compesa

POLÍTICA

GGR-POL-008-02

Vigência: 29/10/2023

**Titulo:**

Política de Gestão de Riscos

**Elaborado/Alterado por:**

GER DE COMPLIANCE, GESTAO DE RISCOS E CONTROLE INTERNO - GGR

**Aprovado por:**

Diretoria Colegiada

# 1. OBJETIVO

A Política de Gestão de Riscos tem por objetivo estabelecer princípios, diretrizes e responsabilidades a serem observadas no processo de gestão de riscos da COMPESA – Companhia Pernambucana de Saneamento, de forma a assegurar a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos do negócio.

# 2. APLICAÇÃO

Este instrumento normativo se aplica a todas as áreas da COMPESA, as quais são integrantes do processo de gerenciamento de riscos, direta ou indiretamente.

# 3. DEFINIÇÕES

**3.1 Símbolos e abreviações**

- **ABNT:** Associação Brasileira de Normas Técnicas;
- **AGR:** Análise Geral de Risco;
- **COSO® ERM:** Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management(Gerenciamento de Riscos Corporativos);
- **IBGC:** Instituto Brasileiro de Governança Corporativa;
- **ISO:** International Organization for Standardization (Organização Internacional para Padronização);
- **KRI:** Key Risk Indicator (Indicador Chave de Risco).

**3.2 Conceitos**

**3.2.1 Risco:** Conforme definido no COSO® ERM, risco é a possibilidade de ocorrência de um evento, oriunda de fontes internas ou externas, capaz de afetar adversamente o atendimento dos objetivos da Companhia. É o efeito da incerteza nos objetivos. [ABNT ISO GUIA 73:2009, definição 1.1]

**3.2.2 Risco de Negócio:** É a exposição a impactos negativos resultantes de eventos esperados ou não esperados de natureza estratégica, operacional, financeira, legal e outros decorrentes da maneira pela qual a organização busca atingir os seus objetivos.

**3.2.3 Gestão de Riscos:** Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. [ABNT ISO GUIA 73:2009, definição 2.1]

**3.2.4 Apetite ao Risco:** Reflete a filosofia de gerenciamento de riscos da Companhia. Quantidade e tipos de riscos que uma organização está preparada para buscar, reter, assumir ou afastar. [ABNT ISO GUIA 73:2009, definição 3.7.1.2]

**3.2.5 Tolerância ao Risco:** Disposição da organização ou parte interessada em suportar o risco após o tratamento do risco, a fim de atingir os seus objetivos. [ABNT ISO GUIA 73:2009, definição 3.7.1.3]

**3.2.6 Identificação de Riscos:** Processo de busca, reconhecimento e descrição de riscos. [ABNT ISO GUIA 73:2009, definição 3.5.1]

**3.2.7 Proprietário do Risco (ou simplesmente Dono do Risco):** Pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco. [ABNT ISO GUIA 73:2009, definição 3.5.1.5]

**3.2.8 Controle Interno:** Um processo conduzido pela estrutura de governança, pela administração e por outros profissionais da entidade, e desenvolvido para proporcionar garantia (segurança) razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade. [COSO® ERM 2016]

**3.2.9 Grau de Exposição:** Grau em que uma organização ou parte interessada está sujeita a um evento. [ABNT ISO GUIA 73:2009, definição 3.5.1.5]

**3.2.10 Governança Corporativa:** Conforme definido pelo Instituto Brasileiro de Governança Corporativa (IBGC), é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle.

**3.2.11 Gestores:** para fins deste instrumento normativo, são considerados gestores todos os gerentes de unidades de negócio, de gerências funcionais e as assessorias que estão ligadas direta ou indiretamente com os riscos inerentes às atividades da COMPESA.

**3.2.12 Diretoria Primária:** para fins deste instrumento normativo, considera-se Diretoria Primária aquela vinculada diretamente com a categoria de risco em análise.

# 4. RESPONSABILIDADES

## 4.1 Elaboração e alteração

A área gestora, a qual é responsável pela elaboração do presente normativo, a partir da identificação da necessidade de revisão e alteração do normativo, irá iniciar o processo de atualização, considerando mudanças nos procedimentos organizacionais, surgimento de novas atividades, melhorias nos processos, demandas das áreas relacionadas ao normativo e outras oportunidades de melhoria.

