COMPANHIA ENERGÉTICA DE BRASÍLIA

SEDE: Setor de Indústria e Abastecimento - SIA, Área de Serviços Públicos, l
Brasília/DF - CEP: 71.215-100 Telefones (61) 3465-9300
CNPJ nº 00.070.698/0001-11 Inscrição Estadual 07.300.027/001-11
Internet: http://www.ceb.com.br

MANUAL DE GESTÃO DE RISCOS

VERSÃO 2018

Texto em vigor aprovado pela Resolução de Diretoria nº 093, de 12.12.2018.

MANUAL DE GESTÃO DE RISCOS

COMPANHIA ENERGÉTICA DE BRASÍLIA – CEB

SUMÁRIO

1. INTRODUÇÃO

O objetivo deste Manual é orientar os gestores no processo de identificação, avaliação, resposta, monitoramento e comunicação dos riscos nas atividades da Companhia, especificando a abordagem, os componentes de gestão e os recursos para gerenciá-los.

A Política de Gestão de Riscos da CEB prevê que a responsabilidade pela elaboração do respectivo Manual é da Diretoria de Planejamento e Gestão de Riscos.

Nesse contexto, o Manual foi elaborado com requisitos mínimos, considerando as necessidades e as características da CEB. Cabe ressaltar a importância da melhoria contínua e sua adequação, a suficiência e a eficácia da estrutura de gestão de riscos para assegurar os aprimoramentos do processo e da metodologia adotada.

Este Manual poderá ser utilizado na Companhia e em suas subsidiárias integrais e controladas que não possuam sua própria Política de Gestão de Riscos.

2. NORMAS E REGULAMENTAÇÕES RELACIONADAS

A Lei nº 13.303/2016, ao dispor sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios, estabelece:

> *Art. 9º A empresa pública e a sociedade de economia mista adotarão regras de estruturas e práticas de gestão de riscos e controle interno...;*
>
> *[..]inciso II - área responsável pela verificação de cumprimento de obrigações e de gestão de riscos;*
>
> *[...]VI - previsão de treinamento periódico, no mínimo anual, sobre Código de Conduta e Integridade, a empregados e administradores, e sobre a política de gestão de riscos, a administradores;*
>
> *[...] e § 2º - A área responsável pela verificação de cumprimento de obrigações e de gestão de riscos deverá ser vinculada ao diretor-presidente e liderada por diretor estatutário, devendo o estatuto social prever as atribuições da área, bem como estabelecer mecanismos que assegurem atuação independente.*

No âmbito do Distrito Federal essas determinações foram regulamentadas pelo Decreto nº 37.967/2017.

O Estatuto Social da CEB, versão 2018, com a alteração aprovada pela 96ª Assembleia Geral Extraordinária dos acionistas, de 20/06/2018, em seu Art. 19, atribui ao Conselho de Administração a competência de:

> *XXVII - implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a CEB, inclusive os relacionados à integridade das informações contábeis e financeiras e à ocorrência de corrupção e fraude.*

O Estatuto prevê, no Art. 31, ser competência do Diretor de Planejamento e de Gestão de Riscos:

> *XII - identificar, avaliar, tratar, monitorar e comunicar perdas operacionais evitáveis pela melhor gestão dos riscos inerentes aos principais processos das empresas controladas da CEB.*

Estabelece ainda, no Art. 32, que a Companhia disporá de áreas dedicadas à gestão de riscos e aos controles internos, vinculadas à Presidência e lideradas pela Diretoria de Planejamento e de Gestão de Riscos, conforme expresso a seguir:

> *§ 1° São atribuições da área responsável pela gestão de riscos, além de outras previstas na legislação própria, a identificação, avaliação, controle, mitigação e monitoramento de riscos a que estão sujeitos os negócios e processos da CEB, com independência de atuação;*
>
> *§ 2° São atribuições da área responsável pelos controles internos, além de outras previstas na legislação própria, a avaliação e o monitoramento da eficácia dos controles internos e do estado de conformidade corporativo;*
>
> *§ 3° A área responsável pelo processo de controles internos deverá se reportar diretamente ao Conselho de Administração em situações em que se suspeite do envolvimento do Diretor-Presidente em irregularidades ou quando um membro se furtar à obrigação de adotar medidas necessárias em relação à situação de irregularidade a ele relatada;*
>
> *§ 4° As funções das áreas dedicadas à gestão de risco e aos controles internos mencionadas no caput deste artigo poderão abranger as subsidiárias da CEB.*

Adicionalmente, o documento que apresenta os Planos de Avaliações de Desempenho e Treinamentos da CEB, prevê no item 3.2:

> *A CEB deverá prever treinamento periódico, no mínimo anual, sobre a Política de Gestão de Riscos aos colaboradores e administradores (§ 2º do art. 9º da Lei no 13.303/2016).*

Ainda nesse sentido, a Política de Gestão de Risco da Companhia, aprovada no dia 29 de junho de 2018, contempla:

Objetivo da Política de Gestão de Riscos da CEB

- Orientar os processos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos inerentes às atividades da CEB, incorporando a visão de riscos à tomada de decisões estratégicas, em conformidade com as regulamentações do Setor Elétrico e as melhores práticas de mercado

Conceitos	Os conceitos a serem utilizados para fins da Política
Diretrizes	As diretrizes definidas para a Gestão de Riscos
Princípios	Os principios a serem observados na Gestão de Riscos
Responsabilidades	Os responsáveis e Proprietários dos Riscos
Processo	As referências técnicas que serão adotadas para a Gestão de Riscos

Figura 1: Objetivo da Política de Gestão de Riscos da CEB.

A Política prevê como Diretriz, no item K:

> *Desenvolver o Método de Priorização de Processos com o objetivo de estabelecer prioridades e definir prazos para gerenciamento de riscos, cujo escopo são os processos organizacionais. A partir de um plano de atuação elaborado com base na Priorização de Processos, serão realizadas as etapas a seguir:*
>
> → *Análise de ambiente e de fixação de objetivos;*
> → *Identificação de eventos de riscos;*
> → *Avaliação de eventos de riscos e controles;*
> → *Resposta a riscos; e*
> → *Informação, comunicação e monitoramento.*

A Política define, também, os responsáveis e proprietários dos riscos:

Papeis e Responsabilidades na Gestão de Riscos

Área Responsável	Conselho de Administração	Conselho Fiscal	Comitê de Auditoria	Auditoria Interna	Consultoria Jurídica	Ouvidoria	Diretoria Executiva	Diretoria de Planejamento e Gestão de Riscos	Outros Gestores da CEB
Funções/Atividades									
Discutir e aprovar as questões estratégicas	CA								
Aprovar o nível de tolerância ao risco e papel das diretorias executivas no gerenciamento de riscos	CA								
Assessorar o CA nas responsabilidade de fixação de diretrizes e de controle superior da CEB, com atribuições específicas de análise, acompanhamento e recomendação sobre questões relacionadas à gestão de riscos			CAE						
Monitorar de forma direcionada os riscos de negócio das subsidiárias integrais e controladas da CEB, por meio de recomendações de ações de mitigação			CAE						
Deliberar sobre decisões estratégicas considerando as análises dos riscos relatadas pela Diretoria de Planejamento e Gestão de Riscos							DE		
Patrocinar a implantação da gestão de riscos nas empresas							DE		
Alocar recursos necessários ao processo e definir a infraestrutura apropriada às atividades de gerenciamento de risco							DE		
Aprovar normas específicas e o grau de apetite a riscos das empresas							DE		
Orientar e promover a aplicação das políticas de gestão de risco de acordo com a legislação vigente e em atendimento às diretrizes definidas								DPGR	
Implantar o gerenciamento de risco e conformidade de forma compartilhada, como foco no monitoramento do desempenho da CEB								DPGR	
Elaborar relatórios periódicos de suas atividades, submetendo-os ao Comitê de Auditoria Estatutário a cada 3 (três) meses ou quando solicitado								DGPR	
Avaliar, de forma sistemática, o processo de gerenciamento de riscos e recomendar melhorias				AI					
Conhecer os riscos mais significantes para a Companhia e monitorar se a Administração está tratando-os de forma adequada;		CF							
Orientar a Companhia em relação às normas aplicáveis e alterações legislativas pertinentes;					CJ				
Assegurar o envio à Diretoria de Planejamento e Gestão de Riscos das denúncias recebidas, respeitados os devidos parâmetros de classificação						OUV			
Coordenar, promover e acompanhar as ações de gestão de riscos na sua área de atuação, avaliando continuamente seus processos, analisando riscos envolvidos e garantindo a efetividade dos controles e conformidade dos processos									OGC
Atuar conforme os princípios de conduta e ética da Companhia									OGC
Desenvolver e aprimorar metodologias de seu processo de forma a potencializar a identificação, tratamento e monitoramento dos riscos específicos, em consonância com esta política, com as diretrizes e com as normas corporativas de gestão de riscos, em articulação com a Diretoria de Planejamento e Gestão de Riscos									OGC
Fornecer à Diretoria de Planejamento e Gestão de Riscos, sempre que demandado, todas as informações necessárias para a avaliação integrada dos riscos, o monitoramento e o reporte para a alta administração									OGC

Figura 2: Papeis e Responsabilidades.

Em suas disposições finais, a Política de Gestão de Riscos prevê que as subsidiárias integrais e controladas da CEB sem correspondente Política de Gestão de Riscos, deverão garantir que os princípios e diretrizes estabelecidos na Política de Gestão de Riscos da Companhia sejam seguidos.

Para a estruturação da Metodologia de Gestão de Riscos da CEB, foram utilizadas, além das regulamentações e normas mencionadas, as orientações do COSO ICIF – Gerenciamento de Riscos Corporativos Estrutura Integrada, as orientações divulgadas por meio da Norma ABNT NBR ISO 31000:2018 e outras boas práticas aplicáveis.

COSO[1]

De acordo com o COSO I, o controle interno auxilia a organização no atingimento de seus objetivos. Um sistema de controle interno eficaz exige a observância às políticas e aos procedimentos, conjugados ao julgamento da organização para determinar qual o nível de controle é suficiente.

Conjugada aos componentes do COSO I – Controle Interno, foi necessário obter inspirações no COSO II – Gerenciamento de Riscos Corporativos, no que se refere à:

→ Condução de um processo de gestão de riscos em uma organização, pelo conselho de administração, diretoria e demais empregados;
→ Aplicação no estabelecimento das estratégias formuladas para identificar, em toda a organização, eventos em potencial capazes de afetá-las; e
→ Administração dos riscos de modo a mantê-los compatíveis com o apetite a risco da organização e possibilitar a garantia razoável do cumprimento dos seus objetivos.

