POLÍTICA DE GESTÃO DE RISCOS E AUDITORIA INTERNA

ÍNDICE

1. OBJETIVO

1.1. A presente Política de Gestão de Riscos e Auditoria Interna ("Política") tem como objetivo definir as principais etapas dos trabalhos da área de Auditoria Interna, Gestão de Riscos e Classificação das Conclusões de Relatórios, bem como estabelecer princípios, diretrizes e responsabilidades a serem observados no processo de gerenciamento de riscos inerentes às atividades de negócio da Iguá Saneamento S.A. ("Companhia"), de forma a identificar e monitorar os riscos relacionados à Companhia ou seu setor de atuação.

2. ABRANGÊNCIA

2.1. Esta Política aplica-se à Companhia e suas controladas ("Grupo Iguá"), bem como a todos os funcionários, gerentes, diretores estatutários e não estatutários, membros do Conselho de Administração, membros de comitês, membros do Conselho Fiscal (se aplicável), representantes e terceiros, direta ou indiretamente relacionados com a Companhia e suas controladas.

3. REFERÊNCIAS

Esta Política tem como referências: (i) as regras de governança corporativa do Estatuto Social da Companhia; (ii) o Código de Conduta da Companhia; (iii) a Política de Divulgação de Informações e de Negociação de Valores Mobiliários; (iv) a Política de Transações com Partes Relacionadas e Administração de Conflitos de Interesse; (v) o Código Brasileiro de Governança Corporativa – Companhias Abertas ("CBGC"); e (vi) o Regulamento do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão ("Regulamento do Novo Mercado").

4. CONCEITOS

4.1. Para fins de aplicação desta Política, os seguintes conceitos devem ser utilizados:

- Limite (ou apetite) do Risco: é a exposição e/ou impacto máximo do Risco que a Companhia está disposta a aceitar, na busca dos seus objetivos e geração de valor. Nem todos os tipos de Riscos são passíveis de aceitação. Portanto, a proposta de limites deverá obrigatoriamente ser fundamentada e formalizada pelas seguintes análises: (i) avaliação do retorno tangível e intangível relacionado ao limite de Risco proposto; (ii) capacidade da Companhia de suportar o impacto do limite de Risco proposto (iii) decisão se o Risco deve ou não ser aceito conforme sua tipologia; (iv) viabilidade da implantação das iniciativas de mitigação (custo e esforço) versus efeito na mitigação do Risco e respectivo retorno; e (v) disponibilidade de recursos (investimento e esforço) para implantação.

- Matriz/Modelagem de Riscos: visa estabelecer uma comparação individual dos Riscos a partir de graus de impacto e probabilidades de ocorrência para fins de priorização e gestão. A matriz de riscos é um organismo em constante evolução e atualizada, sempre que necessário e tempestivamente com o surgimento de eventos de Risco emergentes.

- Risco(s): a possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos da Companhia.

5. DIRETRIZES

5.1. A Companhia está comprometida com a dinâmica de gerenciamento de Riscos, de forma a preservar e desenvolver seus valores, ativos, reputação, competitividade e perenidade dos negócios.

5.2. O objetivo da gestão de Riscos é entendê-los, avaliar e definir ações de resposta para que eventuais perdas sejam previstas e reduzidas, visando manter os Riscos em níveis aceitáveis. A análise de Riscos deve auxiliar o processo de tomada de decisão nos diversos níveis de gestão da Companhia.

5.3. O gerenciamento de Riscos contribui para o monitoramento e para a realização dos objetivos da Companhia. A abordagem da Companhia é integrar o gerenciamento de Riscos no dia a dia na conduta dos seus negócios por meio de um processo estruturado.

5.4. O Departamento de Gestão de Riscos, *Compliance*, Controles Internos ("GRC") e a área de Auditoria Interna ("Auditoria Interna") devem (i) garantir o bom funcionamento do ambiente de controles internos e melhorar o desempenho das linhas de negócio; (ii) identificar ameaças e oportunidades de melhorias por meio da avaliação de riscos; e (iii) apoiar o negócio e avaliar os riscos com total imparcialidade e objetividade.

6. RESPONSABILIDADES

6.1. Compete ao GRC e Auditoria Interna, em conjunto:

(i) realizar o Planejamento Anual de Gestão de Riscos e Auditoria, diagnosticando os riscos em cada unidade de negócio, bem como as ações existentes para redução, recomendando ações corretivas sempre que necessário;

(ii) reportar ao Comitê de Auditoria e Presidente do Conselho de Administração, os riscos mais relevantes e as suas respectivas propostas de mitigação através de controles internos;

(iii) desenvolver e classificar os relatórios de mapeamentos de riscos e *drafts* de resultado de auditoria de acordo com os níveis definidos nesta Política;
(iv) apoiar os gestores na definição de Planos de Ação necessários para tratamento dos Riscos e assegurar a implementação dos Planos de Ação; e
(v) liderar os trabalhos de auditoria interna para detecção de Riscos e para monitoramento da eficácia dos controles internos para mitigar tais riscos.

6.2. Compete à Auditoria Interna:

(i) monitorar e aferir a qualidade e a efetividade dos processos de gestão de Riscos;
(ii) acompanhar e suportar as ações tomadas e a serem tomadas pela equipe de GRC, garantindo o cumprimento do Planejamento Anual dos trabalhos a serem realizados;
(iii) manifestar-se sobre as sugestões de alteração da estrutura operacional de gestão de Riscos e aprovar eventuais sugestões de alteração, caso necessário;
(iv) definir o Apetite dos Riscos da Companhia; e
(v) validar o relatório de consolidação de Riscos da Companhia.

6.3. Compete ao Comitê de Auditoria aprovar a Política e suas futuras revisões.

7. IDENTIFICAÇÃO DOS RISCOS

7.1. O GRC e a Auditoria Interna são os principais responsáveis pela identificação dos fatores (causas) de riscos e implicações nos objetivos (metas e resultados) projetados.

7.2. Os gestores das áreas de negócios da Companhia também são responsáveis por identificar e gerenciar os riscos das respectivas áreas de negócio.

8. DEFINIÇÕES E TIPOS DE RISCOS

8.1. Os riscos podem ser classificados nas seguintes categorias:

- **Estratégico:** são os riscos associados à tomada de decisão da Administração e que podem gerar perda substancial no valor econômico da Companhia. Além disso, podem ocasionar impacto negativo na receita ou no capital da Companhia em consequência de um planejamento falho, da tomada de decisões adversas e mudanças em seu ambiente de negócio.

- **Financeiro:** risco de perda de recursos financeiros pela Companhia, relacionados às exposições cambiais, taxas de juros e flutuações de preços (ex.: falta de processos adequados de aprovação, falta de reconciliação de transações, operações em moeda

estrangeira, preços de commodities, redução da margem de contribuição, acessos indevidos a transações de sistemas, etc.).

- **Operacionais:** riscos relacionados a infraestrutura da Companhia (processos, pessoas e tecnologia), que afetam a eficiência operacional e a utilização efetiva e eficiente de seus recursos.

- **Regulatório/Legal:** riscos relacionados ao cumprimento da legislação aplicável ao setor de atuação, bem como de leis gerais (ambiental, trabalhista, cível e tributário/fiscal).

9. ANÁLISE DOS RISCOS

9.1. Consiste na verificação das causas e consequências dos Riscos, bem como da probabilidade de concretização de referidas consequências.

10. AVALIAÇÃO DOS RISCOS

10.1. A avaliação dos riscos será feita por processos dinâmicos e interativos, liderados pela área de Gestão de Riscos, em conjunto com os gestores de áreas (se necessário), que devem (i) verificar quais riscos precisam de tratamento; e (ii) determinar prioridades na implementação de tratamento do Risco. Para isto, a Companhia adota critérios de impacto e frequência que são utilizados para a definição no mapa de Riscos.

10.2. O critério de impacto deve considerar as diretrizes que a Companhia adota para mensurar o impacto financeiro (perda) relacionado à imagem e à reputação da instituição. O critério da frequência considera quantas vezes, ou periodicidade, da exposição ao risco avaliado.

10.3. A classificação final do grau de risco será definida mediante a combinação entre o impacto e a frequência, conforme abaixo:

- *Muito alto*: riscos com impacto muito alto e frequência alta ou muito alta;
- *Alto*: riscos com impacto muito alto ou alto e frequência moderada;
- *Médio*: riscos com impacto moderado e frequência moderada ou baixa;
- *Baixo*: riscos com impacto baixo e frequência baixa ou insignificante;
- *Insignificante*: riscos com impacto insignificante e frequência insignificante ou baixa.

10.4. Esta classificação resultará no mapa de Riscos que auxiliará a Companhia na priorização do tratamento dos Riscos.

11. TRATAMENTO DOS RISCOS

11.1. A classificação final dos Riscos deve ser levada em consideração para tratamento do mesmo, adotando as seguintes ações perante o Risco:

- **Evitar**: elimina o fato gerador do Risco. Evitar o Risco pode implicar na descontinuação de uma linha de negócios, unidade ou operação, ou processos.

- **Mitigar**: ações deverão ser tomadas para reduzir a probabilidade de materialização e/ou severidade do Risco. Esta resposta envolve o aprimoramento ou criação de controles e melhorias em processos.

- **Compartilhar**: atividades que visam reduzir a probabilidade de ocorrência e/ou severidade do Risco, por meio da transferência ou compartilhamento de uma parte do Risco a terceiros, como, por exemplo, contratação de apólices de seguro, entre outros.

- **Aceitar**: nenhuma ação é tomada para influenciar a probabilidade de ocorrência e/ou severidade do Risco. Riscos cujo impacto seja menor que o custo/benefício do seu gerenciamento podem ser mantidos, desde que conhecidos e aceitos pela Administração do Grupo Iguá formalmente. No entanto, o monitoramento deve ser contínuo.

12. MONITORAMENTO DOS RISCOS

12.1. A partir da identificação dos Riscos, o monitoramento destes deverá ser feito de forma contínua e independente pelo GRC, com objetivo de assegurar a eficácia e adequação dos controles internos e obter informações que proporcionem melhorias no processo de gerenciamento de Riscos.

13. INFORMAÇÃO E COMUNICAÇÃO

13.1. O GRC comunicará, de forma clara e objetiva, a todas as partes interessadas, os resultados de todas as etapas do processo de gerenciamento de Riscos, de forma a contribuir para o entendimento da situação atual e da eficácia dos planos de ação.

14. PLANO ANUAL DE AUDITORIA

14.1. Utilizando como base a priorização de riscos e foco em áreas de maior relevância, os trabalhos são realizados conforme o Plano Anual de Auditoria, aprovado no início de cada exercício pelo Comitê de Auditoria.

14.2. Os trabalhos de auditoria não são limitados apenas ao Plano Anual. Projetos podem ser iniciados após alinhamento formal com as áreas envolvidas, sempre que identificadas necessidades específicas.

15. METODOLOGIA

As atribuições descritas abaixo são de competência da Auditora Interna.

15.1. Planejamento

- Entrevista com os principais gestores do processo;
- Identificação de aspectos chave e fatores críticos; e
- Definição do escopo, objetivo e cronograma do trabalho.

15.2. Execução

- Definição do programa de auditoria e escopo de testes;
- Formalização dos resultados de testes realizados;
- Identificação dos riscos não mitigados para mensuração e classificação; e
- Recomendação de planos de ação e prazos de implantação.

15.3. Reporte

- Elaboração de relatórios dos resultados das auditorias;
- Discussão dos pontos, planos de ação e prazos com os *process owners*; e
- Distribuição do relatório e apresentação ao Comitê de Auditoria.

15.4. *Follow Up*

- Recomendação de ações adicionais para resolução dos pontos indicados; e
- Apresentação dos resultados de planos de ação ao Comitê de Auditoria.

15.5. *Rating* dos Relatórios

Tendo como base os riscos resultantes da combinação das deficiências, a todo relatório confeccionado será atribuído um *rating*, conforme as seguintes premissas:

Rating	**Suporte**
Adequado	A estrutura de controles está operando de forma eficaz e o processo é adequado para atingir os objetivos do negócio. Os Riscos estão mitigados em níveis aceitáveis.

Satisfatório	A estrutura de controles está operando de forma eficaz, porém, os riscos não estão mitigados em níveis aceitáveis.
Insatisfatório	A estrutura de controles e processos não está operando da forma correta e envolve falhas que comprometem os objetivos de negócio e/ou expõem a empresa a riscos relevantes.

16. VIGÊNCIA

16.1. Esta Política foi aprovada pelo Conselho de Administração, encontra-se em vigor a partir da data de sua aprovação e somente poderá ser modificada por deliberação do Conselho de Administração da Companhia.

*****