## 4.2 Revisão e aprovação

Após a elaboração, o normativo deverá ser submetido à revisão de conteúdo e padronização da Gerência de Excelência Organizacional (GEO) com aprovação da Diretoria Colegiada na Reunião de Diretoria (REDIR), com formalização por meio de Resolução de Diretoria (RD), e posterior Aprovação do Conselho de Administração (CA)

## 4.3 Distribuição

A GEO será responsável por disponibilizar este normativo e suas alterações para todas as gerências/áreas interessadas e envolvidas no processo, utilizando o Sistema de Gestão de Normativos (SGN). A área gestora é responsável pela atualização do instrumento normativo quando disponibilizado fora do SGN.

## 4.4 Acesso

A visualização com cópia controlada do instrumento normativo será acessível a todas as gerências/áreas a que se aplica através do SGN e ao público externo por meio do site da COMPESA, quando aplicável.

## 4.5 Uso

A utilização da Política de Gestão de Riscos será feita por todas as gerências/áreas que são integrantes do processo de gerenciamento de riscos, direta ou indiretamente.

## 4.6 Armazenamento e disponibilização

O armazenamento do instrumento normativo será virtual, sendo disponibilizado no SGN, com acesso pela intranet da Companhia. A área gestora é responsável pela publicação externa por meio do site da COMPESA, quando aplicável.

## 4.7 Preservação e recuperação

A preservação deste normativo será de responsabilidade da GEO. As solicitações de outras áreas para a consulta de versões anteriores do documento deverão ser feitas e aprovadas eletronicamente pelo SGN, sendo analisadas pela área gestora. A preservação e recuperação do normativo disponibilizada fora do SGN é de responsabilidade da área gestora.

## 4.8 Controle de alterações

O controle de alterações será feito pela área gestora e registrado no próprio documento, no campo “Histórico de alterações”, conforme item 8 deste normativo.

### 4.9 Retenção e disposição

Apenas a versão vigente do normativo estará acessível no SGN, estando as versões anteriores disponíveis para consulta apenas para a GEO e para a área gestora, bem como retidas em backups.

## 5. DETALHAMENTO

**5.1 Processo de gestão integrada de riscos.**

O processo de gestão integrada de riscos está conectado à busca do alcance dos objetivos estratégicos da Companhia, descritos em seu planejamento estratégico e, dessa forma, ele se integra aos seus demais sistemas de governança.
Por meio do gerenciamento de riscos, a Companhia exerce o controle corporativo dos riscos atuando de modo integrado e independente, preservando e valorizando o ambiente de decisões colegiadas, desenvolvendo e implementando metodologias, modelos e ferramentas de mensuração e controle. Os riscos são proativamente identificados, mensurados, mitigados, acompanhados e reportados, sendo constituído pelas etapas em sequência:


**Figura 1 – Componentes do processo de gestão de riscos**

O detalhamento das etapas do processo de gestão integrada de riscos da COMPESA está descrito na Norma Interna de Gestão de Riscos.

**5.2 Estrutura Organizacional**

A Gestão de Riscos na COMPESA é realizada através de uma estrutura coordenada pelo Conselho de Administração, apoiado pelo Comitê de Auditoria Estatutário e pela Secretaria de Governança, e com o envolvimento ativo de três atores principais: a Gerência de *Compliance*, Gestão de Riscos e Controle Interno, as Diretorias em conjunto com a Diretoria da Presidência e, por fim, os Gestores ligados direta ou indiretamente com os riscos inerentes ao negócio.