Para efeito deste Manual, foram considerados os componentes do COSO e as suas definições, a seguir:

Ambiente de Controle – Compreende os objetivos estratégicos vinculados ao conjunto de normas e processos e a estrutura para fornecer a base para a condução do controle interno por toda a organização, os quais são identificados e abordados:

→ Filosofia de gerenciamento de riscos;
→ Atribuição de autoridade e de responsabilidade;
→ Integridade e valores éticos;
→ Comprometimento da alta administração;
→ Objetivos estratégicos;
→ Objetivos correlatos (operacional, comunicação e conformidade); e
→ Apetite e tolerância a risco.

Avaliação de Riscos – Análise dos riscos relevantes para o alcance dos objetivos e metas da organização, com vistas a dar a resposta apropriada. Os riscos são analisados

[1] *Committee of Sponsoring Organizations of the Treadway Commission: é uma organização privada criada nos EUA em 1985 para prevenir e evitar fraudes nos procedimentos e processos internos das empresas.*

considerando a probabilidade e o impacto como base para determinar o modo pelo qual deverão ser geridos:

→ Identificar riscos de negócio relevantes para os objetivos da organização;

→ Estimar a significância dos riscos;

→ Avaliar a probabilidade de sua ocorrência; e

→ Decidir sobre ações em resposta a esses riscos.

Informação e Comunicação – A comunicação eficaz também ocorre em um sentido mais amplo, fluindo em todos os níveis da organização. As informações devem ser coletadas e comunicadas de forma coerente e tempestiva e todos os níveis de uma organização devem receber informações para identificar, avaliar e responder aos riscos:

→ Comunicação interna ou externa das informações necessárias para apoiar o funcionamento do controle interno, inclusive os objetivos;

→ Cumprimento das responsabilidades; e

→ Tomada de decisões tempestivas.

Atividades de Monitoramento – Atividades gerenciais contínuas ou avaliações independentes ou de ambas as formas. Verificar se os controles internos são adequados e eficientes, examinando:

→ Se os componentes estão presentes como planejado;

→ O alcance dos objetivos operacionais;

→ As informações dos relatórios e sistemas corporativos confiáveis (sistemas operacionais, de Informática, etc.); e

→ O cumprimento de leis, normas e regulamentos.

Norma ABNT[2] NBR ISO 31000:2018

De acordo com essa Norma, os princípios, demonstrados na Figura 3**,** fornecem orientações sobre as características da gestão de riscos eficaz e eficiente, comunicando seu valor e explicando sua intenção e propósito. Esses princípios são a base para gerenciar riscos e convém que sejam considerados quando se estabelecerem a estrutura e os processos de gestão de riscos da organização.

[2] *Associação Brasileira de Normas Técnicas: é o órgão responsável pela normalização técnica no Brasil, fornecendo insumos ao desenvolvimento tecnológico brasileiro. Trata-se de uma entidade privada e sem fins lucrativos e de utilidade pública, fundada em 1940.*

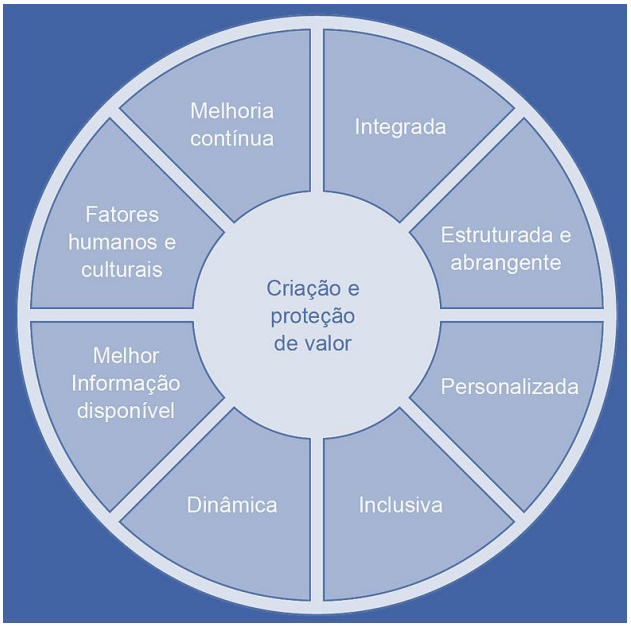


Figura 3: Princípios – ABNT 31000:2018.

Os princípios podem ser assim explicados:

Integrada – A gestão de riscos é parte integrante de todas as atividades organizacionais;

Estruturada e Abrangente – Uma abordagem estruturada e abrangente para a gestão de riscos contribui para resultados consistentes e comparáveis;

Personalizada – A estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos externo e interno da organização relacionados aos seus objetivos;

Inclusiva – O envolvimento apropriado e oportuno das partes envolvidas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada;

Dinâmica – Riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna;

Melhor Informação Disponível – As entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos, explicitamente, leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. Convém que a informação seja oportuna, clara e disponível para as partes envolvidas pertinentes;

Fatores Humanos e Culturais – O comportamento humano e a cultura influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio;

Melhoria Contínua – A gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

A eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão. Isto requer apoio das partes interessadas, em particular da Alta Direção.

A Norma registra que, ao conceber a estrutura para gerenciar riscos, convém que a organização examine e entenda seus contextos externo e interno:

Contexto Externo	Fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais, em âmbito internacional, nacional, regional ou local;
	Direcionadores-chave e tendências que afetem os objetivos da organização;
	Relacionamentos, percepções, valores, necessidades e expectativas das partes interessadas externas;
	Relações e compromissos contratuais;
	Complexidade das redes de relacionamento e dependências.

Figura 4: Contexto Externo ISO 31000:2018.

Contexto Interno	Visão, missão e valores;
	Governança, estrutura organizacional, papéis e responsabilizações;
	Estratégia, objetivos e políticas;
	Cultura da organização;
	Normas, diretrizes e modelos adotados pela organização;
	Capacidades entendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, propriedade intelectual, processos, sistemas e tecnologias);
	Dados, sistemas de informação e fluxos de informação;
	Relacionamentos com partes interessadas internas, levando em consideração suas percepções e valores;
	Relações contratuais e compromissos;
	Interdependências e interconexões.

Figura 5: Contexto Interno ISO 31000:2018.

De acordo com a Norma ABNT 31000:2008, o processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos (Figura 6).

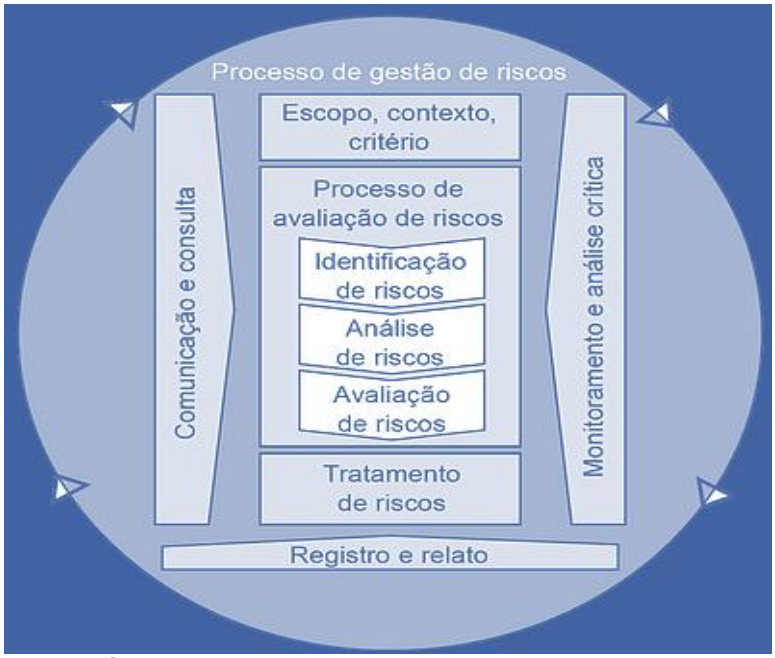


Figura 6: Processo – ISO 31000:2018.

O processo de avaliação de riscos é o processo global de identificação, análise e avaliação de riscos.

O propósito da **identificação de riscos** é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos. Informações pertinentes, apropriadas e atualizadas são importantes na identificação de riscos.

A finalidade da **análise de riscos** é compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. A análise de riscos envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos.

O intento da **avaliação de riscos** é apoiar decisões. A avaliação de riscos envolve a comparação dos resultados da análise de riscos com os critérios de riscos estabelecidos para determinar onde é necessária ação adicional. Isto pode levar a uma decisão de:

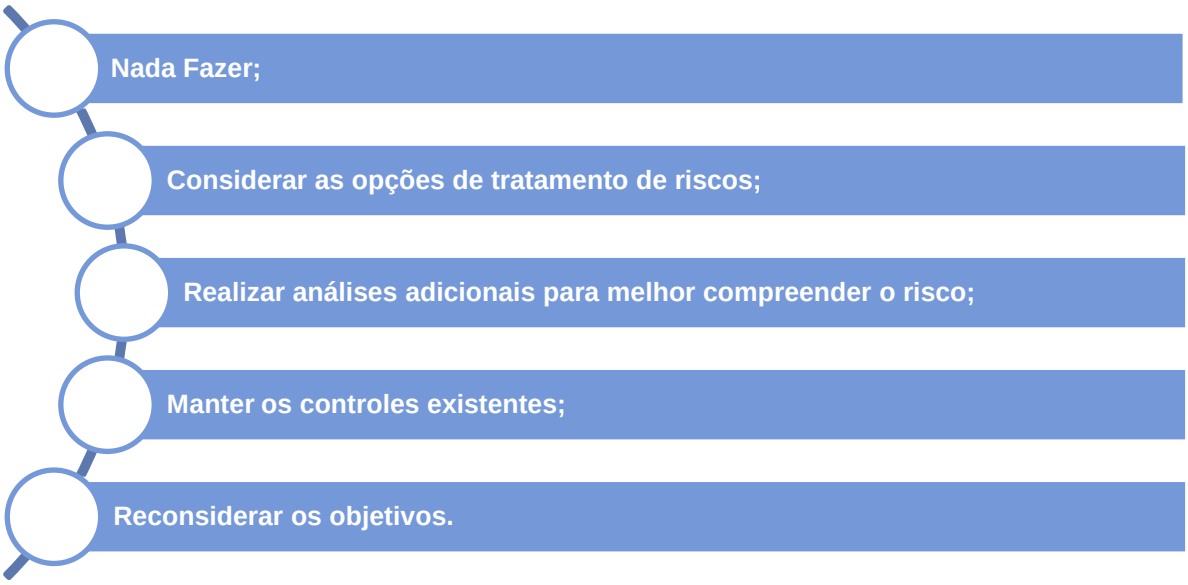


Figura 7: Processo – ISO 31000:2018.

