1. Introdução

A Política Institucional de Gestão de Riscos Corporativos tem por finalidade orientar a empresa para a prática de avaliação de riscos no ambiente corporativo e contribuir com o aprimoramento da governança, do planejamento empresarial e para a preservação e geração de valor da Companhia.

2. Objetivo

2.1 Estabelecer diretrizes, conceitos e competências para a condução do processo de gestão de riscos de acordo com metodologia definida pela Sabesp, com base no modelo internacional COSO ERM: *Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management*, nas normas ABNT NBR ISO 31000 e ABNT ISO GUIA 73.

2.2 Considerar a visão de riscos na tomada de decisões, alinhada com as boas práticas de mercado.

2.3 Gerar valor para a organização e aperfeiçoar as práticas de governança, de forma sistemática, estruturada e integrada aos valores e diretrizes empresariais.

2.4 Disseminar a cultura e promover a atuação da gestão de riscos de forma padronizada em todos os níveis hierárquicos da Companhia.

3. Diretrizes

3.1 A prática da gestão de riscos deve estar alinhada com a Missão, Visão, Valores Éticos e Diretrizes da Companhia, subsidiando de forma integrada o Planejamento Estratégico e seus desdobramentos.

3.2 A cultura de gestão de riscos deve ser disseminada pela autoridade funcional de gestão de riscos e praticada em todos os níveis hierárquicos da Companhia.

3.3 Os processos de trabalho devem incorporar a gestão de riscos de forma sistemática e padronizada, conforme metodologia de gestão de riscos adotada pela Sabesp.

3.4 Os empregados envolvidos com as atividades de gestão de riscos devem ser capacitados, pela autoridade funcional de gestão de riscos, na metodologia adotada pela Companhia.

3.5 Os riscos devem ser identificados e classificados por sua natureza e categoria:

Natureza	**Categoria**
Estratégica:	Governança, Político e Econômico e Negócio;
Financeira:	Contábil, Crédito, Liquidez e Mercado;
Operacional:	Ambiental, Processo e Infraestrutura, Pessoal, Informação e Tecnologia;
Conformidade:	Regulamentos e Legislação.

3.6 Os riscos de processos devem ser identificados, avaliados, tratados, comunicados e monitorados pelas Superintendências e Unidades de Negócio, na execução de suas atividades, sob orientação da autoridade funcional de gestão de riscos.

3.7 Os riscos corporativos devem ser identificados, avaliados, tratados, comunicados e monitorados pelo responsável do risco, sob orientação da autoridade funcional de gestão de riscos.

3.8 A responsabilidade pela aprovação e tratamento dos riscos corporativos é definida por níveis de alçada estabelecidos com base em impacto e probabilidade de ocorrência.

3.9 O processo de gestão de riscos deve ser monitorado por indicadores de desempenho.

3.10 A decisão sobre os controles a serem utilizados para a redução da exposição a riscos deve considerar a natureza e nível de criticidade.

3.11 Na avaliação do nível de criticidade e definição dos planos de ação mitigatórios, a unidade responsável pelo risco corporativo deve promover a ampla discussão com as áreas envolvidas.

3.12 O responsável pelo risco deve utilizar os resultados das avaliações para a revisão dos planos de ação e elaboração de planos de contingência.

3.13 O aperfeiçoamento da gestão de riscos deve ocorrer por ciclos de avaliações e revisões e em resposta a um fato específico.

3.14 A autoridade funcional de gestão de riscos deve prover soluções de forma integrada e eficiente para sustentar o processo de gestão de riscos.

3.15 A efetividade do processo de gestão dos riscos deve ser avaliada anualmente pela Superintendência de Auditoria.

3.16 Os riscos corporativos são comunicados às partes interessadas, a critério da Companhia, pelos canais competentes, alinhados à legislação e às boas práticas de governança corporativa.

3.17 Os riscos corporativos devem ser acompanhados pelo Conselho de Administração, Conselho Fiscal, Comitê de Auditoria e Diretoria Colegiada, por meio de relatórios periódicos das atividades da autoridade funcional de gestão de riscos.

3.18 A autoridade funcional de gestão de riscos é a Superintendência de Gestão de Riscos e Conformidade, vinculada administrativamente e liderada pelo Diretor-Presidente.

3.19 Os profissionais da autoridade funcional de gestão de riscos devem ter acesso a dados e informações necessários à execução de suas atividades, responsabilizando-se pela confidencialidade das informações.

