

POLÍTICA DE GESTÃO DE RISCOS

PI-COR-CPL-001 - REVISÃO 02. DATA 22/02/2024



1 OBJETIVO

Estabelecer diretrizes e competências para a gestão de riscos, de forma que possibilite a identificação, a avaliação, a priorização, o tratamento, a comunicação e o monitoramento dos riscos do negócio. A política visa, ainda, divulgar e estimular a cultura de risco na Cia.

2 REFERÊNCIAS

- Regras de Governança Corporativa do Estatuto Social da Companhia;
- ABNT NBR ISO 31.001 – Gestão de Riscos;
- ABNT NBR ISO 37.001 – Sistemas de Gestão Antissuborno - Requisitos;
- ABNT NBR ISO 37.301 – Sistemas de Gestão de Compliance - Requisitos;
- COSO ICIF e ERM;
- COBIT;
- NIST.

3 ÁREAS ENVOLVIDAS

Esta política aplica-se a todos os colaboradores do Grupo Iguá Saneamento.

4 TERMOS E DEFINIÇÕES

- **Apetite a risco:** Nível máximo ao qual a Empresa está disposta a se expor em relação ao(s) risco(s) para cumprir seus objetivos estratégicos.
- **CA:** Conselho de Administração da Iguá Saneamento.
- **CoAud:** Comitê de Auditoria da Iguá Saneamento.
- **COBIT:** Controle de Objetivos para Informação e Tecnologias. Guia ou conjunto de boas práticas sobre governança de tecnologia de informação empresarial.
- **Conformidade (ou Compliance):** Cumprimento de regulamentações, leis (fiscais, tributárias, trabalhistas, ambientais e outras vigentes para a empresa), *covenants*, contratos e normas, procedimentos, diretrizes e políticas internas que se aplicam ao negócio.
- **Controles Internos:** Controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.
- **COSO:** *The Comittee of Sponsoring Organizations*, é uma organização privada sem fins lucrativos, criada para prevenir e evitar fraudes nos procedimentos e processos internos da empresa através da ética, efetividade dos Controles Internos e governança corporativa.

- **Dono do Risco:** Membro indicado pela Empresa para atuar no monitoramento e tratamento dos riscos que lhe foram designados.
- **NIST:** Instituto Nacional de Padrões e Tecnologia. Agência não reguladora que promove a inovação por meio do avanço da ciência, padrões e tecnologia de medição.
- **Reporte:** Atualização periodicamente aos envolvidos a respeito da situação, avaliação, pontos de atenção e resposta ao risco corporativo.
- **Resposta aos Riscos:** Conjunto de medidas adotadas pela Empresa para tratativa do impacto e/ou probabilidade do risco, podendo se optar por evitar, reduzir, compartilhar ou aceitar o risco.
- **Risco:** Incerteza sobre a possibilidade de ganhos ou perdas para a Empresa, no momento de ocorrência de acontecimentos relacionados aos seus objetivos.
- **Riscos Corporativos:** Riscos que advêm da falta de capacidade da Empresa em se resguardar de eventos desfavoráveis ao cumprimento de suas estratégias.
- **Riscos Transacionais ou Operacionais:** É o risco de perdas causadas por processos, políticas, sistemas ou eventos falhos ou falhos que interrompem as operações de negócios. Erros de Colaboradores, atividades criminosas como fraudes e eventos físicos estão entre os fatores que podem desencadear o risco operacional.
- **SD:** *Significant Deficiency*, deficiência significativa.
- **TAR:** Termo de Aceitação de Risco.

5 ATRIBUIÇÕES E RESPONSABILIDADES

5.1 GERÊNCIA DE COMPLIANCE E CONTROLES INTERNOS

- Garantir ao Conselho de Administração e CEO o acesso à informação clara e objetiva sobre os principais riscos e como estes são geridos de forma tempestiva.
- Ser a guardiã da metodologia de gestão de riscos da Cia.
- Estabelecer e difundir a metodologia de gestão de riscos na Cia.
- Atuar como link entre o Dono do Risco e Diretoria Executiva de Auditoria, Riscos e Compliance, seguido do Comitê de Auditoria.
- Transmitir conhecimento sobre riscos e gestão de riscos aos colaboradores.
- Estabelecer e manter atualizados a Política e os Procedimentos de Riscos e Controles Internos, assim como padrões e mecanismos de reporte próprios de informações.
- Propor a metodologia do cálculo do apetite a risco.
- Calcular e atualizar o valor do apetite a risco anualmente ou quando da ocorrência de eventos relevantes.
- Promover a disseminação de uma cultura de gestão de riscos.
- Assessorar o Dono do Risco na definição ou identificação de iniciativas mitigatórias e indicadores para o monitoramento dos riscos.

