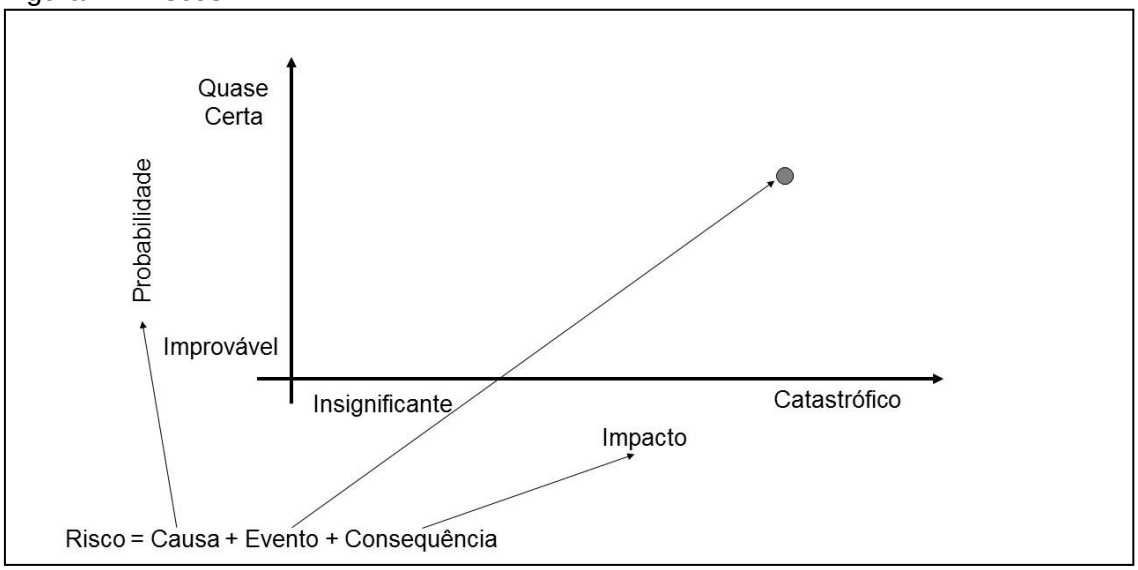
É importante ressaltar que risco e incerteza não são sinônimos. Riscos são eventos em que os resultados podem ser mensurados e suas probabilidades de ocorrência, estimadas.

Frank H. Knight, em um dos primeiros livros a tratar sobre riscos, enfatiza que "a incerteza mensurável, ou risco, como devemos usar o termo, é muito diferente da (incerteza) imensurável..., que é a verdadeira incerteza, e não risco" (KNIGHT, 1921, p.20).

As principais normas de gestão de riscos apresentam definições convergentes, relacionando riscos com a ocorrência de eventos e seus resultados sobre os objetivos. A norma **ABNT NBR ISO 31000:2009 – Gestão de riscos - Princípios e diretrizes** enfatiza que o risco é o efeito da incerteza, definida como um estado, mesmo que parcial, da deficiência das informações relacionada a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade. A norma **COSO - Gerenciamento de riscos corporativos - Estrutura integrada,** acrescenta que riscos são eventos que geram impacto, sendo que os negativos são aqueles que podem impedir a criação de valor ou mesmo destruir o valor existente, e os positivos são aqueles que influenciam favoravelmente a realização dos objetivos, apoiando a criação ou a preservação de valor. O **The Orange Book – Gestão de riscos - Princípios e conceitos** relaciona riscos à incerteza dos resultados. Outras normas, tais como, Cobit, IRM, FERMA, COCO, seguem no mesmo sentido.

A gestão de riscos organizacionais, para ser efetiva, deve ter uma linguagem comum sobre o que são riscos e como mensurá-los. Em geral, os riscos são caracterizados por um evento potencial e o impacto de suas consequências. A magnitude do risco, também chamada de nível de riscos, é caracterizada pela combinação da probabilidade de ocorrência do evento e o impacto de suas consequências (Figura 1).

Figura 1 - Riscos

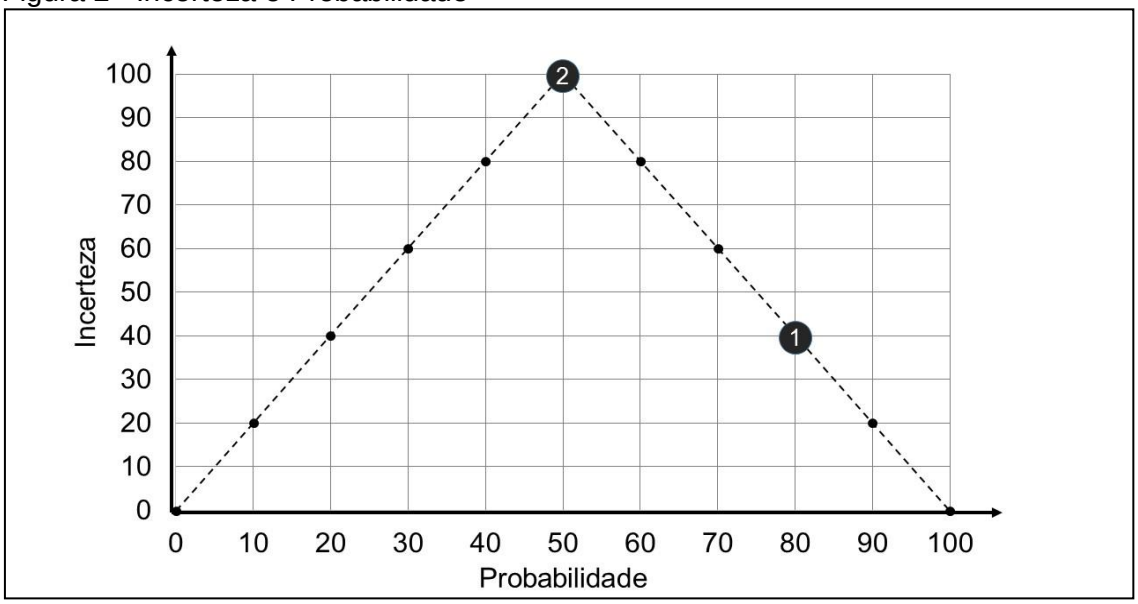


Fonte: Elaborado pelo autor

A avaliação do nível de riscos como uma combinação de probabilidade e impacto pode gerar dúvida, pois implica que os riscos não são diretamente proporcionais à incerteza.

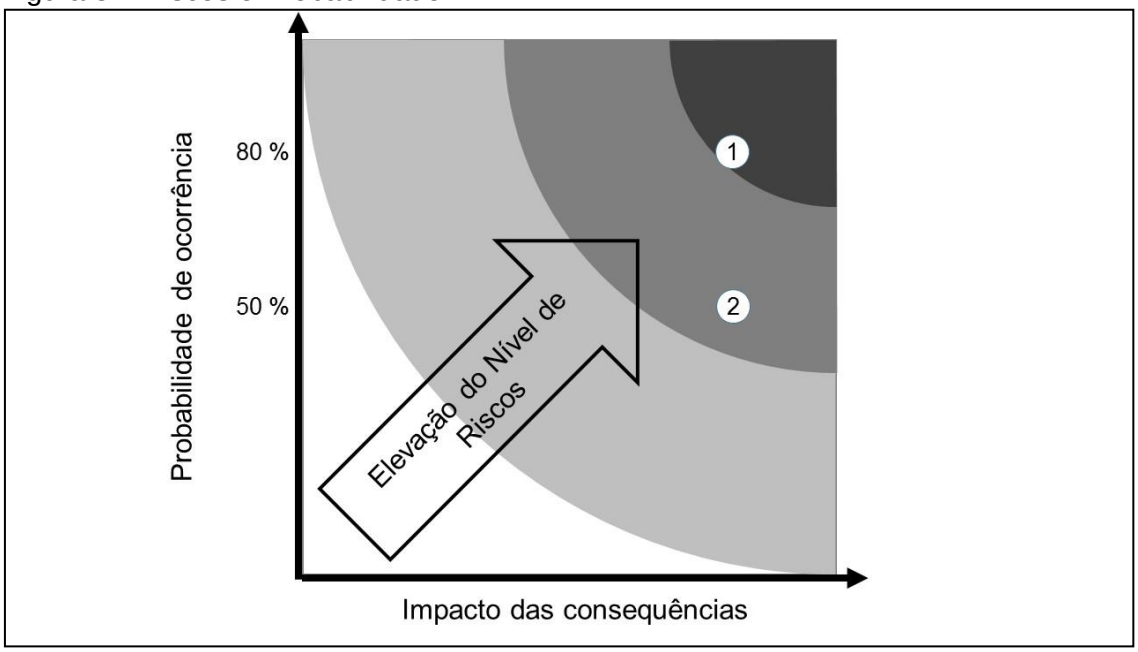
Para ilustra este fato, considere a realização de um concerto ao ar livre. Para os organizados do concerto, um dos riscos relacionado ao objetivo de satisfação dos patrocinados é a presença de público reduzido. Uma possível causa da falta de público é uma forte chuva na hora do concerto. Suponhamos que a probabilidade de chover forte na hora do concerto seja estimada em 80% (situação 1). Os organizadores podem decidir pela manutenção do concerto no dia e hora programado. Neste caso, o nível de riscos será elevado (probabilidade de 80%); contudo, não existe grande incerteza quanto à sua ocorrência. Considere, agora, uma mudança nas condições climáticas alterando a probabilidade de chuva de 80% para cerca de 50% (situação 2). Nessa nova situação, a incerteza e maior (Figura 2), contudo, o nível de risco é menor (Figura 3). Em ambos os casos, a consequência seria a mesma – presença de público reduzida.

Figura 2 - Incerteza e Probabilidade



Fonte: Elaborado pelo Autor

Figura 3 – Riscos e Probabilidade



Fonte: Elaborado pelo Autor

O exemplo também ilustra o fato de que a incerteza está relacionada ao efeito de uma tomada de decisão. Caso os organizadores decidam cancelar o concerto, não haverá incerteza e a chuva deixa de ser relevante.

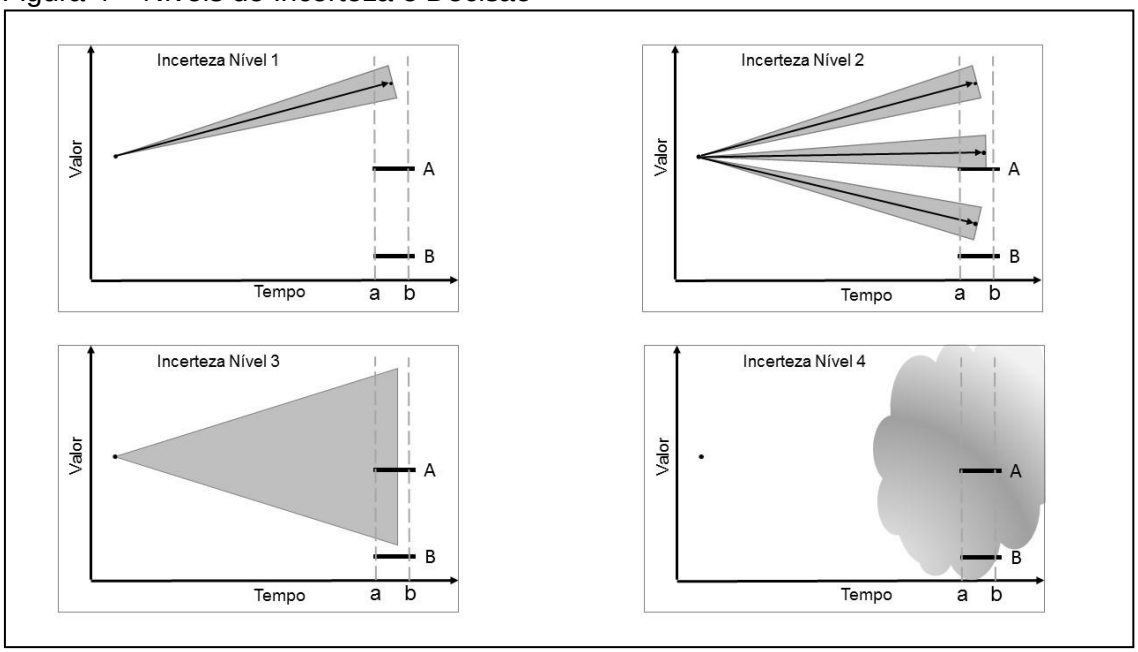
Um aspecto importante da incerteza é que ela não está diretamente associada a uma variável, área ou setor específico, e sim, a uma tomada de decisão. A incerteza, também, não é um valor absoluto e pode ser classificada em níveis. Huges (2000) estabelece quatro níveis básicos de incerteza (Figura 4):

- Nível 1 - Futuro Projetivo – O futuro pode ser visto como uma continuação do passado.
- Nível 2 - Futuros alternativos – Série limitada de resultados possíveis. Variáveis discretas.
- Nível 3 - Futuros em gama contínua – Série ilimitada de resultados possíveis. Variáveis contínuas
- Nível 4 - Futuros ambíguos – Podem ocorrer resultados sem conexão com o presente ou nem mesmo uma gama de possíveis resultados pode ser avaliada.

Para os níveis 1, 2 e 3, é possível calcular e gerenciar os riscos. O nível 4, contudo, cai na definição de incerteza pura, onde não é possível calcular os riscos.

Para identificar o nível de incerteza a ser considerado para o gerenciamento dos riscos é necessário incluir outros dois aspectos, o valor de referência e o tempo.
O valor de referência é ilustrado na figura 3. Caso o valor de referência para a decisão seja o “B”, os níveis 1, 2 e 3 se confundem para uma decisão referenciada ao intervalo de tempo a-b.

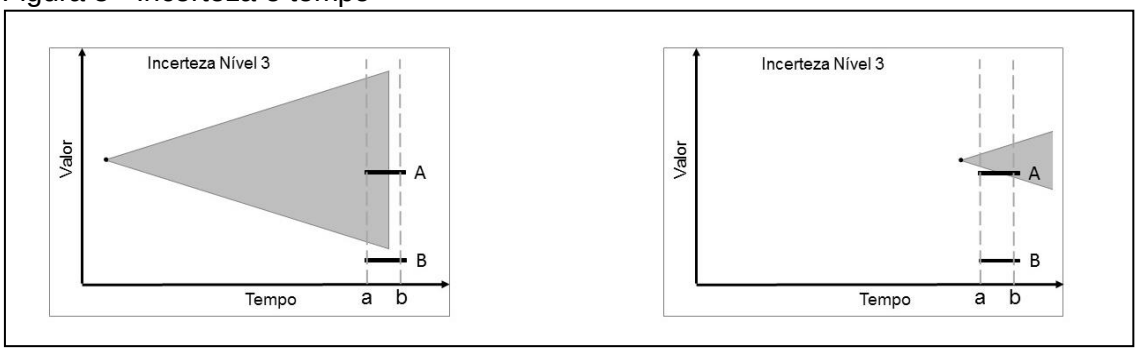
Figura 4 – Níveis de Incerteza e Decisão



Fonte: Adaptado de Courtney, 2001

O fator tempo refere-se à incerteza do futuro, ou mais precisamente ao fato de que quanto mais distante é o futuro, maior será o nível de incerteza. Olhando em sentido contrário, o pressuposto é que, com o passar do tempo, a incerteza tende a diminuir (Figura 5).

Figura 5 - Incerteza e tempo

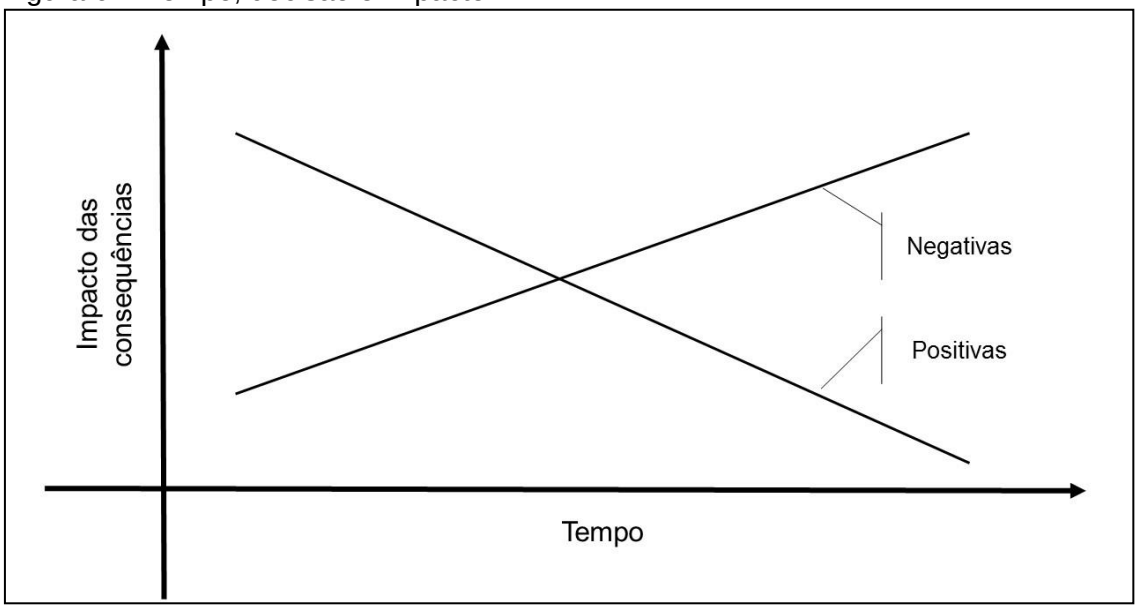


Fonte: Elaborado pelo autor

O tempo é um aspecto fundamental na incerteza, contudo, deixar o tempo passar como forma de tratamento de riscos, nem sempre é possível nem desejado.

O alerta vale para consequências positivas e negativas. Com o passar do tempo, os impactos positivos tendem a diminuir e os negativos a aumentar.

Figura 6 – Tempo, decisão e impacto



Fonte: Elaborado pelo autor

Incerteza e riscos são aspectos relevantes da tomada de decisão. Assim como não existe nível zero de incerteza, não existe nível zero de riscos. O que se pode estimar é o nível de incerteza com o qual a decisão será tomada e, portanto, estimar um nível de risco.

O nível de incerteza com o qual as decisões são tomadas deve ser restrito à chamada incerteza residual (Huges, 2000). Incerteza residual é diferente daquilo que não se sabe. Incerteza residual é aquilo que não é possível saber no momento de uma tomada de decisão, processo chave da governança corporativa.

2 Governança Corporativa e Gestão de Riscos

A gestão de riscos é um dos processos que integram a boa governança corporativa, porém não é o único.

Governança corporativa pode ser definida como o sistema de direção e controle das organizações. A base da governança corporativa empresarial está na teoria de agência. A teoria analisa situações em que o proprietário, ou os acionistas, delegam a um agente especializado, o administrador, o poder de decisão sobre a empresa. Nesta situação pode surgir divergência de entendimento sobre o que cada grupo entende como o melhor para a empresa. A governança corporativa surgiu justamente no sentido de superar este tipo de conflito. A teoria de agência foi proposta por Berle e Means (Berle e Means, 1932). A governança corporativa, em geral, é preconizada no formato de melhores práticas.

2.1 Governança Corporativa

O aspecto central da governança corporativa, o conflito entre proprietários e agentes, não se restringe à área privada, sendo estendido para a área pública.

Segundo o TCU, a “governança no setor público compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade” (Referencial básico de governança aplicável a órgãos e entidades da administração pública, 2014, p.). De acordo com o referencial básico, “para que as funções de governança (avaliar, direcionar e monitorar) sejam executadas de forma satisfatória, alguns mecanismos devem ser adotados: a liderança, a estratégia e o controle”, sendo que no mecanismo de controle estão

inseridos os componentes de **gestão de riscos e controle interno**, auditoria interna e accountability, e transparência (TCU, 2014, p.).

Para o Australian National Audit Office (ANAO), existem apenas dois objetivos da boa governança no setor público: desempenho com foco nos resultados e prestação de contas (accountability) (ANAO, 2014).

O documento australiano considera que os elementos fundamentais da boa governança no setor público são:

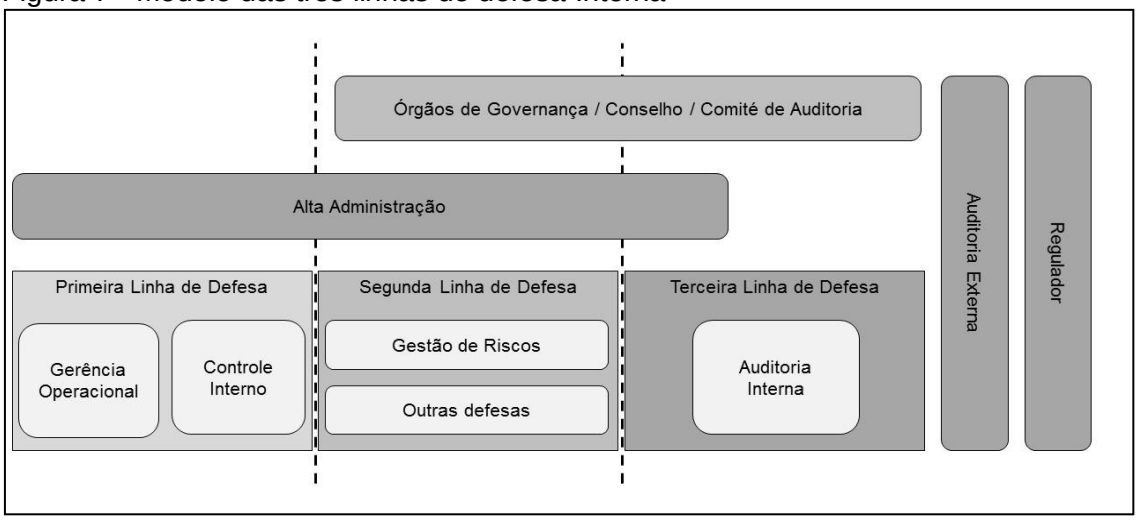
- Forte liderança em todos os níveis com foco em comportamento ético e na melhoria contínua.
- Manutenção de um sistema de governança e processos adequados aos propósitos do órgão.
- Otimização do desempenho através do planejamento, integrado à gestão de riscos, inovação e monitoramento de resultados.
- Avaliação e revisão, com foco em abertura, transparência e integridade.
- Envolvimento construtivo com os stakeholders e promoção de prestação de contas (accountability) através de clareza nos reporte de desempenho e operações com uma participação apropriada em parcerias colaborativas, incluindo parcerias fora do governo.

O guia Estrutura Internacional: Boa governança no setor público (IFAC, 2014), considera que a governança inclui as estruturas, processos e recursos políticos, econômicos, sócias, ambientais, legais e administrativos empregados para garantir que os resultados definidos e planejados pelas partes interessadas (stakeholders) sejam alcançados.

2.1.1 Modelo de melhores práticas de governança

A integração da gestão de riscos à governança corporativa aparece em diversos modelos de melhores práticas, incluindo o modelo das três linhas de defesa (figura 7). Este modelo é uma forma simples de mostrar o papel da gerência operacional e do controle internos como a primeira linha de defesa, da gestão de riscos como a segunda linha e da auditoria interna como a terceira linha. Cada uma dessas linhas desempenha um papel distinto dentro do processo de governança corporativa. O modelo mostra, também, o papel dos órgãos de governança e da alta administração como supervisores da atuação das linhas de defesa.

Figura 7 - Modelo das tres linhas de defesa Interna

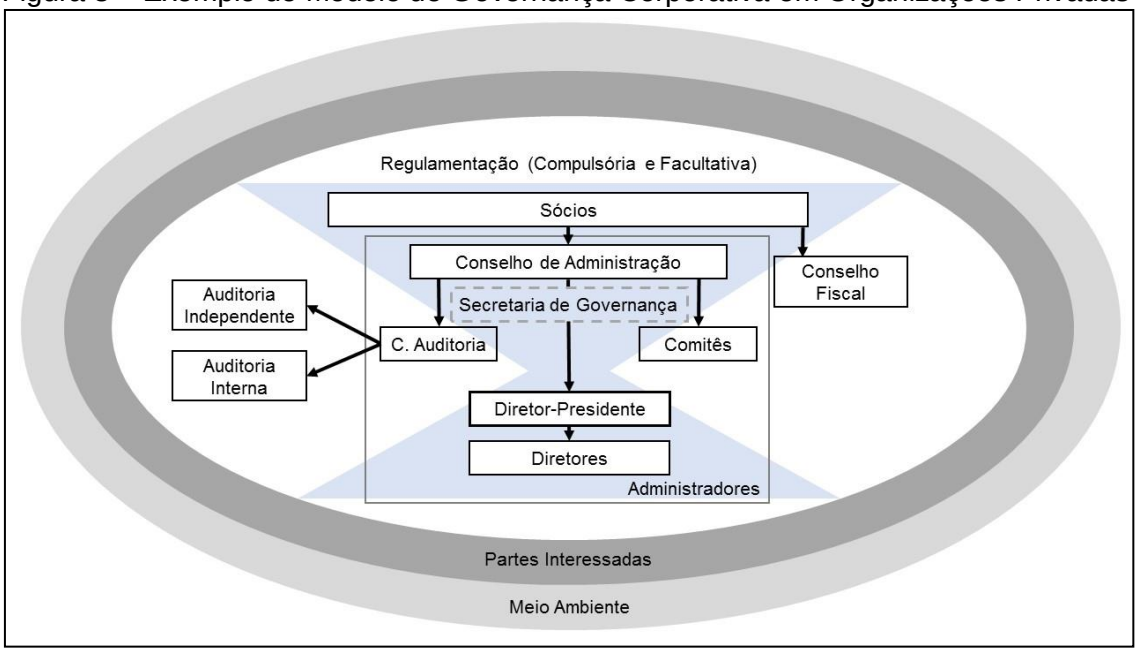


Fonte: Adaptação de FERMA, 2011.