O objetivo do **tratamento de riscos** é selecionar e implementar opções para abordar riscos.

Selecionar a (s) opção (es) mais apropriada (s) de tratamento de riscos envolve balancear os benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, ao esforço ou as desvantagens da implementação.

As opções para tratar o risco podem envolver uma ou mais das seguintes ações:

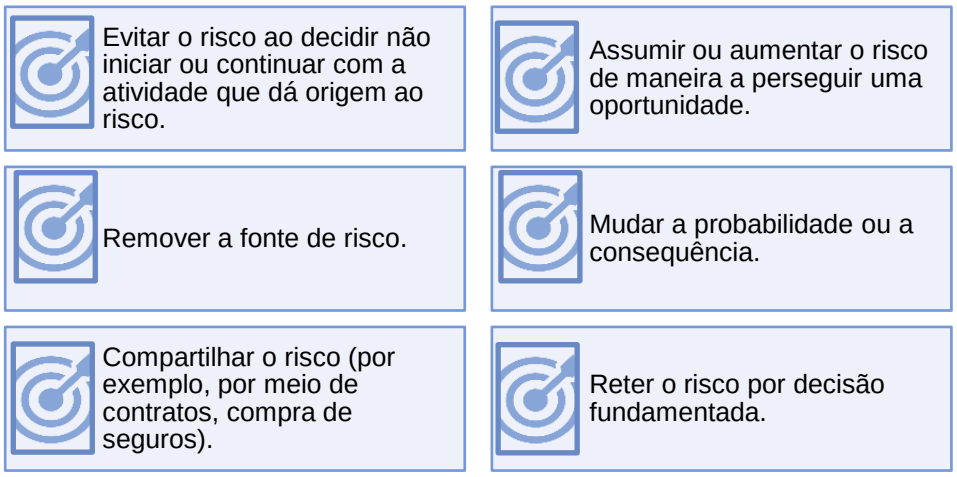


Figura 8: Processo – ISO 31000:2018.

As definições da figura 8 estão previstas na ISO 31000:2018; contudo, a CEB, em sua Política de Gestão de Riscos, adotou somente as tratativas: evitar, mitigar, compartilhar ou aceitar os riscos.

No momento de escolher uma dessas opções, é importante ter a perspicácia de que a justificativa para o tratamento de riscos é mais ampla do que apenas o aspecto econômico. Ademais, convém que se leve em consideração todas as obrigações da organização, compromissos voluntários da Companhia e pontos de vista das partes interessadas. A seleção de opções de tratamento de riscos deverá ser feita de acordo com os objetivos da organização, critérios de risco e recursos disponíveis.

Importante salientar que se não houver opções de tratamento disponíveis ou se as opções de tratamento não modificarem suficientemente o risco, este deverá ser registrado e mantido sob análise crítica contínua.

Contudo, após a escolha de uma das opções disponíveis, é necessário propor **planos de tratamento de riscos** que irão especificar como as opções de tratamento escolhidas serão implantadas de maneira que os arranjos sejam compreendidos pelos envolvidos, e o progresso em relação ao plano possa ser monitorado. O plano de tratamento deverá identificar claramente a ordem em que o tratamento de riscos será implementado.

O Plano de Tratamento deverá incluir, no mínimo:

→ Os responsáveis por aprovar, implantar e implementar o plano;
→ As ações propostas;

→ Os recursos requeridos, incluindo contingências;
→ As medidas de desempenho;
→ As restrições;
→ Os relatos e monitoramento requeridos; e
→ Quando se espera que ações sejam tomadas e concluídas.

A constituição desse plano proporcionará a companhia **monitoramento e análise crítica** dos riscos mapeados. A sua finalidade é assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo.

É salutar que esse ele inclua: planejamento, coleta e análise de informações; registro de resultados e fornecimento de retorno; e incorporados em todas as atividades de gestão de desempenho, medição e relatos da organização.

É necessário que o processo de gestão de riscos e seus resultados sejam documentados e relatados por meio de mecanismos apropriados.

O registro e o relato visam:
→ Comunicar atividades e resultados da gestão de riscos para toda a organização;
→ Fornecer informações para a tomada de decisão;
→ Melhorar as atividades de gestão de riscos; e
→ Auxiliar a interação com as partes envolvidas, incluindo aquelas com responsabilidade direta pelas atividades de gestão de riscos.

O relato é parte integrante da governança da organização. Deve apoiar a alta direção e os órgãos de supervisão a cumprirem suas responsabilidades.

Para a elaboração de um relato deve-se considerar:
→ As diferentes partes envolvidas e suas necessidades específicas de informação e requisitos;
→ O custo, a frequência e a pontualidade do relato;
→ O método de relato; e
→ A pertinência da informação para os objetivos organizacionais e para a tomada de decisão.

Dessa forma, para obter os melhores resultados no decorrer do trabalho de elaboração do Plano de Tratamento, são atributos desejáveis:

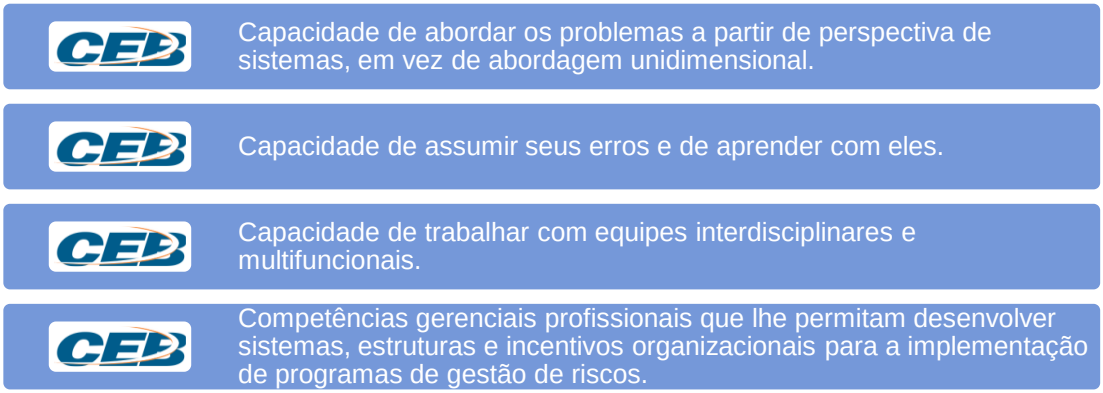


Figura 9: Atributos para Gerenciar Riscos.

3. DEFINIÇÕES E CONCEITOS

Para fins da Política da Gestão de Riscos, a CEB considerou os seguintes conceitos, aqui listados em ordem alfabética:

Área Proprietária de Risco (*Risk Owner*) – Unidade que possui autoridade e responsabilidade pelo gerenciamento do risco na sua área de atuação. O proprietário do risco também pode ser uma pessoa com a responsabilidade e a autoridade para gerenciar o risco;

Apetite a Risco – Grau de exposição aos riscos que a companhia está disposta a aceitar para atingir seus objetivos estratégicos e criar valor para os acionistas;

Evento (envolvendo risco) – Ocorrência ou alteração em circunstâncias relacionadas ao risco;

Fonte de Risco – Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco;

Gestão de Riscos – É o processo de organizar e planejar recursos humanos e materiais de uma companhia, de forma a monitorar seus impactos na organização. Para tanto, utiliza um conjunto de técnicas que direciona o tratamento aos riscos;

Ignorância – Eventos futuros que, no momento da análise, não poderão sequer ser identificados, muito menos quantificados;

Impacto – Efeito resultante da ocorrência do evento;

Incerteza – Evento futuro identificado, ao qual não é possível associar uma distribuição de probabilidade de ocorrência;

Manual de Gestão de Riscos – Documento estruturado e editado de gestão de riscos, especificando a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos;

Perfil de Risco – Descrição de um conjunto qualquer de riscos;

Política de Gestão de Risco Empresarial – Declaração das intenções e diretrizes gerais de uma companhia, relacionadas à gestão de riscos;

Processo de Gestão de Riscos – Aplicação sistemática da Política de Gestão de Risco na identificação, análise, avaliação, tratamento e monitoramento dos riscos;

Riscos – Evento futuro identificado, ao qual é possível associar uma probabilidade de ocorrência, que poderá impactar positivamente ou negativamente a imagem e o resultado de um empreendimento;

Riscos Empresariais – Riscos que devem ser monitorados pela companhia, dada a sua relevância e o interesse corporativo; e

Tolerância ao Risco – É o nível de variação aceitável quanto à realização dos seus objetivos.

Além dos conceitos registrados na Política de Gestão de Riscos da CEB, faz-se necessário apresentar alguns termos e definições que auxiliarão a compreensão e a aplicação da Metodologia de Gestão de Riscos, elaborada para suportar o mapeamento de risco da Companhia.

A seguir, os termos de definições constantes da Norma ABNT NBR ISO 31000:2018:

Consequência – Resultado de um evento que afeta os objetivos.

- → Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos, diretos ou indiretos, nos objetivos;
- → As consequências podem ser expressas qualitativa ou quantitativamente; e
- → Qualquer consequência pode se potencializar por meio de efeitos cascata e cumulativo.

Controle – Medida que mantém e/ou modifica o risco.

→ Controles incluem, mas não estão limitados a qualquer processo, política, dispositivo, prática, ou outras condições e/ou ações que mantêm e/ou modificam o risco; e
→ Controles nem sempre podem exercer o efeito modificador pretendido ou presumido.

Evento – Ocorrência ou mudança em um conjunto específico de circunstâncias.

→ Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas e várias consequências;
→ Um evento pode, também, ser algo que é esperado, mas não acontece, ou algo que não é esperado, mas acontece; e
→ Um evento pode ser uma fonte de risco.

Gestão de Riscos – Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

Parte Interessada – Pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.

Probabilidade – Chance de algo acontecer.

→ Na terminologia de gestão de riscos, a palavra “probabilidade” é utilizada para referir-se à chance de algo acontecer – não importando se definida, medida ou determinada, ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente – utilizando-se termos gerais ou matemáticos (como probabilidade ou frequência durante um determinado período de tempo).

Risco – Efeito da incerteza nos objetivos.

→ Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.

