1. OBJETIVOS

O objetivo deste procedimento é estabelecer as intenções, diretrizes e preceitos para o gerenciamento de riscos da AeC, contemplando a identificação, análise, avaliação, tratamento e divulgação dos riscos.

2. CAMPO DE APLICAÇÃO

Este documento se aplica a todos aqueles que integram os quadros da AeC, sejam acionistas ou colaboradores, em todos os níveis hierárquicos, bem como para terceiros que agem em nome, interesse ou benefício da AeC em acordo com as premissas, restrições e os papéis e responsabilidades descritos na Política de Gestão de Riscos.

3. REFERÊNCIAS

Código de Conduta AeC

ABNT NBR ISO 31000:2018 - Gestão de riscos — Diretrizes

ABNT NBR ISO 31073:2022 - Gestão de riscos — Vocabulário

Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management (COSO-ERM)

POL 032 – Política de Gestão de Riscos

REG-007 Controle de Documentos

4. DEFINIÇÕES

Comitê de Compliance e Riscos Corporativos: grupo formado por colaboradores da AeC que tem por objetivo acompanhar as questões e ações da organização relacionadas ao Compliance e gerenciamento dos Riscos Corporativos, ou seja, tudo que é feito para identificar, prevenir e evitar os riscos.

Control Owner: É o colaborador responsável por identificar os riscos juntamente com a gestão dos riscos e executar, testar e fornecer periodicamente evidências das atividades de controle na plataforma de gestão de riscos.

Controle (de risco): medida que mantém e/ou modifica o risco.
Nota 1: Controles (de risco) incluem, mas não se limitam a qualquer processo, política, dispositivo, prática ou outras condições e/ou ações que mantêm e/ou modificam riscos.
Nota 2: Controles (de risco) nem sempre conseguem exercer o efeito de modificação pretendido ou presumido.

Critérios de risco: termos de referência contra os quais a significância de um risco é avaliada.
Nota 1: Os critérios de risco são baseados nos objetivos organizacionais e no contexto externo e interno.
Nota 2: Os critérios de risco podem ser derivados de normas, leis, políticas e outros requisitos.

Efeito do risco: é o desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.

- **Fonte do risco:** é o elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco.

- **Gerenciamento de risco corporativos:** 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 os critérios de risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. Na AeC os riscos corporativos abrangem todos os riscos da empresa exceto de Segurança da Informação, Privacidade de Dados e LGPD.

- **Gestão de risco:** atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

- **Mapa de calor -** Mapa de calor é uma ferramenta que pode ser utilizada para a análise de riscos, apresentando de forma simples e visual suas relevâncias através do cruzamento das probabilidades e dos níveis de impacto.

- **Matriz de riscos:** matriz gráfica que exprime o conjunto de combinações de probabilidade e impacto de riscos para classificar os níveis de risco. A matriz de riscos é um organismo em constante evolução, atualizada e possui no mínimo os campos: risco, processo, probabilidade e impacto do risco inerente, probabilidade e impacto do risco residual, controles, frequências dos controles, entre outros.

- **Nível de risco:** magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (likelihood).

- **Oportunidade:** combinação de circunstâncias que se espera que sejam favoráveis aos objetivos. **Nota 1:** Uma oportunidade é uma situação positiva em que o ganho é provável e sobre a qual se tem um razoável nível de controle.

- **Política de gestão de riscos:** documento que contém a declaração das intenções e diretrizes gerais relacionadas à gestão de riscos e estabelece claramente os objetivos e o comprometimento da organização em relação à gestão de riscos. Não se trata de uma declaração de propósitos genérica, mas de um documento que, além de declarar os princípios, explica porque a gestão de riscos é adotada, o que se pretende com ela, onde, como e quando ela é aplicada, quem são os responsáveis, dentre outros aspectos.

- **Risco:** efeito da incerteza nos objetivos.

  Nota 1: 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.

- **Risk Owner:** É o proprietário do risco, responsável pelo gerenciamento dos riscos de suas operações, capaz de estabelecer e gerir os controles e planos de ação.

5. GESTÃO DE RISCOS CORPORATIVOS

5.1 Comunicação E Consulta

A Comunicação é um processo que tem por objetivo promover a conscientização e o entendimento

do risco e pode ser realizada através de treinamentos às partes interessadas e por meio dos relatórios sobre a Gestão de Riscos.

A Consulta abrange obter retorno e informação para apoiar a tomada de decisão. Assim sendo, a identificação e análise dos riscos é realizada, utilizando a técnica de Brainstorming, por colaboradores de diferentes áreas, incluindo profissionais da área de gestão de riscos e da área específica (Risk e Control Owner), assegurando que os diferentes pontos de vistas sejam identificados, registrados e considerados na determinação dos critérios dos riscos.