- Manter e coordenar a atualização da matriz de riscos.
- Revisar e atualizar a Régua de Probabilidade e Impacto.
- Reportar a matriz de riscos e o status das ações mitigatórias.
- Monitorar as exposições de riscos da Cia, a adequação dos planos de resposta e a eficácia dos controles internos.
- Definir um plano de trabalho de controles internos baseado nos processos diretamente associados aos riscos corporativos.
- Reportar os resultados dos testes dos controles que atuam na mitigação de riscos corporativos.

5.2 DIRETORIA DE AUDITORIA, RISCOS E COMPLIANCE

- Propor diretrizes e estratégias para a gestão de riscos e controles internos.
- Revisar o planejamento de trabalho para a gestão de riscos.
- Avaliar a matriz de riscos e o tratamento dos riscos.
- Avaliar o andamento das ações para a mitigação dos riscos (planos de ação).
- Acompanhar e garantir o reporte das mudanças na avaliação de criticidade dos riscos para o CoAud.
- Comunicar à Gerência de Compliance e Controles Internos a existência de riscos ainda não mapeados e tratados ou mudança significativa na probabilidade, no impacto ou qualquer outra característica do risco.
- Garantir que a matriz de riscos seja atualizada junto aos Executivos da Empresa sempre que houver atualizações no planejamento estratégico da Cia ou sempre que fatos relevantes ocorrerem.
- Entender a metodologia de cálculo do apetite a risco.
- Monitorar e, quando necessário, solicitar a atualização do apetite ao risco.

5.3 COMITÊ DE AUDITORIA (CoAud):

- Validar as diretrizes para a estrutura, governança e o processo de Gestão de Riscos e Controles Internos.
- Propor o apetite a risco da Cia ao Conselho de Administração.
- Recomendar ao Conselho de Administração as edições desta política.
- Supervisionar os controles internos e gerenciamento de riscos.
- Compreender, avaliar e acompanhar a matriz de riscos.
- Efetuar o reporte ao Conselho de Administração sobre os níveis de risco (altos e significativos).
- Recomendar o aperfeiçoamento da estrutura de Governança de Gestão de Riscos (metodologia, processos, sistemas).

5.4 CONSELHO DE ADMINISTRAÇÃO (CA)

- Aprovar a Política de Gestão de Riscos da Cia.
- Aprovar as diretrizes para o estabelecimento da estrutura, governança e processo de gestão de riscos.
- Aprovar o grau de apetite a risco aceitável da Cia.
- Deliberar sobre medidas necessárias para garantir o alinhamento entre o apetite ao risco e a execução das estratégias.
- Avaliar periodicamente os riscos reportados e acompanhar as ações de gestão de riscos.
- Garantir que os sistemas de gestão de riscos e de controle interno estejam estabelecidos para a prevenção e a mitigação dos principais riscos corporativos.

5.5 DONOS DOS RISCOS (ÁREAS DE NEGÓCIOS)

- Efetuar revisão técnica do risco, do fator deste risco, das respostas e da avaliação do risco e elaborar plano de ação.
- Coordenar a implantação das ações necessárias, inclusive com o envolvimento de outras áreas, alinhadas ao plano de resposta para a mitigação dos riscos.
- Desenvolver indicadores para monitorar os resultados ao risco sob gestão.
- Efetuar reportes periódicos a área de Gestão de Riscos sobre o desenvolvimento de ações para a mitigação dos riscos.
- Realizar a avaliação do risco em relação à sua probabilidade e ao seu impacto.
- Comunicar à área de Compliance e Controles Internos eventuais mudanças significativas na probabilidade e no impacto ou qualquer outra característica do risco.
- Comunicar à área de Compliance e Controles Internos quaisquer mudanças nos controles, iniciativas e planos de ação estabelecidos para mitigação dos riscos.