Os modelos de governança preconizados pelo IBGC (figura 10), com foco na área privada, e pelo TCU (figura 11), com foco na área pública, destacam a importância das

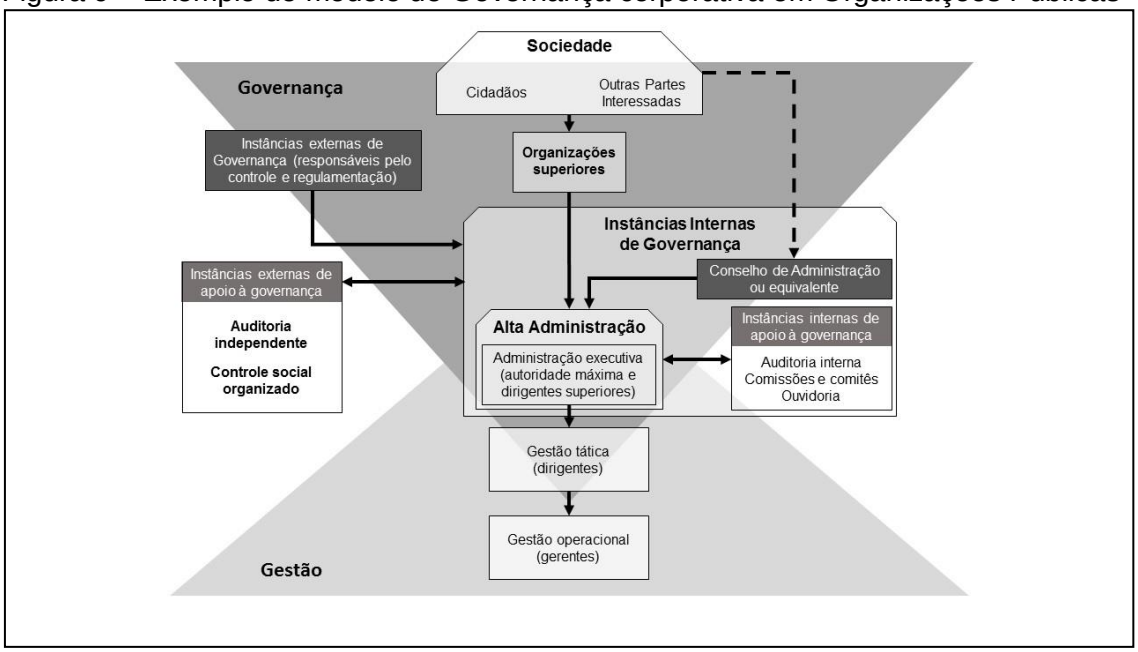
partes interessadas. O modelo do TCU destaca ainda a existência de duas instancias de governança na área pública, uma interna e outra externa.

Figura 8 – Exemplo de Modelo de Governança Corporativa em Organizações Privadas



Fonte: IBGC, 2007

Figura 9 – Exemplo de modelo de Governança corporativa em Organizações Públicas



Fonte: TCU, 2014a

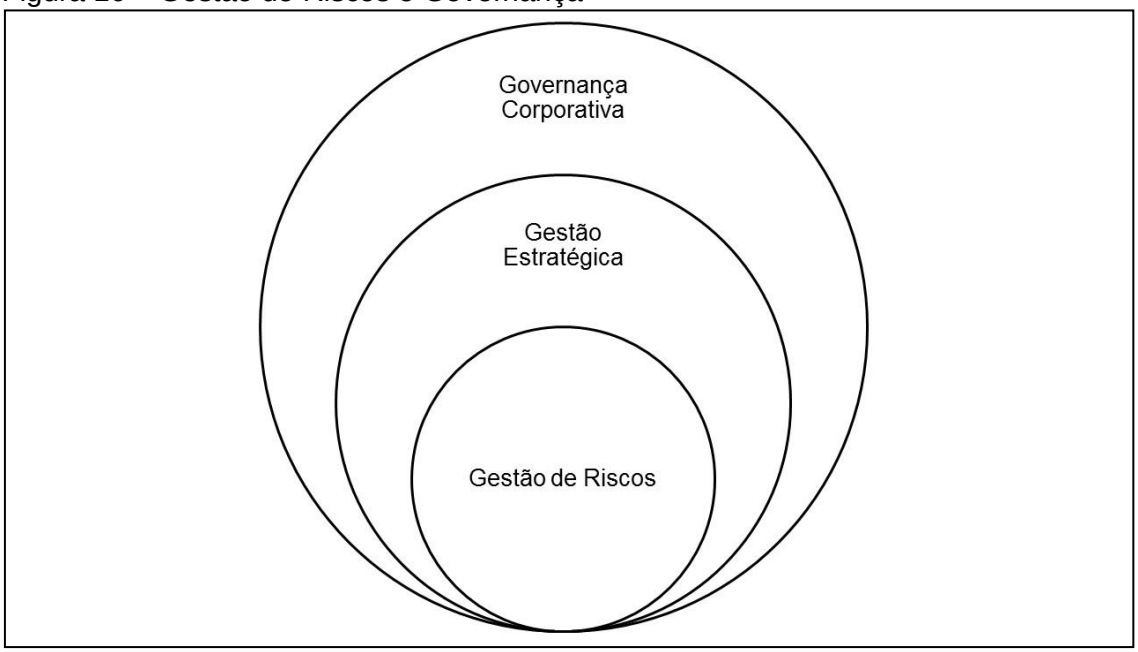
2.2 Gestão de Riscos

A gestão de riscos é uma parte integrante das boas práticas de gestão (Figura 10). Existe uma relação direta entre riscos e oportunidades em todas as áreas de negócios, incluindo a gestão pública. Todas as instituições devem ser capazes de

identificar, mensurar e gerenciar os seus riscos com o propósito de capitalizar as oportunidades e atingir seus objetivos.

A gestão de riscos é uma das principais ferramentas na governança corporativa. A governança fornece os requisitos de estrutura e direção necessários para que uma organização consiga atingir seus objetivos e gerenciar apropriadamente suas operações, ao passo que a gestão de riscos fornece as políticas e procedimentos necessários para que a organização opere com efetividade em um ambiente mutável e incerto.

Figura 10 – Gestão de Riscos e Governança



Fonte: Elaborado pelo autor

A gestão de riscos contribui para a boa governança corporativa na medida em que fornece garantias à gerencia sênior de que os objetivos organizacionais serão atingidos dentro de níveis aceitáveis de riscos residual.

Em instituições privadas, os limites estratégicos das decisões que o diretor executivo (CEO) pode tomar devem ser definidos pelo conselho. O conselho define de um lado o que deve ser feito e de outro o que é proibido. A atuação do diretor executivo entre os dois limites permite gerenciar a tensão inevitável entre as atividades de geração de valor e proteção de valor.

A definição de um espaço limitado de atuação (strategic sandbox) com o qual os gerentes podem raciocinar na execução do modelo de negócios provê os meios para que o conselho e o diretor executivos concordem com o que a organização não deve fazer. Esses limites definem o contexto para o que pode ser feito, permitido ao diretor executivo liderar a organização com foco em aspectos estratégicos, operacionais e financeiros.

Os limites têm fortes impactos na estratégia e reduz o risco de desvios estratégicos. Eles também permitem decisões estratégicas rápidas e ajudam a reduzir perda de esforço em iniciativas que provavelmente não serão aceitas em função de desalinhamento estratégico.

Na área pública, a gestão de riscos segue no mesmo sentido, sendo componente fundamental no suporte da boa governança corporativa, com o propósito de oferecer uma garantia razoável de que os objetivos serão atingidos sem exceder a habilidade do órgão em aceitar ou tolerar riscos.

A forma pela qual um órgão de governo coordena a governança corporativa e a gestão de riscos depende do tamanho, da complexidade das operações, dos serviços

que ele prove e dos recursos disponíveis. A coordenação dessas atividades permite que o órgão desempenhe seus processos, otimize recursos e forneça informações consistentes e de qualidade.

A gestão de riscos é, também, um mecanismo de proteção aos diretores e gerentes em caso de resultados adversos em dois aspectos: na aceitação da ocorrência de eventos de riscos dentro dos níveis predefinidos (probabilidade e impacto) e na mitigação dos impactos desses eventos.

Ao focar também em resultados positivos, a gestão de riscos fornece uma contribuição importante no aspecto de governança corporativa no que se refere à melhoria do desempenho organizacional.

A estrutura de gestão de riscos facilita, ainda, a comunicação e a consulta entre as partes interessadas externas, órgão de governo, a direção e os funcionários de todos os níveis sobre a definição e consecução dos objetivos organizacionais.

A NBR ISO 31000 define gestão de riscos como uma atividade coordenada para dirigir e controlar uma organização no que se refere a riscos.

Para o COSO ERM o gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos (COSO, 2004).

Para o Orange Book riscos são definidos como a incerteza dos resultados, sejam positivos (oportunidades) ou negativos (ameaças) de ações e eventos.

A *International Federation of Accountants* (IFAC) também atrela o gerenciamento de riscos aos objetivos, enfatizando que avaliações de risco deve questionar o estabelecimento dos próprios objetivos (IFAC, 2015). A publicação utiliza a definição de gerenciamento de riscos da ISO 31000 e enfatiza que o gerenciamento de riscos auxilia as organizações a tomar decisões conscientes sobre os objetivos que deseja alcançar, sobre o nível, natureza e apetite aos riscos que querem assumir e sobre os controles necessários para atingir tais objetivos. A publicação enfatiza, ainda que o controle interno obtenha melhores resultados quando considerado como parte do processo de gestão de riscos.

2.3 Controle Interno

O controle interno é parte da estrutura de gestão de riscos das organizações. A gestão de riscos tem um aspecto mais amplo, contudo, o controle interno tem papel fundamental no sucesso da gestão de riscos organizacionais. A gestão de riscos inclui a definição dos objetivos estratégicos enquanto o controle interno deve prover garantia razoável de que eles serão atingidos. O escopo da gestão de riscos é mais amplo, envolvendo alternativas de respostas aos riscos (evitar, aceitar, compartilhar ou reduzir o risco), ao passo que o controle interno trata primariamente da redução de riscos. Mais ainda, a gestão de riscos corporativos engloba os objetivos de resultado que sofrem forte impacto de eventos e atores externos e que geralmente estão fora do controle da organização (COSO, 2014).

Um dos modelos de controle interno mais empregado é o COSO Controle Interno - Estrutura Integrada, que o define como “um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade” (COSO, 2013).

Para o COSO pode existir uma estrutura de controle interno sem que exista uma estrutura de gestão de riscos, contudo, neste caso, os objetivos a serem assegurados referem-se à eficiência e eficácia das operações, confiabilidade das demonstrações e conformidade. A estrutura de gestão de riscos amplia o componente de avaliação de riscos da estrutura de controle interno, agregando uma quarta categoria de riscos – os riscos estratégicos, que extrapolam o escopo do controle interno. Os objetivos

estratégicos são derivados da missão e da visão e os demais objetivos (operações, confiabilidade das demonstrações e conformidade) devem estar alinhados com eles (COSO, 2013)

Na área pública não é diferente. O Tribunal de Contas da União define controle interno como um

> "[...] processo composto pelas regras de estrutura organizacional e pelo conjunto de políticas e procedimentos adotados por uma organização para a vigilância, fiscalização e verificação, que permite prever, observar, dirigir ou governar os eventos que possam impactar na consecução de seus objetivos. É, pois, um processo organizacional de responsabilidade da própria gestão, adotado com o intuito de assegurar uma razoável margem de garantia de que os objetivos da organização sejam atingidos" (TCU, 2009, p.).

Aspectos de controle interno devem ser analisados com atenção quando for empregada a NBR ISO 31000. A ISO não possui norma específica para controle interno, contudo, aspectos de controle e conformidade são abordados em diversas normas, tais como as normas das séries 9000, 14000 e 27000. Para a NBR ISO 31000, o conceito de controle é diferente daquele de controle interno, o que muitas vezes causa dúvida. Para a NBR ISO 31000, controle é parte do tratamento de riscos e inclui processos, política, mecanismos, práticas e outras ações, tendo por objeto a alteração do nível de risco (ABNT, 2009 a), ou seja, para a NBR ISO 31000 controles são tratamentos que servem para mitigar riscos, para a COSO, controles servem para verificar se os tratamentos estão sendo executados em conformidade com o preconizado. Nesse contexto, a natureza desse controle é diferente da dos controles internos, tanto de conformidade à regulamentação quanto de conformidade à eficiência dos processos operacionais.

Para a COSO, controles são as políticas e os procedimentos que direcionam as ações individuais na implementação das políticas de gestão de riscos, diretamente ou mediante a aplicação de tecnologia, a fim de assegurar que as respostas aos riscos sejam executadas (COSO, 2013).

Na área pública, no Brasil, existe ainda outro conflito com o termo controle. A Constituição Federal de 1988 em seu artigo 74 define que:

> Art. 74. Os Poderes Legislativo, Executivo e Judiciário manterão, de forma integrada, sistema de controle interno com a finalidade de: I–avaliar o cumprimento das metas previstas no plano plurianual, a execução dos programas de governo e dos orçamentos da União; II– comprovar a legalidade e avaliar os resultados, quanto à eficácia e eficiência, da gestão orçamentária, financeira e patrimonial nos órgãos e entidades da administração federal, bem como da aplicação de recursos públicos por entidades de direito privado; III – exercer o controle das operações de crédito, avais e garantias, bem como dos direitos e haveres da União; IV–apoiar o controle externo no exercício de sua missão institucional. (BRASIL, 1988, p.58)

Este fato foi explicitado na instrução normativa conjunta nº 001**,** em seu artigo sétimo quando enfatiza que "os controles internos da gestão tratados neste capítulo não devem ser confundidos com as atividades do Sistema de Controle Interno relacionadas no artigo 74 da Constituição federal de 1988 nem com as atribuições da auditoria interna, cuja finalidade específica é a medição e avaliação da eficácia e eficiência dos controles internos da gestão da organização" (BRASIL, 2016, p.4).

2.4 Auditoria Interna

A auditoria interna é uma atividade executada de forma independente, com o propósito de avaliar a efetividade dos controles e a conformidade das operações às normas aplicáveis.

A auditoria interna deve atuar de forma proativa no monitoramento, na avaliação e nas recomendações de melhorias dos controles, procedimentos e normas. Não cabe

à auditoria estabelecer as normas, as estratégias de gestão de riscos, ou os controles para mitigá-los. Essas são atividades próprias de gestão.

A unidade de auditoria interna integra a administração da organização, executa atividade sob demanda e não deve ser confundida com a unidade de controles internos, que é uma unidade de gestão e faz parte da estrutura de linha, executando processos com atribuições relacionadas ao gerenciamento de riscos, seus tratamentos e os controles para mitigá-los.

A auditoria interna é fundamental nas atividades de gestão de riscos e conformidade na organização, nesse sentido, uma das funções do auditor interno é prover garantia (assurance) de que: (1) o controle de riscos é apropriadamente projetado e efetivamente implementado e (2) a estrutura de gestão de riscos é efetiva.

Comparando a auditoria com o controle interno, a principal diferença é que a auditoria não implanta controles, mas a unidade de controles internos pode implantá-los e, neste caso, cabe à auditoria avaliar a efetividade dos controles implantados.

Segundo a Estrutura Internacional de Práticas Profissionais a "auditoria interna é uma atividade independente e objetiva de avaliação (assurance) e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia uma organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança" (IIA, 2013).

Existem, basicamente, três tipos de papéis para auditoria interna no que se refere a gestão de risos: papéis fundamentais, papéis legítimos e papéis que não deve assumir (IIA, 2009):

- Papéis fundamentais da auditoria interna em relação ao gerenciamento de riscos corporativos.
    - Dar garantia (assurance) dos processos de gerenciamento de riscos
    - Dar garantia (assurance) de que os riscos são corretamente estimados
    - Avaliar os processos de gerenciamento de riscos
    - Avaliar o processo de reporte dos principais riscos
    - Revisar o gerenciamento dos principais riscos
- Papéis legítimos da auditoria interna, com salvaguardas.
    - Facilitar a identificação e a avaliação dos riscos
    - Orientar a administração na resposta os riscos
    - Coordenar as atividades de gerenciamento de riscos corporativos
    - Reportar consolidação dos riscos
    - Manter e desenvolver a estrutura do GRC
    - Defender a implantação do GRC
    - Desenvolver estratégias de gerenciamento de riscos para aprovação do conselho
- Papéis que a auditoria interna não deve assumir
    - Estabelecer o apetite ao risco
    - Impor processos de gerenciamento de riscos
    - Garantir administração de riscos
    - Tomar decisões sobre quais as respostas aos riscos
    - Implantar respostas aos riscos em nome da administração
    - Responsabilizar- se pelo gerenciamento de riscos (IIA, 2009, p. 4)

2.5 Conformidade

Conformidade é uma tradução do termo "compliance", que em inglês vem do verbo em inglês "to comply", que significa "cumprir, executar, satisfazer, realizar o que foi imposto", ou seja, compliance é o dever de cumprir, estar em conformidade e fazer cumprir regulamentos internos e externos impostos às atividades da instituição. A palavra em português não expressa exatamente o sentido do termo em inglês. Podemos

dizer, então, que “estar em compliance” é estar em conformidade com leis e regulamentos internos e externos (ABBI, 2009).

Compliance não deve ser confundido com auditoria interna. Atividades de compliance são rotineiras e permanentes, monitorando-as para assegurar, de maneira corporativa e tempestiva, que as diversas unidades da instituição estejam respeitando as regras aplicáveis a cada negócio, ou seja, cumprindo as normas e processos internos para prevenção e controle dos riscos envolvidos em cada atividade. Compliance faz parte da estrutura de controles, enquanto a auditoria avalia essa estrutura. A área de Compliance, como as demais, deve ser objeto de avaliação da auditoria interna (ABBI,2009).

A conformidade (compliance), portanto, deve ser vista como um controle, justamente para mitigar os riscos relacionados à conformidade. Do ponto de vista da gestão de riscos, devemos falar em riscos de não conformidade.

Conformidade, em sentido amplo, diz respeito ao cumprimento de leis e regulamentos que estabelecem padrões mínimos de comportamento. As instituições também devem demostrar comprometimento com padrões de boa governança, melhores práticas, comportamento ético e expectativa das partes interessadas.

Do ponto de vista de riscos, mesmo que a instituição cumpra as leis e regulamento, as ações que trazem impactos negativos para as partes interessadas (acionistas, clientes, empregados etc.) podem gerar riscos de reputação e imagem com graves consequências.

3 Gestão de Riscos Corporativos

Até a década de 1970, a gestão de riscos, na maioria das organizações, estava relacionada à aquisição de uma apólice de seguros e aos chamados riscos negativos, com muito pouco foco em riscos positivos.

Na área pública, a gestão de riscos, em geral, estava restrita à garantia da conformidade. Em qualquer um dos casos, a gestão de riscos era uma atividade particionada em diversos elementos da organização gerenciados seus de forma isolada e com critérios compartimentados.

A Gestão de Riscos Corporativos (ERM) é uma proposta de gerenciamento de riscos de forma integrada, demandando o emprego de modelos convergentes, o que não é muito simples. Os modelos de gestão, em geral, refletem suas áreas de origem: estratégicos, conformidade, seguros, financeira, ambiental, desastres, entre outras.

Gestão de riscos pode ser sintetizada como uma prática de identificar e entender os riscos, sistematicamente, e os controles que são definidos para tratá-los. Em última análise, a gestão de risco é um processo de decisão em que, em um determinado contexto, para uma estratégia específica, processo ou projeto, identifica quais riscos são aceitáveis e quais necessitam de tratamento.

Riscos estão relacionados a valor. Toda decisão aumenta, preserva ou erode valor (COSO, 2012). A correlação entre riscos e valor leva a uma mudança de abordagem em relação ao conceito de evitar riscos. O propósito da gestão de riscos é gerenciar a exposição aos riscos de forma que a organização se exponha apenas o necessário para efetivamente atingir seus objetivos.

O processo de gestão de riscos não é uma ferramenta para que os gestores tenham aversão aos riscos. De fato, a gestão de riscos tem como propósito prover confiança para que os gestores possam aceitar riscos, em níveis pré-definidos e alavancar oportunidades. Uma cultura de aversão aos riscos cria uma gestão inflexível e constrói barreiras para o atingimento dos objetivos. Por outro lado, a aceitação de riscos desproporcionais à sua capacidade de gestão pode ter impactos significativos na organização.

A norma NBR ISO 31000 define risco como o efeito da incerteza sobre os objetivos. A mesma norma segue definindo que um efeito é um desvio em relação ao esperado, podendo ser positivo ou negativo, e que a incerteza é o estado, mesmo que

parcial, da deficiência das informações relacionada a um evento, sua compressão, seu conhecimento, sua consequência ou sua probabilidade.

A definição utilizada pelo NBR ISO 31000 estabelece alguns paradigmas na gestão de riscos. A definição estabelece que os riscos podem ser negativos ou positivos em função de um desvio em relação ao resultado esperado, e que este desvio pode ser em relação à sua ocorrência ou às suas consequências.

Riscos positivos ocorrem quando uma organização realiza ações como: investimentos, altera processos, produtos, dentre outras, com o objetivo de obter um retorno positivo. Os riscos positivos ou de oportunidades são assumidos de forma deliberada para atingir objetivos específicos da organização.

Riscos positivos possuem baixa incerteza quanto à sua ocorrência, tendo em vista que se referem a uma decisão, contudo, sempre existe incerteza quanto ao resultado da decisão. São os riscos mais importantes para o sucesso de longo prazo das organizações. São riscos relacionados a investimentos, fusões, lançamento de novos produtos, inovação, dentre outros.

Riscos negativos por outro lado são intrínsecos ao negócio e referem-se às perdas causadas pela incerteza.

A incerteza tem basicamente dois componentes: (1) incerteza quanto à ocorrência de um evento e (2) a incerteza quanto ao resultado. Evento neste caso pode ser definido como “ocorrência (ou conjunto de ocorrências) ou mudança em um conjunto específico de circunstancias” (ISO 31000, 2009, p.).

Em um dos extremos, estão os riscos que possuem baixa incerteza quanto à sua ocorrência e estão relacionados aos resultados esperados dos processos e projetos executados pelas organizações. Os projetos e os processos são atividades de rotina, em que existe baixa incerteza sobre sua ocorrência – o processo será executado, contudo, sempre existe uma incerteza quanto ao seu resultado. O resultado, neste caso deverá ser confrontado com um valor de referência ou padrão de referência São riscos relacionados à conformidade de processo, qualidade de produtos e resultados de projetos.

No outro extremo estão os riscos em que existe incerteza quanto à sua ocorrência, contudo os resultados podem ser estimados com alguma precisão. Em geral são riscos pontuais, cuja ocorrência, geram apenas perdas para as organizações. Estão nesse grupo os riscos de incêndio, alagamento, acidentes, roubos, etc.

A nomenclatura de classificação dos grupos de riscos tem causado alguma confusão, principalmente pela dificuldade na tradução de alguns termos do inglês para o português. Em algumas publicações, em Inglês, os riscos positivos são chamados de *opportunity risks* (riscos de oportunidade), riscos com incerteza quanto ao resultado são clamados de *control risks* (riscos de controle) e os riscos com incerteza quanto à ocorrência são chamados de *hazard risks*. O termo *“hazard”* tem sido traduzido como perigo, mas não expressa o sentido exato da palavra.

O termo *hazard* é utilizado para identificar a fonte de um risco negativo. Na norma AS/NZS 4360:2004, que foi a fonte da NBR ISO 3100:2009, aparece a definição de *hazard* como *“a source of potential harm”* (fonte de um potencial mal, dano ou prejuízo) (ref.). O *hazard* é o agente que causa o risco, ou a causa do risco. A lógica do raciocínio é a sequência do conjunto – *hazard* + evento + impacto.