5.2 Escopo, Contexto e Critério

O primeiro passo é realizar o estudo do contexto interno, tais como: mapa de contexto da AeC, governa corporativa, normas e diretrizes adotadas pela organização, relatórios de auditorias e outras avaliações disponíveis. O estudo para o contexto externo abrange fatores sociais, culturais, políticos, jurídicos, regulatórios e relacionamentos com partes interessadas.

Para a definição do escopo, são considerados temas relevantes, acordados com os Owners do processo, e mapeados utilizando sistema de gerenciamento em plataforma contratada para este fim, utilizando a Matriz de Probabilidade e Impacto 5X5.

Os riscos Corporativos da Organização, conforme premissas e restrições relatados na POL 032 – Política de Gestão de Riscos, poderão ser analisados pelo prazo mínimo de 5 anos.

Os critérios dos riscos serão mencionados nos itens 5.3.2

5.3 Processo de Avaliação de Riscos

A AeC realiza regularmente o gerenciamento de riscos, tal processo consiste em:

5.3.1 Identificação dos riscos

A identificação dos riscos será realizada sempre que necessário e a reavaliação dos riscos será realizada no mínimo a cada 12 meses. E, a partir da análise dos contextos os riscos são identificados, considerando o escopo determinado acima, bem como utilizando a sua criticidade quanto ao alcance dos objetivos da AeC.

Os eventos podem ser negativos (riscos) ou positivos (oportunidades) e podem ser encontrados, reconhecidos e descritos por diversas formas, são elas:

5.3.1.1 Mapeamento dos eventos da organização

Para mapear os eventos da AeC, pode-se adotar as metodologias usualmente utilizadas no mercado, tais como entrevistas com diretores, superintendentes e gerentes, análise de evidências, verificação de documentos e validações junto as áreas técnicas envolvidas e mapeamento de processos, a fim de coletar dados para encontrar, reconhecer e descrever os riscos.

Como resultado, haverá uma matriz de riscos associada ao escopo e ao cenário definido. Este processo será realizado, no mínimo, uma vez por ano, podendo ocorrer antes, caso seja necessário, pela revisão do planejamento estratégico da AeC e tempestivamente com o surgimento de eventos de riscos emergentes.

5.3.1.2 Auditorias Internas

Novos riscos poderão ser identificados através dos Relatórios de Auditorias e serão analisados quanto a sua criticidade em reuniões junto aos Owners do processo, com o objetivo de verificar a sua relevância e possibilidade de inclusão na Matriz de Riscos Corporativos.

5.3.1.3 Resultado de investigações de denúncias

Após avaliações das denúncias investigadas pelo Canal de Denúncias, o Departamento de Compliance deverá observar se existem riscos não mapeados relacionados àquela denúncia, e se eventual risco não estiver mapeado, reportar a Gestão de Riscos para medidas previstas nesta política.

5.3.1.4 Indicação de qualquer colaborador

Todo colaborador poderá reportar, ao departamento responsável pelo gerenciamento de riscos, aqueles identificados durante sua jornada de trabalho e serão verificados quanto a sua relevância.

5.3.1.5 Categorização dos riscos

Para fins de categorização, os riscos da AeC devem ser categorizados da seguinte forma:

- **ESTRATÉGICO:** riscos que afetam a estratégia da empresa. Podem ser internos gerados dentro da organização, como continuidade dos negócios, alterações na composição da Alta Administração. Os estratégicos de origem externa, isto é, aqueles gerados fora do ambiente de trabalho da empresa, podemos citar as mudanças regulatórias, mudanças climáticas, entre outros;
- **OPERACIONAL**: riscos resultantes de falha, deficiência ou inadequação de quaisquer processos internos envolvendo pessoas, sistemas ou de eventos externos e inesperados, como exemplo os riscos de recursos humanos, fornecedores, etc;
- **COMUNICAÇÃO:** riscos relacionados a confiabilidade de relatórios, como exemplo os Relatórios de Demonstrações Contábeis, etc;
- **REGULATÓRIO:** riscos de a organização ser penalizada ou sofrer consequências negativas pelo descumprimento de leis e regulamentos como exemplo o não atendimento a legislação, Compliance, etc.
- **FINANCEIRO:** São riscos que geram impacto em receitas e despesas podendo impactar o fluxo de caixa da empresa e o resultado, gerando perdas e/ou distorções significativas nas demonstrações financeiras, como exemplo inadimplência, orçamentos, entre outros.

