

Título: GESTÃO DE RISCOS**1. OBJETIVOS**

Estabelecer diretrizes e princípios que nortearão a Gestão de Riscos na Âmbar Energia Amazonas S.A.

2. ABRANGÊNCIA

Esta norma se aplica no âmbito da Âmbar Energia Amazonas S.A.

3. REFERÊNCIAS

- COSO - ERM (Committee of Sponsoring Organizations of the Treadway *Commission*) – *Enterprise Risk Manangement Framework*;
- Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos: Diretrizes;
- Norma ABNT ISO GUIA 31073:2023 – Gestão de Riscos: Vocabulário;
- Política de Gestão de Riscos da Âmbar Energia Amazonas S.A.;
- Resolução Normativa nº. 948/2021, de 18/11/2021, da Agência Nacional de Energia Elétrica - ANEEL.

4. CONCEITOS

- 4.1 Análise da Vulnerabilidade:** Avaliação dos controles, por meio da importância da exposição do risco e da probabilidade de ocorrência dos respectivos fatores, visando à redução do impacto dos riscos nas operações da companhia;
- 4.2 Appetite ou Propensão ao Risco:** Refere-se à disposição de uma empresa em aceitar a possibilidade de perdas ou incertezas em busca de objetivos maiores, como maiores lucros ou crescimento. É a postura da empresa diante de situações que envolvem riscos, podendo variar desde uma postura mais conservadora, evitando ao máximo riscos, até uma mais agressiva, buscando ativamente oportunidades em ambientes incertos;
- 4.3 Área Proprietária do Risco (Risk Owner):** É a pessoa ou grupo de pessoas dentro de uma organização responsável por gerenciar um risco específico ou um conjunto de riscos;
- 4.4 Categoria de Risco:** Segundo nível da classificação dos riscos na Matriz de Riscos. Cada categoria reúne riscos considerados de uma mesma classe;
- 4.5 Control Self-assessment:** Avaliação dos controles internos de uma área proprietária de risco realizada por meio de autoanálise gerencial;
- 4.6 Controle Interno:** Mecanismo manual ou sistêmico que minimiza a possibilidade de ocorrência dos riscos do negócio;

Título: GESTÃO DE RISCOS

- 4.7 Evento de Risco:** Ocorrência ou ação, gerada por uma fonte interna ou externa, que afeta o alcance de uma estratégia corporativa ou um objetivo de negócio;
- 4.8 Fator do Risco:** Descreve determinada circunstância ou atividade que contribui, individualmente ou combinada com outras, para a materialização dos riscos nas operações;
- 4.9 Formulário de Risco ou Relatório Operacional:** Conjunto de tabelas desenvolvido para auxiliar na gestão dos riscos priorizados na companhia, possibilitando compilar em um único documento, as informações relativas aos mesmos, avaliando a vulnerabilidade ao risco e o impacto de sua materialização nas operações ou resultados da companhia;
- 4.10 Gestão Integrada de Riscos – GIR:** Conjunto de ações coordenadas que buscam garantir que os objetivos sejam perseguidos, dentro de limites aceitáveis de risco, alinhando estratégia, processos, pessoas, tecnologia e conhecimentos, para a preservação e a criação de valor para a companhia e seus acionistas;
- 4.11 Impacto do Risco:** Resultado da materialização de um dado risco, medido por critérios preferencialmente quantitativos, como por exemplo: potencial impacto no fluxo de caixa ou no valor econômico, decorrente de perdas de ativos, perdas de receitas, indenizações, multas, aumento de custos, impactos sociais, no meio ambiente ou na reputação e imagem, dentre outros;
- 4.12 Probabilidade do Risco:** Possibilidade de materialização do risco, considerando a atual estrutura de controles que sobre ele atuam;
- 4.13 Incerteza:** Estado, mesmo que parcial, da deficiência de informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade;
- 4.14 Indicador de Risco (Key Risk Indicator – KRI):** Medida utilizada para avaliar como o risco se comporta e para fornecer alertas quanto à exposição ou seu potencial de perda futura;
- 4.15 Materialidade:** Valor de erros ou falhas sistêmicas e operacionais que pode incorrer em alto impacto e influenciar as decisões dos utilizadores da informação (stakeholders);
- 4.16 Matriz de Controle:** Documento que contém os controles estabelecidos pela companhia para detectar e corrigir problemas na aplicação de seus princípios e diretrizes;
- 4.17 Matriz de Riscos:** Conjunto dos riscos identificados pela companhia, classificados em pilares, categorias, fatores de risco, eventos, suas causas e consequências;
- 4.18 Oportunidade:** Possibilidade de que determinado evento ocorra e afete positivamente o alcance de objetivos corporativos ou adicione valor à companhia;