3.20 A Administração da Companhia deve zelar pela adequação dos recursos necessários à autoridade funcional de gestão de riscos para execução das atividades de gestão de riscos da Companhia.

3.21 As competências do Conselho de Administração, Conselho Fiscal, Comitê de Auditoria, Diretoria Colegiada, Comissão de Gestão de Riscos Corporativos, Diretorias,

Superintendência de Gestão de Riscos e Conformidade, Superintendências e Unidades de Negócio estão definidas no Anexo 2 desta Política.

3.22 Os responsáveis pelos riscos devem implementar os planos de ação mitigatórios dentro do prazo estabelecido.

3.22.1 Na impossibilidade de atendimento do prazo, deve-se justificar e solicitar formalmente a sua prorrogação à autoridade funcional de gestão de riscos, com cópia para ciência do respectivo diretor.

3.22.2 Os planos de ação mitigatórios aprovados e não implantados no prazo determinado são comunicados às instâncias competentes.

4. Complementos

Anexos Referenciados (Base de Anexos)	Documentos Referenciados	Informações de Registros
---	-	-

Arquivos Anexados (Arquivos Complementares do Instrumento Organizacional)

PI0028v3 - Anexo 01 - Conceitos.pdf
PI0028v3 - Anexo 02 - Competências.pdf

Descrição

Avaliação de risco	Processo de avaliação que permite que uma organização considere até que ponto os fatores de riscos em potencial podem impactar a realização dos objetivos. A Administração avalia os eventos com base em duas perspectivas – probabilidade e impacto – e, geralmente, utiliza uma combinação de métodos qualitativos e quantitativos.
Boas Práticas de Governança Corporativa	Orientações publicamente reconhecidas, com o objetivo de alcançar e manter transparência, equidade e qualidade das informações, bem como manter reputação positiva perante o mercado e um diferencial na preservação e geração de valor.
Controle	Medida que mantém ou modifica o risco.
Gestão de Riscos Corporativos	É o processo conduzido na organização pelo Conselho de Administração, Comitê de Auditoria, Diretoria Colegiada, Comissão de Gestão de Riscos Corporativos, superintendências, unidades de negócio 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 a exposição de risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. A gestão de riscos está diretamente relacionada ao crescimento sustentável, a rentabilidade, a preservação e geração de valor para a Companhia e seus acionistas, dado que este processo permite a identificação não só de ameaças, como também de oportunidades de aprimoramento e desenvolvimento do negócio.
Identificação de risco	Processos de busca, reconhecimento e descrição de riscos. A identificação de riscos envolve a descrição de fatores, consequências potenciais. Proporcionará gerar uma lista abrangente de riscos (portfólio) baseada em eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos. A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.
Impacto	Resultado ou efeito de um evento de risco. Poderá haver uma série de impactos possíveis associados a um evento. O impacto de um evento pode ser positivo ou negativo em relação aos objetivos correlatos da Companhia.

Descrição

Mapa de risco	Representação gráfica referente ao processo de avaliação de riscos no ambiente corporativo. É apresentado graficamente no layout de mapa 5 X 5, através de posicionamento do nível do risco em quadrante com cor correspondente. Representado no plano cartesiano, por pares ordenados (Probabilidade e Impacto): Eixo X: Probabilidade: Quase Certo (vermelho), Provável (laranja), Possível (amarelo), Baixa (verde claro) e Improvável (verde escuro); Eixo Y: Impacto: Alto (vermelho), Significativo (laranja), Moderado (amarelo), Baixo (verde claro) e Mínimo (verde escuro).
Metodologia de Gestão de Riscos	É o conjunto de definições de padrões na identificação, análise, avaliação, tratamento e monitoramento dos riscos, com base na aplicação do modelo do COSO "Enterprise Risk Management - Integrated Framework", nas normas ABNT NBR ISO 31000 e ABNT ISO GUIA 73, de forma flexível às características e peculiaridades da Sabesp e de seu ambiente de negócios.
Nível de Alçada	É a faixa de administração da organização responsável pela tomada de decisão relacionada às atividades de gestão de riscos, de acordo com o nível de criticidade (impacto e probabilidade) estabelecido no mapa de riscos.
Probabilidade	Chance de um evento 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, e se descrita utilizando-se termos gerais ou matemáticos (como probabilidade ou frequência durante um determinado período de tempo). Fonte: ISO 31000: 2018
Responsável do risco	Área responsável por identificar, avaliar, tratar, comunicar e monitorar riscos corporativos ou de processos.
Risco corporativo	Risco que pode comprometer a capacidade da Companhia de atingir seus objetivos de negócio.
Risco de processo	Risco que pode comprometer resultados de processos.

