



| | |
|---------------------------|---|
| Título | POLÍTICA DE GESTÃO DE RISCOS |
| Objetivo | Estabelecer princípios, diretrizes e responsabilidades a serem observadas no processo de gestão dos riscos da Saneago. |
| Campo de Aplicação | Todas as unidades organizacionais da Saneago. |

1 – OBJETIVO

1.1 – Estabelecer princípios, diretrizes e responsabilidades a serem observadas no processo de gestão dos riscos da Saneago, de forma a possibilitar a sua adequada identificação, análise, avaliação, tratamento, monitoramento e comunicação.

1.2 – São princípios norteadores dessa política:

- Agregar valor e proteger o ambiente institucional;
- Ser parte integrante de todos os processos organizacionais;
- Subsidiar a tomada de decisões;
- Ser baseada nas melhores informações disponíveis;
- Ser transparente e conclusiva;
- Ser dinâmica, interativa e capaz de reagir a mudanças; e,
- Apoiar a melhoria contínua da entidade.

2 – REFERÊNCIA

- ABNT NBR ISO 31000:2009 – Gestão de Riscos: Princípios e Diretrizes;
- Estatuto Social da Saneago;
- COSO – *Committee of Sponsoring Organizations of the Treadway Commission*. Controle Interno: Estrutura Integrada, 2013;
- IBGC – Instituto Brasileiro de Governança Corporativa. Guia de Orientação para Gerenciamento de Riscos Corporativos: Cadernos de Governança Corporativa – nº 3, 2007;
- Lei nº 13.303, de 30 de junho de 2016 – Lei das Estatais; e,
- Regimento Interno da Saneago.

3 – GLOSSÁRIO

- **Ambiente interno:** base de todos os componentes da estrutura de gestão de riscos, compreendendo seu desenho e sistema de gerenciamento e monitoramento. Inclui a estrutura organizacional, os recursos humanos e físicos, a cultura e os valores da companhia (valores éticos e de integridade), as competências e as habilidades;
- **Ameaça:** de origem externa, afeta o risco e normalmente não pode ser controlada;
- **Análise de riscos:** processo de compreensão do risco por meio de dados e informações inerentes prestadas pela autoridade/unidade “dona do risco”, envolvendo ainda a mensuração do risco (ABNT NBR ISO 31000:2009);
- **“Apetite” ao risco:** graduação de risco que a empresa está disposta a incorrer na busca pela realização de seus objetivos estratégicos (IBGC, 2007). É definido pelo Conselho de Administração com o estabelecimento de variações aceitáveis ou pretendidas para cada



objetivo estratégico da empresa;