6 DESCRIÇÃO E CARACTERIZAÇÃO DAS ATIVIDADES (GESTÃO DE RISCOS)

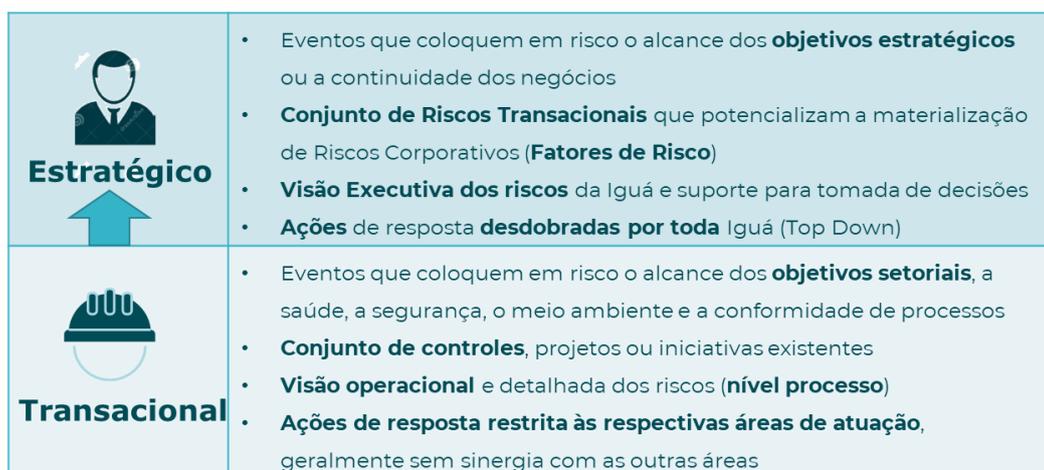
6.1 DIRETRIZES GERAIS

6.1.1 A função de Gestão de Riscos é um processo cíclico e dinâmico que identifica, avalia, monitora e responde aos riscos que possam comprometer o atingimento dos objetivos estratégicos da Companhia ou causar impactos significativos ao seu negócio. Este processo permite que responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo a informações suficientes relacionadas aos riscos aos quais estão expostos, de

forma a suportar decisões e definição de estratégias que aumentem a probabilidade de alcance dos objetivos e minimizem riscos a níveis aceitáveis.

- 6.1.2 Trata-se de uma abordagem preventiva que visa criar meios para gerenciar e manter os riscos sob controle (dentro do apetite estabelecido) de maneira a se antecipar a eventuais incidentes ou crises.
- 6.1.3 Há duas visões distintas e complementares de gestão de riscos: Visão Corporativa e Visão Transacional.
- 6.1.4 A **Visão Corporativa** gerencia riscos que afetam a companhia como um todo e estão diretamente relacionados aos objetivos estratégicos da Organização e a continuidade do negócio.
- 6.1.5 A **Visão Transacional** (camada operacional) gerencia riscos relacionados aos processos, sistemas, contratos e unidades de negócios da Companhia, considerando o impacto específico em cada área. Este tipo de risco detalha e complementa os riscos corporativos estando a eles associados como fatores de risco, conforme ilustrado abaixo:

Figura 01: Visões Distintas da Gestão de Riscos



- 6.1.6 A gestão de riscos está diretamente relacionada ao crescimento sustentável, à rentabilidade, à preservação e à criação de valor para a Cia e para os seus acionistas, dado que este processo permite a identificação não somente de ameaças, como também de oportunidades de negócio.
- 6.1.7 Um efetivo processo de gestão de riscos, que se concretiza pelo cumprimento de boas práticas de Governança Corporativa, tem como finalidade gerenciar os riscos de maneira eficaz, permitindo que responsáveis, em todos os níveis da governança, tenham acesso tempestivo a informações suficientes relacionadas aos riscos aos quais estão expostos, de

forma a suportar decisões e definição de estratégias que aumentem a probabilidade de alcance dos objetivos e minimizem riscos a níveis aceitáveis.

6.1.8 A gestão de riscos, por meio de um enfoque estruturado e da melhor compreensão das inter-relações entre riscos, alinha a estratégia, os processos, as pessoas, a tecnologia e os conhecimentos, aproveitando os benefícios inerentes à diversificação, objetivando a preservação e a criação de valor para a Cia.