A NBR ISO 31000 não utiliza o termo “hazard”, que foi substituído por “risk source” (fonte de risco) na versão em Inglês e definido como “element which alone or in combination has the intrinsic potential to give rise to risk” (ref) (elemento que sozinho ou em combinação tem o potencial intrínseco de originar um risco).

As organizações podem ter atitude e tolerâncias diferentes em relação aos três tipos de riscos.

Em geral as organizações tendem a ter baixa tolerância em relação aos riscos negativos com incerteza quanto à ocorrência, uma vez que geram apenas perdas, e neste caso, as ações apropriadas são eliminá-los. Na prática, como isso não é possível,

as organizações tomam medidas para obter o menor nível de risco possível, desde que seja economicamente viável e em conformidade com a lei e as normas em vigor.

Por outro lado, as organizações, aceitam algum nível de risco negativo com incerteza quanto ao resultado quando implementam mudanças ou executam projetos. Para mitigar o impacto desses riscos, as organizações devem ter recursos reservados para fazer face à ocorrência, identificar e implementar controles para reduzir sua probabilidade.

A gestão de riscos, portanto, tem como propósito permitir que as organizações, sejam públicas ou privadas, atinjam seus objetivos. Com a crescente necessidade de transparência no processo decisório, uma gestão de riscos sistemática fornece os subsídios para um processo de auditoria consistente. A compreensão da exposição aos riscos facilita um planejamento estratégico efetivo, a alocação dos recursos e encoraja uma cultura de gerenciamento proativa em todos os aspectos da organização.

A gestão de riscos deve envolver todos os objetivos organizacionais e considerar todas as incertezas, sejam elas negativas (ameaças) ou positivas (oportunidades). Os objetivos organizacionais cobrem uma ampla gama de atividades e incluem os riscos estratégicos, operacionais, financeiros, transparência, conformidade, projetos, dentre outros.

No caso de organizações públicas, o gerenciamento de riscos é fundamental para o sucesso no cumprimento da missão e na entrega de serviços de qualidade para o cidadão.

O bom gerenciamento de riscos contribui também para aumentar a confiança do cidadão: (1) na capacidade do Governo de entregar os serviços prometidos; (2) no sistema de governança; e (3) na utilização adequada dos recursos públicos.

3.1 Normas de gestão de riscos

Existem diversas normas de gestão de riscos, algumas mais genéricas, como a NBR ISO 31000 e a COSO ERM, e outras mais específicas, como Basileia III e COBIT. Contudo, existe uma grande convergência no que se refere ao processo de gestão de risco que compreende a identificar os riscos, priorizar, tratar, monitorar e revisar.

As três normas mais aplicáveis ao setor público são a NBR ISO 31000, a COSO ERM e O The Orange Book.

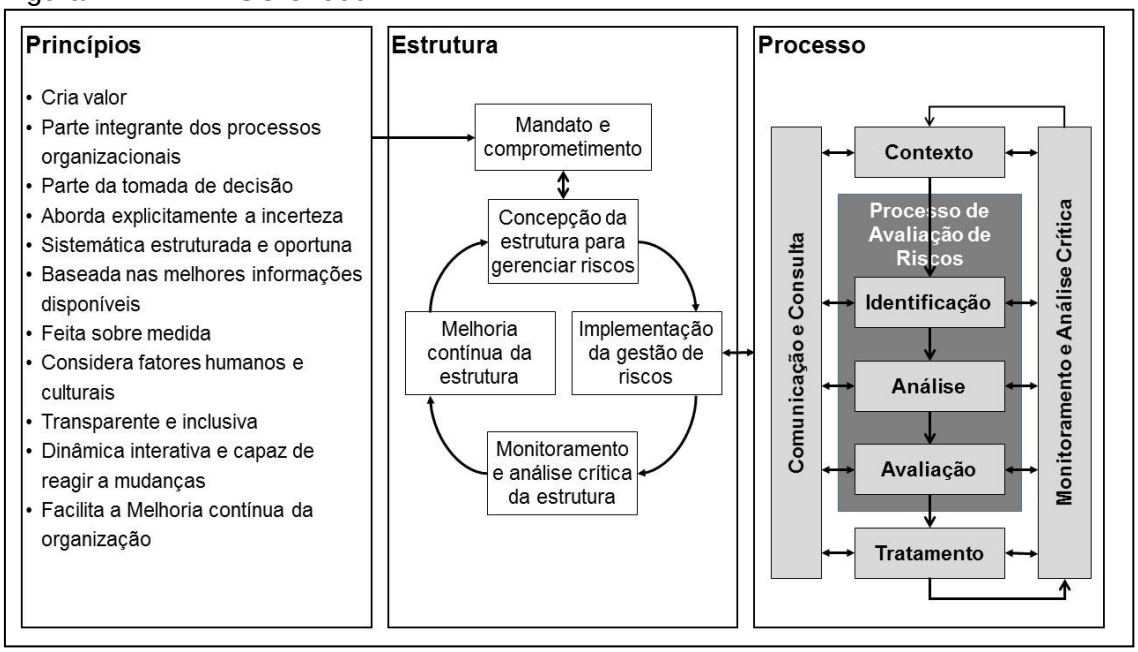
A norma NBR ISO 31000 é derivada da norma AZ/NZS 4360, elaborada pela Austrália em conjunto com a Nova Zelândia, em 1995. O propósito da norma foi especificar os elementos do processo de gerenciamento de riscos que poderiam ser implementados em qualquer tipo de indústria ou setor da economia. A norma não preconiza um modelo de sistema de gestão de riscos. O projeto e a implementação da gestão de riscos seguem as necessidades de cada organização, seus objetivos particulares, seus produtos e serviços, seus processos e práticas especificas empregadas (AS/NZS 4360,1995)

A Norma AS/NZS 4360 sofreu três revisões, sendo a última em 2004. Em 2009, com pequenas alterações, a AS/NZS 4360 foi transformada na ISO 31000.

A NBR ISO 31000 segue a mesma lógica da AS/NZS 4360 e não define um modelo de sistema de gestão de riscos, e sim os elementos do processo de gerenciamento de riscos.

A NBR ISO 31000 é baseada em três componentes básicos: princípios, estrutura e processo (figura 11).

Figura 11 – NBR ISO 31000



Fonte: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009.

A ISO 31000 não é uma norma certificável. Ela é uma norma que descreve uma abordagem genérica para gerenciar qualquer forma de riscos sistematicamente, transparente e com credibilidade, e em qualquer contexto e escopo (ISO 31000).

A norma:

- Estabelece um conjunto genérico de princípios que as organizações precisam satisfazer para gerenciar riscos com efetividade.
- Lista os benefícios da adoção de uma abordagem constante e sistemática de gestão de riscos.
- Estabelece os conceitos que a organização deve adotar no projeto e na estrutura de gestão de riscos.
- Enfatiza a integração do processo de gestão de riscos aos processos organizacionais como forma de criar e melhorar continuamente a estrutura de gestão de riscos.

O modelo COSO ERM é derivado do modelo COSO “Controle Interno - Estrutura Integrada de 1992”,

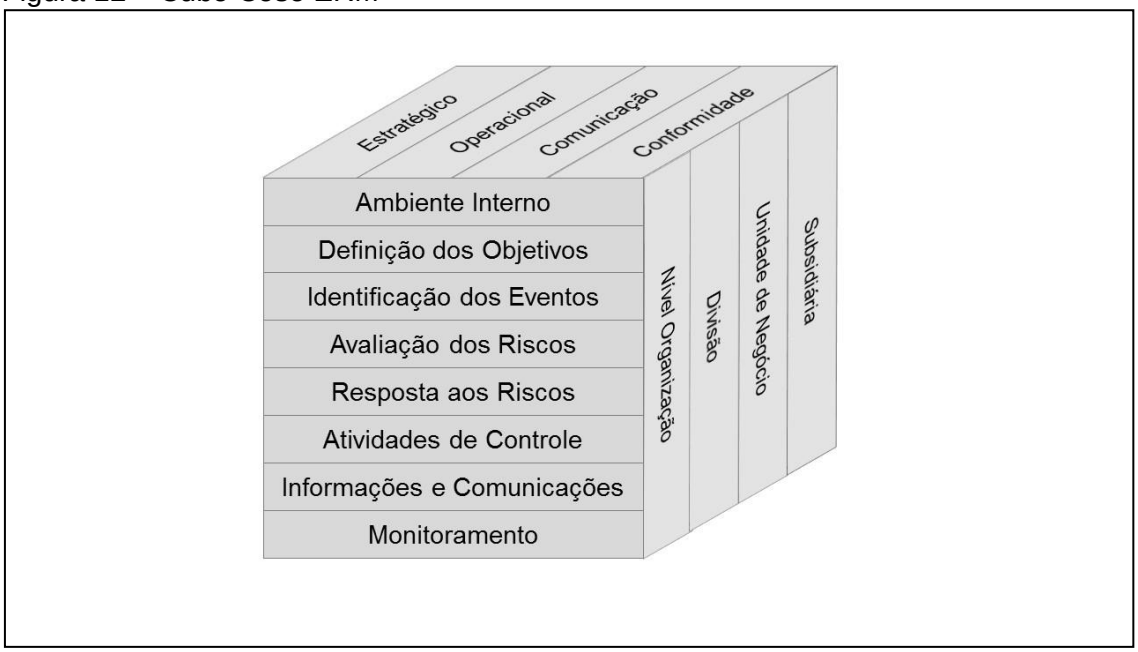
O COSO foi proposto pelo *The Committee of Sponsoring Organizations of the Treadway Commission*, criado em 1985, em uma iniciativa independente, da *National Commission on Fraudulent Financial Reporting*, também conhecida como Treadway Commission. O modelo apresentado em julho de 1992, denominado *Internal Control – Integrated Framework* (Controle Interno – Modelo Integrado), conhecido como COSO I, alterou o conceito tradicional de controles internos, estabelecendo que os controles internos devem fornecer proteção contra riscos. O foco passou de um modelo reativo para um modelo proativo. O modelo COSO foi adotado no setor de governo do Estados Unidos da América (EUA), na sequência de movimentos de reforma do Estado e de reformas administrativas, que tinham como objetivo a redução do déficit público e a diminuição do crescimento do setor estatal.

O COSO é um modelo de controle interno, no entanto, em 2004, foi editado pela COSO o “Gerenciamento de Riscos Corporativos - Estrutura Integrada”, chamado de COSO ERM, que amplia o escopo do controle interno para a gestão de riscos. Basicamente, o COSO ERM inclui, no processo de gestão de riscos, o processo de controle interno. O processo de gestão de riscos, como um todo, é muito similar ao preconizado pela NBR ISO 31000, conforme poderá ser observado no cubo COSO (Figura 12).

O cubo em sua face superior estabelece as classes de objetivos em relação aos quais devem ser avaliados os riscos. Na face lateral, estão os níveis organizacionais para os quais os riscos devem ser desdobrados. Na face frontal, está o processo de gestão de riscos.

O modelo COSO - ERM está baseado no chamado cubo COSO.

Figura 12 – Cubo Coso ERM



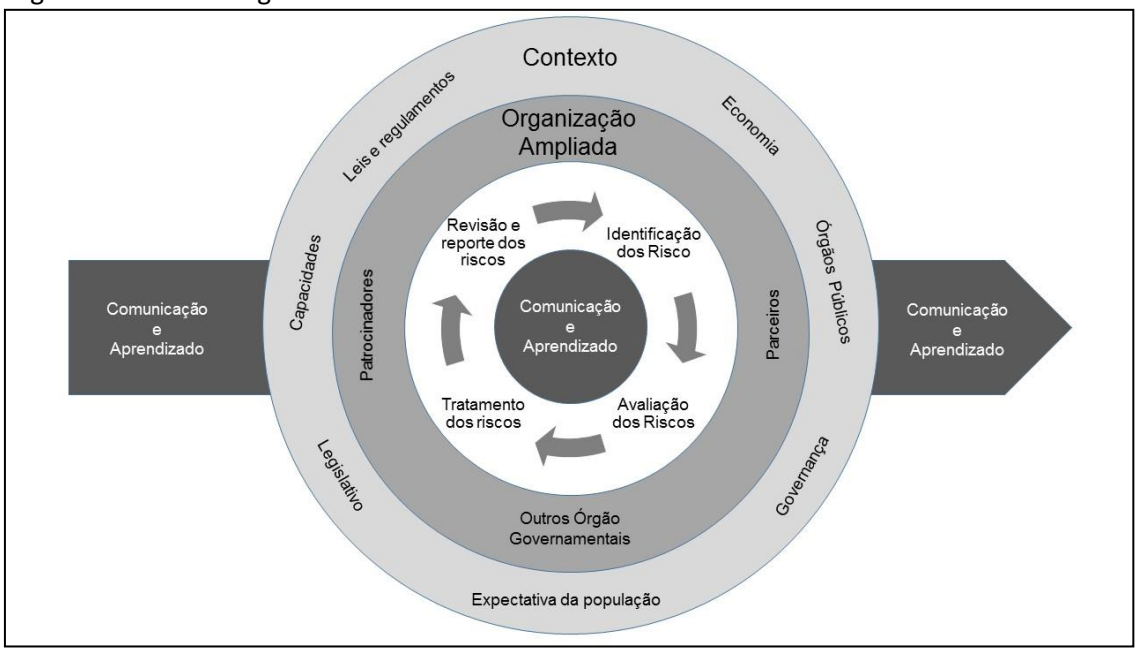
Fonte: THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, 2004.

O modelo COSO ganhou grande aceitação no mercado de capitais, após a edição da Lei Sarbanes-Oxley pelos Estados Unidos da América, conhecida como SOX, que é uma exigência legal para todas as empresas americanas e estrangeiras que tenham títulos e ações negociados em bolsas americanas e preconiza a utilização do modelo COSO de controle interno.

O chamado The Orange Book Gerenciamento de Riscos - princípios e conceitos foi editado pelo HM Treasury do Governo Britânico. O Orange Book é uma publicação básica para introduzir os conceitos de gestão de riscos como recurso para o desenvolvimento e implementação da gestão de riscos em organizações governamentais (UNITED KINGDOM, 2004).

O processo de gestão de riscos muito similar ao da NBR ISO 31000. O Orange Book, contudo, enfatiza o que se chama de organização estendida, ampliando o escopo da gestão de riscos para incluir os parceiros estratégicos. Outro aspecto importante desta norma é a ênfase em aprendizado (Figura 13).

Figura 13 – The Orange Book



Fonte: Orange Book

4 Princípios da Gestão de Riscos Corporativos

Um dos aspectos principais da gestão de riscos e que aparece em todas as normas e modelos são os princípios.

Princípios da gestão de riscos descreve o que é a gestão e quais suas entregas. De forma geral, podemos dizer que a gestão de riscos de ser:

- Proporcional ao nível de riscos enfrentado pela organização;
- Alinhado às atividades da organização;
- Integrado aos demais processos da organização;
- Compressivo, sistemático e estruturado;
- Dinâmico, interativo e que responda às mudanças.

Os princípios devem ter por base a noção de que riscos são itens que possam ser identificados e controlados.

A gestão de riscos deve entregar:

- Conformidade com as leis e regulamento;
- Garantia do gerenciamento dos riscos mais significativos;
- Garantia de que as decisões levem em contas os riscos;
- Efetividade, eficácia e eficiência das estratégias, operações e projetos.

Os princípios estabelecidos pela NBR ISO 31000 são:

- Criar e proteger valor – auxilia a organização a atingir seus objetivos (ver os principais benefícios da gestão de riscos)
- Ser parte integrante de todos os processos organizacionais – deve incluir o planejamento, projetos e mudanças organizacionais e de gestão.
- Ser parte da Tomada de Decisão – como o risco é parte integrante de toda decisão, um gerenciamento de riscos efetivo proporciona escolhas com base em informações, permite priorização de ações e seleção entre opções alternativas.

- Abordar explicitamente a incerteza – a incerteza é inerente a todas as atividades da organização.
- Ser sistemática, estruturada e oportuna – para facilitar a obtenção de resultados repetíveis e confiáveis.
- Basear-se nas melhores informações disponíveis – com o emprego de indicadores de desempenho de objetivos, cujos dados possam ser auditados de forma independente. Os dados podem incluir dados históricos, experiências, resposta, observações, previsões e julgamento de especialistas. Toda hipótese (assumptions) deve ser colocada de forma clara para obtenção dos indicadores.
- Ser feita sob medida – deve considerar os objetivos, capacidades, ambiente em que a organização opera e os riscos que enfrenta.
- Considerar fatores humanos e culturais – deve-se reconhecer as percepções dos stakeholders internos e externos, incluindo as capacidades e atitudes dos diretores com relação ao gerenciamento de riscos.
- Ser transparente e inclusiva - em relação à identificação e análise dos riscos, como as decisões são tomadas e como os riscos são tratados. O alto escalão deve ser regularmente consultado para garantir que incluam informações nos critérios usados para avaliar a efetividade do processo de gestão de riscos.
- Ser dinâmica, interativa e capaz de reagir a mudanças – como os ambientes internos e externos são mutáveis, é necessário monitorar esses ambientes para determinar se os riscos existentes ainda são relevantes e identificar novos riscos. A estrutura de gerenciamento de riscos da organização e o processo são responsáveis pelas mudanças.
- Facilitar a melhoria contínua da organização – com revisões regulares e melhorias da estrutura e dos processos de gestão de riscos. (ABNT ISO 31000, p.7)

5 Estrutura de Gestão de Riscos

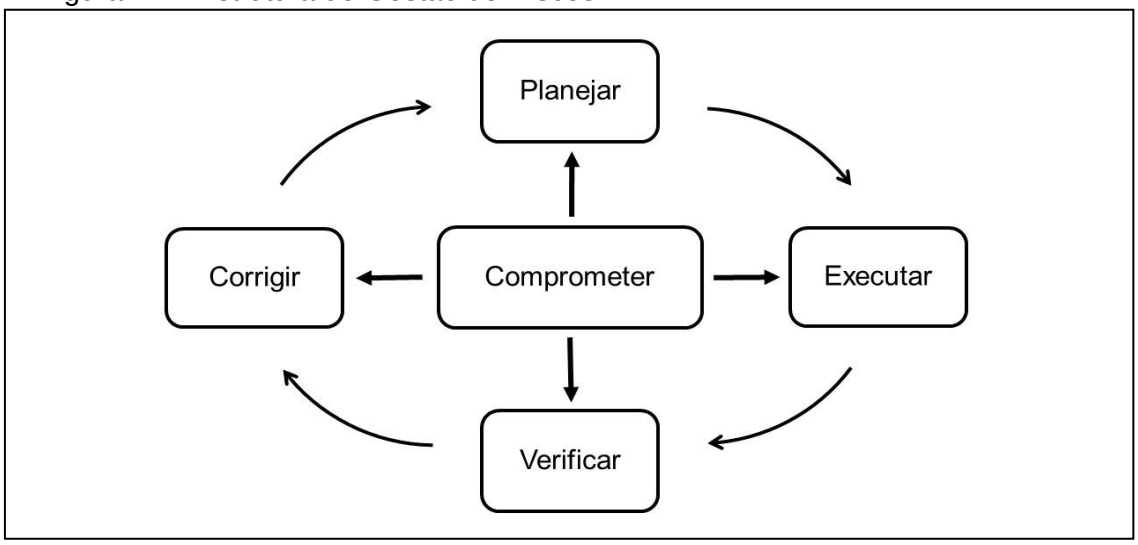
O segundo aspecto significativo é a gestão de riscos como um processo de suporte à uma estrutura dedicada e integrada às demais estruturas e processo da organização.

A NBR ISO 31000 define a estrutura de gestão de riscos como um conjunto de componentes que fornece os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria continua da gestão de riscos em toda a organização. Os fundamentos incluem a política, os objetivos, os mandatos e o comprometimento para o gerenciamento de riscos. Os arranjos organizacionais incluem os planos, relacionamentos, responsabilidades, recursos, processos e atividades.

A estrutura segue um modelo PDCA (Figura 14), com um importante acréscimo que é o chamado mandato e comprometimento. Este PDCA refere-se à estrutura de gestão de riscos (Figura 15).

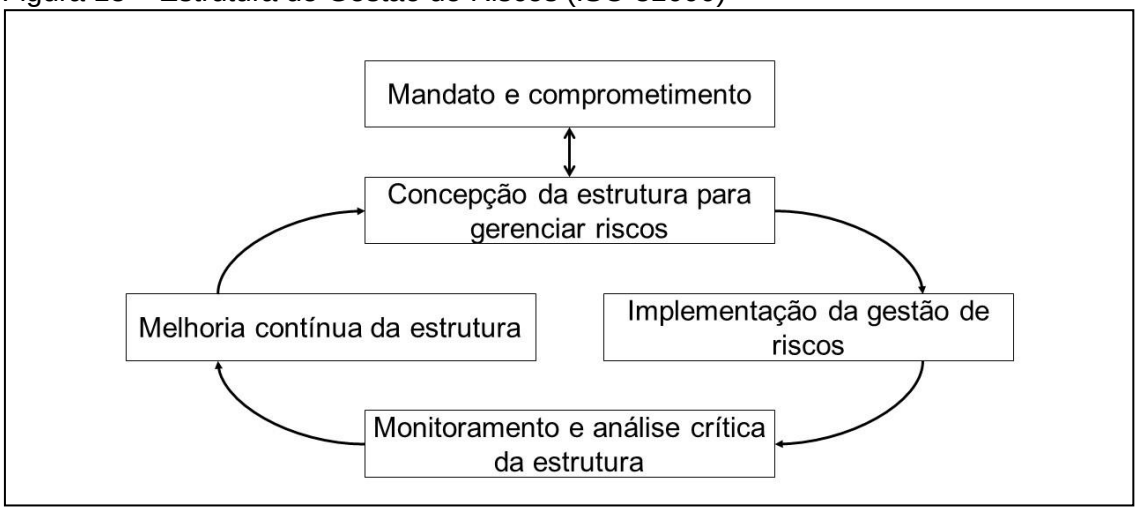
O tópico de implementação da gestão de riscos é outro PDCA, que está explicitado no processo de gestão de riscos.

Figura 14 – Estrutura de Gestão de Riscos



Fonte: Elaborado pelo autor

Figura 15 – Estrutura de Gestão de Riscos (ISO 31000)



Fonte: ISO 31000

5.1 Mandato e comprometimento

A gestão de riscos, para ser efetiva, requer o comprometimento da alta administração e um suporte de todos os níveis gerenciais. A alta administração é responsável pelo estabelecimento do mandato. Ela deve estar comprometida com a estrutura de gestão de riscos e ser a patrocinadora da implementação do processo de gestão e da melhoria contínua.

5.2 Estrutura de governança da gestão de riscos

A gestão de risco, para ser efetiva, deve ter uma estrutura de governança e gestão adequadas. A governança de gestão de riscos deve ser parte integrante da estrutura de gestão organizacional, definindo as responsabilidades e o fluxo de informações no que se refere a riscos e ser dirigida pela mais alta administração.

A estrutura da gestão de riscos é um “conjunto de componentes que fornece os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização” (ABNT ISO GUIA 73:2009)

A implantação de uma estrutura formal de gestão de riscos é a forma mais efetiva de garantir que o processo decisório será suportado por um gerenciamento de riscos consistente e efetivo. A implementação, contudo, deve ser um processo evolutivo e interativo, refletindo a maturidade na gestão de riscos e a complexidade dos riscos enfrentados pela organização.