- **Avaliação de riscos:** processo de comparação do risco mensurado com o critério de risco para avaliar sua significância (ABNT NBR ISO 31000:2009) e forma de tratamento a ser adotada;
- **Categoria de riscos:** natureza genérica para agregação de riscos conforme inter-relação existente (IBGC, 2007). O conjunto de categorias é capaz de representar a organização como um todo, possibilitando uma compreensão rápida e clara dos principais itens de contextualização da empresa em termos de riscos;
- **Identificação de riscos:** processo para levantamento de risco a partir da análise de incertezas em relação a objetivos, processos críticos e mudanças significativas no ambiente da organização (ABNT NBR ISO 31000:2009);
- **Mensuração de riscos:** aferição do risco por meio de atributos relativos ao seu impacto e à sua probabilidade de ocorrência (IBGC, 2007);
- **Monitoramento de riscos:** processo de acompanhamento e supervisão do risco pelos diversos envolvidos (IBGC, 2007);
- **Nível de risco:** classificação do risco dentre níveis conforme resultado da mensuração do risco (ABNT NBR ISO 31000:2009);
- **Plano de tratamento:** corresponde a um modelo de plano de ação, sob metodologias estabelecidas constantes do processo de tratamento ao risco;
- **Reavaliação de riscos:** monitoramento do risco residual e eventual risco secundário por meio do processo de refazer a análise, a avaliação e o tratamento do risco após o período delineado conforme o nível de risco classificado, considerando eventuais fatos novos, bem como alterações no ambiente da organização e as ações efetivadas por meio do último plano de tratamento aprovado;
- **Risco:** “possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos” (COSO, 2013), ou seja, o “efeito da incerteza nos objetivos” (ABNT NBR ISO 31000:2009) dos diversos segmentos da organização;
- **Risco atual/inerente:** equivale ao mensurado no momento da análise de riscos, sendo o valor do risco no tempo presente;
- **Risco positivo:** ocorre quando o efeito da incerteza de um risco impacta positivamente os objetivos;
- **Risco residual:** equivale ao risco remanescente após a implementação do tratamento ao risco, isto é, a parcela do risco que não é eliminada com as ações de resposta ao risco;
- **Risco secundário:** equivale ao risco originário de um tratamento ineficiente, ou seja, indesejado e diferente dos efeitos principais previstos pelo plano de tratamento de riscos, devendo ser gerido junto ao risco primitivo, e não como um novo risco;
- **Tolerância a risco:** margem de erro sobre metas dos indicadores estratégicos, cuja empresa responsável está disposta a assumir (COSO, 2013). Consiste em um desdobramento harmônico do “apetite” associado ao monitoramento *ex-post* (IBGC, 2007), sendo definida pelas Diretorias responsáveis em conjunto com as áreas envolvidas, havendo o estabelecimento de variações aceitáveis ou pretendidas para cada indicador estratégico da empresa;
- **Tratamento de riscos:** processo de atuação sobre o risco por meio do plano de tratamento de riscos (ABNT NBR ISO 31000:2009), elaborado pela autoridade/unidade competente; e,
- **Vulnerabilidade:** de origem interna, afeta o risco e normalmente pode ser tratada.

4 – ESTRUTURAÇÃO

4.1 – A Saneago adota regras de estrutura e práticas de gestão de riscos sob a liderança da Procuradoria Jurídica – PROJU e vinculada hierarquicamente à Presidência – DIPRE.

4.2 – A gestão de riscos abrange coordenações/supervisões/gerências, superintendências, diretorias e



Conselho de Administração, com abordagem *Top-Down*¹ e *Bottom-Up*².

5 – FUNDAMENTAÇÃO

5.1 – A gestão de riscos constitui um processo cíclico/contínuo capaz de identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos inerentes à organização.

5.2 – Os principais objetivos da gestão de riscos na Saneago são:

- Promover a minimização do impacto do risco e/ou de sua probabilidade de ocorrência por meio da maximização dos controles/barreiras; e,
- Subsidiar a estrutura de Governança e a Administração no processo decisório e no planejamento das ações, com informações gerenciais relevantes sobre os diversos riscos que podem afetar o negócio.

6 – DIRETRIZES DA GESTÃO DE RISCOS NA SANEAGO

Tomando por referência o modelo COSO e a norma ABNT NBR ISO 31000:2009, a gestão de riscos na Saneago é estruturada com os componentes seguintes:

6.1 – Ambiente Interno

6.1.1 – Direciona e formata os componentes da gestão de riscos, estruturando seu funcionamento e maturidade. Inclui a estrutura organizacional, governança, políticas, objetivos, estratégias, capacidades, recursos, sistemas de informação, cultura, valores da organização e o seu contexto em um dado momento/data da análise.

6.1.1.1 – O “apetite” ao risco, estabelecido pelo Conselho de Administração, “deve estar alinhado à estratégia da empresa e aos objetivos a ela relacionados, proporcionando o delineamento à tolerância aos riscos, pelas Diretorias, por meio de indicadores estratégicos.

6.2 – Identificação de Riscos

6.2.1 – É proporcionada pela análise de eventos e incertezas que podem afetar os objetivos, processos críticos e mudanças significativas no ambiente da empresa.

6.2.1.1 – Dar-se-á pela coleta de informações e percepções por meio de fontes internas e externas em um dado momento.

6.3 – Análise de Riscos

6.3.1 – Desenvolve a compreensão de riscos pela autoridade/unidade “dona do risco” e pela PR-GGR, desencadeando a mensuração de riscos.

6.3.2 – A mensuração de riscos é realizada com estimativas de seu impacto e de sua probabilidade de ocorrência, utilizando-se de métodos qualitativos e quantitativos.