Matriz de Riscos – Gráfico que relaciona a probabilidade e o impacto de eventos de risco. Em geral, eventos de risco avaliados são representados por uma gradação na cor escolhida; tal gradação representa a decisão do apetite a risco da organização.

Identificar, categorizar e classificar corretamente os riscos facilita a integração e a consolidação da Gestão de Risco, além de auxiliar na comunicação com auditores, reguladores, agências de risco e outras partes interessadas.

A seguir, serão abordados, também, a natureza do risco (econômico-financeiro e não econômico-financeiro) e a categoria de riscos aprovadas pela Companhia.

Risco Econômico-financeiro[3] – Quando o risco está **diretamente** relacionado aos ativos e passivos monetários da organização.

Risco Não Econômico-financeiro – Quando o risco resulta de circunstâncias externas (fenômenos sociais, políticos ou econômicos) ou internas (recursos humanos, tecnologias, procedimentos e outros) à organização.

Figura 10: Natureza e Categoria de Riscos.

As categorias de risco a serem abordadas no manual estão abaixo descritas e definidas:

Categoria dos Riscos	Estratégico
	Negócio
	Legal/Conformidade (Regulatório)
	Reputação/Imagem
	Atuarial
	Fiscal
	Operacional
	Crédito
	Liquidez
	Mercado

Figura 11: Categoria dos Riscos.

[3] *A metodologia menciona os riscos Econômico-financeiros (crédito, liquidez e mercado), entretanto, não contempla a sua identificação, a avaliação e sua mensuração.*

Estratégico – Risco associado à possibilidade de perda resultante do insucesso das estratégias adotadas, levando-se em conta a dinâmica dos negócios (clientes, fornecedores e investimentos) e as alterações políticas e econômicas no País e fora dele, ou seja, qualquer incerteza que afeta a realização das diretrizes estratégicas.

Os riscos estratégicos contribuem para facilitar ou dificultar o alcance dos objetivos estratégicos da organização; logo, podem ter impactos positivos (oportunidades) ou negativos (ameaças) para a organização.

A identificação e a mensuração desses riscos ocorrem por meio de reuniões estruturadas com servidores envolvidos no processo de gestão estratégica, inclusive membros de Diretoria.

Negócio – Risco associado à possibilidade de incerteza inerente as projeções do resultado operacional, levando-se em conta a probabilidade de o volume de negócio não ser suficiente para fazer face aos custos. Está relacionado diretamente com o negócio da empresa e a correspondente estrutura de custos.

Legal/Conformidade (Regulatório) – Risco associado à possibilidade de violações ou do não cumprimento de leis, normas, regulamentos, contratos, códigos de conduta e integridade, políticas e normas internas ou princípios éticos.

Reputação/Imagem – Risco associado à possibilidade de uma percepção negativa da imagem pública da organização, fundamentada ou não, por parte de reguladores, clientes, fornecedores, analistas financeiros, colaboradores, investidores, órgãos de imprensa ou pela opinião pública em geral.

Atuarial – Risco associado à possibilidade da desvalorização potencial dos ativos do fundo de pensão ou da diminuição dos respectivos retornos esperados, que impliquem na realização de contribuições não previstas, ou quando as premissas utilizadas para os cálculos atuariais forem diferentes das que estão sendo efetivamente observadas nos planos de benefícios.

Fiscal – Risco associado a possibilidade de inserção/alterações na legislação, ou a interpretação equivocada da legislação fiscal para aplicação do cálculo dos tributos.

Operacional – Risco associado a possibilidade de perdas diretas ou indiretas resultantes de processos internos inadequados ou falhos, da existência de recursos humanos insuficientes ou inadequados, sistemas ou eventos externos.

Crédito – O risco de crédito representa a possibilidade de inadimplemento da contraparte de qualquer instrumento financeiro, gerando a falta de recebimento para a outra parte. O risco de crédito ocorre nas operações de empréstimos e financiamentos, bem como em todas as outras modalidades de instrumentos financeiros.

Liquidez – O risco de liquidez está associado à possibilidade de perda resultante do descasamento entre a entrada de recursos (captação no mercado, alienação de bens e participações, outras receitas e a obtenção de crédito) para atender às exigências de caixa que impactem o cumprimento de obrigações/compromissos programados.

Mercado – O risco de mercado consiste na possibilidade de ocorrerem perdas derivadas de situações adversas aos preços de mercado, como é o caso das alterações de taxas de juro, taxas de câmbio, de preços do mercado de ações e de mercadorias (*commodities*).

De acordo a Norma ABNT NBR ISO 31000:2018 e com os orientadores do COSO – Controle Interno – Estrutura Integrada, risco é o efeito da incerteza sobre os objetivos de uma organização. Sendo assim, a essência da Gestão de Risco é apoiar a organização a conviver com a incerteza e não, necessariamente, eliminá-la, até porque o efeito pode ser positivo.

O levantamento/mapeamento dos riscos tem como base a cadeia de valor dos processos da organização.

3.1. METODOLOGIA DE GESTÃO DE RISCOS

Gerenciar riscos contribui para incorporar a visão de riscos à tomada de decisões estratégicas, em conformidade com as regulamentações, inclusive do Setor Elétrico e com as melhores práticas de mercado.

Modelo Conceitual da Gestão de Riscos – Síntese:

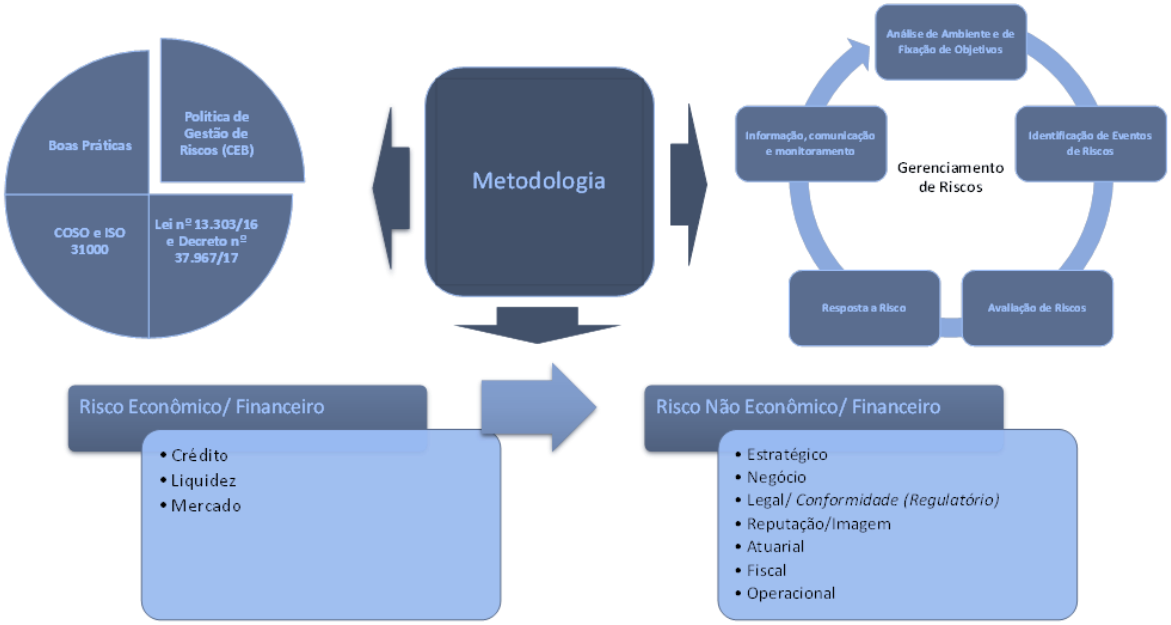


Figura 12: Metodologia de Gestão de Riscos.

Segundo a Norma ABNT NBR ISO 31000:2018, a eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão. Isto requer apoio das partes interessadas, em particular da alta direção.

A aplicação do Modelo de Gerenciamento de Riscos tem por base os processos da Cadeia de Valor/Base de Processos da CEB. Assim, os processos priorizados, de acordo com o método de priorização estabelecido, serão submetidos às etapas do gerenciamento de riscos.

4. ETAPAS DA GESTÃO DE RISCOS

A aplicação da Metodologia de Gerenciamento de Riscos será realizada em cinco grandes etapas, conforme demonstrado na figura seguinte:

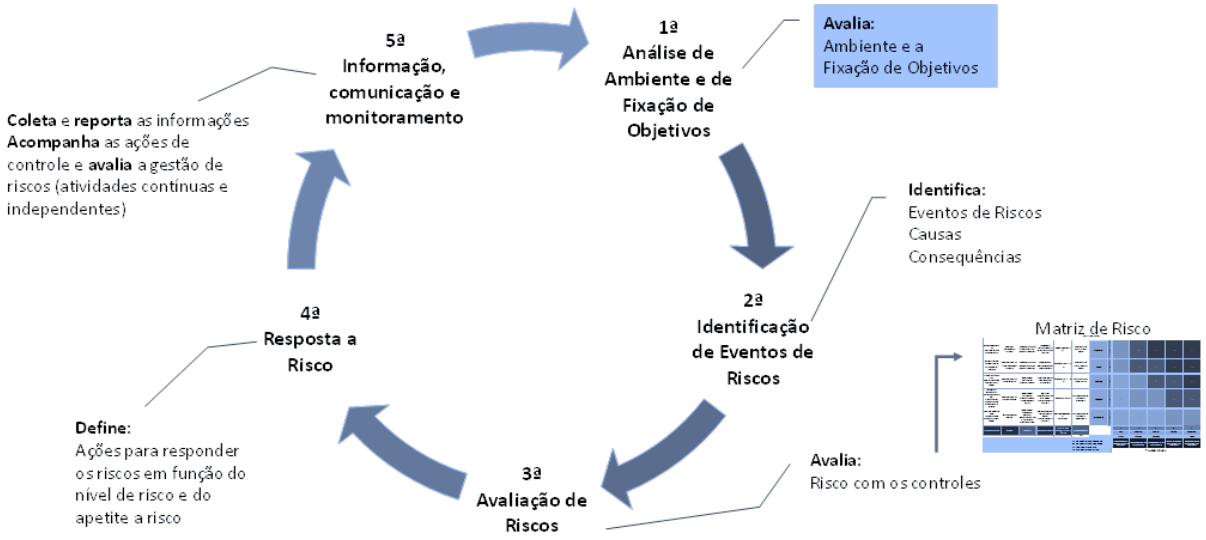


Figura 13: Etapas da Gestão de Riscos.