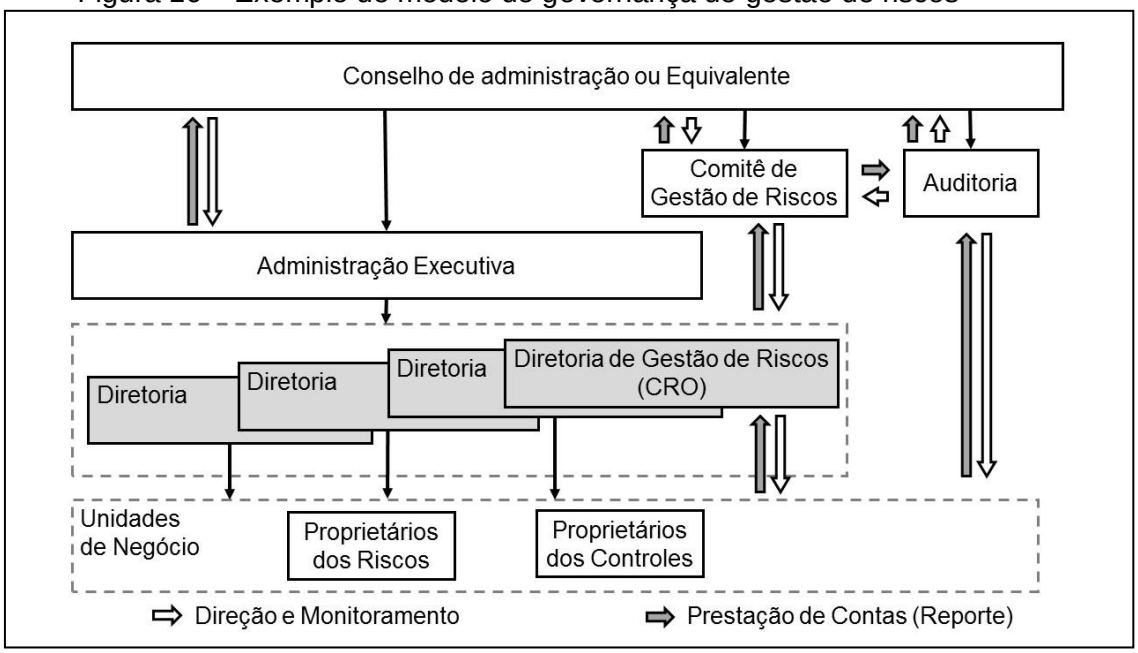
A estrutura de gestão de riscos deve ter um desenho que atenda os objetivos de cada organização e de forma consistente:

- Fornecer aos dirigentes um conhecimento claro dos riscos enfrentados pela organização e o processo de gerenciamento.
- Identificar responsabilidades.
- Aumentar a confiança das partes interessadas na capacidade da organização de alcançar seus objetivos.

A gestão de riscos deve ser orientada por um comitê de riscos, que opera dentro do conselho. Para os modelos em que existem conselheiros internos e externos é recomendado que o presidente do comitê de gestão de riscos seja um membro externo (Figura 16).

Na área pública a gestão de riscos deve ser uma das instâncias de apoio ao processo de governança.

Figura 16 – Exemplo de modelo de governança de gestão de riscos



Fonte:Elaborado pelo Autor

Dentro da estrutura de gestão riscos, as principais normas e modelos identificam a necessidade de um setor (unidade funcional) responsável pela gestão de riscos. O setor deve ter um responsável designado para a tarefa, o Diretor de Riscos ou *Chief Risk Officer* (CRO), em Inglês, e respectiva equipe.

O diretor de riscos é também o primeiro especialista em riscos, designado em inglês por *Risk Champion*. Ele deve ser o responsável pelo projeto (design) da estrutura de gestão de riscos e pelas a atividades do dia a dia associadas com a coordenação, manutenção e integração da estrutura na organização.

O setor de gestão de riscos organizacional deve:

- Coordenar a elaboração e o desenvolvimento da política e da estratégia de gestão de riscos.
- Facilitar o fluxo de informações e a sensibilização sobre riscos na organização.

- Atuar no aconselhamento sobre riscos nos níveis estratégico e operacional.
- Coordenar as diversas atividades funcionais relativas aos riscos, incluindo o assessoramento e o provimento de ferramentas para o pessoal envolvido na gestão de riscos em todos os níveis da organização.
- Conceber e revisar o processo de gestão de riscos
- Elaborara os relatórios de gestão de riscos, incluindo o Registro de Riscos.
- Coordenar os planos de respostas aos riscos, incluindo os planos de contingência.

É importante salientar que o setor de gestão de riscos, bem como o seu diretor, não é o proprietário dos riscos nem dos controles de mitigação. A função de diretor de riscos deve, ainda, ser distinta da função de auditor.

O proprietário dos riscos ou dono dos riscos é o responsável por prestar conta pelos riscos, sendo que esta prestação de contas deve ser parte da descrição de suas funções (Figura 16).

Dentre as atividades de aconselhamento e assessoramento prestadas pela direção de riscos, destacam-se:

- A orientação das gerências operacionais no desenvolvimento e aplicação de métodos e no estabelecimento de processos para identificação, avaliação, tratamento e monitoramento de riscos.
- O assessoramento da Diretoria no desdobramento do apetite aos riscos.
- O assessoramento ao do Conselho de Administração e à Diretoria sobre novos riscos

Os gerentes, em todos os níveis, são responsáveis por gerenciar os riscos enfrentados por seus setores e garantir que seu pessoal execute suas funções conforme o apetite de riscos da organização. Dentre suas responsabilidades se destacam:

- Estabelecer um ambiente que promova uma atenção aos controles internos e responsabilidade por riscos individuais.
- Identificar as incertezas que vão afetar o atingimento dos objetivos da organização.
- Estabelecer políticas, normas de operação e outros itens pertinentes para identificar riscos e gerenciá-los dentro dos níveis aceitáveis e toleráveis.
- Monitorar a efetividade dos controles.

Os proprietários dos riscos são pessoas que têm a responsabilidade por projetar, implementar e monitorar o tratamento de um risco particular. O proprietário do risco é responsável por prestar conta sobre os riscos, garantindo que o risco está sendo gerenciado de acordo com a habilidade da organização em aceitar ou tolerar o risco.

O proprietário do risco deve estar bem informado sobre o processo e os critérios pelos quais o risco foi avaliado e tratado, contudo, não necessariamente é a pessoa que implementa o controle e toma as ações para endereçar e tratar o risco identificado.

O proprietário do controle é a pessoa que implementa o tratamento e executa a ação definida para tratar o risco. O proprietário do controle pode estar em um setor diferente do proprietário do risco.

Outras pessoas, dentro e fora da organização, também são importantes para a gestão de riscos. Pessoal terceirizado e fornecedores devem estar cientes de suas responsabilidades no gerenciamento de riscos em suas atividades do dia a dia. Isso inclui a condução de suas atividades de acordo com todas as políticas e procedimentos, participar da identificação dos riscos e reportar os riscos aos proprietários de acordo com os protocolos de relatórios. O pessoal orgânico, terceirizado e fornecedores devem, também, reportar controles ineficientes e não efetivos.

5.3 Política de gestão de riscos

Outro aspecto central na gestão de riscos é a definição de uma política de gestão de riscos que estabelece aquilo que deverá ser feito (COSO).

O estabelecimento da política de gestão de riscos é responsabilidade da alta administração. Deve ser um documento sintético, em que a organização declara as intenções e diretrizes gerais relacionadas à gestão de riscos.

Uma política de gestão de riscos deve definir a atitude, o apetite e as responsabilidades relativas à gestão de riscos em toda a organização. Além disso, a declaração de intenções deve também refletir todos os requisitos legais aplicáveis, como, por exemplo, o nível de saúde e segurança. Ligado ao processo de gestão de riscos está um conjunto de ferramentas e técnicas que deve ser utilizado nas várias etapas do processo de negócio.

A política de gestão de riscos é uma declaração da intenção e direção do que se refere a riscos e deve ser endossada pela autoridade máxima.

A política deve definir claramente os objetivos da organização em sintonia com o gerenciamento de riscos. A política é central para desenvolver um entendimento comum dos riscos e seu gerenciamento na organização. Ela proporciona a oportunidade de articular a visão de gerenciamento de riscos e descrever os benefícios que proporciona.

Em geral uma política deve incluir:

- A visão e base racional para o gerenciamento de riscos – porque é importante gerenciar riscos.
- Como a política de gerenciamento de riscos se integra como as demais políticas e objetivos da organização.
- Quem é o responsável por prestar conta e gerenciar os riscos.
- O compromisso em disponibilizar os recursos necessários para auxiliar os responsáveis pela gestão de riscos.
- Como será mensurado e reportado o desempenho no gerenciamento de riscos.
- O comprometimento com revisões regulares e melhorias na política de gerenciamento de riscos e sua estrutura em resposta aos eventos ou mudanças nas circunstâncias.
- Um glossário de termos.
- Quem deve ser contatado para questões sobre a própria política.

A Instrução normativa conjunta CGU/MP nº 001, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal, estabelece que a política de gestão de riscos deve especificar ao menos:

- Princípios e objetivos organizacionais.
- Diretrizes sobre:
    - Como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização.
    - Como e com qual periodicidade serão identificados, avaliados, tratados e monitorados os riscos.
    - Como será medido o desempenho da gestão de riscos.
    - Como serão integradas as instâncias do órgão ou entidade responsáveis pela gestão de riscos.
    - A utilização de metodologia e ferramentas para o apoio à gestão de riscos.
    - O desenvolvimento contínuo dos agentes públicos em gestão de riscos;
    - Competências e responsabilidades para a efetivação da gestão de riscos no âmbito do órgão ou entidade.

Dois aspectos importantes da política de gestão de riscos são o suporte efetivo da alta administração em sua implementação e suporte e a mensuração de sua efetividade.

A alta administração deve atuar de forma visível no suporte à gestão de riscos para garantir o comprometimento da gerencia. Esta tem sido apontada como a principal razão pelo não comprometimento das áreas gerenciais com a gestão de riscos. O suporte da alta administração é peça fundamental no estabelecimento de uma cultura positiva de gestão de riscos na organização.

O outro aspecto importante para garantir o comprometimento com a política de gestão de riscos é mensurar o impacto positivo da gestão de risco na organização. A política deve definir os indicadores que medem a contribuição da estrutura de gestão de riscos para os objetivos da organização. Preferencialmente, devem ser utilizados indicadores já existentes na organização, como por exemplo: a quantidade de fraudes detectadas e a quantidade de recomendações da auditoria, dentre outros.

O estabelecimento, manutenção e comunicação de uma política de gestão de riscos demostra o compromisso da organização com a gestão de riscos. Contudo o comprometimento dos gestores e administradores com o gerenciamento de riscos somente será desenvolvido com a criação e sustentação de uma cultura de gerenciamento de riscos na organização.

5.4 Cultura de Gestão de Riscos

A cultura organizacional é um importante componente da gestão de riscos, que surge de comportamentos repetidos dos membros de uma organização, sendo moldados pelos valores, crenças e atitudes dos indivíduos. Está sujeita a ciclos virtuosos ou viciosos. A cultura é mais do que uma declaração de valores, ela está relacionada à transformação dos valores em ações concretas. A cultura varia substancialmente de organização para organização, como por exemplo, entre um restaurante e um órgão público. De forma similar, pode a cultura varia entre diferentes órgãos públicos.

A cultura direciona o desempenho organizacional e engloba as regras de condutas escritas e não escritas. No nível mais básico, a cultura organizacional define os pressupostos que as pessoas utilizam em seu dia a dia. Ela é uma força poderosa que persiste apesar das reorganizações e da saída de pessoas chaves.

Muitos fatores influenciam a cultura organizacional, incluindo as atitudes da alta administração, o código de conduta, políticas de ética e de recursos humanos. Cabe ao conselho da administração, a alta administração e os comitês de auditoria e riscos fornecerem o modelo e direcionar o comportamento correto da cultura relacionada a riscos.

A cultura de riscos está relacionada aos “valores, crenças, conhecimento e entendimento sobre riscos compartilhados por um grupo de pessoas com um propósito comum, em particular os funcionários de uma organização ou equipe ou grupos dentro de uma organização. Este conceito é aplicado para organizações públicas, privadas e sem fins lucrativos, em todos os lugares do mundo” (The Institute of Risk, 2012 Management Risk culture Under the Microscope Guidance for Boards)

Toda organização enfrenta riscos para atingir seus objetivos. A cultura de gestão de riscos organizacionais pode ajudar ou atrapalhar a capacidade de tomar decisões de assumir riscos estratégicos, a fim de obter os resultados desejados.

A cultura de gestão de riscos é o caminho usual para a implementação da gestão de riscos na organização. Ela direciona como as pessoas reconhecem e responde ao risco. Se a organização não tem uma cultura que enfatiza em todos os níveis a importância de gerenciar riscos como parte das atividades diárias de cada pessoa, a política de gerenciamento de riscos não será efetivamente implementada.

Atitudes positivas de uma cultura de gestão de riscos podem ser sintetizadas em:

- Desenvolver um entendimento comum de propósitos, valores e princípios éticos que alinhem os interesses individuais dos funcionários com a estratégia de riscos da organização, apetite, tolerância e abordagem.
- Aplicar a gestão de riscos a todas as atividades, desde o planejamento estratégico até as operações do dia a dia, em todas as partes da organização.

- Implementar um processo de melhoria contínua e aprendizagem para tornar mais efetiva a habilidade coletiva da organização em gerenciar riscos.
- Atuar com tempestividade, transparência e honestidade na comunicação sobre riscos, usando um vocabulário comum que promova um conhecimento compartilhado.

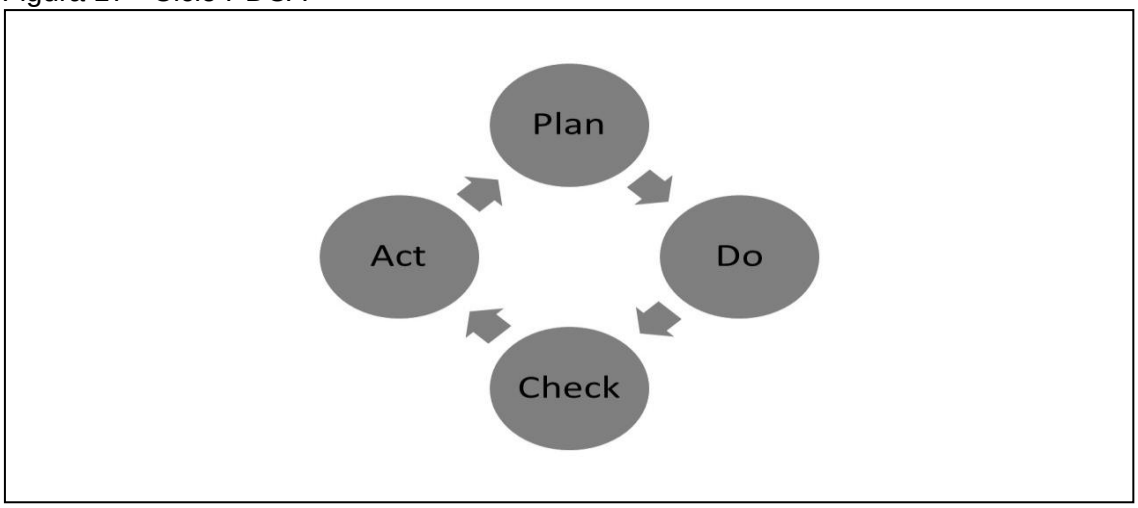
6 Gestão Estratégica e Riscos

A gestão estratégica refere-se como a organização é gerida a longo prazo e seu impacto sobre o futuro da organização.

O termo gestão pode ser definido como o processo de coordenação do trabalho desempenhado por pessoas, de forma que as tarefas sejam executadas de forma eficiente e efetiva.

A gestão estratégica pode ser vista como um ciclo de melhora contínua (Figura 17), semelhante ao ciclo de melhoria de produtos e processos industriais estruturado por Deming no ciclo PDCA: Planejar (Plan), Executar (Do), Monitoramento (Check), Atuar (Act). O ciclo PDCA é uma série sistemática de passos que agrega valor de aprendizado e conhecimento para a melhoria contínua de um produto ou processo. Esta abordagem sistêmica foi primeiramente proposta por Walter Shewhart em seu livro Statistical Method from the Viewpoint of Quality Control, de 1939, em que modelava o processo produtivo como um sistema. Contudo, foi Deming que expandiu a ideia para outras áreas como forma de aprendizado e melhoria.

Figura 17 - Ciclo PDCA



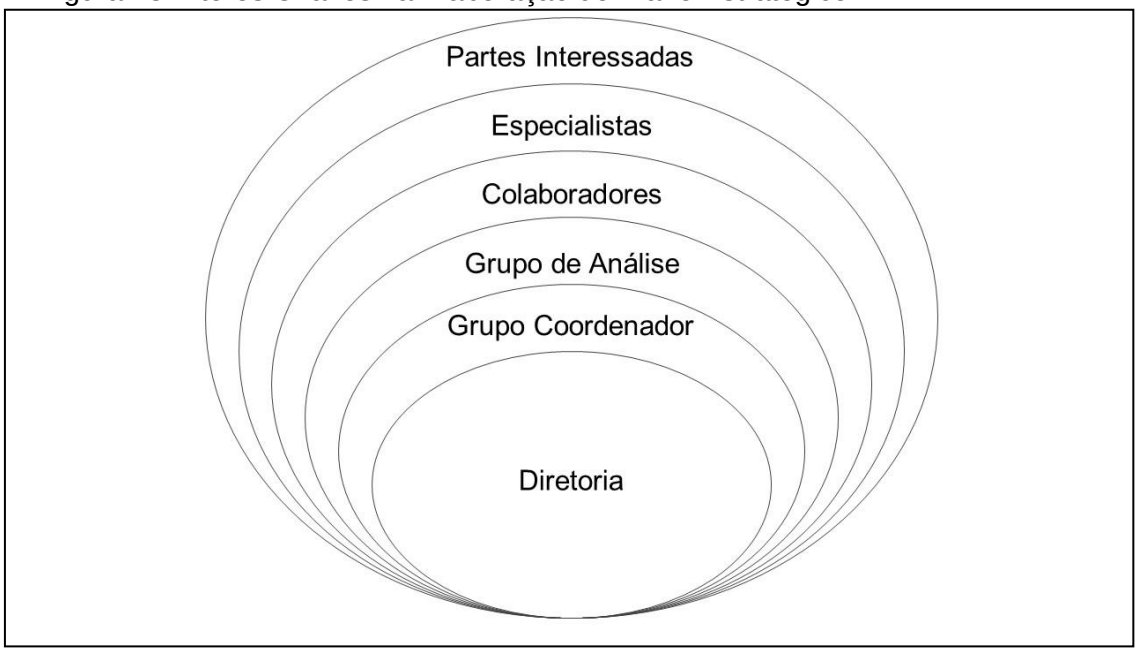
Fonte: Adaptado de Falconi, 2009.

O ciclo PDCA deve ser visto como um ciclo padrão para a gestão estratégica, contudo, seu emprego requer alguns cuidados. A efetividade de uma gestão estratégica está em sua execução, contudo, a origem de problemas de execução, em geral, está em um planejamento superficial.

Uma gestão estratégica efetiva e executável deve começar com um planejamento estratégico alicerçado em um bom diagnóstico da situação presente e em uma análise de futuros alternativos.

Outro aspecto importante é a legitimidade do planejamento. A maioria dos problemas de execução ocorre quando o planejamento é formulado sem a participação dos diversos atores chaves (internos e externos) que impactam na execução da estratégia. A figura 18 mostra os atores que devem participar da elaboração do plano estratégico.

Figura 18. Atores Chaves na Elaboração do Plano Estratégico



Fonte: Elaborado pelo Autor

6.1 Contexto

O planejamento estratégico deve considerar todas as especificidades da instituição para a qual se destina. Mesmo instituições congêneres, como órgãos estaduais com as mesmas funções, apresentam diferenças significativas em suas atuações.

6.2 Análise

O diagnóstico do presente e a análise de cenários futuros são a primeira fase do processo de planejamento (análise) e que será o alicerce para a formulação da estratégia (síntese).

No diagnóstico estratégico, o objeto sob análise deve ser subdividido em seus componentes, com o propósito de gerar o conhecimento, que será posteriormente sintetizado em uma estrutura própria para a execução.

O primeiro passo é a definição de uma estrutura adequada ao processo de diagnóstico (análise). Uma boa estrutura para o diagnóstico é aquela que identifica corretamente os pontos fortes e fracos, oportunidades e ameaças, bem como suas causas e suas consequências. A estrutura de análise não deve ser confundida com uma matriz DOFA. A DOFA não é uma ferramenta de diagnóstico, e sim uma ferramenta de análise do diagnóstico. Por exemplo, antes de lançar uma fraqueza na matriz é necessário identificá-la em um processo diagnóstico.

Uma boa estrutura para o diagnóstico, não necessariamente é uma boa estrutura para a formulação da estratégia tendo em vista que dificilmente uma organização terá como missão corrigir pontos fracos. Organizações, sejam públicas ou privadas, existem para cumprir uma missão e entregar valor às suas partes interessadas (stakeholder).

Uma boa estrutura de formulação da estratégia, portanto, é aquela que mostra como o valor é construído pela organização e como é entregue às suas partes interessadas.

Seguindo a base do método cartesiano, a estrutura diagnóstica parte do geral para o específico, identificando as causas e as consequências dos pontos fracos (problemas) e dos pontos fortes (oportunidades). A organização deve ser analisada tanto do lado de dentro quanto do lado de fora. No lado de dentro, devem ser analisados pelo menos

seus recursos e seus processos ao passo que do lado de fora devem ser analisados os atores e as variáveis externas.

O diagnóstico estratégico segue um padrão de construção de conhecimento organizacional: levantamento de fatos, filtragem dos fatos para obtenção de dados, estruturação de dados para gerar informações e aplicação de critérios para gerar conhecimento.

Para que o diagnóstico seja consistente, permita rastreabilidade e gestão do conhecimento e para que todos os colaboradores tenham a mesma percepção é fundamental que os dados sejam estruturados de forma unificada. A figura 19 apresenta um exemplo de estrutura adequada ao diagnóstico interno e externo.

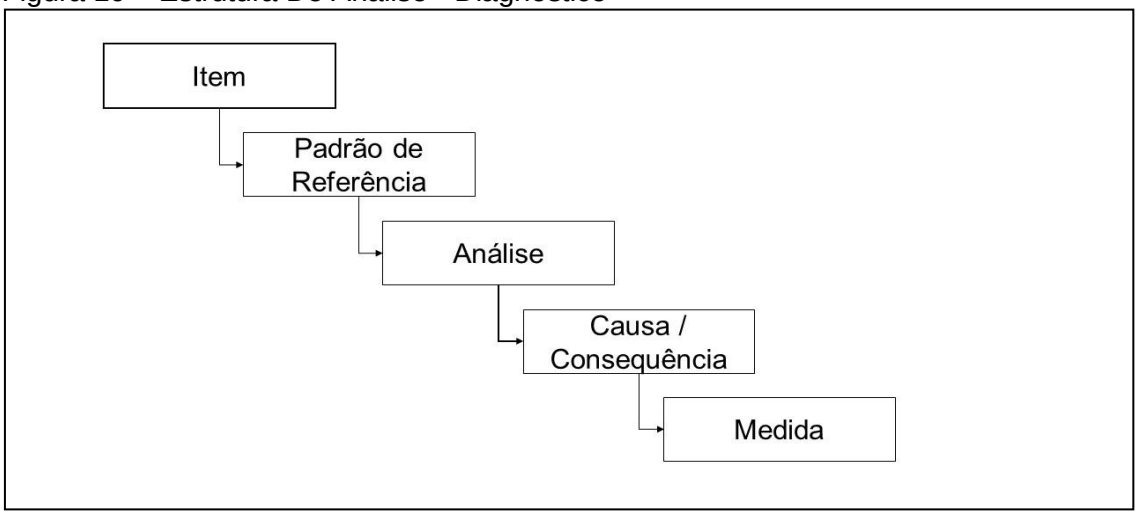
Outro aspecto fundamental do diagnóstico é a rastreabilidade e a gestão do conhecimento gerado, o que somente pode ser obtido com a utilização de um software que consiga estruturar e, principalmente, recuperar os dados segundo filtros específicos.

O diagnóstico estratégico é uma das fases mais importantes do planejamento tendo em vista que está na base da construção do conhecimento organizacional. Um diagnóstico superficial compromete todo o planejamento subsequente.

O diagnóstico estratégico tem por propósito identificar os pontos fortes e pontos fracos do ambiente interno e as oportunidades e ameaças do ambiente externo.

O diagnóstico deve ser participativo. Todos na organização devem contribuir nessa tarefa. Em geral, uma grande parcela do conhecimento organizacional está nas pontas. O processo e a estrutura de análise são padrões para qualquer tipo de diagnóstico: processos, recursos, variáveis externas e atores. (Fig. 19)

Figura 19 – Estrutura De Análise - Diagnóstico



Fonte: Elaborado pelo autor

O diagnóstico estratégico é a matéria prima da gestão estratégica, quer seja para o tratamento dos pontos vislumbrados, quer seja para a definição das questões estratégicas que serão avaliadas na análise prospectiva.

O emprego de uma metodologia científica de análise em que, para cada ponto identificado, são esmiuçadas suas causas e consequências e tem o propósito de definir medidas para o tratamento das causas e a mitigação ou aproveitamento das consequências.

Esta abordagem evita a priorização de problemas e facilita a priorização de soluções, o que é um dos fatores chaves para garantir a efetividade do plano e sua execução.

O diagnóstico é uma fase extremamente importante, é a base sobre a qual será fundamentado todo o plano estratégico, dando-lhe consistência, legitimidade e sustentabilidade. Por isso, deve ser uma construção coletiva de conhecimento

organizacional. Todos na instituição devem ser instados a participar do diagnóstico. A construção do conhecimento organizacional é do tipo “de baixo para cima”, em que a participação das pontas, principalmente dos colaboradores que fazem a ligação da organização do exterior, é de fundamental importância.