6.3.3 – Em função de seu impacto e de sua probabilidade de ocorrência, os riscos são classificados em

¹ Constitui estratégia de processamento de informação e ordenação do conhecimento de cima para baixo.

² Constitui estratégia de processamento de informação e ordenação do conhecimento de baixo para cima.



níveis de severidade distintos demonstrados em uma matriz gráfica, contendo graduações para o seu impacto e para a sua probabilidade de ocorrência.

6.4 – Avaliação de Riscos

6.4.1 – Compreende a comparação entre o risco mensurado durante a análise de risco, também conhecido como risco atual/inerente e o critério de risco adotado para avaliação de sua significância e priorização, bem como o nível de tolerância, expressando o tipo, a qualidade e a prioridade dispensada ao tratamento do risco, direcionando os esforços para minimização de tais riscos por meio de uma estrutura de controles internos alinhada aos objetivos da companhia.

6.5 – Tratamento de Riscos

6.5.1 – Define a resposta ao risco avaliado por meio da elaboração e execução de ações relacionadas a controles internos pela autoridade/unidade “dona do risco”, sob supervisão do responsável pela aprovação do tratamento.

6.5.1.1 – Os controles internos são avaliados quanto à sua viabilidade, por meio de estimativas do seu benefício e do esforço dispendido em sua implantação, utilizando-se de métodos qualitativos e quantitativos.

6.5.2 – A resposta ao risco pela autoridade responsável pela aprovação do tratamento ao risco depende principalmente do “apetite” e tolerância ao risco.

6.5.2.1 – A Saneago possui níveis definidos de alçada específica para propor e aprovar a aceitação ou exploração de riscos, proporcionando maior segurança ao negócio.

6.6 – Categoria de Riscos

6.6.1 – Em razão do setor de atuação e de sua constituição societária, a Saneago está exposta a riscos originários de vulnerabilidades e de ameaças.

6.6.1.1 – Os riscos vinculados a vulnerabilidades endógenas são abrangidos por esta política, nos termos do item 5.1, sendo os principais:

- Ambientais, referente à poluição e/ou à contaminação dos mananciais pela Saneago;
- Financeiros, inerentes à liquidez, ao custo de oportunidade, à gestão de custos e ao não cumprimento do plano de investimentos;
- Degradação e/ou obsolescência da infraestrutura física e tecnológica da Saneago;
- Ineficiência na manutenção dos índices de perdas operacionais e do índice de qualidade de água – IQA;
- Insuficiência de profissionalização/atualização do corpo técnico e gerencial da Saneago;
- Descumprimento de Termos de Ajustamento de Conduta – TAC;
- Atrasos ou descontinuidade das obras de expansão;
- Prejuízos decorrentes de não conformidades presentes em atividades subdelegadas, terceirizadas e/ou subcontratadas;
- Não obtenção ou não renovação de registros, autorizações, outorgas, licenças e alvarás para instalações ou operações de unidades da Saneago;
- Ausência de seguros sobre a totalidade dos riscos;
- Ineficiência no controle sobre as instalações operacionais da empresa, podendo afetar as populações vizinhas, sociedade, clientes e empregados;



- Outros riscos associados à coleta, afastamento e tratamento de esgoto; e,
- Outros riscos associados ao fornecimento de água tratada.

6.6.1.2 – Os riscos vinculados a ameaças exógenas não guardam relação direta com os controles internos estabelecidos, sendo os principais:

- Ambientais, envolvendo clima, estiagem e alta pluviosidade, bem como a degradação de bacias, escassez de políticas de preservação, poluição e/ou contaminação dos mananciais por terceiros;
- Rescisão ou não renovação de contratos de concessão/programa com o poder concedente;
- Financeiros, inerentes ao mercado de capitais, ao câmbio, à taxa de juros, à inflação e ao crédito;
- Econômicos e políticos, eventualmente associados a crises, bem como, políticas fiscais, legislações e regulação do setor;
- Interesses difusos do acionista majoritário, Governo do Estado de Goiás, em relação aos demais acionistas;
- Indisponibilidade e/ou instabilidade da matriz energética necessária para as operações da Saneago; e,
- Prejuízos decorrentes de ações judiciais, arbitrais e/ou processos administrativos.

6.6.1.2.1 – Para os riscos listados neste item 6.6.1.2, a autoridade/unidade “dona do risco”, em especial daqueles inerentes ao meio ambiente, deve manter plano(s) contingencial(ais) para a gestão de continuidade do negócio, envolvendo outros órgãos/entidades, caso necessário, com o objetivo de minimizar os impactos resultantes.

6.6.2 – Os riscos geridos são agregados, concomitantemente, em uma ou mais categorias distintas, possibilitando uma compreensão rápida e clara dos principais itens de contextualização da organização em termos de riscos.

6.6.2.1 – As categorias de riscos da Saneago tomaram por referência o modelo COSO, recomendações do IBGC e os tipos de riscos a que a empresa está exposta.

6.7 – Monitoramento de Riscos

6.7.1 – É desempenhado pela autoridade/unidade “dona do risco” e pelo responsável pela aprovação do tratamento, de forma constante e integrada aos processos organizacionais, envolvendo a revisão, checagem, vigilância, acompanhamento e em resposta a algum fato específico.

6.7.2 – É realizado pela PR-GGR por meio da reavaliação de riscos residuais e eventuais riscos secundários, de acordo com o prazo estabelecido em razão do nível de risco.

6.7.3 – É praticado pela PR-GDC por meio da verificação do cumprimento dos planos de tratamento aos riscos.

6.7.4 – É exercido pelo Conselho de Administração, Comitê de Auditoria Estatutário, Conselho Fiscal, Diretoria Colegiada, Auditoria Interna e Superintendência de Controle Interno por meio de análise dos reportes trimestrais da SUCOI/PR-GGR.

6.8 – Atividades de Controle

6.8.1 – São estabelecidas, principalmente, por meio de ações preventivas, detectivas ou corretivas,



bem como por políticas e documentos normativos elaborados, orientando os objetivos e as diretrizes definidas para a empresa, por meio da minimização, tratamento e controle de seus riscos.

6.8.2 – São realizadas em todos os segmentos da organização, envolvendo vários estágios de processos e tipos de atividades, tais como segregação de função, limite de alçada, responsabilidade por aprovação/autorização, supervisão, verificação/inspeção, segurança de ativos, avaliação de desempenho/performance, soluções tecnológicas com melhores práticas e acompanhamento de indicadores e metas.

6.8.3 – Os controles presentes são identificados e analisados pela autoridade/unidade “dona do risco”. Os controles propostos como tratamento aos riscos são avaliados quanto à viabilidade de sua implantação e analisados pela autoridade/unidade responsável pela aprovação do tratamento ao risco.

7 – MANDATO E COMPROMETIMENTO NA GESTÃO DE RISCOS

A gestão de riscos eficiente requer comprometimento forte e sustentado a ser assumido em todos os segmentos da organização. Desta feita, adicionalmente ao Estatuto da Saneago e Regimento Interno da Saneago, confere:

7.1 – Ao Conselho de Administração:

- Implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e tratamento dos principais riscos a que está exposta a organização;
- Definir o “apetite” ao risco para cada objetivo estratégico da empresa;
- Aprovar o tratamento de riscos classificados no mais alto nível da matriz de riscos;
- Aprovar os relatórios de controle interno, *compliance* e riscos; e,
- Outras atribuições inerentes.

7.2 – Ao Conselho Fiscal:

- Conhecer os relatórios de controle interno, *compliance* e riscos; e,
- Outras atribuições inerentes.

7.3 – Ao Comitê de Auditoria Estatutário:

- Analisar a política de gestão de riscos da empresa e respectivas revisões, submetendo-a à aprovação do Conselho de Administração;
- Supervisionar as atividades desenvolvidas nas áreas de Controle Interno e de Auditoria Interna, e monitorar a qualidade e a integridade dos mecanismos de controle interno, bem como da atuação do Comitê de Elegibilidade Estatutário;
- Conhecer os relatórios de controle interno, *compliance* e riscos;
- Avaliar e monitorar as exposições da organização a riscos; e,
- Outras atribuições inerentes.

7.3.1 – À Auditoria Interna:

- Auditar a PR-GGR com base no plano anual de gestão de riscos e no relatório anual de atividades executadas pela PR-GGR, atuando como terceira linha de defesa;
- Conhecer os relatórios de controle interno, *compliance* e riscos; e,



- Outras atribuições inerentes.

7.4 – À Diretoria Colegiada:

- Propor ao Conselho de Administração “apetite” aos riscos e, de forma harmônica à deliberação do Conselho de Administração e em conjunto com áreas afins, estabelecer tolerância aos riscos para cada indicador estratégico;
- Propor e implementar sistema de controles internos e políticas, alinhado ao “apetite” e tolerância aos riscos;
- Patrocinar a implantação da gestão de riscos na empresa;
- Conhecer os relatórios de controle interno, *compliance* e riscos; e,
- Outras atribuições inerentes.

7.4.1 – Às Diretorias, Superintendências e Gerências/Supervisões/Coordenações:

- Gerir riscos enquanto primeira linha de defesa e participar ativamente do processo de gestão de riscos em segunda linha de defesa;
- Identificar riscos, adotando medidas para sua prevenção e minimização/tratamento;
- Aprovar o tratamento de riscos conforme nível de classificação;
- Implementar sistemas de controles internos, incluindo políticas e normas;
- Conhecer os relatórios de controle interno, *compliance* e riscos; e,
- Outras atribuições inerentes.

7.4.2 – À Presidência – DIPRE:

- Implementar e supervisionar os sistemas de gestão de riscos e de controle interno estabelecidos para a prevenção e tratamento dos principais riscos a que está exposta a organização;
- Aprovar os relatórios de controle interno, *compliance* e riscos; e,
- Outras atribuições inerentes.

7.4.2.1 – À Superintendência de Controle Interno – SUCOI:

- Estabelecer as diretrizes e requisitos do plano de trabalho de gestão de riscos na empresa, bem como o acompanhamento de metas fixadas;
- Aprovar os relatórios de controle interno, *compliance* e riscos;
- Aprovar o plano anual de gestão de riscos e o relatório anual de atividades executadas pela PR-GGR; e,
- Outras atribuições inerentes.

7.4.2.1.1 – À Gerência de Gestão de Riscos – PR-GGR:

- Supervisionar a gestão de riscos da organização, isto é, de descontinuidade do negócio e aqueles relacionados aos objetivos da empresa, conforme atuação em segunda linha de defesa;
- Reportar trimestralmente o relatório de gestão de riscos ao Conselho de Administração, Comitê de Auditoria Estatutário, Conselho Fiscal, Diretoria Colegiada, Auditoria Interna e Superintendência de Controle Interno; e,
- Outras atribuições inerentes.



7.4.2.1.2 – À Gerência de Compliance – PR-GDC:

- Monitorar o tratamento pela autoridade/unidade “dona” dos riscos; e,
- Outras atribuições inerentes.

8 – INFORMAÇÕES ADICIONAIS

8.1 – Este documento atende aos requisitos regulamentares, legais e contratuais, informando às partes interessadas sobre o processo de gestão de riscos estabelecido para a Saneago.

8.2 – Quaisquer dúvidas pertinentes a esta Política de Gestão de Riscos deverão ser encaminhadas à PR-GGR pelo e-mail: pr-ggr@saneago.com.br.

9 – CONTROLE DE ALTERAÇÕES DA POLÍTICA DE GESTÃO DE RISCOS

| Versão | Descrição da alteração | Início da vigência | Fim da vigência |
|--------|------------------------|--------------------|-----------------|
| 00 | Emissão do documento. | 29/06/2018 | 28/06/2019 |

Quadro 1 – Controle de alterações da política de gestão de riscos.

10 – APROVAÇÃO

10.1 – Esta Política foi aprovada pelo Conselho de Administração da Saneago, na data de 28/06/2018, registrada na Ata 360. Toda alteração ou revisão desse documento deverá ser submetida a apreciação do Conselho de Administração da Saneago.