Título: GESTÃO DE RISCOS

4.19 Pilar de Risco: Constitui o primeiro nível da classificação dos riscos na Matriz de Riscos. São cinco os pilares de risco:

4.19.1 Pilar Estratégico: Reúne riscos referentes à tomada de decisões na companhia e/ou aos processos que impactam na continuidade, crescimento, valor da companhia e seus objetivos de negócio;

4.19.2 Pilar Financeiro: Conjunto de riscos decorrentes de processos e atividades que envolvem as finanças e os resultados da companhia;

4.19.3 Pilar Operacional: Engloba riscos relacionados à eficácia e eficiência das operações e atividades rotineiras da companhia;

4.19.4 Pilar de Conformidade: Trata dos riscos relativos ao cumprimento de leis e regulamentações aplicáveis à companhia;

4.19.5 Pilar Cibernético: Engloba riscos relacionados a confidencialidade das informações e as operações de tecnologia da companhia.

4.20 Política de Gestão de Riscos: Documento interno que estabelece princípios, diretrizes do processo e responsabilidades da gestão integrada de riscos da companhia, e orienta os processos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos inerentes às atividades, incorporando a visão de riscos à tomada de decisões estratégicas e em conformidade com as melhores práticas de mercado;

4.21 Riscos Corporativos: É um evento incerto que pode afetar a capacidade de uma empresa de atingir seus objetivos, funcionando como uma ameaça ou uma oportunidade;

4.22 Risco: A possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos;

4.23 Risco Inerente: Risco existente, independentemente de qualquer ação da companhia, vinculado a um determinado processo ou atividade;

4.24 Riscos Empresariais: Riscos que, mesmo não sendo prioritários na companhia, mas que, em virtude da relevância e do interesse corporativo que envolvem, devem ser reportados, em razão da sua responsabilidade com relação ao seu Conselho de Administração, acionistas, investidores e órgãos reguladores/fiscalizadores;

4.25 Responsável pelo Risco (Proprietário/Suplente do Risco): Integrante responsável pelo gerenciamento de determinado risco, relacionado a um processo sob sua responsabilidade. O "Responsável pelo risco" deve estar alinhado com a Gestão Integrada de Riscos em todos os assuntos relacionados ao gerenciamento do risco sob sua responsabilidade;

4.26 Tolerância ao Risco: Faixa de desvios em relação à exposição a riscos, determinada como aceitável por uma empresa durante o desempenho de suas operações;

Título: GESTÃO DE RISCOS

4.27 Vulnerabilidade ao Risco: Identifica o quanto a companhia está propensa à ocorrência do risco;

4.28 Walkthrough: Técnica que auxilia o entendimento do fluxo de transações e a interação dos controles, possibilitando confirmar que os controles dentro do processo foram concebidos e implementados corretamente.

5. RESPONSABILIDADES

5.1 Conselho de Administração

5.1.1 Ter conhecimento sobre as questões estratégicas concernentes ao processo de gestão de riscos, tais como o grau de propensão ao risco da companhia e suas faixas de tolerância;

5.1.2 Deliberar sobre o papel que a Diretoria Executiva deve exercer no gerenciamento dos riscos e a política que deve nortear o processo.