Outro aspecto que não pode faltar em um planejamento estratégico é uma visão de futuro de médio e/ou longo prazo.

O diagnóstico refere-se ao presente e ao passado, contudo, o plano será executado no futuro.

O diagnóstico do presente não é suficiente para um planejamento estratégico efetivo, falta a visualização do futuro de médio e/ou longo prazo, em que a organização estará inserida. A questão do médio e longo prazo depende da atividade em que a organização atua, por exemplo, em se tratando de petróleo e gás, em geral, são utilizados horizontes temporais de até 30 anos. Na área financeira o horizonte é mais restrito, em geral 4 anos.

A definição do horizonte temporal de visualização de futuro de longo prazo deve ser superior ao horizonte temporal do planejamento. A visualização e análise do futuro devem ser de longo prazo, contudo, o planejamento pode ser de médio prazo e a execução de curto prazo. Na área pública, por exemplo, devemos ter um horizonte temporal de longo prazo, em geral superior a 10 anos (visão de estado), um planejamento de médio prazo (plano de governo) e uma execução de curto prazo (execução orçamentária), em geral de um ano.

Para horizontes temporais da ordem de 10 anos, uma das melhores técnicas de análise desenvolvidas é o método de cenários prospectivos, ou simplesmente análise prospectiva, que não deve ser confundida com previsão do futuro. A prospectiva considera que o futuro não pode ser previsto, contudo, pode ser construído e monitorado.

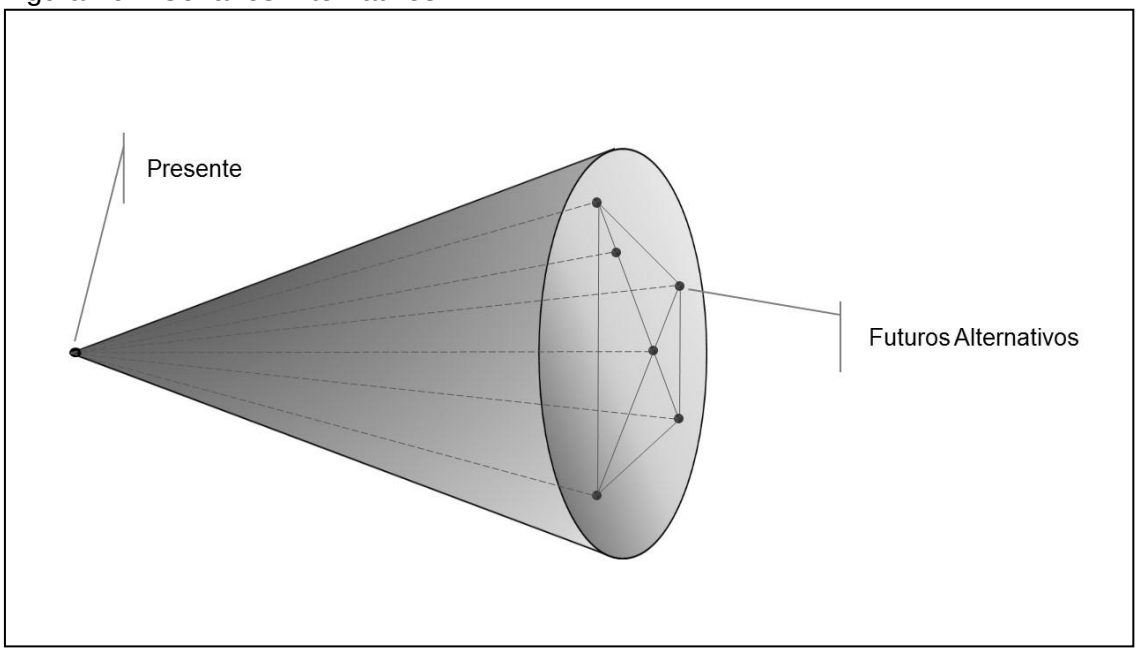
Existem diversas metodologias de construção de cenários prospectivos, desde abordagens totalmente qualitativas até abordagens totalmente quantitativas.

A análise prospectiva tem como propósito a identificação de diversos futuros possíveis (cenários prospectivos alternativos), dentro de um horizonte temporal específico, com o propósito de definir estratégias capazes de: preparar a instituição para o enfrentamento (ou aproveitamento) dos acontecimentos fora de sua competência, e/ou alterar em favor da organização, as probabilidades de ocorrência dos eventos abrangidos parcialmente por sua esfera de competência com base em parcerias estratégicas.

A análise prospectiva deve ser empregada quando a organização enfrenta incertezas de nível 2 e 3 (figura 4). Em geral, é muito mais simples trabalhar com incertezas de nível 2, onde as opções são mutualmente excludentes. Uma boa alternativa para incerteza de nível 3 é transformá-las em incertezas de nível 2, o que pode ser feito pela definição de faixas para as variáveis. A técnica é transformar as variáveis em hipóteses discretas, e se possível, em variáveis binárias.

Neste modelo, as questões estratégicas são transformadas em hipóteses, preferencialmente binárias. O emprego de variáveis binárias probabilísticas (variáveis de Bernoulli) gera cenários como uma partição do espaço de possibilidades. A principal característica dessa modelagem é que todos os cenários alternativos possíveis são representados em um mapa de cenários, o que facilita não somente a definição de estratégias específicas, mas o seu monitoramento futuro (Figura 20).

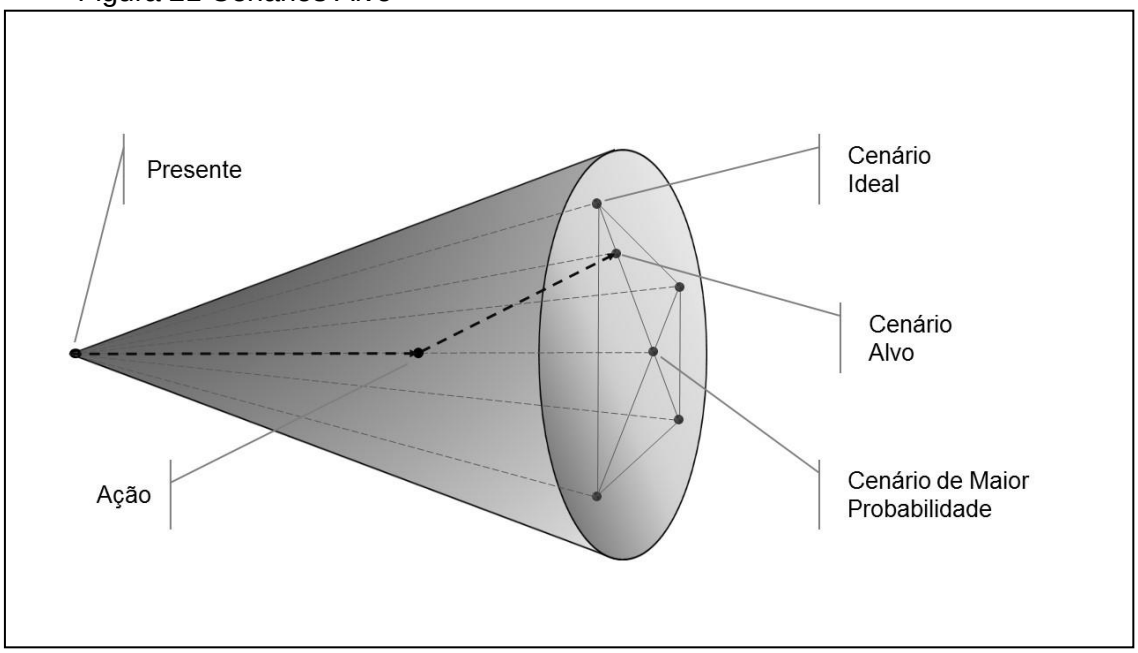
Figura 20 – Cenários Alternativos



Fonte: Elaborado pelo Autor

Mesmo modelando as variáveis como binárias, a quantidade de cenários possíveis é de 2N, desta forma, para 10 variáveis são 1024 cenários possíveis. É inviável trabalhar com essa quantidade de cenários, e em geral, são selecionados de 3 a 4 cenários como referencias: A figura 21 apresenta uma representação com 3 cenários de referência.

Figura 21 Cenários Alvo



Fonte: Elaborado pelo Autor

A estratégia deve ser formulada pela análise das diferenças entre o cenário mais provável e o cenário ideal. Quanto maior a diferença entre esses cenários, maior a ameaça que a instituição irá enfrentar no horizonte temporal definido.

A instituição deve se prepara para o cenário mais provável, pois deve ser este o futuro em que a instituição irá atuar. Contudo, uma análise de cenário não é uma

previsão de futuro. Ao apostar na ocorrência do cenário mais provável, a instituição assume riscos, que devem ser monitorados continuamente.

A melhor forma de reduzir a incerteza do futuro, representado pelo mapa de cenários, é construí-lo ou tentar construí-lo. De fato, o futuro não existe, está sendo construído no presente, contudo, será único. Aumentar a probabilidade de ocorrência de um determinado cenário automaticamente reduz a probabilidade de ocorrência do conjunto dos demais.

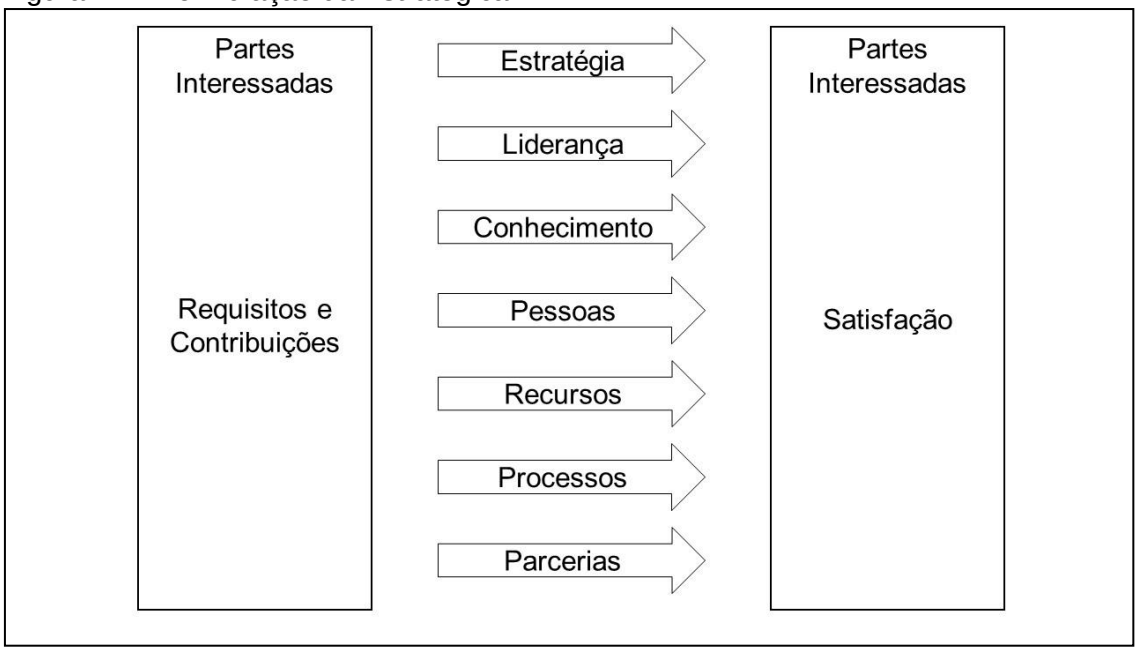
A construção de um futuro melhor, aqui chamado de cenário alvo, em geral é uma estratégia de parcerias. Dificilmente uma organização tem capacidade para construir o futuro sozinha, devendo considerar parcerias com outros atores chaves. Esta é uma estratégia proativa que, contudo, induz riscos.

6.3 Formulação e Tradução

A formulação da estratégia é a fase em que os dados obtidos no diagnóstico e na análise de cenários são sintetizados em uma estrutura de execução e entrega de valor.

A palavra chave na formulação da estratégia é alinhamento. As medidas decorrentes do diagnóstico e da análise de cenários devem ser alinhadas em uma estrutura de entrega de valor às partes interessadas. A estratégia deve ser a base de alinhamento para as lideranças, pessoas, conhecimento, processos e parcerias (Figura 22). Cada um desses aspectos deve ser identificado em objetivos tangíveis e mensuráveis e seus riscos, avaliados.

Figura 22 – Formulação da Estratégica



Fonte: Elaborado pelo autor

Existem diversos modelos de elaboração e de alinhamento propostos na literatura. Podemos encontra desde modelos totalmente estruturados em processos formais e rígidos, até modelos não estruturados em que a estratégia é formulada exclusivamente pelo líder da organização, como uma visão do empreendedor.

Independente do modelo utilizado, o ponto de partida para formulação da estratégia deve ser necessariamente a organização, o ambiente em que está inserida e a avaliação prospectiva.

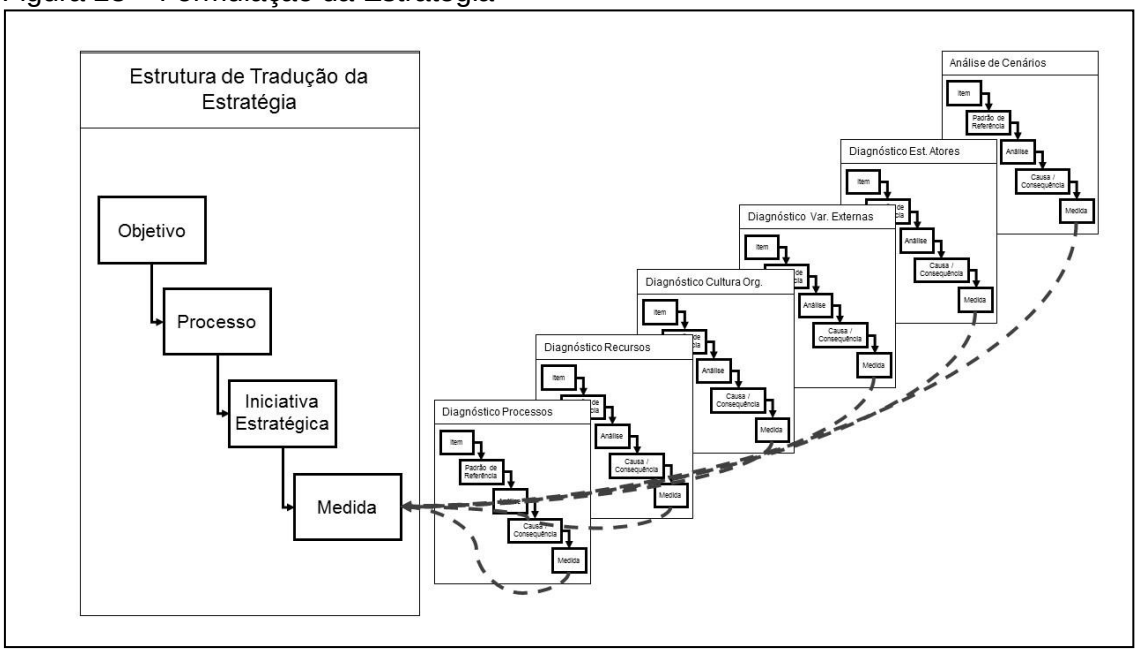
A formulação da estratégia é uma fonte dos principais riscos estratégicos. Formular uma estratégia com objetivos que extrapolam a capacidade da organização gera riscos de execução; por outro lado, estratégias muito aquém dos recursos da organização abrem brechas para a concorrência. Para ser aderente a todas as normas

de gestão de riscos, a formulação da estratégia deve ser definida em torno de objetivos tangíveis. De fato, entendemos que, caso não existam objetivos a serem atingidos, não existem riscos.

Uma das principais causas que dificulta a execução da estratégia está em uma formulação com visão e ambição estratégica distante da realidade organizacional.

A formulação da estratégia deve ser realizada em uma estrutura de síntese, em que as diversas soluções propostas na fase de análise são estruturadas em objetivos estratégicos (Figura 23).

Figura 23 – Formulação da Estratégia



Fonte: Elaborado pelo autor

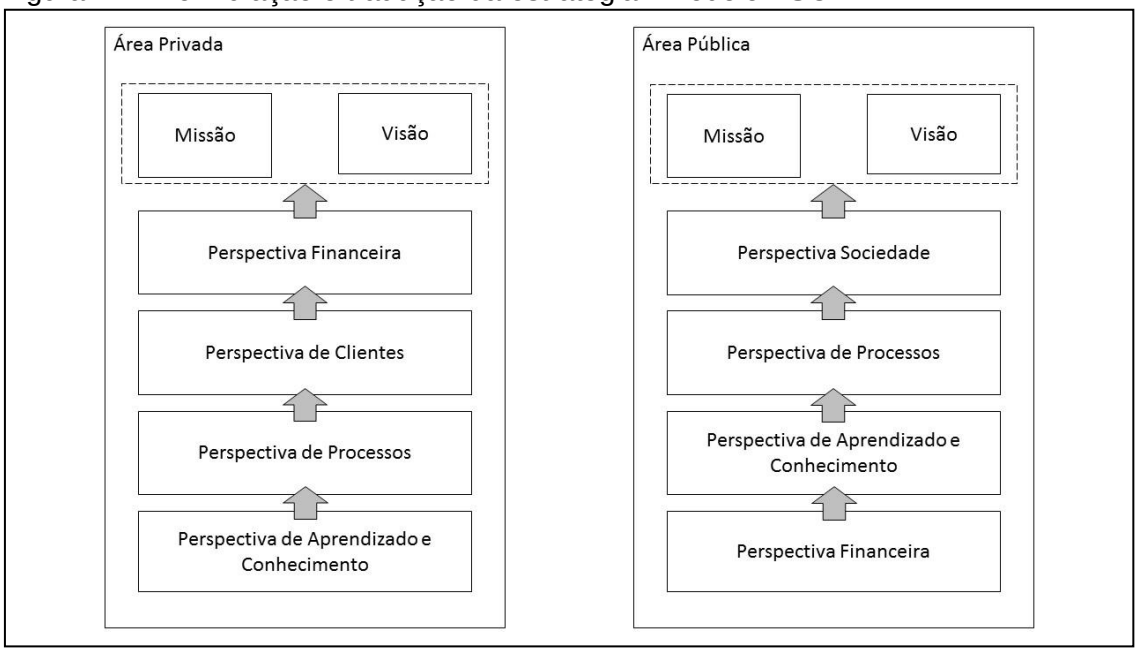
A execução da estratégia necessita de um modelo de tradução e monitoramento, em que a estratégia possa ser traduzida em objetivos com indicadores mensuráveis e metas estabelecidas.

A estrutura de execução deve ser uma sequência lógica de causa e efeito, resultando em uma entrega de valor.

Existem diversos modelos com algumas diferenças e similaridades. Dos principais modelos existentes – Balanced Scorecard, Prisma de desempenho, Pirâmide de desempenho, dentre outros – o Balanced Scorecard (BSC) é um dos mais utilizados.

O BSC foi proposto por Kaplan e Norton como um modelo de avaliação de desempenho para organizações nas quais os recursos intangíveis tem um papel central na geração de valor (Kaplan, 2010).

Figura 24 – Formulação e tradução da estratégia - modelo BSC



Fonte: Adaptado de KAPLAN e NORTON, 2008

Priorização

A priorização é a última fase da formulação da estratégia, o elo entre a formulação e a execução e um dos fatores que impactam diretamente na execução. A priorização fornece a flexibilidade necessária para que um plano estratégico de médio e longo prazo possa ser executado.

Em geral, um plano de médio e longo prazo deve ser robusto o suficiente para sobreviver ao longo de algumas administrações e de alterações moderadas de conjuntura. Para isso, é fundamental que o plano tenha uma quantidade suficiente de iniciativas estratégicas que possam ser distribuídas ao longo de seu horizonte temporal de acordo com critérios de priorização.

A escolha da ordem de execução das iniciativas estratégicas garante que a alta administração possa imprimir a sua estratégia e alterá-la de acordo com a necessidade, sem que seja necessário refazer o plano.

Um dos modelos de priorização mais simples e efetivo é o modelo aditivo linear, que além de sua simplicidade, agrega aspectos técnicos e estratégicos relativos à decisão.

O primeiro passo para executar a priorização é a definição dos critérios, segundo os quais as iniciativas serão priorizadas. Em geral, devem ser balanceados critérios de custo (custo das iniciativas, tempo de execução, quantidade de pessoal envolvido, complexidade) e de benefícios (retorno potencial, impacto na imagem, motivação, expectativa das partes interessadas). Para cada critério deve ser estabelecida uma régua de mensuração e cada iniciativa deve ser avaliada e pontuada na régua, segundo seu grau de contribuição para o critério. Em seguida, o decisor estratégico deve definir o valor relativo de cada critério para a estratégia da organização. O valor final que irá definir a posição relativa de cada inciativa estratégicas é obtido como uma média ponderada da contribuição de cada iniciava para cada critério. O fator de ponderação é o valor atribuído pelo decisor para o critério.

O resultado final do processo de priorização é uma lista ordenada de todas as iniciativas estratégicas. Este é o início do processo de execução, que dependerá da capacidade de execução da organização e dos riscos inerentes à estratégia definida.

6.4 Execução

A execução do que foi planejado ocorre por meio dos processos executados pela organização e dos projetos (iniciativas) estratégicos. Os projetos estratégicos, em geral, destinam-se a melhorar processos existentes ou criar processos novos. Qualquer projeto que não tenha um desses dois propósitos deve ser revisto. Iniciativas estratégicas, em geral, não geram valor, o que de fato gera valor para a organização são os processos executados.

A execução da estratégia deve estará focada na execução dos projetos estratégicos e no acompanhamento do desempenho dos processos que são impactados por esses projetos.

A diferenciação entre projetos e processos é um importante aspecto na execução da estratégia.

Um processo é definido como um conjunto de atividades ou comportamento executados por pessoas ou máquinas para alcançar uma ou mais metas, que agregam sequências contínuas de fatos ou operações que apresentam certa unidade ou que se reproduzem com certa regularidade.

Um projeto, por outro lado, é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo, sendo que sua natureza é temporária com início e término definidos.

Os métodos de gestão de projetos e de processos são diferentes e os riscos associados, também são de natureza diversa.

Gestão de projetos

Todo projeto tem riscos de execução e de resultado. Mesmo que a execução de um projeto tenha sido adequada, no que se refere a custo, prazo e qualidade, ainda assim ele pode não atingir seu objetivo, que é melhorar um processo existente ou, ainda, o novo processo criado pode não ser efetivo.

O gerenciamento de projetos preconizado pelo Instituto de Gerenciamento de Projetos é definido no conjunto de práticas em gerenciamento de projetos *Project Management Body of Knowledge*, mais conhecido como PMBOK.

Segundo Adriano Santana (2011), gerenciar um projeto é administrar as incertezas do projeto, planejando sua execução antes de iniciá-lo, controlando o projeto de modo a assegurar sua conclusão no escopo, prazo e orçamento previstos, além de atender seus requisitos esperados.

Planejar significa estabelecer o objetivo e o escopo do esforço, dividi-lo em fases, definir e refinar as tarefas e estabelecer as responsáveis para alcançar o objetivo proposto, considerando premissas e restrições existentes.

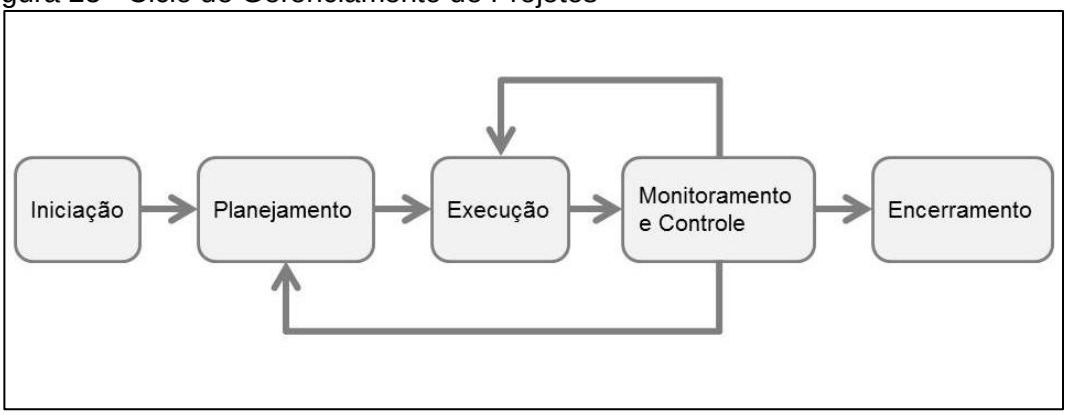
Monitorar significa acompanhar, avaliar e regular o progresso, medindo o desempenho do projeto por meio da comparação entre o realizado e o planejado, tomando ações para atender aos objetivos de desempenho do Plano de Projeto.