5.3.2 Análise de riscos

As análises dos riscos identificados devem ser realizadas, de forma conjunta, entre o setor responsável pela gestão de riscos e os Owners do processo.

Nesta etapa, serão discutidos sobre o evento, causa, fonte de risco, consequência do risco e as medidas de controle existentes, caso haja, além de realizar uma análise crítica acerca da pertinência ou eficácia do controle apresentado, podendo registrar possíveis melhorias ou solicitação de novos controles.

A análise do risco se dará pelo método híbrido envolvendo a avaliação qualitativa e quantitativa, que

possui o foco na percepção das partes interessadas sobre a probabilidade (muito baixo, baixo, médio, alto, muito alto) de um risco ocorrer e seu impacto (muito baixo, baixo, médio, alto, muito alto) sobre aspectos organizacionais e financeiros pertinentes, no caso de ocorrência, ambas avaliações se complementam. Os riscos deverão classificados em:

Risco Inerente: grau do risco antes de qualquer ação de mitigação, é o risco inerente ao processo.

Risco Residual (Atual): grau do risco após a implantação de ações de mitigação e atividades de controle implantadas até o momento.

Risco Target: grau do risco que se deseja alcançar após a implantação de planos de ação.

Os critérios para análise de probabilidade consistem em:

Nível	Descritor	Descrição Probabilidade	Frequência indicativa
1	Muito Baixo	Evento que pode ocorrer em situações excepcionais. Não há histórico conhecido ou não há indícios que sinalizem sua ocorrência (Procedimentos e políticas divulgadas e controles avaliados como eficazes nos testes de controle).	**até 5% chances de sua ocorrência**
3	Baixo	Evento que pode ocorrer em algum momento, porém com baixa frequência (Procedimentos e políticas divulgadas e controles avaliados como eficazes).	**de 5% à *14%* chances de sua ocorrência.**
5	Médio	Médio - Evento que pode ocorrer em algum momento com frequência razoável. (Procedimentos e políticas divulgadas, entretanto controles avaliados como parcialmente eficazes).	**de 15% à *45%* chances de sua ocorrência.**
8	Alto	Alto - Evento que se repete com elevada frequência ou há muitos indícios que ocorrerá. (Procedimentos e políticas divulgadas e/ou controles avaliados como ineficazes).	**De *46*% à 80% chances de sua ocorrência.**
10	Muito Alto	Evento com altíssima probabilidade de ocorrência Muito Alto - (Inexistência de procedimentos, políticas e/ou iniciativas de mitigação).	**mais 80% chances de sua ocorrência.**

Tabela 1- Escala de Probabilidade

A frequência indicativa poderá ser utilizada quando for possível calcular a tendência do risco, conforme o resultado do teste do controle.

Já a análise do impacto obedecerá os seguintes critérios:

		VETOR PRINCIPAL	DEMAIS VETORES				
Nível	**Descritor**	**OPERAÇÕES**	**Segurança do Trabalho**	**Meio Ambiente**	**Pessoas**	**Jurídico**	**Imagem**
1	Muito Baixo	Comprometimento irrelevante ao projeto, negócio ou alcance dos objetivos (Não atendimento as oportunidades e/ou melhorias, etc).	Nenhuma lesão	Sem danos ambientais	Ausência de efeitos negativos na saúde mental, física e no bem-estar dos colaboradores	Não conformidades ou desvios de conduta de baixo impacto (remediáveis) aplicadas por áreas internas resultando em advertências, ações preventivas e implementação de pequenas melhorias.	Visibilidade negativa pontual em canais institucionais e/ou pessoais, mídia online e/ou offline, local e/ou regional
3	Baixo	Comprometimento parcial ao projeto, negócio, entretanto não impede o alcance dos objetivos (Documentos com a revalidação vencida, etc)	Lesões tratadas com primeiros-socorros internamente, riscos à saúde do colaborador	Danos ambientais de baixa proporção	Efeitos negativos pequenos na saúde mental, física e no bem-estar dos colaboradores	Não mensurar adequadamente os riscos e o passivo trabalhista da empresa, atos ilícitos, não conformidades ou desvios de conduta em apuração por órgãos externos com potencial aplicação de multas/indenizações, mas sem necessidade de provisionamento	Visibilidade negativa de pouco alcance em canais institucionais e/ou pessoais, mídia online e/ou offline, local e/ou regional,