5.2 Diretoria Executiva

5.2.1 Determinar a alocação de recursos necessários ao processo de gestão de riscos;

5.2.2 Analisar e aprovar a matriz de riscos da companhia;

5.2.3 Analisar e aprovar a lista de riscos prioritários e seus respectivos proprietários.

5.3 Compliance

5.3.1 Coordenar e definir os padrões a serem seguidos no que tange aos processos da Gestão Integrada de Riscos, os seus sistemas de suporte e as formas e a periodicidade dos seus reportes;

5.3.2 Apoiar e garantir a identificação e o monitoramento dos riscos pelas áreas proprietárias, de acordo com as políticas e técnicas aprovadas pela Alta Direção;

5.3.3 Garantir que os riscos inerentes às atividades da companhia sejam devidamente mapeados, tratados e monitorados pelas áreas proprietárias, de forma a mitigar ou até mesmo evitar sua materialização;

5.3.4 Coletar os dados para a elaboração da matriz de riscos da companhia, por meio de entrevistas com os representantes da Alta Direção e das áreas de negócios, emitindo relatórios institucionais e/ou de outras técnicas;

5.3.5 Obter informações sobre o grau de vulnerabilidade aos riscos mencionados e o nível do impacto ao qual a companhia estará exposta no caso da materialização dos mesmos;

Título: GESTÃO DE RISCOS

- 5.3.6** Analisar a periodicidade, a relevância e a capacidade do dado e medir o impacto do fator de risco ao qual está relacionado;
- 5.3.7** Apoiar a área proprietária do risco na elaboração de métricas para mensuração do impacto e de recomendações e planos de ação referentes aos principais riscos analisados;
- 5.3.8** Monitorar e comunicar a evolução dos riscos analisados;
- 5.3.9** Apoiar a Alta Direção na elaboração de reportes internos e externos relacionados a riscos;
- 5.3.10** Efetivar as ações necessárias ao estabelecimento do ambiente de controles para auxílio no tratamento dos riscos identificados pelas áreas proprietárias;
- 5.3.11** Realizar a consolidação do ambiente de controles internos da companhia, a partir das informações recebidas das áreas;
- 5.3.12** Prover informações sobre os controles mais utilizados no mercado para mitigação dos fatores do risco em análise;
- 5.3.13** Realizar o walkthrough de forma a testar as informações apresentadas a respeito de cada um dos controles apontados como implementados.

5.4 Áreas Proprietárias de Riscos

- 5.4.1** Gerenciar os riscos inerentes às suas atividades, identificando-os, avaliando-os e tratando-os de modo a otimizar as decisões, com o intuito de, através do aproveitamento das oportunidades, obter vantagens competitivas e garantir a geração de valor para acionistas e demais partes interessadas;
- 5.4.2** Preencher o Formulário de Risco (documento disponibilizado pelo departamento de *Compliance*), validando as informações que os compõem e assinando um parecer confirmando sua legitimidade;
- 5.4.3** Desenvolver e executar o Plano de Ação das atividades específicas a serem implementadas para a melhoria de controles ineficazes ou inexistentes, de forma que os riscos inerentes ao processo sejam mitigados.

6. DIRETRIZES

6.1 Identificação dos Riscos

- 6.1.1** Os riscos aos quais a companhia está exposta devem ser mapeados e classificados;
- 6.1.2** A matriz de riscos da companhia deve ser organizada segundo os pilares estratégico, operacional, financeiro, de conformidade e cibernético;

Título: GESTÃO DE RISCOS

6.1.2.1 Os pilares são subdivididos em categorias de risco, e para cada categoria devem ser identificados os eventos de riscos, para os quais são definidos os principais fatores e impactos.

6.1.3 A matriz de riscos da companhia deve ser baseada em um número de eventos de forma que não seja muito detalhada, para não tornar o tratamento de um só risco complexo e demorado, e nem muito sucinta, para não deixar de tratar todos os riscos.

6.2 Avaliação dos Riscos

6.2.1 O grau de vulnerabilidade aos riscos e o nível do impacto ao qual a companhia está exposta, no caso da materialização dos mesmos deve ser obtido por meio de questionários, relatórios ou outras técnicas;

6.2.2 Deve ser desenvolvida uma lista de riscos considerados prioritários, a partir da avaliação das informações coletadas e do grau de propensão aos riscos definidos;

6.2.3 Os riscos destacados na lista de riscos prioritários devem ser analisados seguindo as seguintes etapas:

- a) Identificação da área proprietária do risco;
- b) Contextualização e Perfil do Risco;
- c) Elaboração da Matriz de Controles;
- d) Mensuração do grau de vulnerabilidade da companhia ao risco analisado, preenchido através da realização do *control self-assessment* e/ou do *walkthrough*;
- e) Levantamento de dados para avaliação do impacto do risco sobre as atividades da companhia;
- f) Consolidação e cruzamento dos dados referentes ao impacto e à vulnerabilidade do risco, indicando a posição do mesmo em relação ao grau de materialidade da companhia e gerando o mapa de risco;
- g) Elaboração de Planos de Ação;
- h) Definição de protocolos e coleta de dados para o cálculo de indicadores de riscos.