O PMBOK subdivide o gerenciamento de projetos nas seguintes fases:

I. Abertura do projeto - processo de desenvolvimento de um documento que formalmente autoriza um projeto e define os requisitos iniciais que satisfaçam as necessidades e expectativas das partes interessadas;
II. Elaboração do plano de gerenciamento do projeto – processo de documentação das ações necessárias para definir, preparar, integrar e coordenar todos os planos auxiliares;
III. Gerenciamento da execução do projeto - processo de realização do trabalho definido no plano de gerenciamento do projeto, para atingir os objetivos do projeto;
IV. Monitoramento e controle dos resultados do projeto – processo de acompanhamento, revisão e regulação do progresso para atender aos objetivos de despenho definidos no plano de gerenciamento do projeto;

V. Controle integrado de mudanças - processo de revisão de todas as solicitações de mudanças, aprovação de alterações nas entregas, ativos de processos organizacionais, documento de projeto e planos de gerenciamento do projeto;
VI. Encerramento do projeto - processo de finalização de todas as atividades de todos os grupos de processos de gerenciamento do projeto, a fim de terminar formalmente o projeto ou a fase.

Figura 25 - Ciclo de Gerenciamento de Projetos



Fonte: Adaptado de SANTANA, 2011

Processos

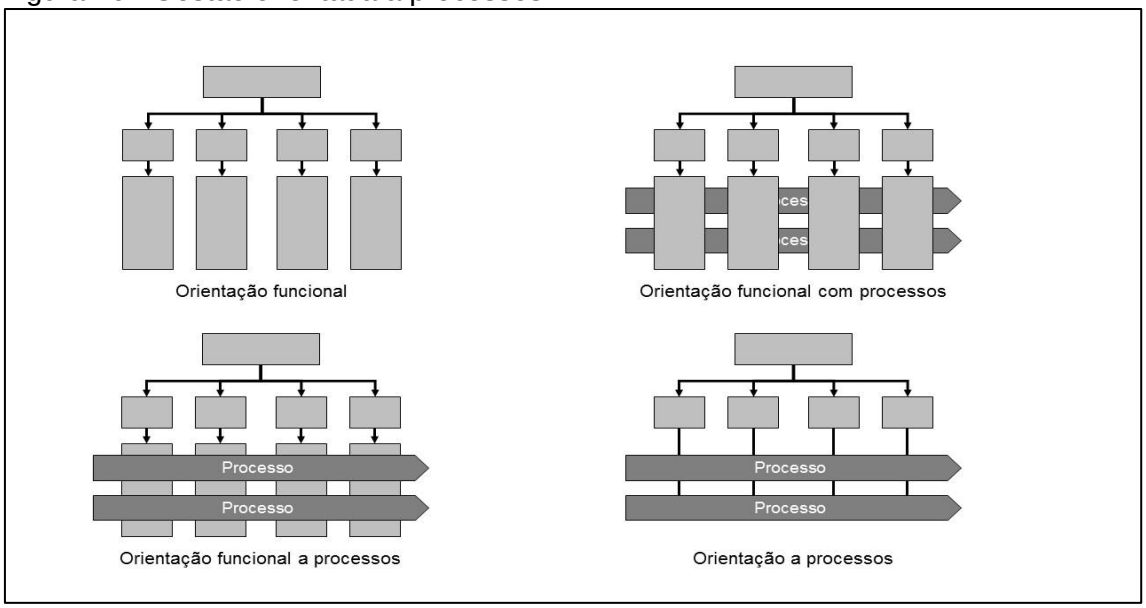
O aspecto central na gestão de processos é a avaliação contínua, a análise e a melhoria de desempenho e os riscos associados.

Para o gerenciamento de processos devem ser definidos os seguintes itens:

I. Uma estrutura de medição centrada no cliente;
II. Um esquema do nível dos processos organizacionais;
III. Um plano de gerenciamento e melhoria dos processos organizacionais.

Diversas empresas e órgão públicos utilizam uma visão departamental, com os processos sendo geridos de forma transversal o que pode gerar alguns riscos nas interfaces departamentais e, devem ser avaliados na gestão de riscos (Figura 26).

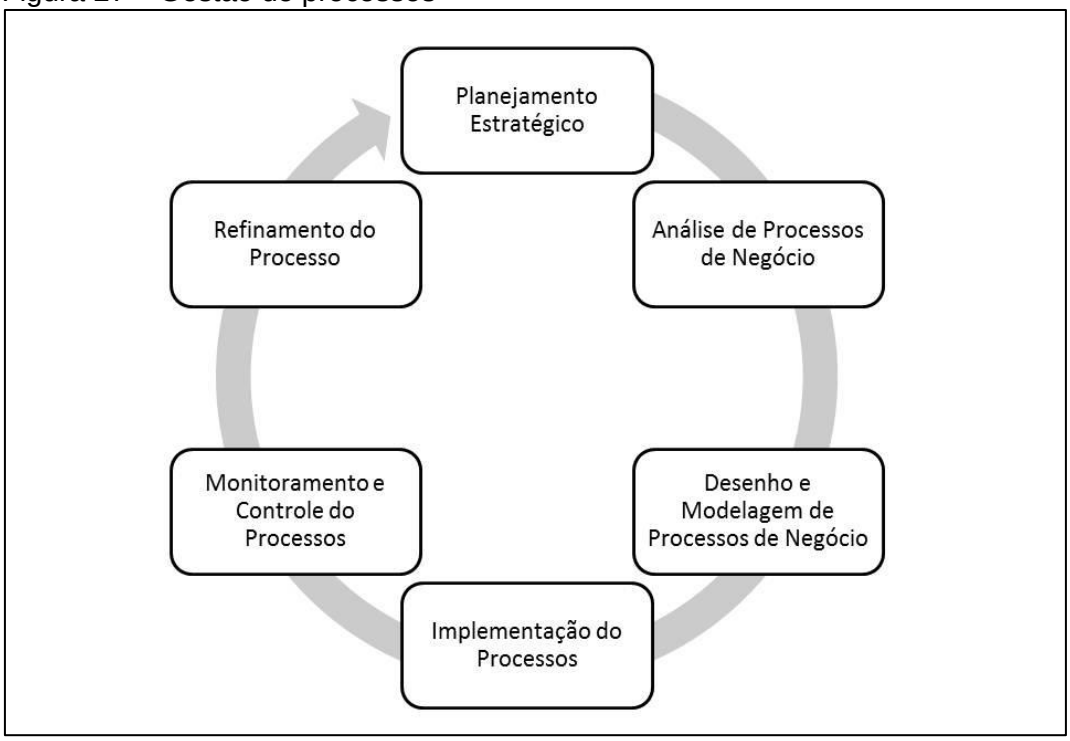
Figura 26 - Gestão orientada a processos



Fonte: MORAIS, 2016

A figura 24 mostra o ciclo completo de gestão de processos preconizado pelo CBOK v3.0, composto de 6 fases.

Figura 27 – Gestão de processos



Fonte: ASSOCIATION OF BUSINESS PROCESS MANAGEMENT PROFESSIONAL, 2013

O monitoramento de processos está associado ao conceito de desempenho de processos que tem métrica e medição associadas com o trabalho ou saída do processo.

O monitoramento de desempenho de processo utiliza dois tipos de indicadores: esforço e resultado.

Indicadores de esforço referem-se às causas, condições ou entradas e à execução inerente ao processo ou atividade. Em geral, são índices numéricos estabelecidos sobre as principais causas que afetam o processo.

Indicadores de resultado referem-se às consequências, resultado, saída ou produto da atividade ou processo. Em geral, são índices numéricos estabelecidos sobre as consequências.

As métricas e medições de desempenho de processo são baseadas em quatro dimensões:

I. Tempo – relacionada à duração do processo;
II. Custos – relacionada a valor monetário;
III. Capacidade – relacionada ao volume de uma saída;
IV. Qualidade – relacionada ao real em relação ao ótimo ou máximo, podendo ter várias formas.

Segundo Kaplan e Norton (2008), uma das fases críticas para a execução da estratégia é a definição de indicadores e, principalmente, de suas respectivas metas. Os autores sugerem duas técnicas para a definição das metas: dividir as lacunas de valor total em metas para cada tema ou definir metas para cada tema estratégico, como base na lógica de causa e efeito do mapa estratégico. Desta forma, preconizamos a definição dos temas estratégicos como uma combinação de indicadores, o que facilita a definição das metas específicas.

Os indicadores devem ser estruturados em árvores, o que facilita a identificação dos pontos chaves para a melhoria dos processos.

6.5 Revisão

A revisão é uma atividade transversal a todo o processo de gestão estratégica. As revisões devem ser periódicas e chamadas de Reunião de Análise da Estratégia (RAE), e/ou inopinada, fruto de mudanças bruscas no ambiente externo.

O propósito das RAEs é avaliar a estratégia e promover os ajustes e modificações necessárias. Kaplan e Norton (2008) preconizam três tipos de reuniões gerenciais para monitorar, aprender, agir e adaptar – Reuniões de Análise da Operação, Reuniões de Análise da Estratégia e Reuniões de Teste e Adaptação da Estratégia.

Segundo os autores, as Reuniões de Análise da Operação analisam o desempenho departamental, funcional e financeiro recente e tratam de problemas imediatos a serem resolvidos. As Reuniões de Análise da Estratégia examinam os indicadores e iniciativas do mapa estratégico, com o propósito de verificar o progresso, as barreiras e os riscos referentes à implementação da estratégia. As Reuniões de Teste de Adaptação da Estratégia analisam se a estratégia está funcionando e se suas premissas fundamentais continuam válidas à luz de dados recentes sobre os indicadores estratégicos. Os participantes dessas reuniões também analisam as mudanças nos ambientes competitivo e regulatório e consideram novas ideias e oportunidades a serem prosseguidas pala empresa.

As Reuniões de Análise da Estratégia (RAEs) são realizadas uma vez por mês, com o objetivo de avaliar o desempenho recente da estratégia e fornecer orientação contínua para a sua implementação. São transnacionais e envolvem membros do Comitê Executivo da instituição, gestores de temas estratégicos e outros gestores com habilidade em funções ou negócios específicos. As RAEs devem ser conduzidas pelo Decisor Estratégico da instituição e devem incluir entre seus participantes o Comitê Executivo da Organização.

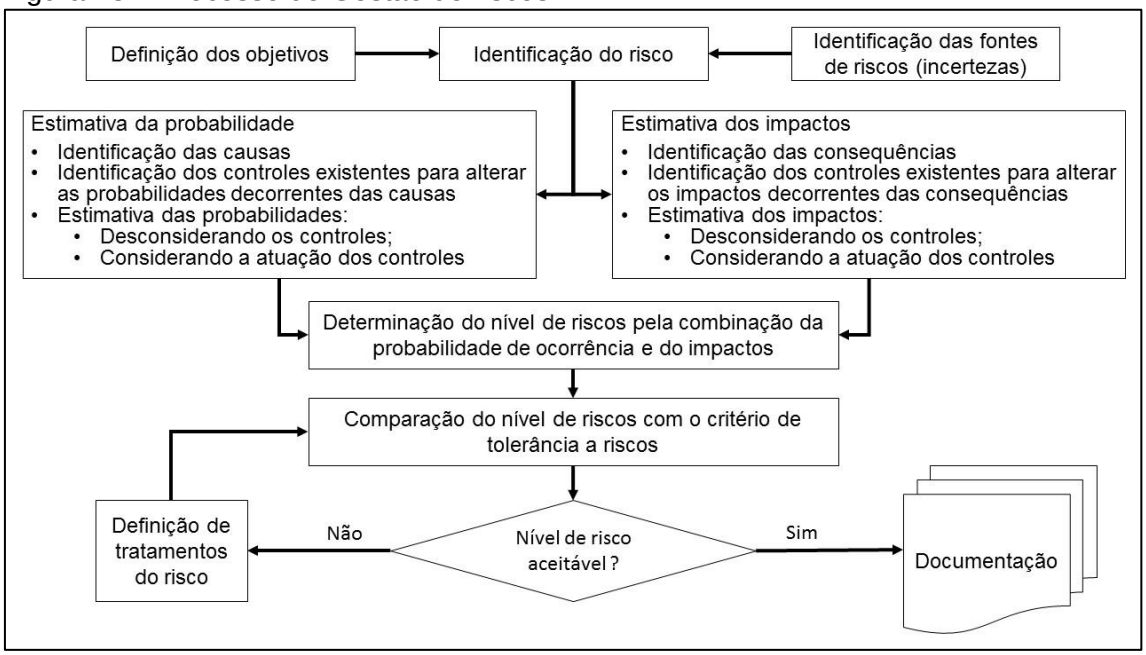
As reuniões de análise da estratégia não devem questionar a validade da estratégia. O propósito é avaliar se a execução da estratégia está no rumo certo. Devem ser identificados os entraves para a execução da estratégia e onde as dificuldades na implementação ocorrem. Além disso, devem fazer a identificação das causas dos problemas e propor providências para eliminar esses obstáculos e definir responsabilidades para a consecução dos resultados almejados.

7 Processo de Gestão de Riscos

A gestão de riscos deve ser integrada aos demais processos organizacionais. O processo é o dia a dia da gestão. Com pequenas variações, todas as normas e modelos de gestão de riscos convergem para o mesmo processo (Figura 28). As diferenças pontuais existentes são derivadas da natureza dos riscos enfrentados e das atividades de tratamento.

A execução do processo de gestão de risos depende da definição prévia de um contexto no qual ele estará inserido.

Figura 28 – Processo de Gestão de riscos



Fonte: Elaborado pelo autor

7.1 Contexto da gestão de riscos

O contexto descreve os parâmetros internos e externos que serão levados em consideração na gestão de risco, estabelece o escopo, os critérios de análise e as políticas de gestão de riscos.

O contexto da gestão de riscos deve ser aderente ao contexto da gestão estratégica. O diagnóstico, bem como a análise de cenário, deve ser utilizado para a definição dos riscos.

Em geral, são definidos três os contextos básicos – o contexto interno, o contexto externo e o contexto de gestão de riscos.

O contexto externo está relacionado ao ambiente no qual a instituição está inserida. É composto basicamente pelas variáveis externas e pelos atores. O contexto deve identificar e analisar os atores chaves que serão considerados no desenvolvimento dos critérios de risco e os principais direcionadores (drives) do ambiente externo.

O contexto interno está relacionado à estrutura com a qual a organização busca atingir seus objetivos, expresso pelos recursos disponíveis (tangíveis e intangíveis), pelos processos que executa e, principalmente, pelo seu plano estratégico, visualizado em seu mapa estratégico. Deverão ser identificados, ainda, os aspectos que afetam a forma como os riscos serão gerenciados.

O contexto da gestão de risco estabelece como os riscos serão gerenciados. Define o escopo do gerenciamento de riscos, o processo, as metas, as responsabilidades, metodologia e indicadores de desempenho e os critérios de análise e avaliação de riscos.

7.1.1 CRITÉRIOS

A gestão de riscos envolve uma forma lógica e estruturada de pensar e se comunicar e requer uma linguagem estruturada para suportar o processo. É importante o emprego de uma terminologia comum para garantir uma comunicação efetiva e evitar ambiguidades na descrição dos riscos e seus tratamentos, não somente dentro da organização, mas também com os parceiros e as partes interessadas. Essa linguagem comum deve ser definida nos critérios de gestão de riscos.

Os critérios de gestão de risco estabelecem a base para a avaliação dos riscos: as dimensões de avaliação, sua mensuração, a forma como as dimensões são

combinadas para a definição dos níveis de risco, o apetite aos riscos (quais níveis são aceitáveis e toleráveis), e as naturezas das causas e consequências.

O propósito da definição das dimensões é estabelecer uma linguagem comum e um sistema padrão de mensuração que possa ser utilizado para avaliar e comparar os riscos enfrentados por todos os setores da organização.

Em geral, são empregadas duas dimensões para avaliação de riscos, quer sejam positivas ou negativas: (1) probabilidade (plausibilidade) e (2) impacto das consequências. Alguns riscos, contudo, necessitam de outras dimensões de avaliação. Um exemplo são os riscos de baixa probabilidade, que raramente ocorrem ou nunca ocorreram no passado e que podem ocorrer com uma velocidade de propagação muito grande e que geralmente ocorrem sem indícios que possam alertar para uma ocorrência iminente. Outros riscos podem afetar atividades chaves da organização para os quais não existam ou não seja possível desenvolver planos alternativos ou de contingência. Para esses e outros caso de natureza específica, algumas organizações acrescentam outras dimensões, tais como: vulnerabilidade, velocidade de propagação e exposição.

Para cada dimensão considerada devem ser definidas réguas (escalas ou padrões) de mensurações. As réguas devem ser compostas de níveis e respectivas definições que permitam desenvolver interpretações consistentes e serem aplicadas por diferentes pessoas. Quanto mais descritivas e simples forem as réguas, mais consistente será suas interpretações.

A quantidade de níveis é outro ponto importante. As réguas devem possibilitar a diferenciação efetiva entre os diversos riscos. Uma régua de 5 níveis permite uma diferenciação melhor do que uma de 3, contudo uma de 10 níveis pode estar inserindo uma precisão desnecessária, que aumenta o tempo e o custo de análise, sem benefícios significativos.

As réguas devem ser estabelecidas em função da natureza dos riscos enfrentados, do tamanho, da complexidade e da cultura de cada organização.

7.1.1.1 Tipologia de Riscos

A tipologia de riscos é importante para a classificação dos riscos e seu gerenciamento. Não existe uma tipologia, ou categorização, padrão de estrutura ou categorização os riscos. Elas devem facilitar a gestão e não o contrário.

A tipologia deve ser distinta das consequências, e estas devem ser utilizadas para avaliar os níveis de riscos e priorizar seu tratamento.

Cada organização pode estabelecer uma tipologia que melhor se adapte ao seu modelo de gestão de riscos, tais como – riscos relativos à infraestrutura (incêndio, desabamento, enchente), riscos relativos às pessoas (quantitativo, saúde, capacitação). Um determinado risco, por exemplo, um incêndio, pode ter impacto sobre consequências diversas: pode impactar ativos, saúde e segurança dos funcionários e gerar ações legais contra a organização.

A NBR ISO 31000 não especifica uma tipologia. O COSO estabelece as tipologias de riscos estratégicos, operacionais, comunicação e conformidade, ao passo que, o Orange BOOK utiliza a tipologia de riscos estratégicos, programas, projetos e operações.

A Instrução normativa conjunta CGU/MP nº 001, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal, recomenda:

> **Art. 18.** Os órgãos e entidades, ao efetuarem o mapeamento e avaliação dos riscos, deverão considerar, entre outras possíveis, as seguintes tipologias de riscos:
>
> - Riscos operacionais: eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

- Riscos de imagem/reputação do órgão: eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional;
- Riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade; e
- Riscos financeiros/orçamentários: eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações (BRASIL, 2016, p.10)

7.1.1.2 Mensuração de plausibilidade.

A probabilidade representa a possibilidade que um dado evento venha a ocorrer. A probabilidade pode ser expressa em termos qualitativos ou quantitativos. Quando forem utilizados valores numéricos sejam de porcentagem ou frequência, devem ser especificado o período de tempo em relação ao tempo de vida do projeto ou do ativo.

A mensuração de plausibilidade ou de probabilidade em geral está relacionada à forma como definimos probabilidade. Em geral, existem três formas de definição de probabilidade:

- O chamado conceito clássico define probabilidade como a relação entre o número de resultados favoráveis sobre o número de resultados possíveis: Ex. A probabilidade de sair a face com o número 4, em um lançamento de um dado, é de 1/6.
- Probabilidade como conceito de frequência. Este cálculo de probabilidade é utilizado quando existe uma série histórica e a probabilidade é definida como a relação entre o número de ocorrências favoráveis observadas na série e o total de ocorrências observadas. Ex: A probabilidade de chover num determinado dia de um ano em uma cidade pode ser estimada com base em uma série histórica. Neste caso, basta contar o total de dias em que chove no ano anterior e dividir pelo total de dias no ano.
- O terceiro conceito está relacionado à confiança na ocorrência de um evento. Exemplo: Qual a probabilidade de chover amanhã em uma determinada cidade? Neste caso, a série histórica não tem grande utilidade. Para estimar essa probabilidade, devemos olhar fora da série e identificar quais as variáveis que impactam na ocorrência ou não de chuva. Repare que o fato de que chove cerda de 40% dos dias em uma cidade, não nos diz muito sobre a probabilidade de chover amanhã.

As réguas de plausibilidade/probabilidade podem ser definidas com base nas formas de definição de probabilidades. A Figura 29 é um exemplo que considera 5 faixas.

Figura 29 – Exemplo de tabela de probabilidades

Tabela de probabilidades		
Probabilidade	Estimativa de probabilidade	
	Probabilidade	Ocorrência Esperada
Improvável	Inferior a 5%	Uma vez a cada 20 anos.
Pouco provável	De 6% a 34%	Uma vez a cada 10 anos.
Provável	De 35% a 75%	Uma vez a cada 5 anos.
Provável	De 76% a 94%	Uma vez a cada ano.
Quase certa	Superior a 95%	Diversas vezes no ano

Fonte: Elaborado pelo autor

7.1.1.3 Mensuração de Impactos

Os impactos referem-se à extensão com que a ocorrência do evento afeta a organização. Os impactos, em geral, são estabelecidos em relação às consequências, que podem incluir diversos aspectos, tais como: impactos sobre ativos, reputação, conformidade, saúde e segurança, dentre outros.

A mensuração dos impactos deve estar definida em réguas específicas. As réguas devem ser discretas para que seja possível comparar riscos tangíveis e intangíveis (Figura 30).

Para cada tipo de consequência devem ser definidos os níveis de impactos. As réguas devem ser consistentes, tanto com relação à escala do impacto, como consistentes entre si, ou seja, um impacto de nível moderado na consequência financeira deve ser compatível com um impacto moderado na consequência de interrupção de serviço.

Figura 30 – Exemplo de tabela de Impactos

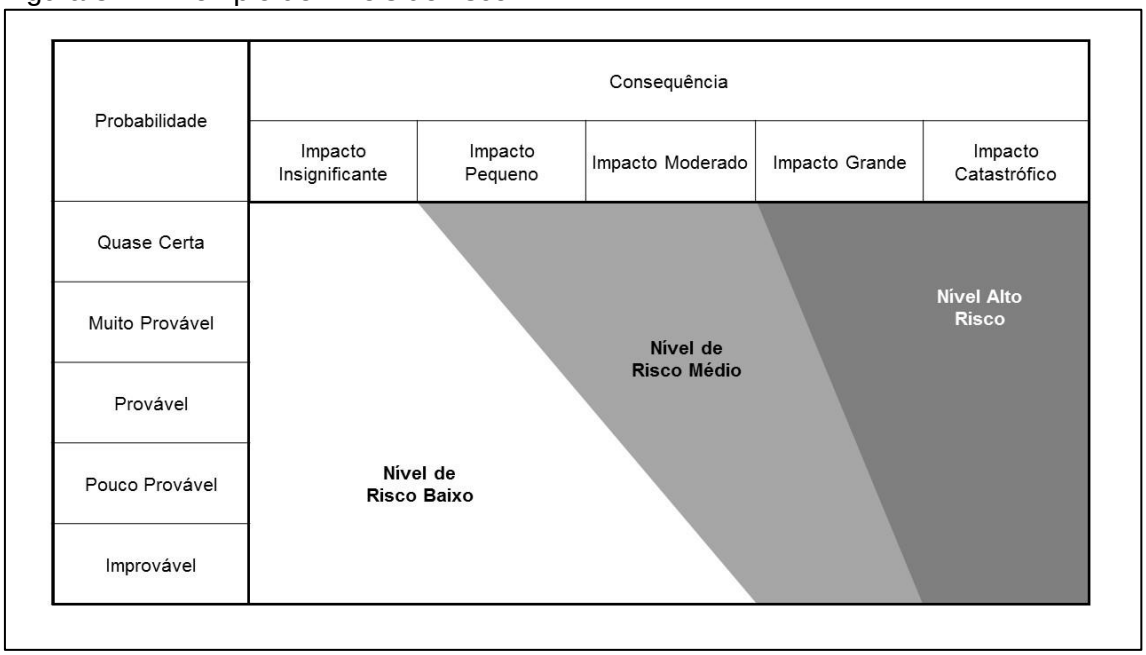
Tabela de Consequências		
Impacto	Tipo da Consequência	
	Financeiras	Interrupção do serviço
Insignificante	Perdas inferiores a 0,1% do orçamento	Interrupção do serviço em uma unidade (podendo ser assumido por outra unidade do mesmo grupo)
Pequena	Perdas entre 0,1% e 0,5% do orçamento	Interrupção do serviço em uma unidade (não podendo ser assumido por outra unidade do mesmo grupo)
Moderada	Perdas entre 0,5% e 2% do orçamento	Interrupção do serviço de um grupo de unidades (podendo ser assumido por outro Grupo)
Grande	Perdas entre 2% e 5% do orçamento	Interrupção do serviço de um grupo de unidades (não podendo ser assumido por outro Grupo)
Catastrófica	Perdas superiores a 5% do orçamento	Interrupção completa do serviço prestado pela instituição

Fonte: Elaborado pelo autor

7.1.1.4 Níveis de Riscos

Níveis de riscos são combinações da probabilidade de ocorrência com os impactos das consequências do evento de riscos. Alguns autores recomendam trabalhar com a multiplicação dos valores desses dois aspectos. Contudo, essa opção dificulta a definição dos tratamentos mais adequados, tendo em vista que riscos de baixa probabilidade e alto impacto são bem diferentes dos riscos de alta probabilidade e baixo impacto. As opções de tratamento de primeiro são geralmente o estabelecimento de planos de contingência e do segundo, de melhoria de processos.

Figura 31 – Exemplo de níveis de risco



Fonte: Elaborado pelo autor

Em geral, a avaliação do nível dos riscos é efetuada em duas condições. A primeira é o risco inerente à atividade, processo, projeto e equipamento. A segunda é o risco residual, que permanece mesmo depois dos tratamentos (controles) aplicados. Algumas instituições incluem uma terceira condição, chamada de nível de riscos desejado, que será obtido depois da aplicação de novos tratamentos. Contudo, esta última condição somente será obtida quando da implantação efetiva dos novos controles. No momento em que o novo tratamento for implementado, o nível desejado passa a ser o novo nível residual.

7.1.1.5 Apetite aos Riscos

O termo apetite aos riscos é a quantidade de risco estabelecida, de modo amplo, que uma organização está “disposta a aceitar para cumprir sua missão e atingir sua visão, enquanto a tolerância a risco é o nível aceitável de variação referente à realização dos objetivos” (COSO, 2014, p.110).

A organização ao estabelecer seus objetivos e as metas correspondentes deve definir quais riscos serão assumidos, e em que níveis, e qual a contrapartida de geração de valor é esperada. A definição do apetite aos riscos é de responsabilidade da alta administração, que além de estabelecer o apetite aos riscos deve comunicá-lo de forma clara à toda a organização. Cabe também à alta administração revisar o apetite aos riscos e monitorar a aderência dos riscos assumidos pela organização com o apetite estabelecido

Uma organização com apetite agressivo aos riscos, em geral, define objetivos agressivos, ao passo que uma organização com aversão a riscos tende a definir objetivos mais conservadores.

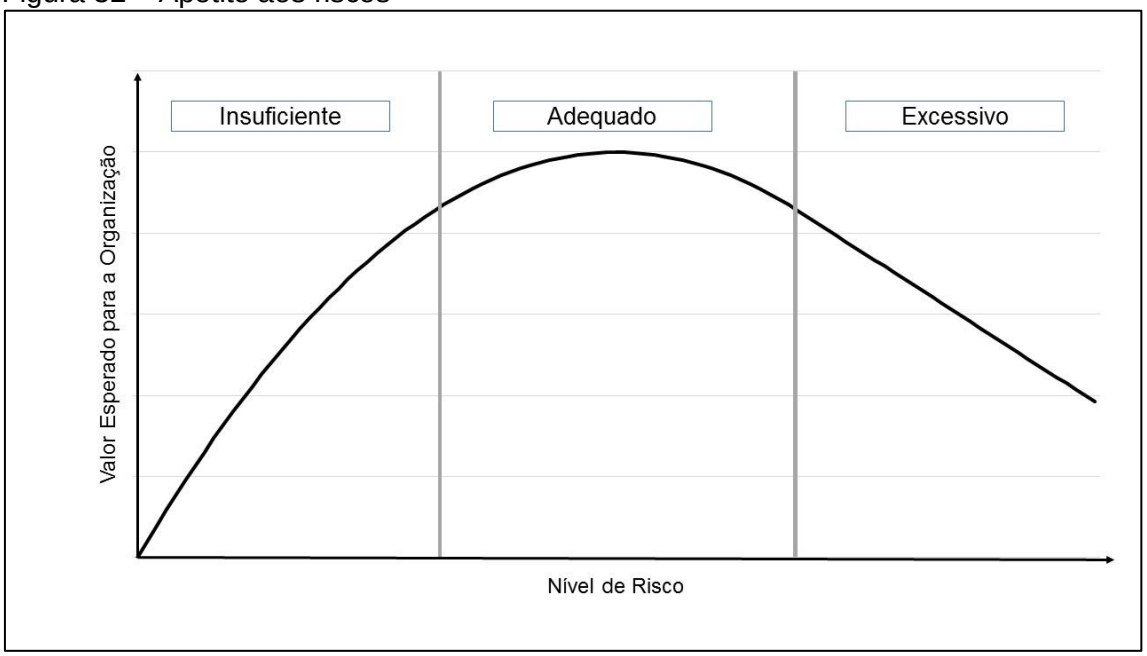
Definidos os objetivos estratégicos, as estratégias organizacionais decorrentes devem ser alinhadas ao apetite aos riscos. Uma comunicação efetiva do apetite aos riscos direciona o estabelecimento dos objetivos operacionais, permitindo o alinhamento de toda a organização no que se refere aos riscos.

A gestão de riscos organizacionais não deve ser um processo isolado da estratégia ou do dia a dia da tomada de decisão. A integração da gestão de riscos, ou mais precisamente a gestão de riscos organizacionais (ERM) é fundamental para que os gestores e diretores saibam quanto de riscos é aceitável quando considerando os

caminhos para atingir os objetivos. Somente com uma avaliação clara dos riscos, em confronto com o apetite, é possível balancear riscos e oportunidades.

Avaliando riscos do ponto de vista de geração de valor, o apetite aos riscos refere-se à quantidade de riscos que uma organização está disposta a aceitar para atingir seus objetivos e gerar valor. Esta noção é importante tendo em vista que um apetite muito baixo aos riscos pode limitar a capacidade da organização de gerar valor ou de aproveitar oportunidades (Figura 32)

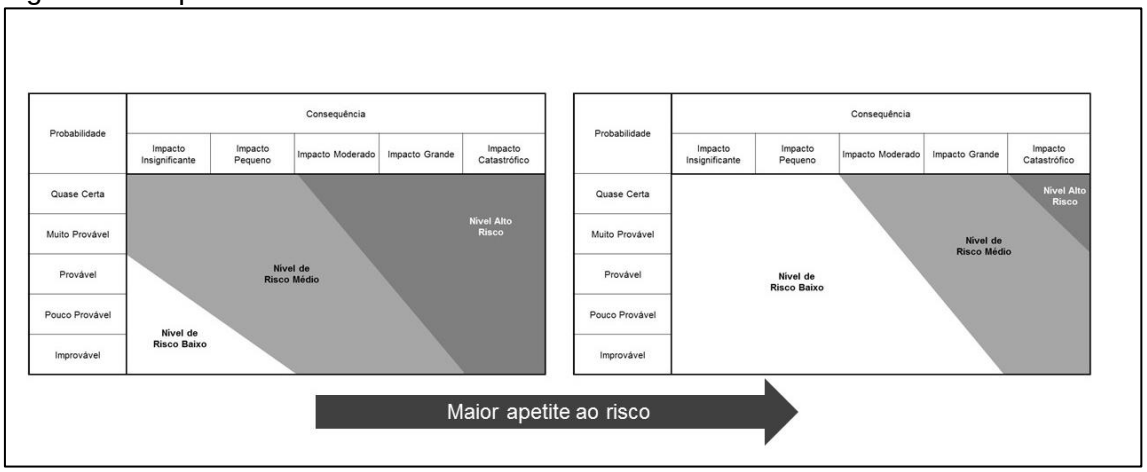
Figura 32 – Apetite aos riscos



Fonte: Elaborado pelo autor

O apetite aos riscos é a definição dos níveis de riscos resultantes da combinação da probabilidade de ocorrência do evento de risco com o impacto de suas consequências. Uma organização que considera a ocorrência de qualquer risco como nível alto tem baixo apetite aos riscos, ao passo que uma organização que considera qualquer risco como de nível baixo tem um grande apetite aos riscos (Figura 33).

Figura 33 – Apetite ao Risco



Fonte: Elaborado pelo Autor

7.1.1.6 Atitude Frente aos Riscos

A atitude frente aos riscos define como a organização irá tratar e gerenciar os riscos. A organização deve definir em que condições os riscos podem ser aceitos, quais ações são requeridas, a periodicidade de seu monitoramento e o nível organizacional em que serão geridos. Devem ser definidos, também, quais ações serão implementadas caso algum risco escale para o nível considerado.

Figura 34 – Exemplo de atitude frete aos riscos

Atitude Frente ao Riscos			
Atitude	Níveis		
	Baixo	Médio	Alto
Apetite ao Risco	Aceitáveis com os controles atuais	Aceitáveis com excelentes controles	Riscos não aceitáveis
Ação requerida	Nenhuma ação requerida	Implementar Tratamento quando os benefícios excederemos custos	Implementar tratamento
Monitoramento e Reporte	Semestral	Mensal	Contínuo
Agravamento para este nível	Gestão pela área funcional	A gestão pela área funcional com reporte para a diretoria	Gestão pela diretoria

Fonte: NEW SOUTH WALES, 2012

7.1.1.7 Avaliação dos controles

A avaliação de um determinado risco em seu nível residual pressupõe a existência de um controle que reduza o risco nível de riscos avaliado como inerente. Sem o controle, existe apenas o nível inerente. A existência do controle é condição necessária, porém não é suficiente. Para que o nível do risco seja, de fato, reduzido para o nível residual o controle deve ser efetivo.

A avaliação da efetividade dos controles deve estar pautada em três aspectos principais: projeto, implementação e operação.

O projeto refere-se à capacidade do controle de reduzir o nível de riscos avaliado como inerente para o residual, considerando uma atuação isolada ou em conjunto com outros controles. Uma deficiência em projeto existe quando um controle operando conforme projetado não consegue reduzir o risco para o nível residual desejado.

A implementação refere-se à existência, de fato, do controle e sua operação. Um controle corretamente projetado somente será efetivo se estiver em operação. Por outro lado, um controle não pode ser implementado de forma efetiva se o projeto não for adequado. Uma deficiência em implementação existe quando um controle com projeto adequado não é implementado adequadamente.

A operação efetiva de um controle refere-se a uma aplicação consistente, por meios adequados, por pessoas qualificadas e durante períodos relevantes. Um controle não pode ser adequadamente operado se não for adequadamente projetado e implementado. Uma deficiência em operação existe quando um controle adequadamente projetado e implementado não é operado da forma como foi projetado, ou quando a pessoa que opera o controle não tem a autoridade ou a competência necessária para operá-lo de forma afetiva.

Um controle efetivo é aquele que é adequadamente projetado, implementado e operado (Figura 35).

Figura 35 – Exemplo de tabela de avaliação de controles

Efetividade dos Controles			
Controles	Aspecto		
	Projeto	Implementação	Operação
Efetivo	Adequado	Adequada	Adequada
Aceitável	Adequado	Adequada	Aceitável
Aceitável	Adequado	Aceitável	Aceitável
Aceitável	Aceitável	Aceitável	Aceitável
Não aceitável	Adequado	Adequado	Deficiente
Não aceitável	Adequado	Aceitável	Deficiente
Não aceitável	Adequado	Deficiente	Deficiente
Não aceitável	Aceitável	Deficiente	Deficiente
Não aceitável	Deficiente	Deficiente	Deficiente

Fonte: Adaptado de NEW SOUTH WALES, 2012

Um dos aspectos importantes da efetividade dos controles é sua confiabilidade, que pode ser expressa como função de sua efetividade da seguinte forma:

- Efetivos – Existem controles para a mitigação do risco, estão em operação e são aplicados consistentemente. Os gestores estão seguros de que os controles são efetivos e confiáveis. É requerido monitoramento contínuo.
- Aceitável – Os controles são parcialmente efetivos, requerem monitoramento contínuo e podem necessitar de adequação (redesenho), melhorias suplementação.
- Não aceitáveis – Os gestores não podem confiar que o risco esteja sendo mitigado em qualquer nível. Os controles precisam ser revistos.

7.2 Identificação dos Riscos

A identificação dos riscos é o processo de encontrar, descrever e reconhecer incertezas que podem aumentar o inibir a habilidade da organização em atingir seus objetivos. Riscos estão associados aos objetivos e estratégias dentro de um contexto definido (contexto interno, contexto externo e contexto de gestão de riscos). A melhor forma de identificar riscos é relacioná-los a eventos que podem ocorrer e que podem interferir na habilidade da organização em atingir seus objetivos.

Existem diversas ferramentas e técnicas para identificar riscos, muitas das quais estão descritas na NBR ISO 31010. Cada organização deve selecionar as ferramentas mais adequadas para identificar os riscos de acordo com sua capacidade e maturidade na gestão de riscos e, de acordo com a natureza dos riscos enfrentados.

A identificação dos riscos deve indicar as fontes de risco (incerteza que provoca o risco), objetivos impactados, eventos de riscos e suas causas e consequências.

A identificação dos riscos deve ser a mais ampla possível, visto que riscos não identificados não são tratados nem acompanhados.

A identificação de riscos pode ser um processo simples, conduzido pelo diretor de riscos. O processo envolve discussões com indivíduos chaves (internos e externos), incluindo pessoas com profundo conhecimento do negócio (executivos e gerentes, atores externos, clientes e especialista). As discussões podem ser em forma de entrevistas estruturadas ou semiestruturadas, workshops direcionados ou brainstorming. O diretor de riscos deve atualizar os participantes sobre informações relevantes de interesse para a identificação dos riscos. O apoio de consultorias especializadas, também, não deve ser descartado.

As principais ferramentas empregadas nesta fase são:

- Listas de verificação baseadas em fontes potencias de riscos.

- Registros históricos de riscos identificados previamente ou falhas ocorridas no passado.
- Avaliação de evidências com base em dados históricos.
- Brainstorming.
- Abordagem baseadas em equipes de especialistas.
- Técnica de construção de cenários de riscos.
- Técnicas específicas.
- Auditorias e inspeções físicas.

A identificação dos riscos deve considerar, também, os riscos que surgem durante o processo de planejamento e revisão da estratégia.

A identificação dos riscos deve ser também, um processo contínuo para confirmar a validade dos riscos previamente avaliados e identificar novos riscos que aparecem durantes as atividades diárias da organização, incluindo os registros de acidentes, reclamações, denúncias, desvios em relação às normas específicas, investigações, auditorias internas e externas, ou simplesmente durante as rotinas de trabalho.

Cada uma das técnicas de identificação de riscos tem suas limitações. Técnicas baseadas em experiência e registros históricos devem ser consideradas com ressalvas para riscos associados a processos pouco conhecidos, novos sistemas ou implementação de novas políticas, programas e projetos. Independentemente do método e da técnica utilizada, é importante que a identificação dos riscos seja integrada à estratégica, ao negócio e às operações.

Um aspecto importante nesta fase é a documentação dos riscos identificados e do processo de identificação, bem como, dos atores (stakeholders) envolvidos no processo. Os riscos devem ser descritos e documentados de forma que as pessoas que não participaram do processo de identificação possam entendê-los. A identificação deve indicar pelo menos: (1) as fontes dos riscos, (2) o evento e (2) os impactos relevantes nos objetivos da organização. Em geral, os riscos possuem diversas causas e diversas consequências e, neste caso, deve ser avaliada a melhor forma de descrevê-los, se por combinação das causas e consequências se por identificação em separado.

Após a identificação, os riscos devem ser organizados pela tipologia, pelos objetivos afetados ou ambos.

7.3 Análise dos Riscos

Análise dos riscos é um processo para ampliar o entendimento da natureza dos riscos e do nível de riscos que a organização enfrenta, com o propósito de decidir quais riscos necessitam de tratamento. A análise de riscos deve ser toda documentada, permitindo revisões e auditorias futuras.

A análise de riscos consiste no estabelecimento da valoração de cada risco com base nos critérios definidos no contexto de gestão de riscos. A análise deve ser iniciada com uma abordagem qualitativa, seguida por uma abordagem quantitativa para riscos mais significativos, quando for o caso.

A abordagem qualitativa consiste em analisar cada risco de acordo com sua descrição e enquadrá-lo em réguas de avaliação (probabilidade, impacto, vulnerabilidade, velocidade de propagação e exposição) pré-definidas.

A abordagem qualitativa é fácil de ser aplicada e pode ser utilizada para valoração de riscos com impactos intangíveis, tais como saúde e reputação e em geral apresenta resultados sem imprecisões significativas. Por outro lado, não permite avaliar a iteração entre os riscos e tem pouco poder discricionário, dificultando avaliações do tipo custo x benefício.

Técnicas qualitativas incluem workshops interfuncionais, pesquisas, benchmarking e analise de cenários qualitativos.

A abordagem quantitativa, por outro lado, requer valores numéricos, tanto para avaliara a probabilidade de ocorrência quanto para os impactos. A precisão da análise

quantitativa depende da precisão e da complementariedade dos dados numéricos disponíveis e da validade dos modelos utilizados.

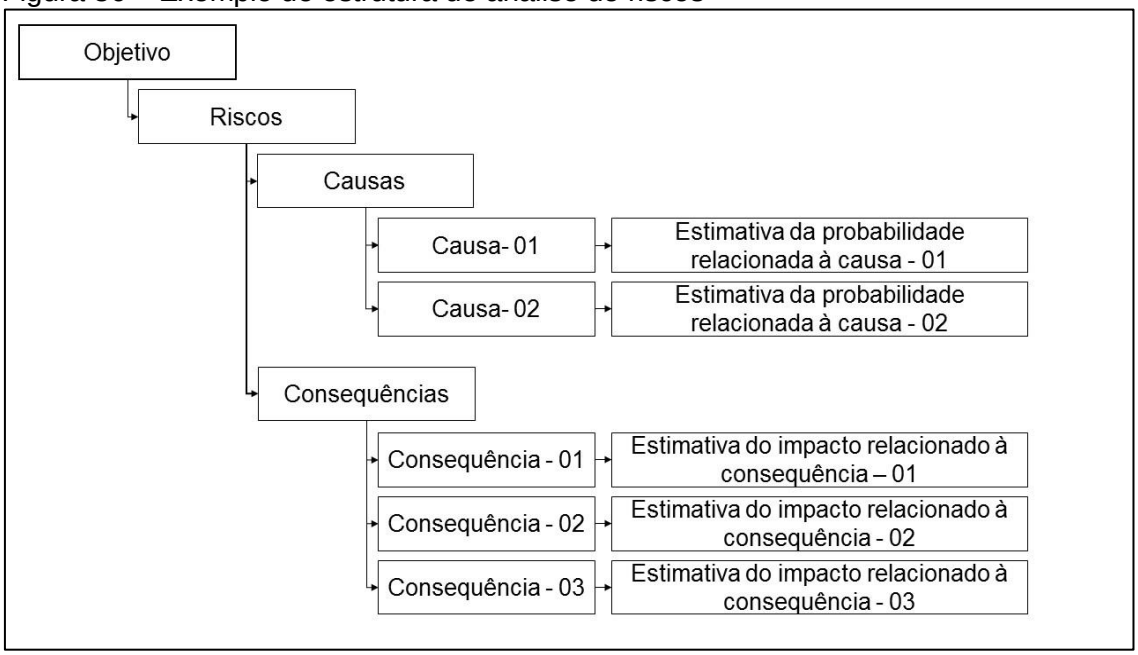
A abordagem quantitativa tem maior poder discriminatório, permite a avaliação de iteração entre riscos, permite avaliações tipo custo x benefício e alocação de capital com base em riscos. Por outro lado, é mais complexa, requer tempo e custo para sua realização, principalmente quando requer desenvolvimento e validação de modelos específicos. Um fator relevante na abordagem quantitativa é que o resultado pode apresentar imprecisões significativas quando os dados de entrada apresentam grande incerteza.

Técnicas quantitativas incluem estimativas de distribuições futuras (aderência) modelos econométricos simulações e análise de cenários probabilísticos.

A análise dos riscos envolve a definição das probabilidades de ocorrência de cada evento de risco e o impacto de suas consequências sobre os objetivos da organização. A probabilidade de ocorrência de um evento de risco está associada às causas do evento. O impacto sobre a organização está associado às consequências do evento de risco (Figura 36).

Um evento de riscos pode estar relacionado a diversas causas e sua ocorrência ter diversas consequências. Cada consequência pode ter um nível de impacto diferente na organização, assim como cada causa gerar uma probabilidade diferente de ocorrência do risco. Neste caso existem algumas abordagens que podem ser utilizadas. Uma possível solução é considerar a consequência de mais alto valor e utilizar a probabilidade associada a esta consequência, nas condições de riscos inerente e residual. Em casos específicos podemos considerar conjunto de causas que podem agir de forma conjunta e o efeito cumulativo de consequências, contudo este é um complicador que somente deve ser utilizado em riscos específicos. Em qualquer caso, caso existem incertezas sobre o nível de risco, estas devem ser identificadas e documentadas.

Figura 36 – Exemplo de estrutura de análise de riscos



Fonte: Elaborado pelo Autor

A análise de riscos deve identificar, também, os controles existentes que reduzem a probabilidade de ocorrência do evento de risco ou previnem suas consequências, em caso de riscos negativos, ou maximizam as consequências e alavancam a probabilidade de ocorrência, em caso de riscos positivos. Na identificação dos controles devem, também, estar indicada sua efetividade.

As probabilidades e os impactos dos eventos de risco devem ser estimados e combinados para a definição do nível de cada risco, de acordo com a matriz de riscos e o apetite aos riscos definido no contexto.

A efetividade da gestão de riscos é dependente de uma análise correta. Mesmo que a organização tenha um processo de gestão de riscos bem projetado, métodos e ferramentas para gestão de riscos, a análise de riscos é em última análise, a uma atividade dependente de um julgamento subjetivo.

7.4 Avaliação e Priorização

O propósito da avaliação dos riscos e determinar o nível dos riscos, tanto do ponto de vista individual quanto em comparação com os demais (avaliação relativa) e, desta forma priorizar os maiores riscos positivos e negativos e gerenciá-los dentro dos limites estabelecidos evitando, de um lado, assumir riscos superiores à capacidade da organização e de outro, perder oportunidades potenciais.

A avaliação dos riscos deve ser um portfólio dos principais riscos enfrentados pela organização. O portfólio, também chamado de perfil de riscos, deve considerar quando for o caso, além dos aspectos principais: probabilidade e impacto, os de vulnerabilidade e velocidade de progressão.

O portfólio dos riscos enfrentados pela organização deve ser documentado para permitir o passo seguinte que é a comunicação às partes interessadas e a elaboração do plano de tratamento de riscos.

A avaliação dos riscos deve ser efetuada em dois passos. O primeiro passo é ordenar os riscos segundo dois ou mais aspectos, sendo o mais usual, o emprego de uma matriz probabilidade x impacto. Os níveis de riscos são designados pelas áreas de cruzamento entre a probabilidade e o impacto, como por exemplo: extremo, muito alto, alto e baixo. As fronteiras entre os níveis variam de acordo com o apetite aos riscos. Uma organização com grande apetite aos riscos tem as fronteiras deslocadas para a direita. Algumas organizações podem definir fronteiras assimétricas, colocando maior ênfase na probabilidade ou no impacto (Figura 37).

O segundo passo é o refinamento da avaliação inicial com a inclusão de outros aspectos que podem incluir o emprego de matriz de impacto x vulnerabilidade, velocidade de propagação e disparidade (gap) entre a situação atual (risco residual) e desejada (nível desejado).

Algumas organizações consideram, ainda, a priorização dos riscos dentro de um mesmo grupo pelo tipo de consequência, como por exemplo: dentro do grupo de riscos avaliados como muito alto, considerar prioritários os riscos com impactos em saúde, segurança e reputação em detrimento dos riscos com que apresenta apenas impactos financeiros significativos.

Para riscos específicos que envolvam ganhos e perdas financeiras, é possível agregar as distribuições de probabilidades individuais em uma única distribuição ou empregar técnicas de simulação quantitativas que reflitam o portfólio como um todo. Os modelos de agregação variam significativamente de organização para organização, mesmo na indústria de serviços financeiros. Na agregação de riscos em modelos quantitativos é muito importante incluir os parâmetros de validade, pelo menos o horizonte tempo, a margem de erro e o nível de certeza.

A organização deverá definir quais são os níveis de riscos considerados aceitáveis para cada um dos objetivos atingidos.

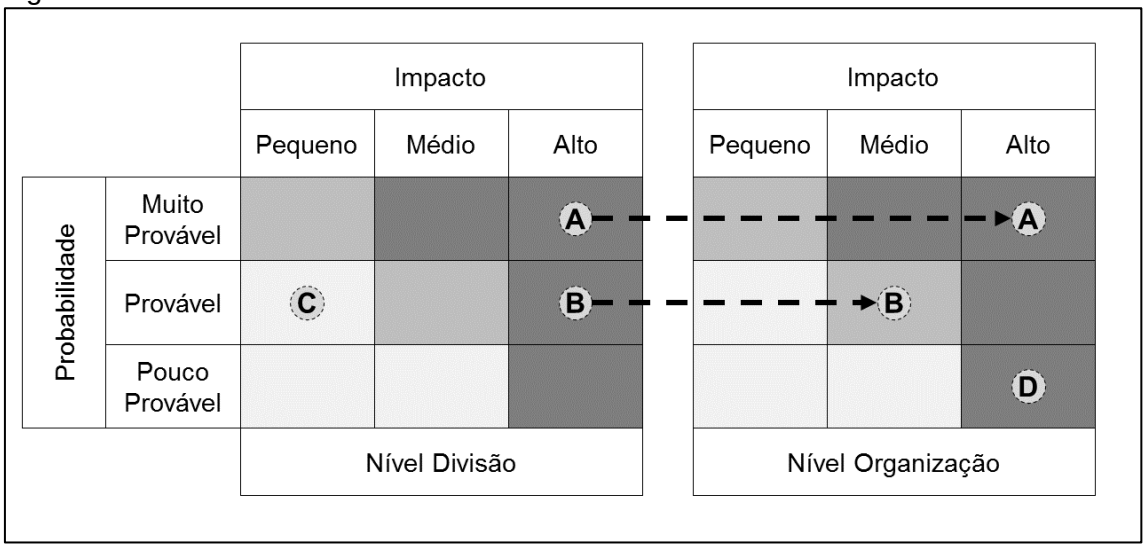
Figura 37 – Exemplo de matriz probabilidade x impacto

Probabilidade	Consequência				
	Impacto Insignificante	Impacto Pequeno	Impacto Moderado	Impacto Grande	Impacto Catastrófico
Quase Certa	Baixo	Médio	(2) Médio	Alto	Alto
Muito Provável	Baixo	Médio	Médio	Alto	(1) Alto
Provável	Baixo	Baixo	Médio	Médio	Alto
Pouco Provável	Baixo	(3) Baixo	Médio	Médio	Alto
Improvável	Baixo	Baixo	Baixo	Médio	Alto

Fonte: Elaborado pelo autor

A avaliação de riscos deve ser desdobrada por toda a organização, empregando o mesmo modelo, de forma que os riscos, enfrentados por unidades especificas, possam ser comparados e priorizados. Em geral, a avaliação dos riscos do ponto de vista de uma unidade, quando comparados com o ponto de vista da organização, podem sofrer alterações no impacto, não na probabilidade (Figura 38).

Figura 38 - Desdobramento dos níveis de riscos.



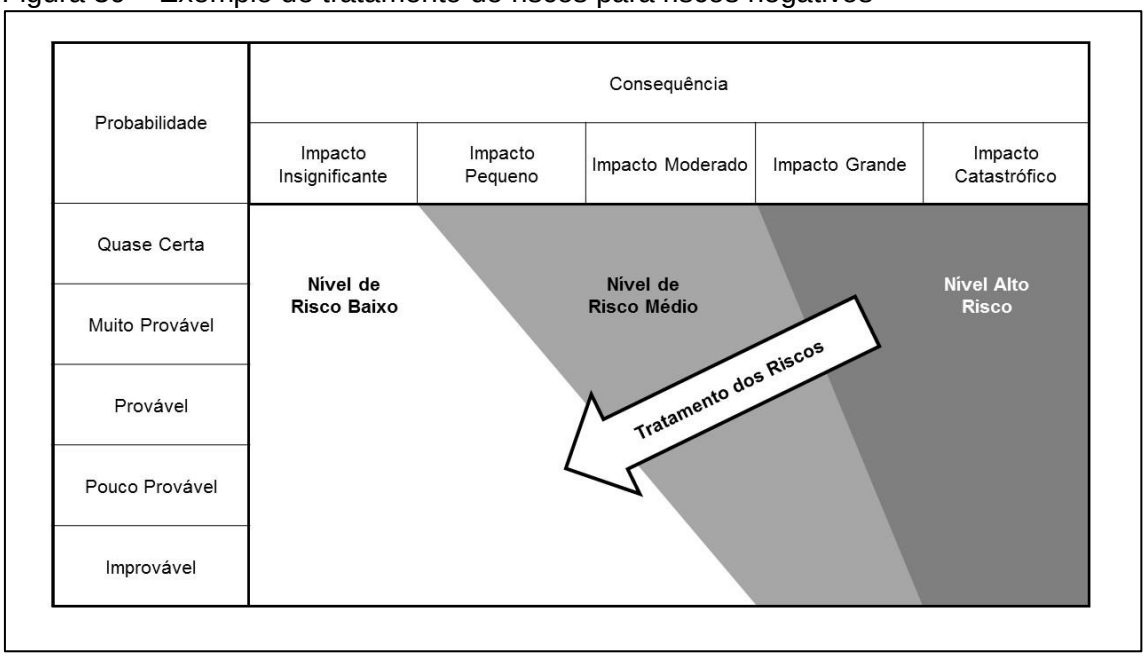
Fonte: Adaptado de NEW SOUTH WALES, 2012

7.5 Tratamento

O resultado do processo de avaliação dos riscos serve como subsídio primário para a avaliação das opções de tratamento, análise de custo e benefício, elaboração dos planos de tratamento de riscos e formulação das estratégicas de gestão.

O tratamento dos riscos envolve a definição das medidas de tratamento que são adequadas para cada risco. Em geral as opções são: (1) aceitar, (2) reduzir, (3) compartilhar e (4) evitar. O propósito do tratamento dos riscos é adequar os níveis para a situação desejada conforme mostrado na figura 39 no caso de riscos negativos.

Figura 39 – Exemplo de tratamento de riscos para riscos negativos



Fonte: Elaborado pelo autor

Em se tratando de riscos negativos, as opções de tratamento devem ser adequadas à natureza dos riscos.

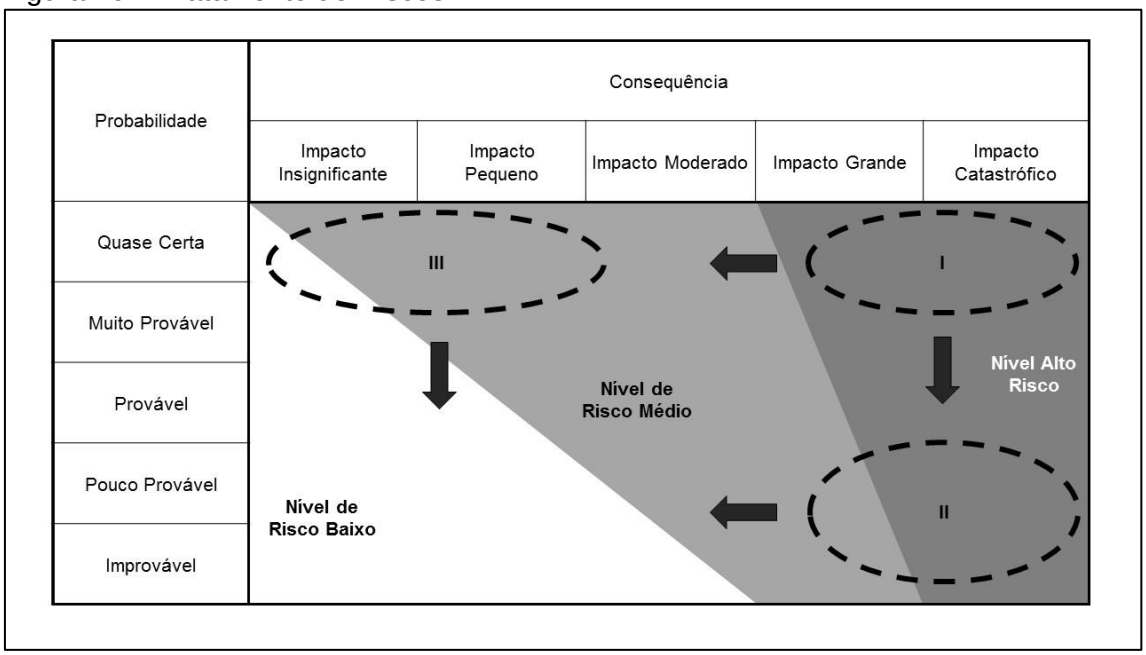
Na matriz de probabilidade X impacto, podemos considerar três tipos básicos de tratamento de acordo com o posicionamento do risco na matriz (Figura 40)

Os riscos na área I deverão ser tratados com a redução de sua probabilidade de ocorrência e seu impacto.

Os riscos na área II possuem baixa probabilidade de ocorrência e alto impacto. O tratamento mais adequado é a definição de planos de contingência, o que acarreta a redução do seu impacto.

Os riscos na área III são de baixo impacto e elevada probabilidade de ocorrência. Em geral, são riscos que podem ser tratados com melhoria de processo e procedimentos. Esta área geralmente recebe uma grande atenção do gerenciamento pela ocorrência frequente desses eventos e pode resultar em uma alocação de recursos excessiva.

Figura 40 – Tratamento de Riscos



Fonte: Elaborado pelo autor

Em geral as opções de tratamento dos riscos envolvem ações no sentido de:

- Evitar o risco
- Alterar as probabilidades dos eventos de risco
- Alterar as consequências dos eventos de risco
- Compartilhar riscos
- Reter riscos

7.6 Monitoramento

O monitoramento dos riscos tem como objetivos assegurar que esses estejam nos níveis residuais definidos.

Alterações nos níveis de riscos podem estar relacionadas com alterações nas probabilidades de ocorrência dos eventos potencias de riscos, alteração nos impactos e alterações na efetividade dos controles.

Alterações na probabilidade de ocorrência dos riscos ou nos impactos devem ser monitoradas por Indicadores Chaves de Riscos, os Key Risk Indicators (KRI). Os KPIs devem ser desenvolvidos em função da natureza dos riscos.

7.7 Comunicação e consulta

A comunicação e a consulta são atividades essenciais no processo de gestão de riscos. A efetividade do gerenciamento de riscos depende, entre outros aspectos de envolver as partes interessadas, assegurando que entendam a gestão de riscos, se envolvam e contribuam no processo.

Comunicação é a troca de informações e pontos de vistas. Deve ser um processo multidimensional, onde ideias e perspectivas são trocadas entre áreas funcionais sem barreiras hierárquicas.

Consulta é o processo de utilizar a comunicação para a tomada de decisão. A consulta não é um resultado, ou um fim em si mesma. Consulta é um meio de se obter um resultado. A consulta permite às partes interessadas a oportunidade de influenciar decisões, contudo não é um processo de tomada de decisão conjunta. O propósito da

consulta é receber informações úteis e avaliar todos os pontos de vista relevantes na identificação e avaliação dos riscos.

No processo de consulta, a organização deve considerar quais itens são adequados ao processo de consulta e quais devem ser tratados com sigilo.

Figura 41 – Comunicação e consulta

<table>
<tr><td></td><td></td><td colspan="4">Interesse do ator pelo objetivo</td></tr>
<tr><td></td><td></td><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td rowspan="4">Influência do ator no objetivo</td><td>4</td><td colspan="2">Fornecer Informação</td><td colspan="2">Dialogar</td></tr>
<tr><td>3</td><td colspan="2">Atores com alto grau de influência e que sofrem pouco impacto. Importantes para divulgação. Devem receber a informação correta.</td><td colspan="2">Atores com alto grau de influência e fortemente impactados. São importantes no suporte da instituição. Devem compreender detalhadamente os riscos e a forma como estão sendo tratados.</td></tr>
<tr><td>2</td><td colspan="2">Coletar Informações</td><td colspan="2">Consultar</td></tr>
<tr><td>1</td><td colspan="2">Atores com pouca influência e que sofrem pouco impacto. São importantes como fonte de informação para o processo decisório</td><td colspan="2">Atores com pouca influência e fortemente impactados. São, em geral, os que recebem ou que acessam os serviços. São importantes para que se possam compreender suas necessidades e suas percepções</td></tr>
</table>

Fonte: Adaptado de NEW SOUTH WALES, 2012

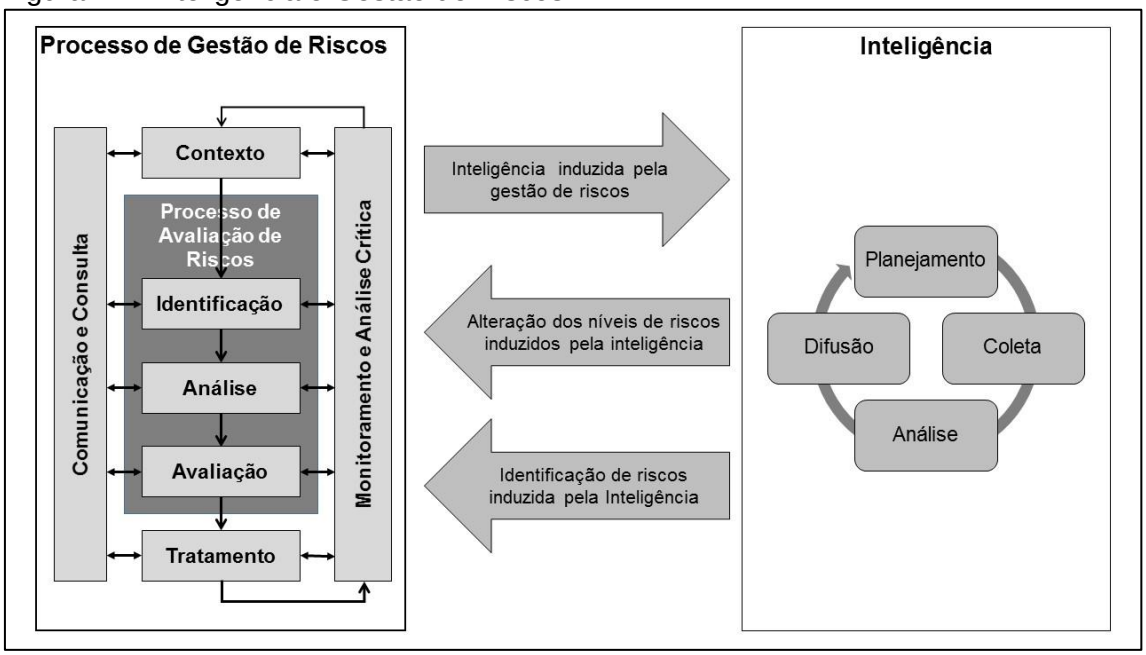
8 O Papel da Inteligência

Inteligência, genericamente, é o produto tangível resultante da submissão a um processamento de duas ou mais informações ou inteligência básica disponível sobre o contexto organizacional, para apoiar um processo de decisão específico.

A atividade de inteligência deve estar orientada para o apoio de decisões que permitam atuar em tempo real frente às ameaças e oportunidade que se apresentam (capacidade de reação e disponibilidade e robustez antecipativa), bem como atuar em situações proativas (capacidade de antecipação).

A inteligência é uma ferramenta relevante no monitoramento dos indicadores chaves e risco (KRIs) e na identificação de novos riscos de fonte externa. Conforme mostrado na figura 42, a inteligência tanto é induzida pelo processo de gestão de riscos em função da necessidade de monitorar os indicadores chaves de riscos como é indutora do processo na identificação de riscos.

Figura 42 - Inteligência e Gestão de Riscos

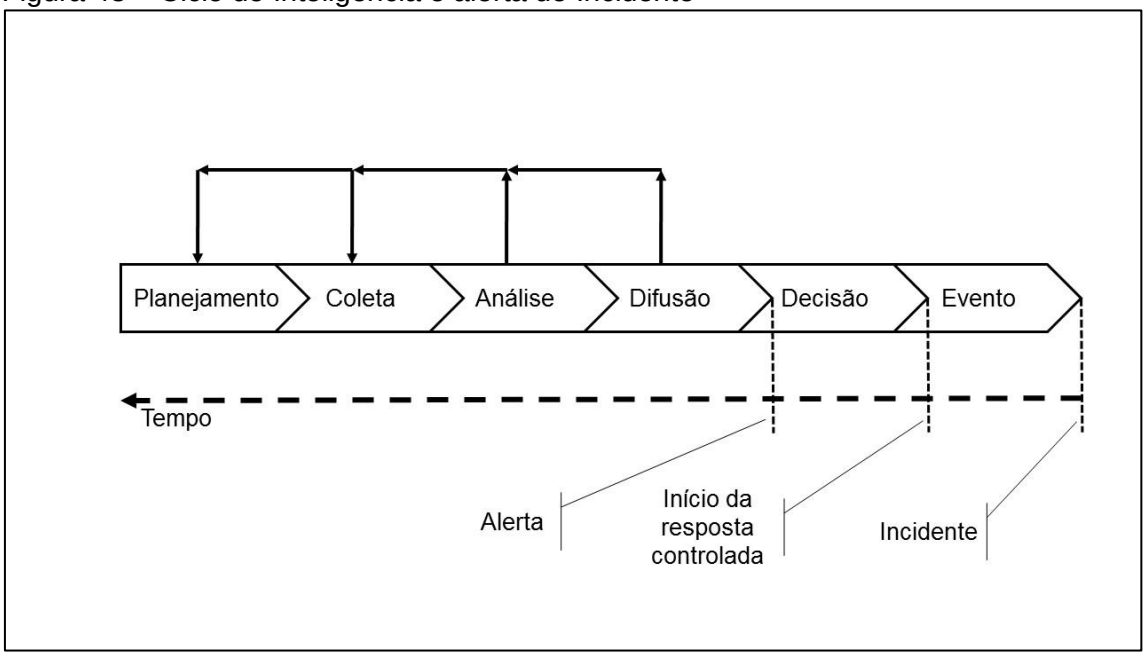


Fonte: Elaborado pelo autor

.

Para eventos de baixa probabilidade e alto impacto, em que a fonte potencial do risco é externa à organização, a inteligência é fundamental no fornecimento de alertas de antecipação. Neste caso, o ciclo básico de inteligência deve considerar o tempo para acionamento do plano de contingência previsto (Figura 43).

Figura 43 – Ciclo de Inteligência e alerta de Incidente



Fonte: Elaborado pelo autor

9 Protocolos e documentos

Dentre os relatórios que devem ser produzidos pela atividade de gestão de riscos incluem a exposições individuais (por unidade operacional) e agregadas (Apetite por Risco da organização), a adequação dos processos, controles e metodologias utilizados pelas Gerências Operacionais no gerenciamento de riscos e a adequação da Estrutura de Gerenciamento de Riscos da organização, especialmente diante de mudanças no Perfil de Risco ou nos cenários interno e externo.

Quando for determinado o nível com que o gestor de riscos produz seus relatórios, deve-se considerar a habilidade com que ele produz relatórios “francos e honestos”, alertando para riscos e como eles estão sendo gerenciados.

Figura 44 – Registro de riscos

Relatório de Avaliação de Riscos			
Número	Nome	Descrição	
Objetivos afetados	Responsável	Partes Interessadas	
Pior caso			
Probabilidade	Consequência	Nível	
Situação atual			
Probabilidade	Consequência	Nível	
Controle	Descrição		Efetividade do controle
Risco residual			
Probabilidade	Consequência	Nível	
Tratamento	Recurso Necessário	Responsável	Cronograma de Implementação
Monitoramento			
Comunicação e consulta			
Comentários			
Responsável	Setor	Data	Data da próxima revisão

Fonte: Adaptado de NEW SOUTH WALES,2012

10 Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). Gestão de riscos - Princípios e diretrizes. ABNT NBR ISO 31000:2009. Rio de Janeiro, 2009

_____. Gestão de riscos - Vocabulário. ABNT ISO GUIA 73:2009. Rio de Janeiro, 2009b

_____. Gestão de riscos — Técnicas para o processo de avaliação de riscos. ABNT NBR ISO/IEC 31010:2012. Rio de Janeiro, 2012.

ASSOCIATION OF BUSINESS PROCESS MANAGEMENT PROFESSIONAL (ABPMP). Guia para a gerenciamento de processos de negócios. CBOK v. 3. 2013

AUSTRALIAN NATIONAL AUDIT OFFICE (ANAO). Sector Governance. Strengthening performance through good governance. Barton, 2014.

AUSTRALIAN/NEW ZEALAND STANDARD (AS/NZS). Risk Management – Principles and guidelines. AS/NZS 4360:2004. Sydney, 2004

Berger G. A atitude prospectiva. Tradução de Kneipp N. Parcerias estratégicas, v. 19, pp. 311-8, 2004.

BERNSTEIN, P. L. Desafio aos deuses. Rio de Janeiro: Campus, 1997.

BRASIL. Guia de orientação para o gerenciamento de riscos versão 1.0 final. Brasília, 2013.

BRASIL. Instrução Normativa Conjunta CGU/MP Nº 001, DE 10.05.2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Brasília, 2016.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Internal Control – Integrated Framework. USA, 1992.

_____. Enterprise Risk Management -- Integrated Framework. Jersey City, 2004.

_____. Controle Interno - Estrutura Integrada. Jersey City, 2013.

COURTNEY, H. Previsão 20/20. São Paulo: Cultrix, 2001.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). Gerenciamento de riscos corporativos: uma análise das diretrizes e das práticas. 2015.

FRANCO F. L. Prospectiva estratégica: uma metodologia para a construção do futuro. 2007. 167p. Tese (Doutorado em Engenharia de Produção). COPPE/UFRJ, 2007.

FALCONI, V. O verdadeiro poder. Nova Lima: Falconi, 2009

FRANCO, F. L, et.al. Strategic alliances: Tools for constructing the future. Business Strategy Series v. 12 n. 2, 2011.

FEDERATION OF EUROPEAN RISK MANAGEMENT ASSOCIATIONS (FERMA). Adaptação da Guidance on the 8th EU Company Law Directive da ECIIA/FERMA. Brussels, Belgium, 2011.

GORDON, T. J. The Delphi Method. Futures Research Methodology, V 2.0. AC/UNU Millennium Project, 1994.

HERRING, J., KALB, C. Selecting the Right Competitive Intelligence Organizational Model. Competitive Intelligence, v.15, n. 1, 2012.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). Guia de orientação para o gerenciamento de riscos corporativos - São Paulo, SP, 2007.

_____. Principais modelos. Disponível em <http://www.ibgc.org.br/inter.php?id=18167>. Acessado em 19 de agosto de 2016.

THE INSTITUTE OF INTERNAL AUDITORS (IIA). IIA Position paper: The role of internal auditing in enterprise-wide risk management. USA, 2009.

_____. Internacional standards for the professional practice of internal auditing (standards). USA, 2012.

INTERNATIONAL FEDERATION OF ACCOUNTANTS (IFAC). From Bolt-On To Built-In: Managing Risk as an Integral Part of Managing an Organization. New York, 2015

INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS (INTOSAI). Guidelines for Internal Control Standards for the Public Sector, Vienna, Austria, 2004.

KAPLAN R. S, NORTON, D. P. A Execução Premium. Rio de Janeiro: Elsevier, 2008.
KAPLAN R. S. Conceptual Foundations of the Balanced Scorecard, Working Paper. Harvard Business School. Boston: Harvard University, 2010.
KNIGHT F. H. Risk, uncertainty and profit. New York: Houghton Mifflin Company, 1921.
KNIGHT F. H. Risk, uncertainty and profit. New York: Sentry, I964.
LE GOFF, J. As raízes medievais da Europa. Petrópolis, Vozes, 2011.
MARCIAL, E. C. & GRUMBACH, R. J. S. Cenários prospectivos: como construir um futuro melhor. 5 ed. Rio de Janeiro: FGV, 2008.
MORAIS, N. Notas de aula. Goiânia, 2016.
NEW SOUTH WALES. Risk management toolkit. Sidney, 2012
SANTANA, A. Notas de aula. Goiânia, 2011.
TRIBUNAL DE CONTAS DE UNIÃO (TCU). Critérios Gerais de Controle Interno na Administração Pública, Brasília, 2009.
_____. Levantamento de auditoria. Elaboração de indicador para medir o grau de maturidade de entidades públicas na gestão de riscos. Brasília, 2012.
_____. Referencial básico de governança aplicável a órgãos e entidades da administração pública. Brasília, 2014 a.
_____. TC 020.830/2014-9. Governança pública em âmbito nacional. Brasília, 2014 b.
_____. União Acórdão nº 1273/2015 – TCU – Plenário. Situação da governança pública em âmbito nacional - esferas federal, estadual, distrital e municipal. Brasília, 2015.
_____. Critérios Gerais de Controle Interno na Administração Pública, Brasília, 2009.
UNITED KINGDOM - HM TREASURY. The Orange Book Management of Risk - Principles and Concepts. Norwich, 2004.
_____. Risk Management Assessment Framework: a tool for departments. Norwich, 2009.
UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (GAO), Standards for Internal Control in the Federal Government, USA, 2014.