1. Conselho de Administração

a) Avaliar e aprovar a Política Institucional de Gestão de Riscos Corporativos;
b) conhecer a metodologia de gestão de riscos corporativos;
c) verificar a eficácia dos procedimentos de gestão e controle dos riscos corporativos;
d) avaliar e aprovar os níveis de alçada de riscos que definem as responsabilidades para aprovação e tratamento dos riscos;
e) avaliar e aprovar periodicamente o mapa de riscos corporativos e planos de ação mitigatórios de alçada do Conselho de Administração;
f) acompanhar e avaliar semestralmente a evolução de implantação dos planos de ação mitigatórios dos riscos corporativos de sua alçada.
g) conhecer o resultado da avaliação da efetividade do processo de gerenciamento de riscos, realizada pela Superintendência de Auditoria;
h) conhecer o relatório das atividades de gestão de riscos.

2. Conselho Fiscal

a) Conhecer a Política Institucional de Gestão de Riscos Corporativos e sua metodologia;
b) conhecer o plano anual de trabalho de gestão de riscos corporativos;
c) conhecer o mapa de riscos corporativos;
d) conhecer os níveis de alçada de riscos que definem as responsabilidades para aprovação e tratamento dos riscos;
e) conhecer a evolução dos planos de ação mitigatórios dos riscos corporativos;
f) conhecer o relatório das atividades de gestão de riscos.

3. Comitê de Auditoria

a) Analisar e opinar sobre a Política Institucional de Gestão de Riscos Corporativos e sobre a metodologia de gestão de riscos corporativos adotada pela Companhia;
b) acompanhar o plano anual de trabalho de gestão de riscos corporativos;
c) analisar e opinar sobre os níveis de alçada de riscos que definem as responsabilidades para aprovação e tratamento dos riscos;
d) conhecer o mapa de riscos corporativos;
e) acompanhar semestralmente a evolução dos planos de ação mitigatórios dos riscos corporativos;
f) conhecer o relatório das atividades de gestão de riscos.

4. Diretoria Colegiada

a) Aprovar a Política Institucional de Gestão de Riscos Corporativos e submeter ao Conselho de Administração;
b) aprovar a metodologia de gestão de riscos corporativos e submeter ao Conselho de Administração;
c) aprovar o Regimento Interno da Comissão de Gestão de Riscos Corporativos;
d) aprovar a indicação dos membros da Comissão de Gestão de Riscos Corporativos;
e) avaliar e aprovar os níveis de alçada de riscos que definem as responsabilidades para aprovação e tratamento dos riscos;
f) acompanhar a evolução do plano anual de trabalho de gestão de riscos corporativos e apoiar o seu desenvolvimento;
g) avaliar e aprovar periodicamente o mapa de riscos corporativos e planos de ação mitigatórios, submetendo ao Conselho de Administração os riscos que excederem seu nível de alçada;
h) acompanhar semestralmente a evolução de implantação dos planos de ação mitigatórios dos riscos corporativos de sua alçada;
i) conhecer o relatório das atividades de gestão de riscos.

5. Diretorias (inclui Presidência)

a) Conhecer a Política Institucional de Gestão de Riscos Corporativos e metodologia adotada pela Companhia;
b) aprovar o plano anual de trabalho de gestão de riscos corporativos e apoiar o seu desenvolvimento (exclusiva da Presidência);
c) conhecer o Regimento Interno da Comissão de Gestão de Riscos Corporativos;
d) conhecer e acompanhar o plano anual de trabalho de gestão de riscos corporativos;
e) conhecer os níveis de alçada de riscos que definem as responsabilidades para aprovação e tratamento dos riscos;
f) aprovar os riscos corporativos de sua Diretoria;
g) submeter à Diretoria Colegiada os riscos que excederem o nível de alçada das Diretorias (exclusiva da Presidência);
h) acompanhar a evolução dos planos de ação mitigatórios dos riscos corporativos;
i) apoiar a execução dos trabalhos de identificação, análise, avaliação, tratamento, comunicação e monitoramento dos riscos;
j) avaliar e aprovar a mensuração e os planos de ação mitigatórios de sua diretoria;
k) indicar o membro representante da Diretoria na Comissão de Gestão de Riscos Corporativos.

6. Comissão de Gestão de Riscos Corporativos

a) Avaliar a Política Institucional de Gestão de Riscos Corporativos e as propostas de alterações;
b) conhecer a metodologia de gestão de riscos corporativos;
c) avaliar o Regimento Interno da Comissão de Gestão de Riscos Corporativos e as propostas de alterações;
d) avaliar os níveis de alçada de riscos que definem as responsabilidades para aprovação e tratamento dos riscos;
e) acompanhar o plano anual de trabalho em gestão de riscos corporativos;
f) avaliar a proposta de disseminação de cultura da gestão de riscos em todos os níveis da empresa;
g) acompanhar bimestralmente a evolução de implantação dos planos de ação mitigatórios dos riscos corporativos;
h) reportar semestralmente a evolução de implantação dos planos de ação mitigatórios dos riscos corporativos de alçada da Diretoria Colegiada.
i) acompanhar os indicadores de riscos corporativos;
j) avaliar o mapa de riscos corporativos;
k) conhecer e acompanhar os trabalhos de identificação, análise, avaliação, tratamento, comunicação e monitoramento dos riscos de responsabilidades das Diretorias e Superintendências;
l) assessorar a Diretoria Colegiada nos assuntos relacionados à gestão de riscos corporativos;
m) conhecer os recursos aprovados para execução dos planos de ação;
n) conhecer o relatório das atividades de gestão de riscos.

7. Superintendências e Unidades de Negócio

a) Conhecer e aplicar a metodologia de gestão de riscos;
b) conhecer os níveis de alçada de riscos que definem as responsabilidades para aprovação e tratamento dos riscos;
c) identificar, analisar, avaliar, tratar, comunicar e monitorar os riscos de sua competência;
d) acompanhar a evolução dos planos de ação mitigatórios dos riscos, de sua competência;
e) propor à Diretoria o tratamento e os planos de ação mitigatórios e para os riscos de sua competência;
f) elaborar e manter atualizado o mapa de riscos em sua área de atuação, em conjunto com a Superintendência de Gestão de Riscos e Conformidade - PK;
g) definir e acompanhar os indicadores de riscos;
h) utilizar os resultados das avaliações de riscos para priorizar a elaboração e/ou revisão de planos de contingência.

8. Superintendência de Gestão de Riscos e Conformidade (PK) – Autoridade Funcional

a) Disseminar a cultura da gestão de riscos em todos os níveis da empresa, nos termos do Estatuto Social;
b) propor e manter atualizada a Política Institucional de Gestão de Riscos Corporativos e o Regimento Interno da Comissão de Gestão de Riscos Corporativos;
c) capacitar a liderança e os empregados envolvidos nas atividades de gestão de riscos para aplicação da metodologia adotada pela Companhia.
d) elaborar proposta de níveis de alçada de riscos e submetê-la à aprovação da Diretoria Colegiada;
e) elaborar o plano anual de trabalho e submetê-lo a aprovação da Presidência;
f) executar o plano anual de trabalho;
g) propor medidas de apoio ao desenvolvimento da gestão de riscos ;
h) propor os critérios para avaliação, mapeamento e classificação de riscos;
i) contribuir na elaboração do mapa de riscos corporativos;
j) consolidar e garantir a distribuição do mapa de riscos corporativos, de acordo com os níveis de alçada definidos;
k) gerenciar o sistema de gestão de riscos com o objetivo de consolidar os resultados das avaliações de riscos;
l) acompanhar a evolução de implantação dos planos de ação e reportar à Comissão de Gestão de Riscos Corporativos, Diretoria Colegiada, Conselho Fiscal, Comitê de Auditoria e Conselho de Administração;
m) monitorar os indicadores dos riscos corporativos;
n) assessorar a Comissão de Gestão de Riscos Corporativos;
o) propor a metodologia e executar a comunicação interna dos riscos corporativos às áreas envolvidas;
p) alinhar a prática do gerenciamento de riscos com a Missão, Visão, Valores e Diretrizes da Companhia;
q) elaborar e acompanhar os indicadores de desempenho do processo de gestão de riscos;
r) apresentar relatórios periódicos das atividades de gestão de riscos à Diretoria Colegiada, aos Conselhos de Administração e Fiscal, Comitê de Auditoria e à Comissão de Gestão de Riscos Corporativos.

9. Superintendência de Auditoria

a) Avaliar, anualmente e de forma sistemática, a efetividade do processo de gestão riscos e recomendar melhorias;
b) apresentar o resultado da avaliação da efetividade do processo de gerenciamento de riscos ao Conselho de Administração;
c) conhecer o mapa de riscos corporativos;
d) considerar o mapa de riscos corporativos para elaboração da programação de trabalho de auditoria interna da Sabesp.