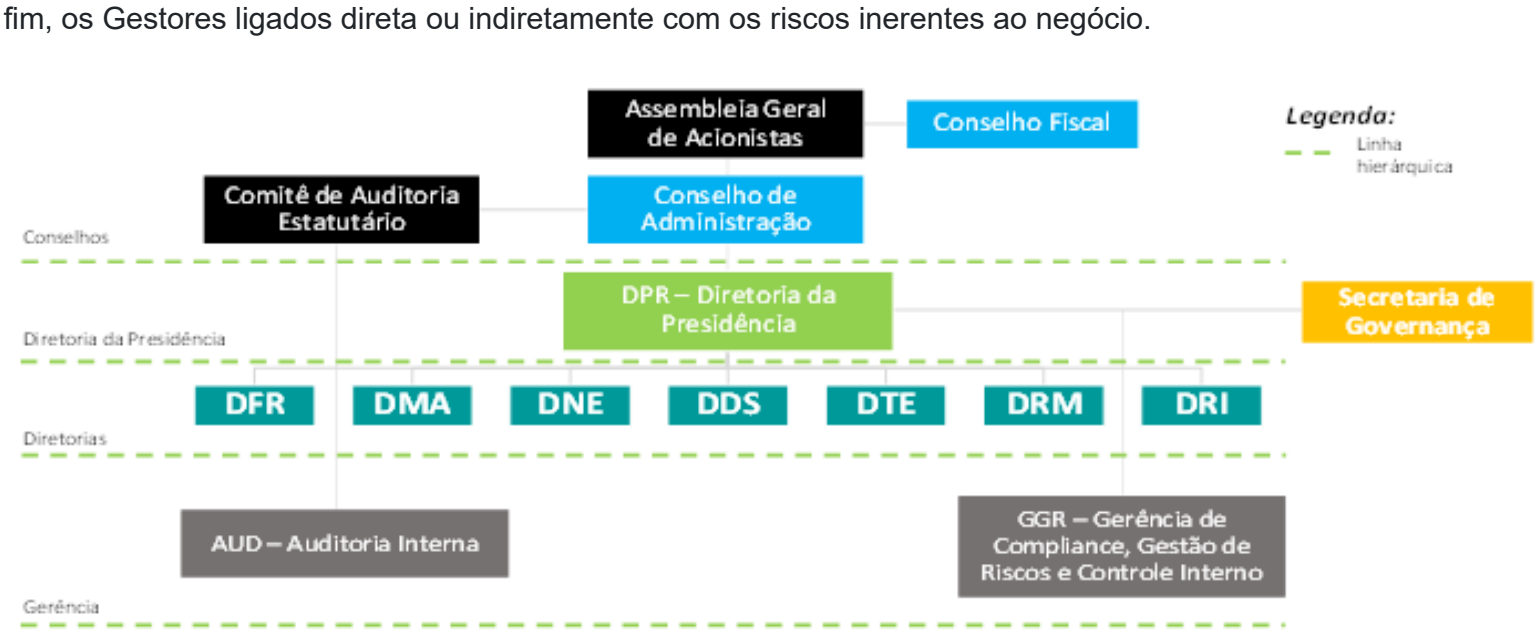


**Figura 2 – Estrutura Organizacional da Gestão de Riscos**

A Gerência de *Compliance,* Gestão de Riscos e Controle Interno atua de forma imparcial e independente, se reportando diretamente para a Diretoria da Presidência, através da Secretaria de Governança, e para o Conselho de Administração, quando necessário.

### 5.3 Competências e responsabilidades

**a) Conselho de Administração:** exerce atividades de aprovação visando assegurar o equilíbrio, a transparência e a integridade das informações, diante do cumprimento das suas principais atribuições, a saber:

- Aprovar as diretrizes da Política de Gestão de Riscos;
- Aprovar a metodologia e os documentos chaves (exemplos: Política de Gestão de Riscos, Norma Interna de Gestão de Riscos, metodologias etc. a serem utilizados para a condução do processo de Gestão de Riscos;
- Aprovar o apetite e a tolerância aos de riscos da Companhia definidos pela Diretoria Colegiada;
- Aprovar o sistema de gestão de riscos e de controle interno estabelecido para a Companhia e proposto pela Diretoria Colegiada;
- Aprovar o plano de resposta aos riscos com nível de exposição extrema proposto pela Diretoria Colegiada;
- Implementar e supervisionar, por meio dos demais órgãos de governança, os sistemas de Gestão de Riscos e de Controle Interno estabelecidos para a prevenção e mitigação dos principais riscos a que está exposta a Companhia, inclusive os riscos relacionados à integridade das informações contábeis e financeiras e os relacionados á ocorrência de corrupção e fraude;
- Aprovar o Plano de Negócio e a Estratégia de longo prazo em conformidade com a Análise de Riscos e Oportunidades para os próximos 5 (cinco) anos, proposta pela Diretoria Colegiada.

**b) Comitê de Auditoria Estatutário:** exerce atividades de apoio ao Conselho de Administração, a exemplo de:

- Avaliar o grau de aderência dos processos da estrutura de gerenciamento de riscos às políticas estabelecidas;
- Propor recomendações ao Conselho de Administração sobre políticas, estratégias e limites de gerenciamento de riscos;
- Submeter periodicamente ao Conselho de Administração relatório sobre os resultados do monitoramento dos riscos inerentes às atividades da Companhia e que possam afetar o atendimento aos seus objetivos;
- Acompanhar de forma sistemática os Indicadores de Riscos, com o objetivo de garantir sua eficácia;
- Incentivar o cumprimento da Política de Gestão de Riscos e a Norma Interna de Gestão de Riscos;
- Analisar o apetite ao risco, proposto pela Diretoria Colegiada, e submetê-lo à aprovação do Conselho de Administração;
- Acompanhar o perfil de risco, performance, exposições versus limites e controle dos riscos.

**c) Diretoria Colegiada:** exerce atividades de gerenciamento dos riscos do negócio e submete as decisões ao Conselho de Administração, a exemplo de:

- Avaliar e priorizar os riscos do negócio e submeter para aprovação do Conselho de Administração;
- Implementar e supervisionar os sistemas de gestão de riscos e de controle internos estabelecidos para a Companhia;
- Aprovar o mapeamento dos riscos e a execução de trabalhos específicos nos processos;
- Aprovar o plano de resposta aos riscos com grau de exposição média e alta;
- Deliberar sobre as discordâncias na avaliação e/ou sobre o plano de resposta para riscos de impacto baixo, médio, alto ou extremo;
- Definir as medidas de mitigação dos Riscos e submeter à aprovação do Conselho de Administração, no que couber;
- Elaborar e apresentar, ao Conselho de Administração, o plano de negócios e a estratégia de longo prazo, em conformidade com a análise de riscos e oportunidades, para o exercício anual seguinte contemplando o horizonte para os próximos 5 (cinco) anos;

**d) Diretoria Primária:** no que concerne à Gestão de Risco, cabe à Diretoria Primária as seguintes atribuições:

- Aprovar a definição do Proprietário do Risco proposta pela Gerência de *Compliance*, Gestão de Riscos e Controle Interno (GGR);
- Subsidiar os Proprietários dos Riscos com os recursos necessários para tratamento e Gestão dos riscos inerentes a sua área de atuação;

- Responsabilizar-se, em conjunto com os Proprietários dos Riscos, pelos Riscos atribuídos à sua área de atuação;
- Aprovar o plano de resposta aos riscos com grau de exposição baixa;
- Assegurar o cumprimento da Política de Gestão de Riscos e a Norma Interna de Gestão de Riscos nas áreas sobre sua coordenação;
- Controlar os Riscos, em conjunto com o Dono do Risco, dentro dos limites de tolerância definidos pela Alta Administração;
- Integrar o gerenciamento de riscos aos procedimentos de monitoramento através de indicadores gerenciais;
- Supervisionar a implantação dos planos de resposta e monitoramento dos riscos envolvidos nas operações sob sua gestão e desenvolvidos pelos Proprietários dos Riscos em conjunto com a Gerência de *Compliance*, Gestão de Riscos e Controle Interno.

**e) Gerência de *Compliance*, Gestão de Riscos e Controle Interno:** exerce atividades de planejamento e gestão de riscos corporativos da companhia, em conjunto com os donos dos riscos, para tanto, é permitido o acesso a todas as unidades que compõem a COMPESA e a seus respectivos dados e informações. Entretanto, a GGR não possui autoridade hierárquica sobre estas unidades. A GGR possui as seguintes responsabilidades:

- Realizar estudos e análises qualitativas e quantitativas de riscos estratégicos, financeiros, operacionais, etc.;
- Propor e revisar metodologia de avaliação, apetite, tolerância e gestão de riscos corporativos;
- Promover a atualização da Análise Geral de Risco – AGR na periodicidade disposta na Norma Interna de Gestão de Riscos;
- Planejar os processos e riscos a serem mapeados na ótica de identificação e aperfeiçoamento da estrutura de controles;
- Identificar e monitorar riscos, inclusive por meio do estabelecimento de *KRIs* em conjunto com os donos dos Riscos, avaliando vulnerabilidade e impacto da ocorrência, propondo medidas para controle e priorização dos riscos;
- Acompanhar a implementação, pelos gestores das unidades, dos planos de ações provenientes dos trabalhos de auditoria interna e gestão de riscos;
- Realizar articulação e dar suporte às demais áreas da empresa, auxiliando na definição dos responsáveis primários dos riscos e na sua gestão;
- Validar, com a Diretoria Primária, os donos dos riscos propostos.
- Assessorar os responsáveis primários dos riscos quanto à exposição e tolerância ao risco, bem como à definição e execução de ações mitigatórias de controles internos e respostas aos eventos;
- Revisar relatório de análise de riscos contendo classificação, plano de resposta e estratégias de monitoramento;
- Disseminar o dicionário de riscos na Companhia visando à uniformização e à padronização dos conceitos;
- Disseminar a cultura de controles internos com base em modelos reconhecidos internacionalmente (ex.: COSO®);
- Conduzir processos de autoavaliação de controle interno;
- Manter uma base de dados de riscos e controles internos relacionados aos processos de negócio da Companhia em plataforma sistêmica;
- Realizar reportes à Alta Administração, através da Secretaria de Governança, quanto ao cenário de riscos da Companhia;
- Apontar ao Comitê de Auditoria Estatutário, através da Secretaria de Governança, a ocorrência de não conformidades, falhas, desvios, irregularidades e/ou ilegalidades observadas;
- Realizar a gestão do ambiente de controles internos, de acordo com políticas, certificações legais, regulatórias e demais diretrizes para mitigar o risco;
- Orientar e desenhar controles internos junto às áreas da Companhia, alinhados ao processo de avaliação dos riscos para implementação e priorização das ações mitigatórias;
- Dar suporte no monitoramento e avaliação dos controles internos dos processos de negócio (financeiros, corporativos, tecnológicos, operacionais, etc) para tomada de decisão a fim de garantir a conformidade das práticas de gestão de riscos;
- Assegurar e acompanhar a revisão e atualização periódica dos controles internos implementados;
- Assessorar a auditoria interna e externa no levantamento de informações e documentações solicitados para fins de desempenho de suas atividades.

**f) Auditoria Interna:** no que concerne à Gestão de Riscos, cabe à Auditoria Interna, fornecer avaliações independentes, imparciais e tempestivas acerca da efetividade da Gestão de Riscos e os respectivos controles implantados.

**g) Secretaria de Governança:** desenvolver o sistema de governança corporativa da Companhia considerando-se as concepções de gerenciamento de risco e controle interno definidos pela Alta Administração. Nesse contexto, Gestão de Riscos, cabe à Secretaria de Governança:

- Receber, analisar e encaminhar, para aprovação pelos respectivos órgãos competentes, os documentos relacionados à Gestão de Riscos tais como Política de Gestão de Riscos, Norma Interna de Gestão de Riscos, Análise Geral de Risco.
- Apoiar a Gerência de *Compliance*, Gestão de Riscos e Controle Interno (GGR) no gerenciamento dos riscos definidos pela Alta Administração;
- Realizar reportes à Alta Administração – recebidos através da Gerência de *Compliance*, Gestão de Riscos e Controle Interno – quanto ao cenário de riscos da Companhia;
- Apontar ao Comitê de Auditoria Estatutário, a ocorrência de não conformidades, falhas, desvios, irregularidades e/ou ilegalidades observadas através do processo de Gestão de Riscos e Controle Interno.

**h) Gestores das unidades (responsáveis primários ou donos dos riscos – *risk owners*):** responsáveis primários pela Gestão de Riscos relacionados aos processos de negócio em que participam e/ou lideram, são de suas responsabilidades:

- Ter conhecimento prévio e efetuar o monitoramento dos riscos e controles, direta ou indiretamente, envolvidos nas operações sob sua gestão;
- Identificar as áreas, causas e consequências associadas aos riscos;
- Controlar os riscos dentro dos limites de tolerância definidos pela Companhia;
- Propor e implantar controles e elaborar planos de ação para melhoria dos processos e mitigação dos riscos;
- Buscar obter os recursos necessários para mitigar os riscos;
- Participar do processo de avaliação do apetite e limite de tolerância dos riscos;
- Monitorar o nível de exposição aos riscos, inclusive apurando e reportando os KRIs;
- Reportar incidentes de riscos à GGR;
- Executar as suas tarefas em linha com as diretrizes da Política e Gestão de Riscos.
- Executar suas atividades e decisões em linha com as premissas desta política ou outras diretrizes da COMPESA, de forma a minimizar a exposição da Companhia a riscos;
- Reportar periodicamente à Gerência de *Compliance*, Gestão de Riscos e Controle Interno dos eventos relevantes, que afetem o grau de exposição da COMPESA a riscos;
- Assegurar a implantação dos planos de resposta e monitoramento dos riscos envolvidos nas operações sob sua gestão, de acordo com as deliberações tomadas em conjunto com a Gerência de *Compliance*, Gestão de Riscos e Controle Interno, Comitê de Auditoria Estatutário, Secretaria de Governança ou Alta Administração.

### 5.4 Plano de Treinamento

O programa de treinamento deverá abranger todos os empregados da COMPESA, observando seu grau de participação nas funções de Gestão de Riscos, a fim de assegurar que a cultura de gestão de riscos seja disseminada por toda a Companhia propiciando a compreensão ampla e clara dos objetivos da gestão de riscos.

### 5.5 Limite de Tolerância

Os limites de tolerância são definidos com base na variação aceitável do apetite ao risco e na filosofia de riscos adotada pela Alta Administração. Tais limites são definidos pela Alta Administração e balizam a classificação da avaliação dos riscos e processos na dimensão de “impacto”. A figura 3 ilustra as graduações do apetite ao risco da COMPESA:

| Impacto | Critérios para avaliação qualitativa | Critérios para avaliação quantitativa |
|---|---|---|
| **Extremo** | • Perdas financeiras que podem comprometer a rentabilidade do negócio.<br>• Perda de clientes chave ou de Market share.<br>• Pagamento de multas elevadas ou penalidades severas com impacto na imagem e reputação da empresa.<br>• Perda de grandes investimentos ou retorno muito abaixo do esperado. | Valor envolvido acima de 2% da Receita Líquida |
| **Alto** | • Perdas financeiras significativas.<br>• Perda de clientes ou de um grande número de transações.<br>• Pagamento de multas elevadas ou penalidades severas.<br>• Perda de grandes oportunidades de negócio ou investimentos com prazo indefinido de retorno. | Valor envolvido entre 0,5% e 2% da Receita Líquida |
| **Médio** | • Perdas financeiras consideráveis.<br>• Insatisfação de clientes, podendo resultar em perda de transações.<br>• Pagamentos de multas ou outras penalidades.<br>• Perda de oportunidades de negócio.<br>• Descumprimento de procedimentos internos, leis e regulamentações. | Valor envolvido entre 0,1% e 0,5% da Receita Líquida |
| **Baixo** | •Perdas financeiras imateriais.<br>•Insatisfação de clientes.<br>•Pagamentos de multas ou outras penalidades de pequena relevância. | Valor envolvido abaixo de 0,1% da Receita Líquida |

Figura 3 - Critérios para avaliação do impacto

## 5.6 Grau de Exposição

O grau de exposição deverá ser graduado em quatro níveis, definidos com base no impacto e na vulnerabilidade, utilizando-se da escala a representada na Figura 4:

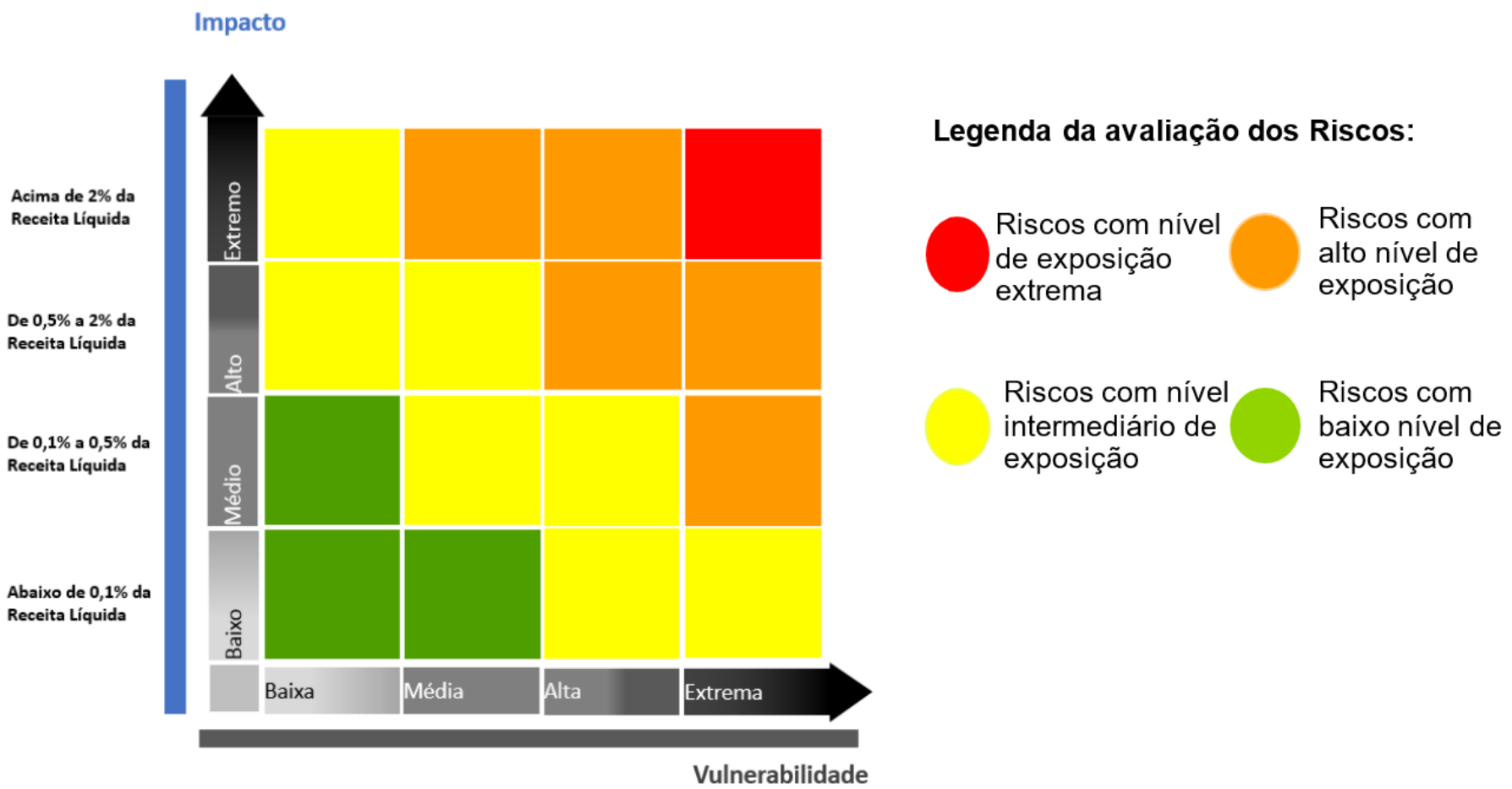


Figura 4 – Mapa de Riscos

O enquadramento da exposição ao risco se refere à extensão à qual a Companhia está exposta ou desprotegida em relação aos impactos negativos após avaliação dos controles existentes.

## 5.7 Estratégia de tratamento de riscos

No processo de aceitação de riscos, considera-se que o nível atual do risco está abaixo do apetite ao risco estabelecido e é assumido pela Companhia, não existindo ações definidas para o seu tratamento. Nesse caso, a decisão deve ser submetida à aprovação de acordo com a alçada descrita a seguir:

| Tabela de alçadas para aceitação de riscos pela Administração | | |
|---|---|---|
| Risco Residual | Proposta de aceitação | Alçada de aceitação / Reporte |
| 4 – Extremo | Diretoria Colegiada | Conselho de Administração |
| 3 – Alto | Diretor | Diretoria Colegiada |
| 2 – Médio | Gerente | Diretor |
| 1 - Baixo | | |

Figura 5 – Tabela de alçadas para aceitação de riscos pela Administração

A aceitação de riscos residuais classificados como extremo deverá ser avaliada e aprovada pelo Conselho de Administração. Para os casos de eventos extraordinários que possuam riscos eminentes não previamente identificados, a decisão de aceitação do risco poderá ser tomada pela Diretoria Colegiada, porém deverão ser reportados posteriormente para o Conselho de Administração.

### 5.8 Dicionário de Riscos

O Dicionário de Riscos Corporativos classifica e categoriza os riscos em uma linguagem comum, considerando as características e o ambiente de negócio da empresa.

O Dicionário de Riscos Corporativos da COMPESA contempla informações segregadas em quatro principais temas, quais sejam:

**a) Risco Estratégico:** Representado pela incerteza no alcance dos objetivos estabelecidos. Pode ser decorrente de mudanças adversas no ambiente de negócios, da utilização de premissas inadequadas na tomada de decisão ou da execução da estratégia de maneira diferente da que foi planejada.

**b) Risco Financeiro:** Representado pela possibilidade de perda financeira relacionada aos mercados financeiros, tais como perdas devidas a movimentos de preços e taxas de juros ou descumprimentos de obrigações financeiras.

**c) Risco Operacional:** Representado pela possibilidade de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. Essa definição inclui o risco legal associado às atividades desenvolvidas pela Organização.

**d) Risco Legal:** Representado pela possibilidade de a Companhia não conduzir seus negócios em conformidade com leis, normas, regulamentos e códigos de conduta aplicáveis às suas atividades, podendo, consequentemente, causar danos à sua imagem e prejuízos de ordem financeira decorrentes de demandas judiciais e de sanções legais.

Cada tema está segregado em grupos e em cada grupo estão as categorias de riscos pertinentes à COMPESA.


Figura 6 – Legenda do dicionário de riscos

O universo de riscos aplicáveis à COMPESA está segmentado e demonstrado na Análise Geral de Riscos – AGR vigente.

## 6. INSTRUMENTOS NORMATIVOS RELACIONADOS

- GGR-NI-003-01
- GGR-POL-007-03
- Código de Conduta e Integridade;

## 7. REFERÊNCIAS

- Lei 13.303/2016 – 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.

- Associação Brasileira de Normas Técnicas - ABNT NBR ISO 31000 :Gestão de Riscos - Princípios e Diretrizes, Rio de Janeiro, 2018;

- ABNT ISO GUIA 73/2009 - DEFINIÇÃO 1.1, Risco: efeito da incerteza nos objetivos;

- ABNT ISO GUIA 73/2009 - DEFINIÇÃO 2.1, Gestão de Riscos: atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos;

- ABNT ISO GUIA 73/2009 – DEFINIÇÃO 3.7.1.2, Apetite ao Risco: quantidade e tipos de riscos que uma organização está preparada para buscar, reter, assumir;

- ABNT ISO GUIA 73/2009 – DEFINIÇÃO 3.7.1.3, Tolerância ao Risco: disposição da organização ou parte interessada em suportar o risco após o tratamento do risco, a fim de atingir os seus objetivos;

- ABNT ISO GUIA 73/2009 – DEFINIÇÃO 3.5.1, Identificação de Riscos: processo de busca, reconhecimento e descrição de riscos;

- ABNT ISO GUIA 73/2009 – DEFINIÇÃO 3.5.1.5, Proprietário do Risco: pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco;

- COSO ERM: Gerenciamento de Riscos Corporativos - Estrutura Integrada, 2016;

- COSO ERM: Gerenciamento de Riscos Corporativos - Estrutura Integrada, 2017;

- Instituto Brasileiro de Governança Corporativa (IBGC).


## 8. HISTÓRICO DE ALTERAÇÕES

| Nº da Versão | Data | Natureza da Revisão e/ou Alteração | RD vinculada |
|---|---|---|---|
| 1 | 27/06/2019 | Emissão inicial de documento. | 011/2019 |
| 2 | 29/10/2021 | Atualização do organograma constante na figura - 2 - pág. 4; • Atribuição da Diretoria Primária : " Integrar o gerenciamento de riscos aos procedimentos de monitoramento através de indicadores gerenciais" (pág. 6) • Incluir no texto da letra "e": "em conjunto com os donos dos riscos" (pág. 7) • Incluir no item 6 Instrumentos Normativos Relacionados: "GGR – NI- 003 – 01 Norma Interna de Gestão de Riscos" (pág. 14) • Incluir no item 7 Referências: pág. 14 | 017/2021 |

## ANEXOS

**ANEXO 1 - RD 017/2021**

Resolução de Diretoria Vinculada