6.1.9 Com o objetivo de padronizar a Gestão de Riscos na Iguá, fica estabelecido que:

- A gestão de riscos deve estar incorporada à cultura da Cia, estando presente em todos os processos e atividades.
- A liderança deve promover uma cultura de gestão de riscos em todos os seus níveis hierárquicos e nas suas respectivas áreas de atuação, bem como assegurar a aplicação dos princípios e a aderência aos procedimentos de gestão de riscos.
- A Alta Administração dá o tom para toda a Cia, reforçando a importância e instituindo responsabilidades de supervisão sobre o gerenciamento de riscos.
- A tomada de decisões baseada em riscos deve ser incorporada à gestão, visando à preservação e à criação de valor à Cia.
- A gestão de riscos deve ser integrada aos processos de Gestão, Conformidade, Controles Internos e Auditoria Interna, promovendo a identificação antecipada de riscos e sua gestão conservadora e tempestiva.
- Os riscos identificados devem ser analisados e classificados por natureza, categoria, origem dos eventos (internos ou externos) e seus impactos na organização. Se necessário deverá haver planos de ação, com a nomeação dos Donos dos Riscos e plano de monitoramento definido.
- A independência no processo de gestão de riscos e a segregação de funções entre os tomadores de riscos e os responsáveis pelo seu monitoramento devem ser assegurados.
- O monitoramento contínuo dos riscos e a incorporação na gestão de rotinas são vitais para assegurar a eficácia da gestão de riscos e seu aperfeiçoamento através de ciclos de avaliação e revisões frequentes, visando à melhoria contínua do processo.
- As análises, as respostas e as aprovações dos **riscos corporativos**, após a validação da sua criticidade, devem ser apresentadas aos seguintes níveis:

Níveis	
Alto	Comitê de Auditoria e Diretoria Executiva
Significativo	Gerências e Diretoria Executiva
Moderado ou Baixo	Gerências

- As análises, as respostas e as aprovações dos **riscos transacionais**, após a validação da sua criticidade, devem ser apresentadas aos seguintes níveis:

Níveis	
Alto e Significativo	Gerências e Diretoria
Moderado ou Baixo	Gerências

- Eventuais aceitações de riscos de qualquer natureza deverão observar o estabelecido no *TM-COR-RCI-001 - Termo de Aceitação do Risco - TAR* e deve ser aplicado a toda a empresa incluindo riscos identificados em auditorias internas.

6.2 ALINHAMENTO ESTRATÉGICO E MODELO INTEGRADO

- 6.2.1 O gerenciamento de riscos é parte integrante do processo de elaboração dos objetivos estratégicos e está diretamente alinhado com estes objetivos, estabelecendo um ciclo integrado e virtuoso de retroalimentação entre as linhas de defesa da Companhia para uma cobertura mais ampla dos fatores de riscos internos e externos diante dos resultados esperados.
- 6.2.2 A estrutura de gestão de riscos apoia a integração da governança, em todos os níveis, atividades e funções significativas, englobando as mais diversas áreas e especialidades, atuando com sinergia para proteger o negócio e suportar a liderança no monitoramento e adequação tempestiva de sua estratégia frente as eventuais alterações no ambiente de riscos.

Figura 02: Modelo Três Linhas de Defesa IIA



6.3 CONTEXTO E ESCOPO

6.3.1 Nesta primeira etapa é realizado um levantamento de informações e estudo do contexto externo (ambiente financeiro, econômico, regulatório, socioambiental e relações com os stakeholders) e contexto interno (governança, estrutura organizacional, estratégia, processos, sistemas, contratos, relatórios de auditoria e outras avaliações disponíveis) para definição de escopo, isto é, atividades e temas críticos que serão objeto de mapeamento, chegando assim aos cenários de risco a serem melhor avaliados.

6.4 IDENTIFICAÇÃO DE RISCOS

- 6.4.1 Com base no resultado do cenário de riscos são identificados quais riscos podem ajudar ou impedir a Iguá no alcance de seus objetivos, bem como seus responsáveis (Dono do Risco).
- 6.4.2 Para encontrar, reconhecer e descrever os riscos, a Iguá utiliza entrevistas com executivos e conselheiros, coleta de dados, análise de evidências, documentos, pesquisas e validações junto as áreas técnicas envolvidas. Como resultado haverá uma lista de riscos associada ao escopo e ao cenário definido.

6.5 CATEGORIZAÇÃO DOS RISCOS

6.5.1 Para fins de categorização, os Riscos na Iguá devem ser divididos da seguinte forma: Estratégico, Socioambiental, Financeiro, Operacional, regulatório e Tecnológico.

Categoria	Descrição
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. Potencial Impacto decorrente de decisões, investimentos devidos e falta de capacidade de resposta às mudanças no ambiente.
Socioambiental	Riscos de perdas no resultado e balanço da empresa, causadas por danos diretos ou indiretos ao meio ambiente. Potencial impacto decorrente de ocorrência de um evento associado à gestão inadequada de questões ambientais.
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.). Potencial impacto decorrente principalmente de divulgações financeiras não confiáveis ou enganosas.
Operacional	Riscos de perdas resultantes de processos internos inadequados, falhas tecnológicas, erros humanos ou de sistemas, o que inclui ainda os riscos ambientais, sociais ou relacionados a fraudes. Estão relacionados a infraestrutura da Companhia (processos, pessoas e tecnologia), que afetam a eficiência operacional e a utilização efetiva e eficiente de seus recursos. Potencial impacto decorrente de problemas operacionais, como falhas nos controles internos.
Regulatório	Riscos relacionados ao cumprimento da legislação aplicável a área de atuação, bem como de leis gerais (ambiental, trabalhista, cível e tributário/fiscal). Potencial impacto decorrente do descumprimento de leis ou regulamentos ou processos movidos por clientes ou contrapartes.
Tecnológico	Riscos que consistem na perda, uso indevido, acesso ou divulgação não autorizada de informações ou dados pessoais de partes interessadas, internas ou externas, podendo ameaçar os negócios ou prejudicar a imagem da Companhia.
Imagem e Reputação	Riscos de perda de imagem e reputação da Companhia, como cobertura negativa da mídia, perda de participação de mercado, causando danos a empresa ou podendo parar as operações. Exposição grave ou penalidades severas para os gestores / colaboradores, ocasionando danos irreparáveis a imagem da empresa.

- 6.5.2 Tendo em vista as inúmeras definições de riscos e a necessidade de uma linguagem comum a todos os envolvidos no processo, a Iguá adota um Dicionário de Riscos através da segmentação dos riscos em categorias, subcategorias e Tipos de riscos, considerando as características e o ambiente de negócio da companhia.
- 6.5.3 Os desdobramentos das Categorias, Subcategorias e Tipos de riscos são apresentados no Dicionário de Riscos.
- 6.5.4 As descrições dos Tipos de riscos são apresentadas no documento *LI-COR-RCI-001 - Lista do Dicionário de Riscos Corporativos Iguá*.

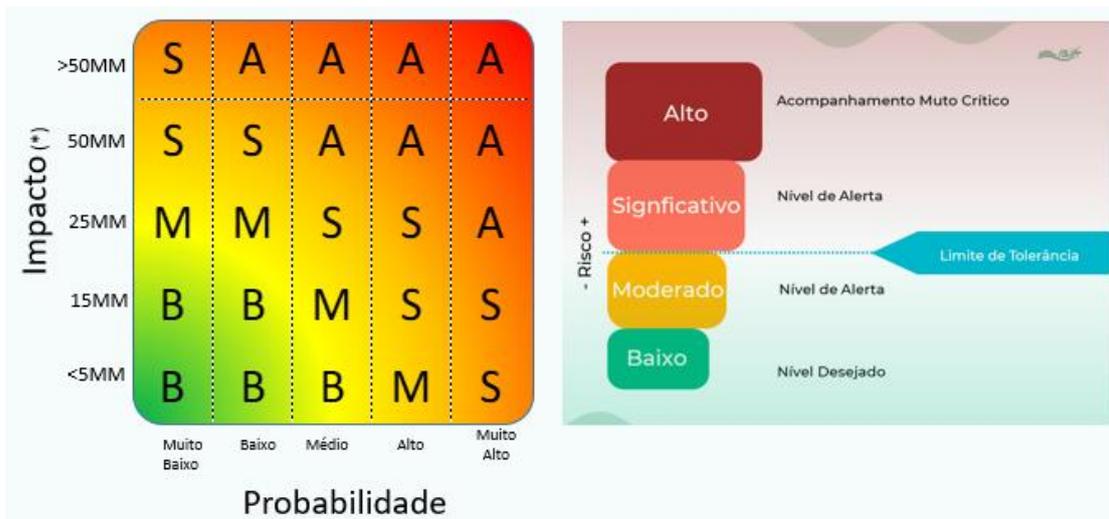
6.6 ANÁLISE (IMPACTO E PROBABILIDADE)

- 6.6.1 A área de Compliance e Controles Internos deve avaliar o impacto e a probabilidade de materialização dos riscos em conjunto com os gestores responsáveis, bem como a assertividade destas análises e a efetividade dos controles e planos de ação.
- 6.6.2 Os riscos identificados (risco inerente) serão mensurados considerando o nível de probabilidade e frequência e de impacto, conforme avaliação realizada pela área de Compliance e Controles Internos em conjunto com os respectivos donos do risco. A classificação final do grau de risco será definida mediante a combinação entre o impacto e a frequência.
- 6.6.3 A análise de riscos deve determinar o Nível de Exposição ao Risco (Alto, Significativo, Moderado ou Baixo) já considerando controles e iniciativas implementadas (risco residual).

6.7 APETITE AO RISCO

- 6.7.1 O Apetite ao Risco é uma declaração do mais alto nível da Organização (Conselho de Administração) sobre o quanto a companhia está disposta a aceitar os riscos para atingimento de seus objetivos. Composto pelos níveis de risco "Desejável, Alerta e Intolerável", ele estabelece os limites dentro dos quais o Conselho espera que a Administração opere, e determina parâmetros para análise dos riscos, bem como serve de base para priorização e decisão do tratamento (resposta) adequado.

Figura 04: Heat Map e Appetite a Risco



6.7.2 O Heat Map acima estabelece a classificação do risco com base em uma análise (real ou estimada) de probabilidade (chance de materialização) e impacto (em R\$MM). Ao lado dele o Appetite define o limite de tolerância aos riscos como sendo não tolerados casos com nível de exposição ao risco “Alto” e “Significativo”.

6.7.3 Além dos aspectos quantitativos resultantes da análise de impacto e probabilidade, também são considerados no Appetite parâmetros qualitativos como julgamento profissional e as seguintes assertivas:

- A Iguá não tolera a falta de conformidade e/ou má conduta de executivos, colaboradores ou terceiros com leis, regras e regulações aplicáveis;
- A Iguá não tolera negligências operacionais que afetem os níveis de serviços dos seus clientes;
- A Iguá não tolera desperdício de recursos e atos que possam causar dano ao seu patrimônio, de terceiros, ao patrimônio público ou ao meio ambiente; e
- A Iguá não tolera exposição negativa de sua marca que possa afetar sua imagem, reputação, atividades do negócio e partes interessadas.

6.7.4 A Análise do vetor financeiro é com base no resultado do EBITDA da Cia, conforme régua de impactos financeiros:

Abaixo seguem valores atualizados no EBITDA contábil de dezembro/2022.

Mínimo	Baixo	Moderado	Significativo	Alto
Impactos financeiros negativos no caixa abaixo de R\$ 5 milhões.	Impactos financeiros negativos no caixa entre R\$ 5 e R\$ 15 milhões.	Impactos financeiros negativos no caixa entre R\$ 15 e R\$ 25 milhões.	Impactos financeiros negativos no caixa entre R\$ 25 e R\$ 50 milhões.	Impactos financeiros negativos no caixa acima de R\$ 50 milhões.
~ 0 a 1%	~ 1 a 3%	~ 3 a 5%	~ 5 a 10%	~ Acima 10%

6.8 CLASSIFICAÇÃO E ACOMPANHAMENTO DOS RISCOS

6.8.1 O processo de gestão de riscos inclui além da identificação de riscos e fatores de riscos a classificação e o acompanhamento do tratamento deles. Desta forma, após análise os riscos identificados são classificados como "Alto", "Significativo", "Moderado" ou "Baixo", sendo os riscos "Altos" e "Significativos" acompanhados pela Alta Administração e Conselho em pautas fixas e recorrentes em suas reuniões ordinárias ou em reuniões extraordinárias que assegurem tempestividade na deliberação de quaisquer riscos e fatores considerados urgentes e relevantes.

6.8.2 A classificação é definida através da avaliação e aplicação de um conjunto de critérios de probabilidade (histórico de ocorrência ou projeção estimada da possível materialização dos fatores de risco) e impacto (potenciais consequências derivadas da ocorrência do risco), considerando:

- Planejamento e objetivos estratégicos;
- Parâmetros proporcionais ao porte da Companhia atualizados periodicamente;
- Vetores quantitativos (não apenas financeiros) e qualitativos abrangentes;
- Appetite ao Risco (definido pela Administração e Conselho de acordo com cada risco em específico); e
- Controles e iniciativas mitigatórias (risco residual).

6.8.3 O detalhamento da metodologia e critérios de classificação, bem como dos mecanismos de resposta e monitoramento dos riscos estão nos procedimentos (PR-COR-RCI-001 – Procedimento de Gerenciamento de Riscos e Controles Internos), devidamente aprovado e aderente a normas e melhores práticas de mercado.

6.9 TRATAMENTO E RESPOSTA AOS RISCOS

6.9.1 As Áreas de Negócio devem desenvolver ações preventivas e corretivas para responder de forma apropriada, efetiva e mitigar os riscos da Companhia, para isso é necessário:

Resposta ao Risco	Descrição
Aceitar	<p>Esta estratégia é adotada quando não é possível ou prático responder ao risco utilizando as outras estratégias. Quando a Alta Administração decide por aceitar o risco, significa que estão concordando em enfrentar o risco, se e quando ele ocorrer. Um plano de contingência emergencial ou plano de solução paliativo devem ser desenvolvidos para essa eventualidade.</p> <p>Geralmente são definidas ações para tratar todos os riscos identificados, ou cuja avaliação final ficou abaixo do risco residual esperado. Excepcionalmente, de forma fundamentada e conforme governança e alçada competente</p>

	<p>estabelecida no <i>PR-COR-RCI-001 – Procedimento de Gerenciamento de Riscos</i>, é aprovado um <i>TM-COR-RCI-001 – Termo de Aceitação do Risco - TAR</i>. Trata-se de um “de acordo” formalizando que não haverá uma ação/iniciativa em função, por exemplo, de inviabilidade técnica ou financeira, custo x benefício da solução entre outros fatores.</p> <p>Vale ressaltar que não se aplica TAR para casos com nível de exposição ao risco acima do Apetite ao Risco da Companhia ou apontados por Auditorias como <i>Significant Deficiency (SD)</i>.</p>
Compartilhar/Transferir	Envolve encontrar outra parte que esteja disposta a assumir a responsabilidade e arcar com os impactos do risco, caso ocorra (ex: seguros, títulos e garantias).
Evitar	O risco pode ser evitado através da remoção da causa do risco ou ao executar a operação de uma forma diferente, porém ainda assim em linha com o alcance dos objetivos da empresa. Nem todos os riscos podem ser evitados/eliminados, e esta abordagem pode ser onerosa.
Reduzir / Diminuir	A mitigação de riscos reduz a probabilidade e/ou o impacto de um evento de risco adverso para um limite aceitável (risco residual esperado) por meio da implantação de controles e iniciativas. A implementação do controle e/ou iniciativas pode ocorrer de forma imediata ou prazos definidos através de planos de ação estabelecidos.

6.9.2 Nesta fase deve-se selecionar e implementar as melhores opções de resposta ao risco, avaliar a eficácia desta resposta, decidir se o risco remanescente é aceitável e, se for aplicável, realizar tratamentos adicionais. Deve-se balancear benefícios, custos, esforços, vantagens e desvantagens da implementação. Sendo possível:

- Realizar análises adicionais para melhor compreensão do risco;
- Aprimorar os controles e iniciativas existentes, e avaliar a necessidade de novas implementações;
- Contratação de seguro para compartilhamento dos riscos e retenção monitorada;

6.9.3 Para maior detalhamento dos mecanismos de resposta ao risco (controles e iniciativas) vide o *PR-COR-RCI-001 – Procedimento de Gerenciamento de Riscos e Controles Internos*.

6.10 VIGÊNCIA

6.10.1 A Matriz de Risco Transacional será revisada anualmente no ciclo vigente ou tempestivamente quando necessário.

6.10.2 A Matriz de Risco Corporativa (Iguá Saneamento e Operações) será revisada bianualmente ou quando houver necessidade tempestiva.

7 FORMULÁRIOS/MODELOS

- LI-COR-RCI-001 – Lista do Dicionário de Riscos Iguá
- MP-COR-RCI-001 – Mapa da Cadeia de Valor do Saneamento - Iguá

8 ANEXOS

Não aplicável.