6.3 Tratamento dos Riscos

6.3.1 Com base na tolerância/propensão ao risco da companhia, deve-se definir qual tratamento será dado a cada risco:

Título: GESTÃO DE RISCOS

- a) **Evitar:** a companhia opta por abandonar as atividades que possam gerar riscos ou provocar sua exposição aos mesmos;
- b) **Aceitar:** a companhia entende que a exposição ao risco e o seu impacto são pouco relevantes e que, por essa razão, o esforço para mitigar o risco ou transferi-lo seria maior do que o valor do impacto causado por sua materialização;
- c) **Transferir:** a companhia reduz o impacto e/ou a sua vulnerabilidade ao risco através da transferência de suas consequências a outros agentes ou partes;
- d) **Mitigar:** a companhia busca minimizar o impacto e/ou a sua vulnerabilidade ao risco tratado por meio de atividades e/ou planos de ação.

6.3.2 Os planos de ação devem ser priorizados para definição da ordem de implementação, com base em sua relevância e eficácia no que tange à opção de tratamento escolhida.

6.4 Monitoramento dos Riscos

- 6.4.1** A situação do risco deve ser acompanhada por meio do desempenho dos indicadores e de relatórios periódicos, levando em consideração a propensão e a tolerância ao risco definidas;
- 6.4.2** A implantação e o acompanhamento dos planos de ação e o alcance das metas estabelecidas devem ser realizados por meio de atividades gerenciais contínuas e avaliações independentes;
- 6.4.3** Todo o processo de identificação, avaliação e tratamento dos riscos deve ser contínuo e sistemático;
- 6.4.4** O monitoramento dos controles implementados deve ser feito através do *walkthrough*.

6.5 Comunicação dos Riscos

- 6.5.1** Durante todo o Processo de Gestão de Riscos, as áreas responsáveis pelos riscos priorizados e de Governança (Alta direção) devem ser informadas a respeito da situação do risco;
- 6.5.2** Em paralelo ao processo de gestão de riscos devem ser realizadas ações complementares para tornarem mais robustas suas estruturas básicas. Essas ações tratam da revisão periódica da Política de Gestão de Riscos, da matriz de riscos e da definição de responsabilidades das demais áreas de negócios envolvidas no processo.

Título: GESTÃO DE RISCOS

7. HISTÓRICO

- 7.1 As anotações das alterações nesta Norma devem ser realizadas e acompanhadas pelo Departamento de Planejamento e Controle – DFP, em conjunto com Área Gestora, seja de conteúdo ou modificação da legislação pertinente, registrando a versão atual do normativo aprovado.

8. REGISTROS

- 8.1 Devem ser considerados como registro desta Norma todos os documentos existentes e anexados ao processo, obedecendo à classificação e temporalidade, de acordo com o estabelecido pelo Conselho Nacional de Arquivos - CONARQ e legislação pertinente.

9. DISPOSIÇÕES GERAIS

- 9.1 Toda e qualquer situação que não esteja contemplada nesta norma será analisada pela área gestora do processo e submetida à Diretoria Executiva;
- 9.2 As eventuais necessidades de alterações desta norma, com o objetivo de otimização dos processos ou sua atualização face às novas legislações sobre o assunto, devem ser submetidas à Diretoria Executiva, com as devidas justificativas;
- 9.3 Esta norma deve ser reavaliada a cada 02 (dois) anos, ou quando houver necessidade de revisão pela Área gestora do normativo, sendo sua vigência considerada a partir da data de sua aprovação;
- 9.4 O não cumprimento dos termos desta norma sujeita o colaborador infrator às penalidades previstas nas normas internas e legislação em vigor.