		VETOR PRINCIPAL	DEMAIS VETORES				
Nível	**Descritor**	**OPERAÇÕES**	***Segurança do Trabalho***	***Meio Ambiente***	***Pessoas***	***Jurídico***	***Imagem***
5	Médio	Comprometimento razoável ao projeto, negócio ou alcance dos objetivos, porém recuperável (Ineficiências operacionais e de processo, etc).	Lesões com tratamento médico externo e sem afastamento, equipamentos descalibrados	Danos ambientais contidos com auxílio interno e imediatamente	Efeitos negativos na saúde mental, física e no bem-estar dos colaboradores com afastamentos do trabalho	Não conformidades ou desvio de conduta aplicadas por órgãos externos, necessidade de provisionamento de despesas, mas passível de reversão.	Visibilidade negativa de médio alcance em canais institucionais e/ou institucionais, mídia online e/ou offline, local e/ou regional, nacional
8	Alto	Comprometimento da maior parte do projeto, negócio ou alcance dos objetivos, de difícil reversão (pandemia, greve, falta de profissionais qualificados, impossibilidade de participar de licitações, certificações, etc)	Lesões graves com incapacidade temporária com hospitalização, sanções e multas; Perda de AVCB, Perda de Alvará de Funcionamento	Danos ambientais controláveis com auxílio externo, sanções e multas, passivo ambiental, não atendimento as legislações ambientais, perda do direito do uso dos recursos hídricos	Afastamento temporário do colaborador, pelo INSS, devido a danos psicossociais relativos ao ambiente de trabalho	Processos de larga abrangência que possam culminar na imposição de sanções, de órgãos fiscalizatórios, regulatórios, associações, responsabilização criminal, civil ou administrativa aos gestores e membros do conselho de administração, *passivo trabalhista,* suborno, corrupção, conflitos de interesses	Visibilidade negativa expressiva em canais institucionais e/ou pessoais, mídia online e/ou offline, local e/ou regional, nacional

		VETOR PRINCIPAL	DEMAIS VETORES				
Nível	**Descritor**	**OPERAÇÕES**	**Segurança do Trabalho**	**Meio Ambiente**	**Pessoas**	**Jurídico**	**Imagem**
10	Muito Alto	Comprometimento total ao projeto, negócio ou alcance dos objetivos, de forma irreversível (Interrupção de fornecimento de energia, perda de autorizações)	Morte ou deficiência permanente	Danos ambientais de difícil controle	Afastamento permanente do colaborador devido a danos psicossociais relativos ao ambiente de trabalho	Decisões judiciais ou administrativas resultando em grandes penalizações, multas, proibição da prestação de serviços e/ou necessidade de provisionamento de despesas	Visibilidade negativa massiva em canais institucionais e/ou pessoais, mídia online e/ou offline, local e/ou regional, nacional e/ou internacional

Tabela 2 - Escala de impacto

A partir da combinação entre probabilidade e impacto em uma matriz, estabelece-se o nível de risco

Nível de risco: Probabilidade X Impacto

Vale ressaltar que os parâmetros de probabilidade e impacto acima são réguas iniciais que serão melhor analisadas no momento da análise do risco, estando sujeitos a adequação e enquadramento da probabilidade real ou estimada aplicável a cada caso.

É de responsabilidade do Risk Onwer informar tempestivamente a área de Gestão de Riscos acerca da inclusão, exclusão, alteração na classificação dos riscos, alteração de Control Owner, entre outros.

5.3.3 Avaliação do risco

A avaliação dos riscos faz uma compreensão dos riscos a partir da comparação dos resultados da análise do risco com os critérios estabelecidos para determinar onde é necessária ação adicional.

As decisões a serem tomadas podem envolver;

- Fazer nada;
- Considerar as opções de tratamento de riscos;
- Realizar análises adicionais para melhor compreender o risco;
- Manter os controles existentes;
- Reconsiderar os objetivos.

5.3.2.1 Nível de risco

Riscos acima do limite de exposição: **faixa vermelha**
Riscos com necessidade de monitoramento: **faixa amarela**
Riscos que podem ser aceitos: **faixa verde**

5.3.2.2 Priorização dos riscos

Concluída a análise e obtida a classificação, os riscos "altos" e "muito altos" deverão ter seu tratamento priorizado, com estabelecimento de plano de ação pelo Risk Owner para reduzir a probabilidade e/ou impacto do risco, e são passíveis de serem abordados na Reunião do Comitê de Compliance e Riscos Corporativos juntamente com a Diretoria responsável pelo risco.
Convém que os riscos classificados como "muito alto" recebam direcionamentos advindos do Comitê de Compliance e Riscos Corporativos.