4.1. ANÁLISE DE AMBIENTE E DE FIXAÇÃO DE OBJETIVOS

Esta etapa tem por finalidade colher informações do ambiente interno e de fixação de objetivos no que se refere a fatores e situações relevantes que possam contribuir com o processo objeto do mapeamento de riscos.

Ambiente Interno – A administração estabelece a filosofia quanto à gestão de riscos e determina um apetite a risco. O ambiente interno influencia os conceitos básicos sobre a forma como os riscos e os controles serão identificados e abordados pela organização.

A análise do ambiente interno inclui, entre outros elementos: integridade, valores éticos; delegação de autoridade e competências; estrutura de governança, políticas; e práticas de recursos humanos. É, ainda, a base para todos os outros componentes da estrutura de gestão de riscos, provendo disciplina e prontidão para a gestão de riscos.

Fixação de Objetivos – Os objetivos devem existir antes que a administração identifique as situações em potencial que poderão afetar a realização desses. O gerenciamento de riscos corporativos contribui para que a administração adote um processo para estabelecer objetivos e que os escolhidos propiciem suporte, alinhem-se com a missão da organização e sejam compatíveis com o apetite a risco.

A análise de fixação de objetivos inclui verificar, em todos os níveis da organização (departamentos, divisões, processos e atividades), se os objetivos foram fixados e comunicados. A explicitação de objetivos, alinhados à missão e à visão da organização, é

necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução.

As informações poderão ser obtidas, primordialmente, por meio de pesquisas em: regimento interno; planejamento estratégico; projetos; orçamento; relatórios gerenciais; relatórios dos órgãos de fiscalização e controle; relatórios contábeis; e reclamações da ouvidoria.

Para iniciar o mapeamento de riscos é desejável que o processo esteja mapeado, pois, nesse caso, as informações do mapeamento serão utilizadas. Para os casos em que o processo não esteja mapeado, deverá ser preenchido o **Formulário I**, desenvolvido com a finalidade de colher informações para o seu entendimento e permitir a realização do mapeamento de riscos do processo priorizado, além das informações do ambiente interno e de fixação de objetivos.

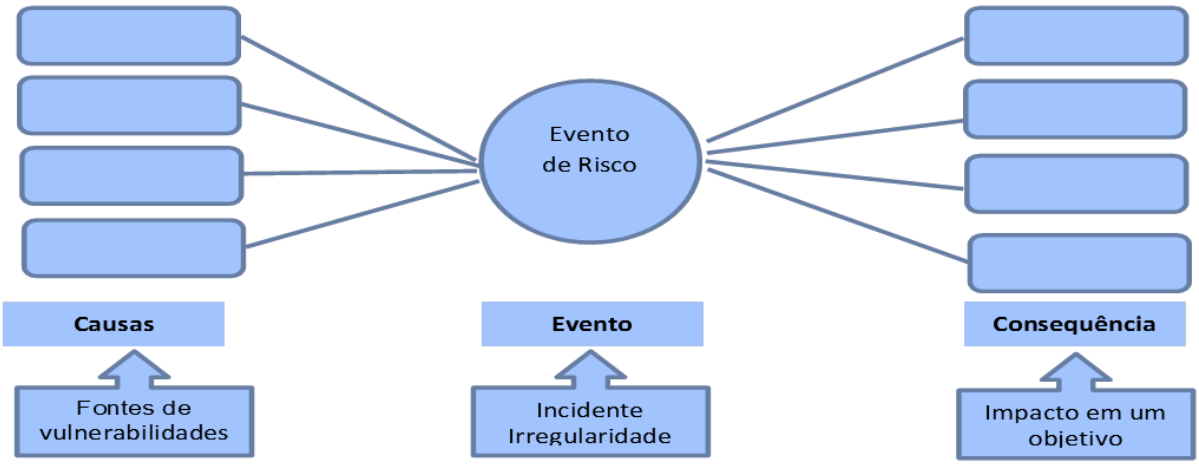
Ressalte-se que esta etapa não é obrigatória nos casos em que os processos estiverem mapeados, mas é fundamental para os processos sem mapeamento.

4.2. IDENTIFICAÇÃO DE EVENTOS DE RISCOS

Esta etapa tem por finalidade identificar e registrar os eventos de riscos que comprometam o alcance do objetivo do processo e da organização. Considere, neste momento, o resultado da **Análise do Ambiente e de Fixação de Objetivos (4.1)** e as informações do processo já mapeado ou as informações coletadas e registradas no **Formulário I**.

A cada risco identificado, são associadas causas e consequências, ou seja, elementos que, individualmente ou combinados, têm o potencial intrínseco de dar origem ao risco, e os efeitos possíveis caso o risco ocorra.

Componentes do Evento de Risco:



Formulário 1: Componentes do Evento de Risco.

Os eventos identificados, suas causas e consequências (componentes do evento de riscos), deverão ser registrados no Mapa de Riscos-CEB.xlsx.

IDENTIFICAÇÃO DE EVENTOS DE RISCOS					
ÁREA	EVENTOS DE RISCO	CAUSAS	EFEITOS CONSEQUÊNCIAS	CATEGORIA DO RISCO	NATUREZA DO RISCO

Figura 14: Mapa de Riscos-CEB – Identificação de Eventos de Riscos

Identificados os eventos, os seus componentes (causas e consequências) passa-se para a etapa seguinte que é a avaliação dos riscos.

Destaca-se alguns conceitos para facilitar o preenchimento do formulário e para obtenção de informações necessárias ao cumprimento desta etapa:

Causas – Condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo.

Fonte de Risco – Elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco.

Evento de Risco – A possibilidade de um conjunto específico de circunstâncias ocorrer e influenciar a realização dos objetivos, podendo gerar impacto tanto negativo quanto positivo ou ambos. Os que geram impacto negativo representam riscos que podem impedir o cumprimento dos objetivos; e os de impacto positivo podem contrabalançar os de impacto negativo ou podem representar oportunidades.

Consequência – O resultado de um evento de risco sobre os objetivos (estratégicos, operacionais, comunicação, conformidade).

Antes de iniciar a identificação dos eventos de riscos, deve-se ter bem claro o objetivo do processo que se deseja alcançar.

Aspectos importantes no momento de identificar e registrar um evento de risco:

→ Os eventos de riscos representam uma possibilidade, portanto, deverão ser descritas as falhas e inadequações que poderão ocorrer e não somente aquelas que já ocorreram;
→ Envolve a identificação das causas e suas consequências/efeitos;
→ Atentar, também, para as falhas que implicam em descumprimento de normas internas e externas e que geram ou podem gerar penalidades (ex.: advertências, impedimentos, etc.) e/ou sanções (ex.; multas) para a organização;
→ Não é necessário detalhar riscos não significativos. Uma boa prática é agregar riscos até obter uma significância razoável. Na prática, isso significa que riscos excessivamente pequenos podem ser agregados para entrar de forma mais significativa na análise. Excesso de detalhe eleva muito o custo de manutenção da documentação associada;
→ Não é necessário descrever dois riscos que possuem conjuntos de controles associados idênticos. Agregar esses riscos em uma mesma descrição é uma boa saída para evitar redundâncias na matriz de risco; e
→ Descarte de riscos irrelevantes para a organização, que na prática só implicam em um aumento do custo de manutenção das matrizes de risco.

Como identificar os eventos de riscos?

Existem várias técnicas que auxiliam na identificação de eventos de risco: questionários e *checklist*; *whorkshop* e reuniões (*Brainstorming*); inspeções e auditorias, fluxos e análise de dependência, etc. Este Manual prevê a utilização de reuniões (*Brainstorming*) e de Gravata-borboleta[4] (*Bow-tie*).

[4] *A Gravata-borboleta (Bow-tie) que é um modelo de diagramação, com objetivo de descrever e analisar os caminhos de um evento desde as causas (fatores) até as consequências (efeitos), onde será desenvolvida atividade que permitirá coletar e compartilhar ideias e gerar discussão entre os participantes sobre a possibilidade de ocorrência de eventos que podem impactar os objetivos do processo selecionado para análise.*

Identificados e registrados os eventos de riscos e os seus componentes (causas e consequências) no Mapa de Riscos, indique a Categoria do Risco, bem como a sua natureza: econômico-financeiro ou não econômico-financeiro.

4.3. AVALIAÇÃO DE RISCOS

Os riscos devem ser avaliados sob a perspectiva de impacto e probabilidade. Normalmente, as causas se relacionam à probabilidade de o evento ocorrer e as consequências associadas ao impacto, isso caso o evento se materialize.

A avaliação de riscos deve ser feita por meio de análises quantitativas e qualitativas ou da combinação de ambas. Os riscos devem ser avaliados quanto às suas condições inerentes, residuais ou a conjugação de ambos.

A Matriz de Riscos é uma ferramenta que permite aos gestores mensurar, avaliar e ordenar os riscos. Ela foi elaborada considerando a escala de probabilidade e impacto (5x5) e está distribuída em quatro níveis, que representam os níveis de riscos dimensionados em função do apetite a risco definido pela CEB. A seguir, de forma resumida, a Matriz de Risco aprovada:

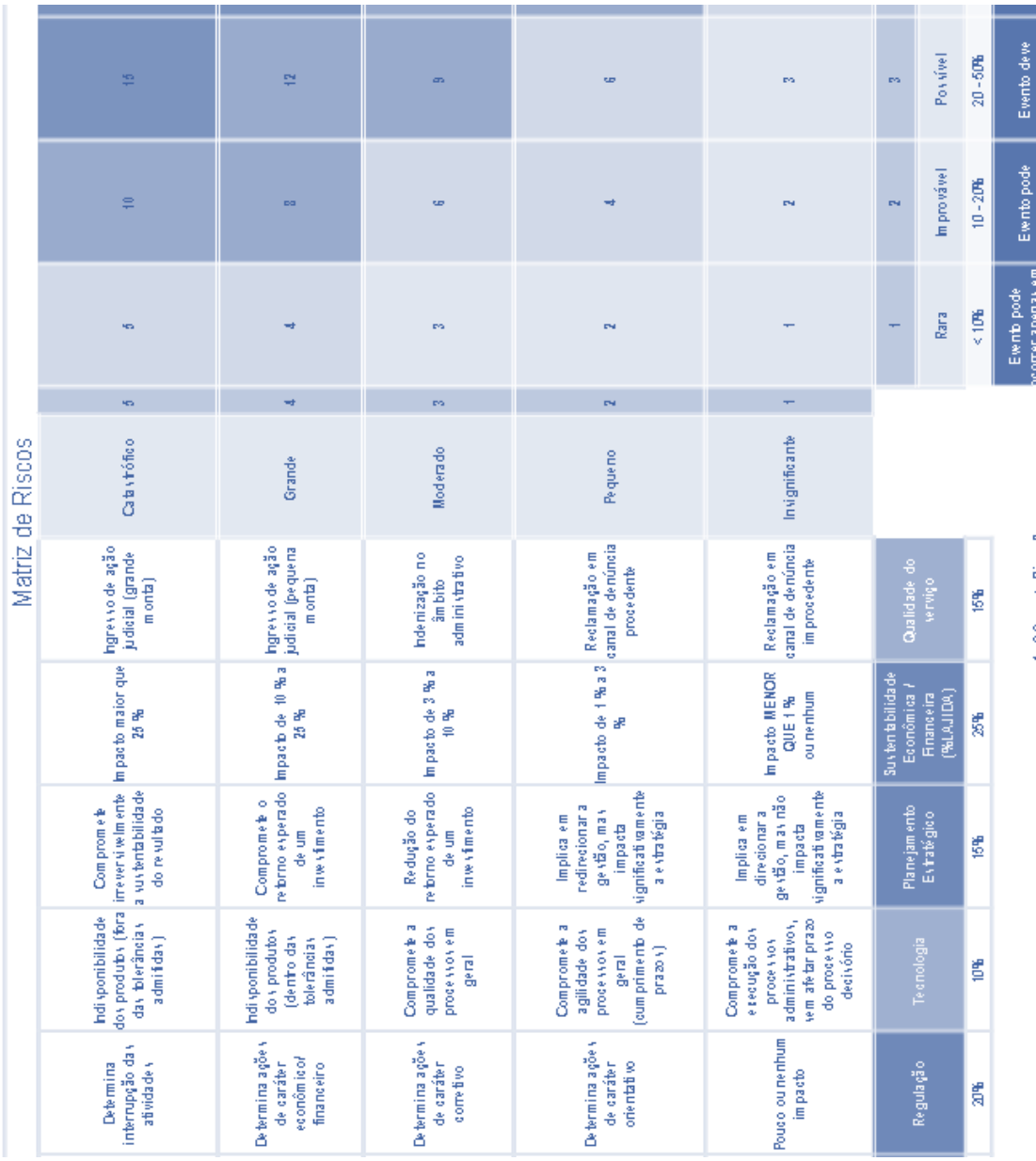


Figura 15: Matriz de Risco – CEB.

A Planilha “Mapa de Risco.xlsx” possui a “aba” “Cálculo do Risco” desenvolvida para a aplicação da Matriz de Risco da CEB e para obter os **níveis de riscos**.

4.3.1. AVALIANDO O IMPACTO – ASPECTOS AVALIATIVOS

Para o cálculo do impacto da matriz é necessário permear, primeiramente, dentre os aspectos avaliativos, qualitativos e quantitativos, atribuindo-lhes notas de zero a cinco para cada aspecto, que são:

- Aspectos Qualitativos
  - Parcimônia na Gestão
  - Regulação
  - Tecnologia
  - Planejamento Estratégico
  - Qualidade do serviço

- Aspectos Quantitativos
  - Sustentabilidade Econômica / Financeira (%LAJIDA)

As notas, de zero a cinco, representam a escala do impacto de cada aspecto avaliativo, ou seja, o 5 (cinco) indica que o impacto para a organização é catastrófico e o 1 (um) que o impacto é insignificante. Entretanto, a nota zero[5] representa que determinado aspecto avaliativo não está contido no evento de risco e não influenciará na nota do impacto. De forma resumida, segue quadro com as notas e sua interpretação no impacto na matriz:

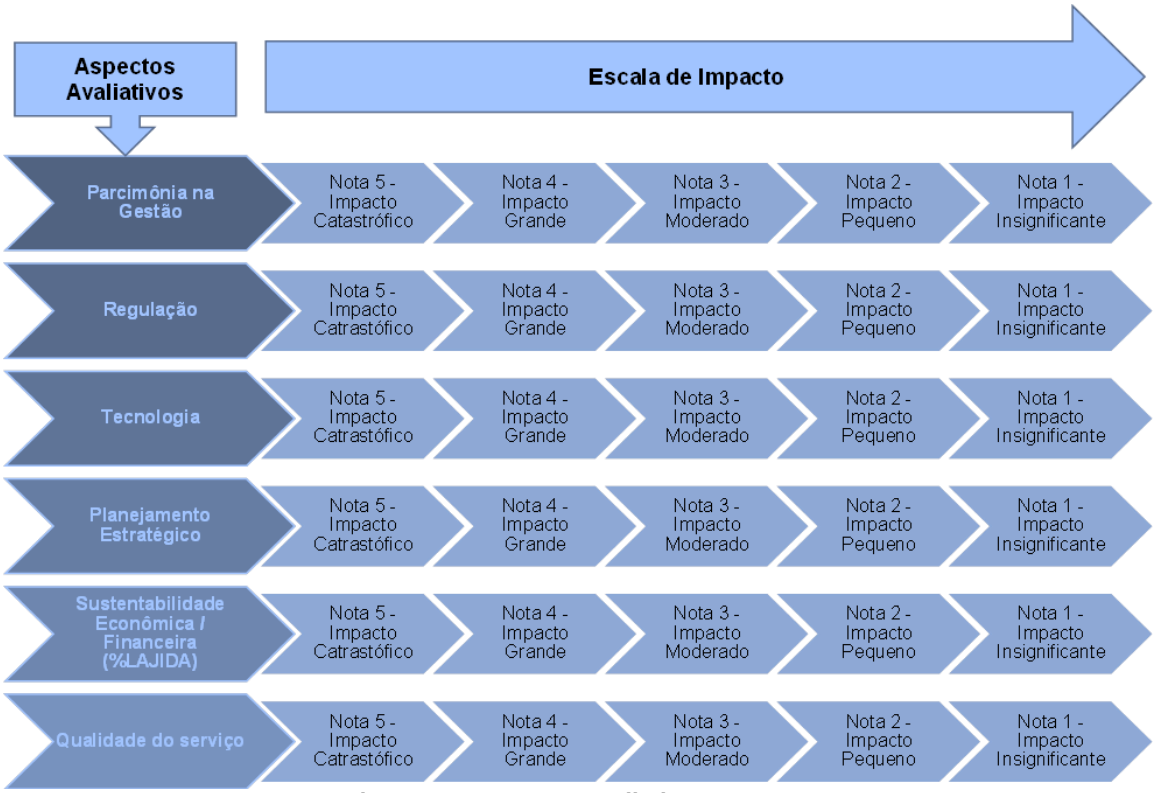


Figura 16: Aspectos Avaliativos – Notas.

[5] *A nota zero indica que um ou mais aspecto avaliativo não se aplica a um determinado risco. Em contraponto, se for atribuído nota zero a todos os aspectos avaliativos, na verdade o evento identificado não gera risco à empresa. Logo, não deve ser compilado no MAPA DE RISCO – CEB.*

Os conceitos definidos para atribuir as notas dos aspectos avaliativos estão apresentados a seguir, devendo ser utilizados como balizador no momento de atribuir a nota. A nota de cada aspecto do impacto deverá ser inserida na aba “Cálculo do Risco”.

Evento com potencial de levar ao colapso do negócio/serviço.	Determina interrupção das atividades.	Indisponibilidade dos produtos (fora das tolerâncias admitidas).	Compromete irreversivelmente a sustentabilidade do resultado.	Impacto maior que 25%	Ingresso de ação judicial (grande monta).	**Catastrófico**
Evento crítico, mas que com a devida gestão pode ser suportado.	Determina ações de caráter econômico/ financeiro.	Indisponibilidade dos produtos (dentro das tolerâncias admitidas).	Compromete o retorno esperado de um investimento.	Impacto de 10% a 25 %	Ingresso de ação judicial (pequena monta).	**Grande**
Evento significativo que pode ser gerenciado em circunstâncias normais.	Determina ações de caráter corretivo.	Compromete a qualidade dos processos em geral.	Redução do retorno esperado de um investimento.	Impacto de 3% a 10%	Indenização no âmbito administrativo.	**Moderado**
Evento cujas consequências podem ser absorvidas, mas é necessário um esforço da gestão para minimizar o impacto.	Determina ações de caráter orientativo.	Compromete a agilidade dos processos em geral (cumprimento de prazos).	Implica em redirecionar a gestão, mas impacta significativamente a estratégia.	Impacto de 1% a 3%	Reclamação em canal de denúncia procedente.	**Pequeno**
Evento cujo impacto pode ser absorvido por meio de atividades normais.	Pouco ou nenhum impacto.	Compromete a execução dos processos administrativos, sem afetar prazo do processo decisório.	Implica em direcionar a gestão, mas não impacta significativamente a estratégia.	Impacto MENOR QUE 1% ou nenhum.	Reclamação em canal de denúncia improcedente.	**Insignificante**
Parcimônia na Gestão	**Regulação**	**Tecnologia**	**Planejamento Estratégico**	**Sustentabilidade Econômica / Financeira (%LAJIDA)**	**Qualidade do serviço**	

Figura 17: Aspectos Avaliativos – Atribuição da Escala de Impacto.

Após a atribuição da nota a cada aspecto avaliativo será realizada a ponderação entre as métricas, no intuito de possuir uma nota final do impacto do risco identificado.

A ponderação entre as métricas representa a decisão da organização para cada Aspecto Avaliativo, em que o maior peso representa maior relevância no risco avaliado para a organização.

Seguem, de forma resumida, os percentuais das ponderações, aprovadas pela CEB, para cada aspecto avaliativo:

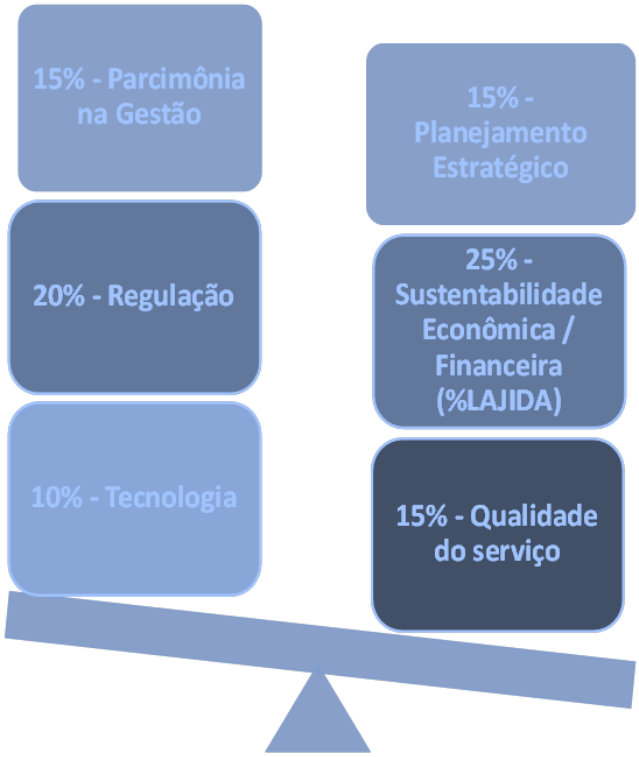


Figura 18: Ponderação Atribuida aos Aspectos Avaliativos.

As notas dos aspectos avaliativos inseridos na aba “Cálculo do Risco” serão ponderadas pelo seu respectivo peso. E a soma de todas as métricas ponderadas resultará na nota final do impacto do risco. Porém, a atribuição de nota zero exclui o aspecto avaliativo e o seu referido peso não influenciará na nota final do impacto. Registra-se que a planilha está parametrizada para o recálculo.

4.3.2. AVALIANDO A PROBABILIDADE

A probabilidade representa a possibilidade de que um determinado risco ocorrerá. Poderá ser determinada objetiva ou subjetivamente, qualitativa ou quantitativamente.

Via de regra, as estimativas de probabilidade de riscos são conduzidas utilizando dados de eventos passados observáveis, os quais fornecem uma base mais objetiva do que as estimativas inteiramente subjetivas. Mas o julgamento dos gestores, embasados na experiência passada da própria organização ou pessoal, faz parte da definição do nível de probabilidade. Contudo, os executivos devem reconhecer as limitações inerentes ao julgar e serem criteriosos.

Rara	Improvável	Possível	Provável	Quase certo
< 10%	10 - 20%	30 - 50%	50 - 90%	>90%
Evento pode ocorrer apenas em circunstâncias excepcionais	Evento pode ocorrer em algum momento	Evento deve ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado que ocorra na maioria das circunstâncias

Figura 19: Probabilidade.

Definida a melhor probabilidade para cada risco identificado, com base nas métricas apresentadas e no julgamento, a nota deverá ser inserida na aba “Cálculo do Risco” para se encontrar o nível de risco.

Os pesos dos aspectos avaliativos (balanceamento entre as métricas) tanto para o impacto quanto para a probabilidade foram atribuídos em reunião com a participação da Diretoria de Planejamento e Gestão de Riscos e os representantes das áreas.

4.3.3. NÍVEIS DE RISCO – IMPACTO X PROBABILIDADE

Uma vez mensurado o risco com a aplicação da Matriz de Risco (atribuição de notas ao impacto e a probabilidade), obtém-se os níveis de riscos dimensionados em função do apetite a risco definido pela CEB.

Assim, o nível de risco é expresso pelo resultado da multiplicação da nota do impacto e da probabilidade. Desta forma, os níveis de risco serão classificados como Pequeno, Moderado, Alto e Crítico. O intervalo de pontuação para a classificação dos riscos foi assim definido:

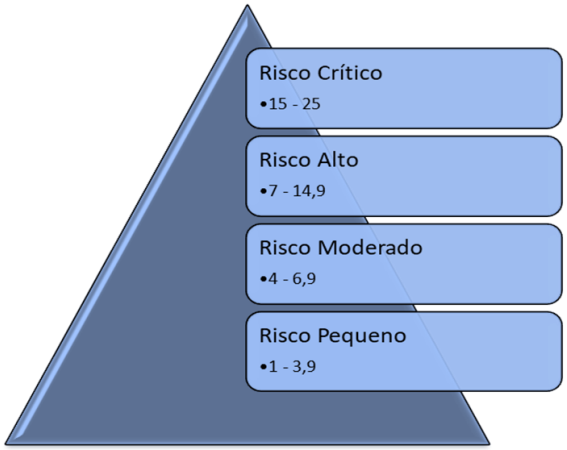


Figura 20: Níveis de Riscos – Intevalos.

Dependendo da classificação do nível de risco, as respostas deverão ser adotadas na forma pré-estabelecida, considerando as alçadas definidas pela Companhia, conforme segue:

Nível de Risco	Resposta ao Risco	Alçada
Risco Crítico	Evitar	DE
	Mitigar	DE
	Compartilhar	DE
	Aceitar	DE
Risco Alto	Evitar	DE
	Mitigar	DE
	Compartilhar	DE
	Aceitar	DE
Risco Moderado	Evitar	SUP
	Mitigar	SUP
	Compartilhar	SUP
	Aceitar	DA
Risco Pequeno	Evitar	GA
	Mitigar	GA
	Compartilhar	GA
	Aceitar	GA

Figura 21: Alçadas – Nível de Risco x Resposta ao Risco[6].

4.4. RESPOSTA A RISCO

[6] *GA – Gerente da Área; SUP – Superintendente da Área; DA – Diretor da Área; DE – Diretoria Executiva*.

Conhecido os níveis de riscos da avaliação dos eventos identificados, foram definidas as seguintes respostas: **evitar**, **mitigar**, **compartilhar** ou **aceitar** os riscos.

Cabe destacar que os eventos de impacto positivo representam oportunidades e deverão ser canalizados de volta para os processos de fixação de estratégias ou objetivos.

Identificados e mensurados os riscos em potencial, que podem afetar negativamente a realização de seus objetivos, adota-se uma das estratégias, definidas na Matriz de Riscos – CEB aprovada, em função do nível de risco e submete-se à alçada definida:

Nível de Risco	Resposta ao Risco	Descritivo da resposta ao risco	Alçada
Risco Crítico	Evitar	• Indica que nenhuma opção de resposta foi identificada para reduzir ou transferir a probabilidade e o impacto a nível aceitável. Reter o risco por decisão fundamentada. • Descontinuar as atividades que geram riscos. • Custo desproporcional, capacidade limitada diante do risco.	Diretoria Executiva
Risco Alto	Mitigar	• Indica que o risco calculado será reduzido a um nível compatível com a tolerância a riscos. • Adotar medidas para reduzir a probabilidade ou impacto dos riscos, ou ambos.	Diretoria Executiva
Risco Moderado	Compartilhar	• Reduzir a probabilidade ou impacto pela transferência ou compartilhamento de uma parte do risco. (seguro, transações de hedge ou terceirização da atividade). • Nem todos os riscos podem ser transferidos – imagem e reputação.	Superintendente da Área
Risco Pequeno	Aceitar	• Indica que o risco calculado está dentro da tolerância a risco. • Não adotar medidas para atenuar a probabilidade ou o impacto dos riscos.	Gestor da Área

Figura 22: Resposta a Riscos.

Para responder aos riscos é necessário o estabelecimento de políticas e procedimentos, que executados atenderão ao tratamento definidos pela CEB.

As atividades de controles devem estar distribuídas por toda a organização, em todos os níveis e em todas as funções. Incluem uma gama de controles internos da gestão, bem como a preparação prévia de plano de ações para responder aos riscos.

Podem ter natureza preventiva ou de detecção e abranger uma série de atividades manuais e automáticas, como autorizações e aprovações, verificações, reconciliações e revisões de desempenho do negócio. A segregação de funções é geralmente inserida na seleção e no desenvolvimento das atividades de controle.

Para registrar as ações que deverão ser adotadas com a finalidade de dar resposta aos riscos é recomendável a elaboração de um plano de ação.

O Plano de Ação é um conjunto de ações necessárias para adequar os níveis de riscos, por meio da adoção medidas que implantem novos controles ou aperfeiçoem os controles atuais do processo.

Aspectos importantes a serem observados na elaboração de um plano de ação deverão levar em consideração se há necessidade de atuar nas causas ou atenuar o impacto, caso o risco se materialize.

Existem situações em que a ação ideal não possa ser implantada ou não possa ser estabelecida no curto prazo em função da sua complexidade, alto custo ou alto nível de interveniência. Nesses casos, devem ser propostas, complementarmente, medidas alternativas, um controle compensatório (concebido para contrabalancear uma falha na estrutura de controles ou diminuindo sua severidade).

Os controles devem ser propostos, ainda, sob a ótica de custo x benefício; um controle não deve custar mais caro do que o evento de risco que se pretende reduzir a níveis aceitáveis.

Modelo de Plano de Ação:

Plano de Implementação de Controle									
Diretoria/Coordenação:									
Macroprocesso:									
Processo:									
Subprocesso / Atividade									
Objetivo do Processo:									
Gestor Responsável pelo Processo:									
Responsável (eis) pela Análise:									
Período da Análise:									
Risco	Nível de Risco	Resposta ao Risco	Alçada	Ações Propostas	Área Responsável pela Implementação do Controle Proposto	Responsável Implementação do Controle Proposto	Intervenientes	Data de Início	Data de Conclusão
Risco 1									
Risco 2									
Risco "n"									

Figura 23: Modelo de Plano de Ação.

4.5 INFORMAÇÃO, COMUNICAÇÃO E MONITORAMENTO

A informação e comunicação, durante todas as etapas do processo de gestão de riscos, devem atingir todas as partes interessadas, devendo ser realizada de maneira clara e objetiva. É importante obter o adequado nível de profundidade, o canal a ser utilizado e a pontualidade da informação.

O estabelecimento de uma linha interna de comunicação eficiente fomenta a interação entre as áreas responsáveis pelo gerenciamento do risco, em que se evidencia:

→ A importância do gerenciamento de riscos corporativos eficaz;
→ A disseminação da cultura de gestão de riscos;
→ Os objetivos da organização;
→ O apetite a riscos e a respectiva tolerância;
→ Uma linguagem comum de riscos; e
→ As funções e as responsabilidades das áreas gestoras dos processos ao conduzir o gerenciamento de riscos.

Em linha com a Política de Gestão de Riscos, a Diretoria de Planejamento e Gestão de Riscos é responsável por orientar e promover a aplicação das políticas de gestão de riscos; e, em articulação com as demais áreas operacionais, deverá potencializar a identificação, o tratamento e o monitoramento dos riscos.

O monitoramento contínuo e a análise crítica periódica do processo de gestão de riscos e seus resultados devem ser uma parte planejada do procedimento, com responsabilidades estabelecidas.

Com o foco no monitoramento da CEB, a Diretoria de Planejamento e de Gestão de Riscos, cumprindo a Política de Gestão de Riscos, elaborará relatórios periódicos de suas atividades, submetendo-os ao Comitê de Auditoria Estatutário a cada 3 (três) meses ou quando solicitado.

5. REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Associação Brasileira de Normas Técnicas – ABNT. Gestão de Riscos: Princípios e Diretrizes. Norma Brasileira ABNT NBR ISO 31000: Segunda Edição, 2018.

COSO ERM. Gerenciamento de Riscos Corporativos – Estrutura Integrada, 2004.

COSO. Gerenciamento de Riscos Corporativos – Estrutura Integrada. 2007. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e *Pricewaterhouse Coopers Governance*, *Risk and Compliance*, Estados Unidos da América, 2007.

IBGC. Guia de Orientação para Gerenciamento de Riscos Corporativos, 2011.

IBGC. Gerenciamento de Riscos Corporativos – Evolução em Governança e Estratégia, 2017.

6. ANEXOS

6.1. FORMULÁRIO I – ANÁLISE DE AMBIENTE/FIXAÇÃO DE OBJETIVOS

Este formulário tem por finalidade auxiliar o Analista de Risco no acolhimento das informações do ambiente interno e de fixação de objetivos, no que se refere aos fatores e às situações relevantes, que possam contribuir com o processo objeto do mapeamento de riscos.

O ideal é que o processo objeto do mapeamento de riscos esteja ou seja desenhado. Caso não seja possível, registre no formulário as informações obtidas sobre o processo para permitir o mapeamento dos riscos.

As informações poderão ser obtidas por meio de pesquisas no (s): regimento interno; planejamento estratégico; projetos; orçamento; relatórios gerenciais; relatórios dos órgãos de fiscalização e controle; relatórios contábeis; e denúncias recebidas da ouvidoria.

O Formulário I será utilizado para registrar as informações coletadas sobre o Ambiente Interno e a Fixação de Objetivos:

Informações sobre o Ambiente Interno e Fixação de Objetivos		
Ambiente Interno: compreende o tom de uma organização e fornece a base pela qual os riscos são identificados e abordados.		
Existência:	Sim	Não
Código de Ética/Normas de Conduta	( )	( )
Estrutura de Governança	( )	( )
Políticas e Práticas de Recursos Humanos	( )	( )
Alçadas	( )	( )
Normas Internas	( )	( )
Fixação de Objetivos: é uma precondição à identificação de eventos, à avaliação de riscos e às respostas a esses riscos.		
Existência:	Sim	Não
Missão	( )	( )
Visão	( )	( )
Objetivos Estratégicos	( )	( )
Informações sobre o Macroprocesso		

Informações sobre o Ambiente Interno e Fixação de Objetivos		
Coordenação do Macroprocesso/Processo:		
Macroprocesso		
Processo		
Objetivo do Macroprocesso/Processo		
Grandes Atividades do Processo	1. 2. 3. 4. 5	
Leis, Regulamentos e Normas internas		
Sistemas:		
Controles Existentes:		Periodicidade:
1.		
2.		

As informações obtidas sobre o ambiente e a fixação de objetivos, em conjunto com as informações do macroprocesso/processo (legislação, normas, fluxograma das atividades, responsáveis, controles existentes, etc.), são fundamentais para a realização do mapeamento de riscos (identificação, avaliação, respostas a riscos, monitoramento e comunicação).

Os conceitos a seguir, estão sendo disponibilizados para o melhor entendimento dos termos constantes do formulário. É pertinente dizer que, as definições de ambiente interno e fixação de objetivos, estão no item 4.1 deste manual.

Macroprocesso – O nível mais alto de processo identificado por uma empresa. O propósito de um macroprocesso está relacionado com o seu papel de alcançar a missão global de um negócio.

Processo – Qualquer atividade ou conjunto de atividades que tornam um *input*, adiciona valor a ele e fornece um *output* a um cliente específico; é uma subdivisão do macroprocesso. Um conjunto de processos assume o desenvolvimento completo de um macroprocesso.

Subprocesso – Uma subdivisão de um processo que representa um conjunto de atividades. Há uma diversidade de níveis de subprocessos entre hierarquia de processos e atividades.

Atividade – Um conjunto de tarefas desempenhadas para atender uma função dentro de uma operação específica.

Controle – A medida que mantém e/ou modifica o risco.

Periodicidade – Classificação que visa explicitar que os diversos controles existentes, para mitigar um determinado risco, podem estar sendo executados muitas vezes em tempos diferentes (diário, trimestral, semestral e anual).

6.2. FORMULÁRIO II – IDENTIFICAÇÃO DE EVENTO DE RISCOS

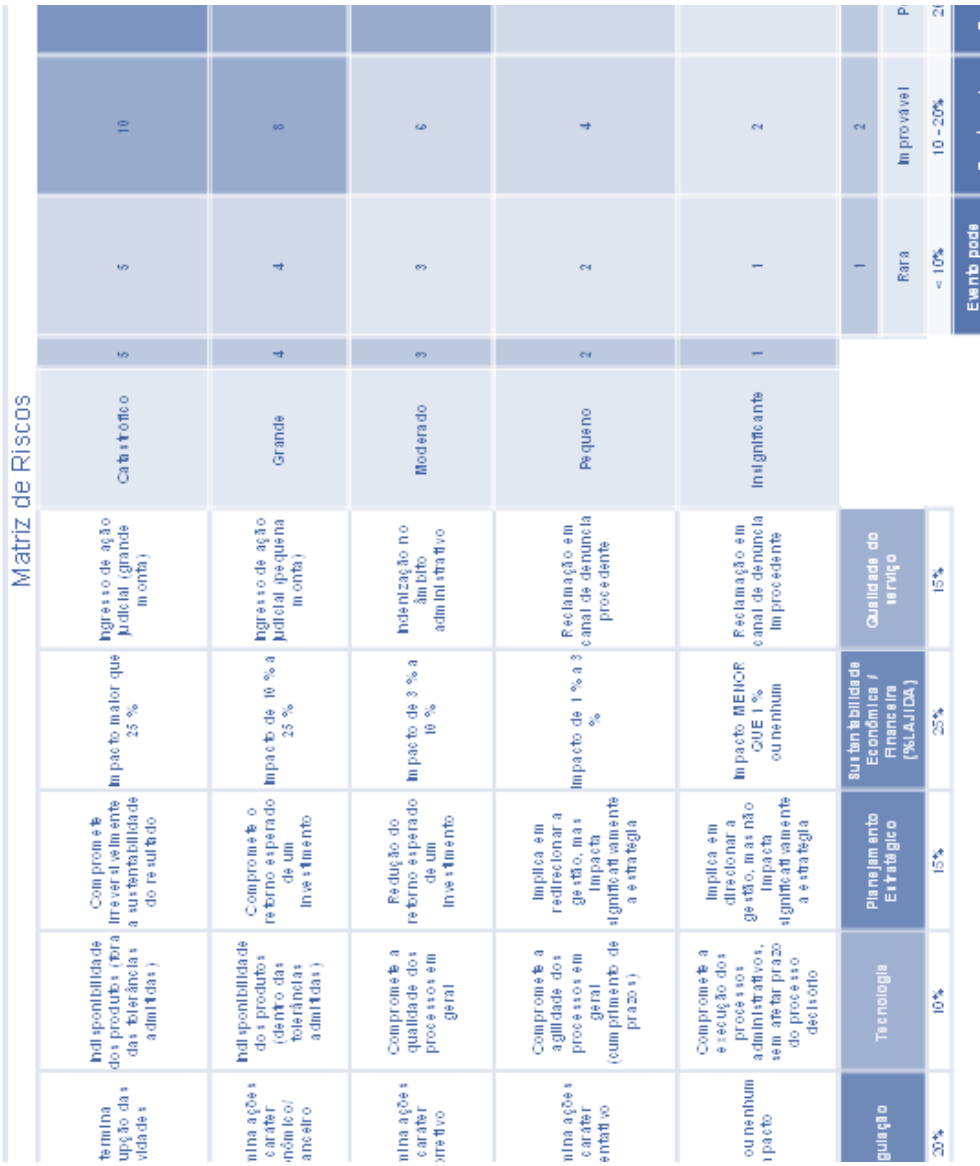
Este formulário tem por finalidade auxiliar o Analista de Risco na identificação e registro dos eventos de riscos que comprometem o alcance do objetivo do processo e, consequentemente, dos objetivos organizacionais.

Ele é definido como Mapa de Riscos e será preenchido conforme as orientações do item 4.2 deste Manual na planilha de Excel® “Mapa de Riscos – CEB.xlsx”.

6.3. FORMULÁRIO III – AVALIAÇÃO DE RISCOS

Este formulário tem por finalidade auxiliar o Analista de Risco na avaliação dos riscos identificados, considerando os seus componentes (causas e consequências).

A Matriz de Riscos que será aplicada, considerando a escala de probabilidade e impacto (5x5), está distribuída em quatro níveis, que representam os níveis de riscos dimensionados em função do apetite a risco definido pela CEB. A seguir, de forma resumida, apresenta-se a Matriz de Risco aprovada:



As orientações para o preenchimento deste formulário estão no item 4.3 deste Manual e devem ser utilizadas no preenchimento da planilha de Excel® “Mapa de Riscos – CEB.xlsx”.

Níveis de Risco – Impacto x Probabilidade

Uma vez mensurado o risco, com a aplicação da Matriz de Risco (atribuição de notas ao impacto e a probabilidade), obtém-se os níveis de riscos. Desta forma, os níveis de risco serão classificados como risco: Pequeno, Moderado, Alto e Crítico, conforme o exemplo a seguir:

AVALIAÇÕES DOS RISCOS			
IMPACTO	PROBABILIDADE	IMPACTO X PROBABILIDADE	NÍVEL DE RISCO
3,70	5	18,50	Risco Crítico
1,40	2	2,80	Risco Pequeno
4,85	1	4,85	Risco Moderado
3,25	4	13,00	Risco Alto

Dependendo da classificação do nível de risco a organização deve tratar de forma pré-estabelecida na metodologia e na orientação do Formulário IV.

6.4. FORMULÁRIO IV – RESPOSTA A RISCOS

Este formulário tem por finalidade auxiliar o Analista de Risco na aplicação da estratégia a adotar (evitar, mitigar, compartilhar ou aceitar), para responder aos riscos identificados e avaliados.

Conhecido o nível de risco, será adotada a estratégia e a alçada definida na Matriz de Riscos – CEB, essas informações serão preenchidas na planilha de Excel® “Mapa de Riscos – CEB.xlsx” e deverá seguir as orientações constantes no item 4.4 deste Manual.