5.4 Tratamento do risco

Nesta fase, o departamento responsável pelo gerenciamento dos riscos, em conjunto com o Control Owner, deverá selecionar e implementar as melhores opções de resposta ao risco, avaliar a eficácia desta resposta, decidir se o risco remanescente é aceitável e, se for aplicável, realizar tratamentos adicionais criando planos de ação ou solicitando que seja realizado um trabalho de melhoria contínua para a redução do grau do risco. Deve-se balancear benefícios potenciais, custos, esforços da implantação, vantagens e desvantagens da implementação. Além disso, as áreas, em conjunto, deverão:

- Realizar análises adicionais para melhor compreensão do risco;
- Recalibrar o grau do risco, se aplicável;
- Aprimorar os controles e iniciativas existentes, e avaliar a necessidade de novas implementações.

As possibilidades de tratamento dos riscos são:

Aceitar: Não há a necessidade iniciativas de mitigação.

Compartilhar: Compartilhar riscos com empresas terceiras.

Monitorar: Acompanhar o grau do risco através dos controles internos executados em intervalos planejados.

Mitigar: Reduzir a probabilidade e/ou impacto de um evento a níveis aceitáveis, através dos controles internos e/ou planos de ação.

Eliminar: Excluir completamente o evento do risco podendo descontinuar uma atividade ou interrompendo um processo.

O departamento responsável pelo gerenciamento dos riscos corporativos deverá acompanhar as medidas de controle indicadas pelos Control Owners, em acordo com a periodicidade definida para cada controle, podendo ser mensalmente, trimestralmente, semestralmente*, entre outros*, além de solicitar

nova análise indicando se o risco ainda existe, se novas medidas de controle foram implantadas ou se não houve avanços.

As Atividades de Controle, se estabelecidas de forma tempestiva e adequada, podem vir a prevenir ou administrar os riscos inerentes ou em potencial da entidade. São exemplos de algumas tipologias de atividades de controle:

- Procedimentos de autorização e aprovação;
- Segregação de funções (autorização, execução, registro, controle);
- Controles de acesso a recursos e registros;
- Verificações;
- Conciliações;
- Avaliação de desempenho operacional;
- Avaliação das operações, dos processos e das atividades.

5.5 Monitoramento e análise crítica

O departamento responsável pelo gerenciamento dos riscos corporativos realiza atividades gerenciais contínuas de monitoramento e análise crítica permanente dos riscos através das atividades de controles existentes e acompanhamento dos planos de ação no que se refere aos prazos, notificando o Risk Owner por e-mail e/ou em reunião específica sempre que o prazo expirar, além de avaliar se a ação realizada está de acordo com o que foi determinado.

Os controles e testes não podem deixar de serem executados pela ausência do Control Onwer ou qualquer outro motivo.

Se constatada a ineficácia da medida de controle, o departamento responsável pelo gerenciamento dos riscos corporativos juntamente com os Owners deverá sugerir novos controles mais aderentes ao processo.

O plano de ação poderá ser encerrado, somente após o seu cumprimento total, parcial ou após justificativa aceitável da impossibilidade de cumprimento e o mesmo poderá será encerrado com o status de Não Atendido e/ou Atendido com ressalvas.

Poderão ser implantados questionários de autoavaliação de controles, onde o Control Owner avaliará os controles quanto a exposição e materialização dos riscos.

As avaliações independentes, realizadas pelas auditorias internas e externas e são analisadas e a depender da sua criticidade poderá ser considerada na Matriz de Riscos Corporativos.

5.6 Registro e relato

Todas as etapas do processo de gestão de riscos devem ser registradas e ter sua documentação de suporte e de evidências armazenadas na plataforma de gestão de riscos, resultando em uma Matriz de Riscos, com informações disponíveis a qualquer tempo para suportar a tomada de decisão, melhorar as atividades de gestão e auxiliar na interação necessária para efetiva prevenção e mitigação dos riscos.

Apesar de haver um ciclo periódico de revisão dos riscos ativos, que ocorre anualmente, pode ocorrer, ocasionalmente, a identificação de novos riscos ou reavaliação dos existentes.

As informações acerca da Gestão de Riscos Corporativos são informadas:

- Semanalmente – através do e-mail de Status Report à Coordenação de Compliance;
- Mensalmente – através do Book de Riscos para a Alta Liderança do Departamento de Compliance, bem como ao Comitê de Compliance e Riscos Corporativos:
- Anualmente – através de Reunião da Reanálise dos Riscos juntamente aos Owners do processo.

6. MAPA DE CALOR

O cálculo *é realizado* pela atribuição de ratings de avaliação a serem preenchidos na Matriz de Riscos que associados a fatores ponderados são multiplicados e resultam no grau do risco, conforme ilustrado abaixo: