Metodologia de Gestão de Riscos

Aprovado na 369ª Reunião Ordinária do Conselho de Administração da CASAL, realizada em 28/01/2026

SUMÁRIO

1.OBJETIVO:

Essa metodologia de Gestão de Riscos tem como objetivo estabelecer os procedimentos e etapas que a CASAL deve seguir para identificar, analisar, avaliar, tratar, monitorar e comunicar riscos, garantindo conformidade com a Política de Gestão de Riscos Corporativos.

Por meio deste guia, busca-se assegurar uma abordagem estruturada, sistemática e integrada, alinhada as melhores práticas de governança corporativa, a Lei nº 13.303/2016 (Lei das Estatais), a ISO 31000:2018.

2. ABRANGÊNCIA:

Esta Metodologia aplica-se a todos os níveis organizacionais da Companhia, os quais são integrantes do processo de gerenciamento de riscos, direta ou indiretamente.

3. REFERÊNCIAS NORMATIVAS:

- ✓ Lei nº 13.303/2016 (Lei das Estatais);
- ✓ Norma ISO 31000:2018 (Gestão de Riscos);
- ✓ COSO;
- ✓ Política de Gestão de Riscos Estratégicos;
- ✓ Código de Ética e Conduta;
- ✓ Demais normativos internos e externos e/ou documentos de referência aplicáveis a Gestão de Riscos e ao setor de saneamento.

4. RESPONSABILIDADES

Na CASAL, a gestão de riscos é uma responsabilidade compartilhada com todos os colaboradores, incluindo membros dos Conselhos, Comitês e Diretoria. Para fortalecer essa cultura e garantir uma abordagem estruturada, a Companhia adota o Modelo das Três Linhas, do Instituto dos Auditores Internos do Brasil (IIA Brasil), como referência na governança, controle interno e gestão de riscos corporativos.

4.1. Papel da Alta Administração na Gestão de Riscos

Responsáveis: Diretoria Colegiada e Conselho de Administração.

Atuação: A Alta Administração tem papel fundamental na tomada de decisões estratégicas, assegurando que a gestão de riscos seja eficaz e alinhada aos objetivos da empresa.

Principais responsabilidades:

- ✓ Dirimir conflitos decorrentes da implementação da Gestão de Riscos;
- ✓ Garantir os recursos necessários para aplicação dos controles e mitigação de riscos;
- ✓ Definir o apetite ao risco da empresa e aprovar diretrizes estratégicas;
- ✓ Monitorar indicadores-chave de risco e tomar decisões baseadas em análises estruturadas.

4.2. Primeira Linha de Defesa – Gestão

Responsáveis: Donos dos Riscos e demais colaboradores.

Atuação: São responsáveis diretos por identificar, avaliar, tratar e monitorar os riscos dentro dos processos, projetos e operações sob sua gestão.

Principais responsabilidades:

- ✓ Gerenciar os riscos em suas áreas, sendo responsáveis pela identificação, análise, avaliação e monitoramento contínuo desses riscos;
- ✓ Implementar e manter controles internos eficazes;
- ✓ Garantir conformidade com normas e regulamentos;
- ✓ Tomar decisões baseadas nos riscos identificados;
- ✓ Mitigar riscos antes que se tornem problemas críticos;
- ✓ Definir e executar planos de ação e contingência, garantindo a continuidade das operações em caso de materialização de riscos;
- ✓ Desenvolver indicadores para monitorar a variação dos riscos sob sua responsabilidade, garantindo que as respostas aos riscos sejam adequadas;
- ✓ Reportar periodicamente à área de Gestão de Riscos sobre as mudanças significativas nos riscos sob sua responsabilidade, identificando quaisquer novos riscos ou alterações nas características dos riscos existentes;
- ✓ Engajar-se ativamente na cultura de riscos, promovendo sua aplicação prática;
- ✓ Outras responsabilidades inseridas na Política.

4.3. Segunda Linha de Defesa – Gestão de Riscos e Compliance

Responsáveis: Setor de Gestão de Riscos e Compliance.

Atuação: Atua como um suporte à primeira linha, desenvolvendo políticas e metodologias, monitorando riscos estratégicos e garantindo que os controles sejam aplicados de forma adequada.

Principais responsabilidades:

- ✓ Planejar e coordenar a Gestão de Riscos junto aos donos dos riscos (1ª linha);
- ✓ Criar, disseminar e atualizar a metodologia e a política de gestão de riscos;
- ✓ Monitorar riscos estratégicos e setoriais, orientando gestores na implementação de práticas eficazes;
- ✓ Fornecer treinamento e suporte técnico sobre gestão de riscos e compliance;
- ✓ Apoiar a identificação e avaliação dos riscos, auxiliando na criação de controles internos;

- ✓ Outras responsabilidades inseridas na Política.

4.4. Terceira Linha de Defesa – Auditoria Interna

Responsáveis: Auditoria Interna

Atuação: Realiza avaliações independentes e objetivas, verificando se a gestão de riscos e os controles internos são eficazes e aderentes às diretrizes corporativas.

Principais responsabilidades:

- ✓ Avaliar a eficácia do gerenciamento de riscos, por meio da auditoria dos controles internos;
- ✓ Fornecer relatórios para a alta administração e ao Comitê de Auditoria Estatutária;
- ✓ Emitir recomendações para aprimoramento dos controles internos;
- ✓ Identificar falhas ou desvios na execução das estratégias de gestão de riscos.

5. METODOLOGIA DE GERENCIAMENTO DE RISCOS

A gestão de riscos na CASAL segue as etapas do ciclo de gerenciamento de riscos, alinhadas às melhores práticas de gestão e governança corporativa, como a ISO 31000.

5.1. IDENTIFICAÇÃO E ANÁLISE DOS RISCOS

Objetivo: Mapear os riscos Estratégicos, Operacionais, Financeiros, Conformidade, ESG e de Negócios que podem impactar a CASAL.

Procedimentos:

- ✓ Analisar o ambiente interno e externo;
- ✓ Realizar entrevistas com gestores;
- ✓ Utilizar ferramentas como: SWOT, brainstorming, checklists e análise histórica;
- ✓ Classificar os Riscos.

Resultado esperado: Listar os riscos identificados e categorizados.

1º passo – Utilizar ferramentas para Identificação de Riscos:

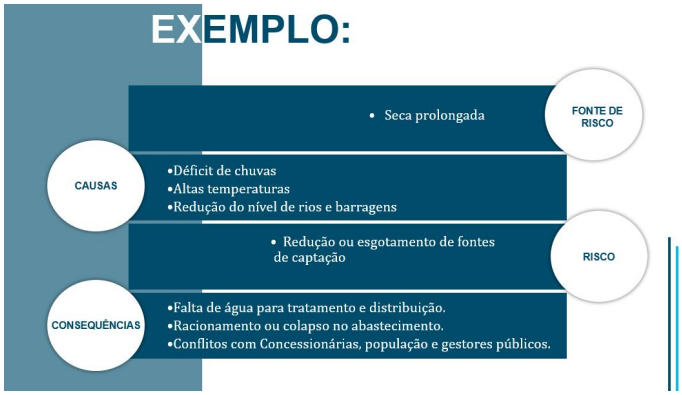
Para identificarmos os riscos, inicialmente precisamos conhecer o contexto, por meio de aplicação de técnicas que possibilitem o levantamento de informações.
A CASAL poderá utilizar as técnicas abaixo para identificar os riscos, ou outras que se adaptem melhor ao cenário a ser analisado:

a) BRAINSTORMING: é executado com o livre fluxo de conversação entre um grupo de pessoas conhecedoras de um tema/processo para identificar falhas, fragilidades, perigos e riscos potenciais ou já conhecidos. Os participantes devem ser estimulados ao debate, principalmente nas questões mais polêmicas.
Vantagens: o debate estimula informações.
Desvantagens: a presença de colegas pode inibir a franqueza, pode haver predominância de opiniões de determinadas pessoas.

b) WHAT IF - "E SE" (SWIFT): é a técnica do pensamento de azar Como o próprio nome diz, é uma técnica onde você vai fazer uma série de questionamentos de possibilidades de erros no processo (e se a planilha não chegar no horário, e se o dado for alterado, e se você faltar, e se o produto vencer, e se o sistema estiver fora do ar ...).
V**antagens:** é rápida, aumenta o senso de responsabilidade dos entrevistados, aumenta a percepção de riscos potenciais para os responsáveis que passam a entender que você o ajudará.
Desvantagens: exige um "pensamento de azar" bem desenvolvido, o entrevistado com pouco conhecimento pode não identificar riscos.

c) BOWTIE: é uma ferramenta de levantamento de risco muito útil por se visual, de fácil entendimento e que representa de forma eficaz o risco, proporcionando uma oportunidade para identificar e avaliar os riscos. Devido à causa "x", poderá ocorrer o risco "y", acarretando em "z".

CAUSAS (devido a)	EVENTO DE RISCO (poderá ocorrer)	CONSEQUÊNCIAS (acarretando em)
Causa 1		Consequência 1



2º passo - Classificação e tipologia dos Riscos Estratégicos

Uma vez identificados os riscos, eles devem ser classificados considerando os critérios estabelecidos na matriz a seguir:

RISCOS			
Classificação	Descrição	Tipologia	Descrição
Riscos Estratégicos	A organização não tem controle por serem eminentemente de origem externa; Afetam diretamente ou indiretamente o negócio em seus fundamentos.	Riscos Macroeconômicos e Políticos	Novas interpretações (jurisprudência) de leis existentes;
			Alterações no cenário Político;
			Alterações de políticas monetárias ou de leis que afetam o negócio;
			Crise econômica gerada por eventos pouco prováveis. Exemplos: pandemia e catástrofes naturais.
		Riscos de Concorrência	Mudança de ambiente concorrencial por mudanças nos incumbentes ou entrada de novos concorrentes;
			Dumping de concorrente com alto poder no mercado;
			Entrada de tecnologia disruptiva que altera o ambiente competitivo.

Riscos de Conformidade	Ligados às atitudes da Governança, colaboradores ou terceiros envolvidos no negócio que possam ser considerados ilegais ou antiéticos.	Riscos Reputacionais	São decorrência da materialização de certas situações inadequadamente tratadas e não prevenidas na organização, tais como discriminação racial ou sexual, assédio moral ou sexual, concorrência desleal, destruição de reputação de terceiros, etc.
		Riscos Regulatórios	São decorrência de procedimentos considerados ilegais como não cumprimento de normas trabalhistas, tributárias ou emitidas pelos reguladores das atividades da empresa e ações consideradas criminosas no relacionamento de negócios com clientes ou concorrentes.
Riscos Financeiros	Riscos que impactam diretamente a saúde financeira da organização, como variações cambiais, contas a receber e a pagar, comercial e aumento de custos	Riscos de Liquidez	Falta ou excesso de caixa para cobrir os compromissos financeiros comerciais e dívidas bancárias, tributárias e trabalhistas devido a diversos eventos.
		Riscos de Mercado	Variações de taxas de juros, indexadores de inflação e taxas de câmbio que podem afetar o balanceamento de ativos e passivos da organização, gerando perdas nos resultados financeiros ou impactos negativos na solvência.
		Riscos de Crédito	Incapacidade dos devedores da organização em cumprir as obrigações para com ela, exigindo ações de cobrança administrativas ou judiciais e podendo gerar problemas de liquidez e perdas de resultados.

Riscos Operacionais	Eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas que possam implicar na possibilidade da ocorrência de perdas	Risco de Falhas Operacionais	Falhas geradas por colaboradores, equipamentos, terceiros nas suas atividades operacionais dentro da organização gerando problemas de qualidade, perdas de materiais e produção.
		Riscos de Segurança (Física ou Virtual)	Problemas gerados por roubos, assaltos com consequências que impactam pessoas ou bens materiais; Problemas com fraudes envolvendo a organização, seus dirigentes e seus colaboradores; Impactos gerados por invasão de hackers nos sistemas e informações da organização, seus dirigentes e colaboradores.
		Riscos de Continuidade de Negócio	Impactos causados na operação da organização por desastres, greves, incêndios, problemas urbanos que impeçam acesso físico ou virtual de suas instalações
Riscos ESG	Envolvem impactos da empresa para o meio ambiente, relações com a sociedade e aspectos de governança corporativa	Riscos Ambientais	Processos de produção que emitem poluentes para o ar, água ou solo, afetando o equilíbrio ecológico de uma região.
		Riscos Sociais	Práticas inadequadas na operação em regiões vulneráveis ou utilizando colaboradores com alta vulnerabilidade social, inclusive mão de obra infantil ou escrava.
		Riscos de Governança	Práticas corporativas antiéticas de gestão, de atuação no mercado ou perante a concorrência.

			Tratamento não equitativo a investidores minoritários e desrespeito a direitos de stakeholders.
Riscos de Negócio	Afetam os negócios da organização e estão ligados a fatores operacionais e de marketing, afetando o relacionamento com os clientes, fornecedores e sua posição no mercado.	Riscos de Produtos	Problemas com a qualidade, preço, posicionamento ou imagem do produto no mercado, podendo tornar a demanda inferior ao necessário para se atingir o ponto de equilíbrio financeiro e reduzir a participação de mercado da empresa.
		Riscos de Suitability	Problemas de relacionamento com os clientes devido à venda incorreta pela falta de informações sobre o produto ou sobre sua adequação em relação às necessidades dos clientes, gerando reclamações e atritos

5.2. AVALIAÇÃO DOS RISCOS

Objetivo: Avaliar os riscos quanto à sua probabilidade de ocorrência e impacto nos objetivos estratégicos. Por meio dela, é possível saber qual a chance, a probabilidade de os riscos virem a acontecer e calcular seus respectivos impactos nos processos da Companhia.

Procedimentos:

- ✓ Determinar a probabilidade de ocorrência;
- ✓ Determinar a impacto de ocorrência;
- ✓ Classificar os riscos em níveis de criticidade;
- ✓ Utilizar a Matriz e o Mapa de Riscos.

RESULTADO ESPERADO: Riscos priorizados conforme sua criticidade.

1º passo – Avaliar a probabilidade e o impacto

Para análise do risco inerente e do risco residual, o nível do risco será calculado com base em dois critérios: probabilidade x impacto. Para tanto, utilizaremos 2 réguas, que utilizam escalas de 1 a 5:

Probabilidade:

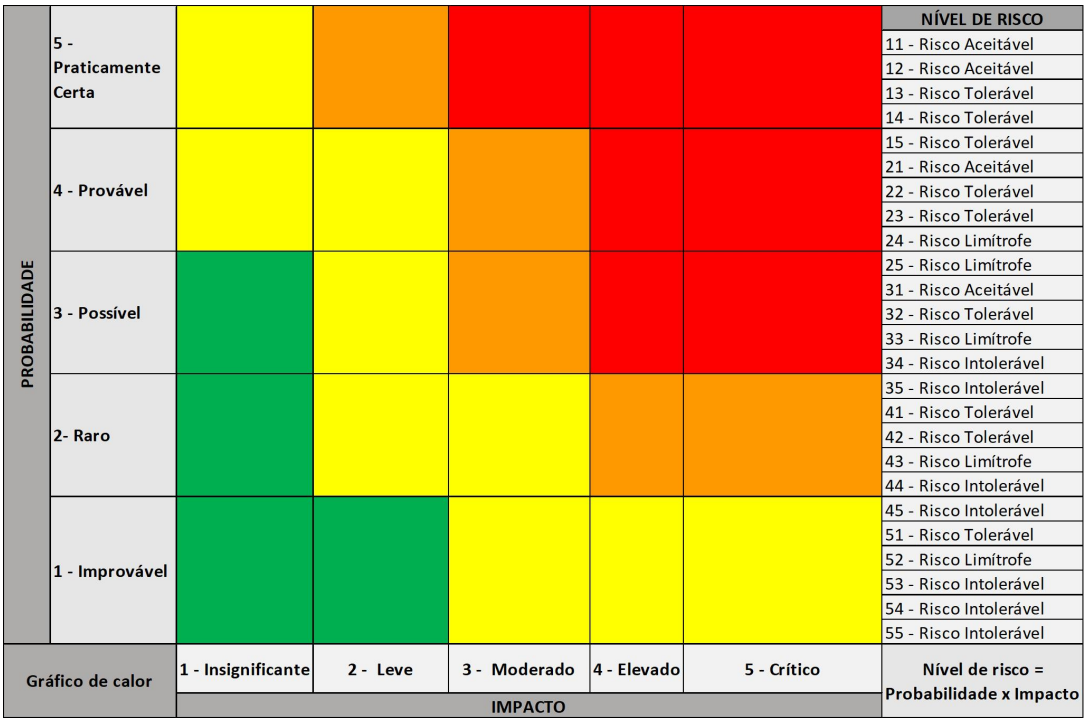
PROBABILIDADE	Descrição	
	1-Improvável	O evento poderá ocorrer de forma inesperada, havendo poucos elementos ou informações que indicam essa possibilidade. Poderá ocorrer em menos de uma vez por ano.
	2-Raro	O evento poderá ocorrer de forma inesperada ou casual, pois as circunstâncias pouco indicam essa possibilidade. Poderá ocorrer em menos de uma vez por ano.
	3-Possível	De alguma forma o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade. Poderá ocorrer ao menos uma vez por semestre.
	4-Provável	De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade. Poderá ocorrer ao menos uma vez por mês.
	5-Praticamente Certa	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente a possibilidade. Poderá ocorrer uma vez por semana ou mais.

Impacto:

	Descrição	
IMPACTO	**1-Irrelevante**	Compromete minimamente o atingimento do objetivo ou não altera o alcance do objetivo/resultado.
		Pode gerar pedido de informações
		Sem impacto na imagem
		Valor envolvido abaixo de < 0,1% da Receita Líquida mensal
	2-Leve	Compromete em alguma medida o alcance do objetivo, mas não impede o alcance da maior parte do objetivo/resultado.
		Pode gerar notificação ao gestor ou determinações de correções;
		Impacto na imagem não extrapola o ambiente interno
		Valor envolvido entre 0,1% e 0,5% da Receita Líquida mensal
	3-Moderado	Compromete razoavelmente o alcance do objetivo/resultado.
		Pode gerar imposição de penalidades leves/medianas
		Impacto na imagem se estende para as partes envolvidas
		Valor envolvido entre 0,5% e 1% e da Receita Líquida mensal
	4-Elevado	Compromete a maior parte do atingimento do objetivo/resultado.
		Pode gerar imposição de penalidades relevantes;
		Impacto na imagem pode chegar à mídia provocando exposição por um curto período de tempo
		Valor envolvido entre 1% e 2% da Receita Líquida mensal
	5-Crítico	Compromete totalmente ou quase totalmente o atingimento do objetivo/resultado.
		Pode gerar imposições de processos criminais, administrativos e/ou fiscais;

		Impacto na imagem com algum destaque na mídia provocando exposição significativa
		Valor envolvido >2% da Receita Líquida mensal

2º passo – Cálculo dos níveis de criticidade



PROBABILIDADE							NÍVEL DE RISCO
	5 - Praticamente Certa						11 - Risco Aceitável
							12 - Risco Aceitável
							13 - Risco Tolerável
							14 - Risco Tolerável
	4 - Provável						15 - Risco Tolerável
							21 - Risco Aceitável
							22 - Risco Tolerável
							23 - Risco Tolerável
							24 - Risco Limítrofe
	3 - Possível						25 - Risco Limítrofe
							31 - Risco Aceitável
							32 - Risco Tolerável
							33 - Risco Limítrofe
							34 - Risco Intolerável
	2- Raro						35 - Risco Intolerável
							41 - Risco Tolerável
							42 - Risco Tolerável
							43 - Risco Limítrofe
							44 - Risco Intolerável
	1 - Improvável						45 - Risco Intolerável
							51 - Risco Tolerável
							52 - Risco Limítrofe
							53 - Risco Intolerável
							54 - Risco Intolerável
							55 - Risco Intolerável
Gráfico de calor		1 - Insignificante	2 - Leve	3 - Moderado	4 - Elevado	5 - Crítico	Nível de risco = Probabilidade x Impacto
		IMPACTO					

O mapa de Riscos é a representação gráfica dos riscos mapeados. O nível de criticidade dos riscos é graficamente representado por cores para que seja facilmente identificado no processo.

3º passo – Nível de criticidade dos Riscos

Classificação do Nível de Criticidade		
Classificação	Descrição	Medida de Controle
Intolerável	Risco acima do limite de tolerância de exposição. É aquele cuja magnitude é tão elevada que não pode ser justificado sob nenhuma circunstância, independentemente dos benefícios associados à atividade ou da probabilidade de sua ocorrência.	Mitigar; ações corretivas urgentes; controle emergencial.
Limítrofe	Risco muito próximo ao limite de tolerância de exposição. É o risco que está na linha tênue entre o aceitável e o tolerável. Exige análise criteriosa para decidir se é possível aceitá-lo temporariamente ou se será necessária ação corretiva.	Mitigar; monitoramento rigoroso, controle contigencial.
Tolerável	Risco com necessidade de monitoramento. Risco que não é desejável, mas pode ser temporariamente aceito desde que haja controle ativo e plano de redução contínua. Só é permitido quando não há alternativa viável imediata e os benefícios superam os riscos de forma justificada.	Otimizar; monitoramento e controle preventivo.
Aceitável	Risco aceito. Risco considerado baixo o suficiente para ser aceito como parte natural da atividade. Não requer ações adicionais de controle, além das rotineiras.	Acompanhar, monitorar.

A aprovação dos níveis de criticidade dos riscos, que definem as responsabilidades para aprovação e tratamento dos riscos deve ser realizada observando as alçadas de aprovação abaixo:

Nível	Medidas de Gestão	Alçada de aprovação	Responsável pelo Monitoramento
Intolerável	Aos riscos intoleráveis as ações deverão ser imediatas, sendo necessário monitorá-los continuamente para observar se houve mudanças pelo transcurso do tempo ou por ações de tratamento.	*Conselho de Administração*	*Dono do risco*
Limítrofe	O risco nesta faixa está próximo de ultrapassar a tolerância, sendo necessária a adoção de medidas no curto ou médio prazo. Deve-se monitorar estes riscos com frequência regular e rotineira para verificar se há mudanças ao longo do tempo e/ou após a implementação de ações de tratamento.	*Direx*	*Dono do risco*
Tolerável	Apesar de tolerável, o risco nesta faixa demanda atenção, podendo ser ou não necessária a adoção de medidas no médio ou longo prazo. É importante monitorar estes riscos periodicamente para verificar se há mudanças ao longo do tempo e/ou após a implementação de ações de tratamento (se houver).	*Diretoria da Área*	*Dono do risco*
Aceitável	Ao risco aceitável, nenhuma ação precisará ser tomada de imediato, podendo ou não haver monitoramento periódico para verificar se há mudanças ao longo do tempo.	*Superintendência da área*	*Dono do risco*

4º passo: Associação entre Apetite e Nível de Criticidade do Risco

O Apetite a risco refere-se ao nível e tipo de risco que a CASAL está disposta a aceitar para alcançar seus objetivos estratégicos e operacionais, para o acionamento da governança de Gestão de Riscos. Já a Tolerância a Risco define os limites de variação aceitável no nível de exposição antes da necessidade de adoção de medidas corretivas.

Nível de Criticidade	Apetite Correspondente	Ação/Recomendação
Intolerável	Muito Baixo	Ações corretivas urgentes.
Limítrofe	Baixo	Monitoramento rigoroso e mitigação.
Tolerável	Moderado	Controles e monitoramento.
Aceitável	Alto (raro)	Acompanhamento e monitoramento.

5º passo: Tolerância ao Risco e Escalonamento

A tolerância ao risco é determinada pelo Nível de Criticidade (Impacto x Probabilidade). A resposta ao risco deve seguir o seguinte escalonamento:

Nível de Criticidade	Ação Necessária	Responsável	Escalonamento
Aceitável	Acompanhamento rotineiro.	Donos dos Riscos	Reporte periódico a Superintendência, Diretoria da Área e área de Gestão de Riscos.
Tolerável	Reavaliação de controles. Ações preventivas se necessário.	Donos dos Riscos	Reporte periódico a Superintendência, Diretoria da Área e área de Gestão de Riscos.
Limítrofe	Adoção de planos de mitigação e contingência. Monitoramento intensificado.	Donos dos Riscos + SUDEO + CGR	Reporte periódico e imediato a Superintendência, Diretoria da Área, à Diretoria Executiva, ao Comitê de Auditoria e Conselho de Administração.
Intolerável	Ação imediata. Pode incluir suspensão de atividades, remediação urgente ou reporte.	Donos + SUDEO + CGR + Diretoria da área	Reporte imediato à Diretoria Executiva, ao Comitê de Auditoria e Conselho.

5.3. AVALIAÇÃO DE CONTROLES

Após a identificação do risco e a avaliação do nível do risco Inerente, deve ser analisado se há algum tipo de controle.

Objetivo: Avaliar a efetividade dos controles existentes e identificar a necessidade de novos controles para mitigar os riscos.

Procedimentos:

- ✓ Identificação dos controles internos já implementados;
- ✓ Verificar se os controles estão reduzindo os riscos conforme esperado;
- ✓ Identificar as falhas e vulnerabilidades nos controles;
- ✓ Propor melhorias e ajustes nos controles.

Resultado esperado: Controles internos eficazes e aprimorados.

1º passo - Tipos de Controle:

	ESCALA	
CONTROLES	**1-Inexistente**	Controle não existe, não funciona ou não foi implementado;
	2-Fraco	Controle não institucionalizado, não está na esfera de conhecimento pessoal dos operadores do processo; em geral realizados de maneira manual;
	3-Mediano	Controle razoavelmente institucionalizado, mas pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.
	4-Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.
	5-Forte	Controle institucionalizado e sustentado por ferramentas adequadas, podendo ser considerado em um nível de "melhor prática"; mitiga o risco em todos os aspectos relevantes.

5.4. TRATAMENTO E RESPOSTAS AOS RISCOS

Objetivo: Definir e aplicar estratégias adequadas para tratar os riscos identificados.

Resultado esperado: Plano de ação com medidas de resposta para cada risco identificado.

1º passo - Formas de Respostas e tratamentos aos Riscos:

Dependendo do nível de criticidade dos riscos (Aceitável, Tolerável, Limítrofe e Intolerável), pode-se identificar as categorias de resposta aos riscos: evitar, compartilhar, reduzir ou aceitar, e dessa forma, adotar medidas de tratamento e controle necessários para cada nível.

RESPOSTA E TRATAMENTO AOS RISCOS	**Evitar**	Evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco. É o caso de um risco muito acentuado e de difícil, impossível ou estrategicamente indesejável mitigação.
	Compartilhar	É aplicável para situações em que o meio de mitigação do risco analisado é a transferência ou o compartilhamento do mesmo com terceiros. É o exemplo da contratação de uma apólice de seguros, como meio de mitigar o risco. O relacionamento com o terceiro para o qual o risco foi transferido deve ser bem gerenciado para assegurar a efetiva transferência do risco.
	Reduzir	Estratégia viável econômica e operacionalmente para reduzir impacto e/ou probabilidade como meio de mitigação do risco analisado. Necessita de plano de ação a ser elaborado pelos donos do risco e sua equipe.
	Aceitar	Aceitar o risco sem fazer nada a respeito. A decisão deve ser fundamentada. Esta opção deveria ser usada quando: • o nível de risco é considerado baixo; • a capacidade da organização para fazer alguma coisa é limitada; • o custo é desproporcional ao benefício; • nenhuma resposta é considerada eficaz para reduzir a probabilidade ou o impacto do risco, a um custo aceitável, entre outros. No caso de aceitar o risco, pode se verificar a possibilidade de retirar controles considerados desnecessários.

2º passo - Priorização De Riscos:

Definidas as respostas e tratamento aos riscos, deve ser realizada a priorização dos riscos, ou seja, entre os riscos mapeados, quais serão priorizados com base em nível de criticidade.

5.5. MONITORAMENTO E COMUNICAÇÃO

Objetivo: Acompanhar a evolução dos riscos e atualizar as estratégias conforme necessário.

Procedimentos:

- ✓ Monitoramento contínuo dos indicadores dos riscos;
- ✓ Reuniões periódicas de acompanhamento com as áreas responsáveis;
- ✓ Comunicação transparente dos riscos às partes interessadas;
- ✓ Atualização da Matriz de Riscos conforme mudanças no ambiente.

Resultado esperado: Relatórios periódicos de acompanhamento dos riscos.

A área de Gestão de Riscos é responsável por coordenar e monitorar o processo os riscos junto aos donos dos riscos. Já a diretoria deverá monitorar as variações de criticidade dos riscos priorizados e reportar variações significativas ao Comitê de Auditoria Estatutário e ao Conselho de Administração, sempre que o nível de tolerância aos riscos for atingido.

5.6. REVISÃO E MELHORIA CONTÍNUA

Objetivo: Aprimorar constantemente o processo de gestão de riscos.

Procedimentos:

- ✓ A revisão da Política de Gestão de Riscos será avaliada e revisada a cada dois anos ou sempre que demandada pela área de Gestão de Riscos, Diretoria, Comitê de Auditoria ou Conselho de Administração;
- ✓ Aprimoramento dos controles internos;
- ✓ Treinamentos e capacitações para gestores e colaboradores;
- ✓ Auditorias internas para avaliar a eficácia das ações implementadas.

Resultado esperado: Gestão de riscos eficiente e integrada à estratégia da CASAL.

6. MATRIZ (PLANILHA) DE RISCO

Todas as informações acima devem ser registradas em uma planilha/sistema de riscos, a ser revisada anualmente ou a qualquer momento, considerando o rumo dos acontecimentos relacionados aos objetivos estratégicos e a mudança no agravamento do impacto ou probabilidade dos riscos.

7.REVISÃO

A Metodologia será avaliada e revisada sempre que demandada pela área de Gestão de Riscos, Diretoria, Comitê de Auditoria ou Conselho de Administração.

As alterações realizadas nesta Metodologia deverão ser submetidas a análise da Diretoria Colegiada, seguida da validação do Comitê de Auditoria Estatutário e, posteriormente, à aprovação pelo Conselho de Administração.

8.CONTROLE DE REGISTROS

Os registros gerados pelas atividades desenvolvidas em função deste procedimento são controlados da seguinte forma:

Nome do Registro	Responsável	Permissão de Acesso	Meio de arquivo	Ordenação	Local de arquivo	Tempo de Arquivo	Forma de Disposição
Planilha de Monitoramento	SUDEO/ GEQUAI	Livre	Eletrônico	Cronológica	Google Drive	Até a próxima atualização	Deletar

GLOSSÁRIO

- ✓ **Gestão de Riscos:** É um processo sistemático e contínuo que visa identificar, analisar, avaliar, tratar e monitorar os riscos que podem afetar os objetivos de uma organização.
- ✓ **Risco:** É o efeito da incerteza nos objetivos estratégicos da Companhia. O Risco poderá ser positivo, negativo ou ambos, e poderá abordar, criar ou resultar em oportunidades e ameaças.
- ✓ **Origem do Risco**: Fator interno ou externo que pode desencadear um evento de risco.
- ✓ **Evento de Risco:** é a ocorrência ou mudança em um conjunto de circunstâncias. Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas e várias consequências. É a manifestação do risco.
- ✓ **Partes Interessadas:** Pessoa ou organização que pode afetar, ser afetada ou perceber-se afetada por uma decisão ou atividade.
- ✓ **Contexto Organizacional:** Ambientes interno e externo nos quais a organização opera, influenciando a identificação e o gerenciamento de riscos.
- ✓ **Fatores de Riscos:** é qualquer elemento (pessoas, processos, sistemas, estrutura organizacional, infraestrutura física, tecnologia, eventos ...) que, individualmente ou de maneira combinada, contribui para a geração, aumento ou modificação de um risco.
- ✓ **Risco Inerente:** Risco intrínseco da atividade na Companhia; ou seja, é o risco ao qual uma organização está exposta antes da aplicação de qualquer controle ou medida de mitigação
- ✓ **Risco Residual:** Risco que permanece após a implementação de medidas de controle e mitigação.
- ✓ **Classificação dos Riscos** - Processo de categorização dos riscos em grupos como Estratégicos, Operacionais, Financeiros, Conformidade, ESG e de Negócio:
- ✓ **Avaliação dos Riscos:** Processo de análise da criticidade dos riscos identificados, considerando impacto e probabilidade, para estabelecer prioridades de tratamento.
- ✓ **Probabilidade:** Chance de um evento de risco ocorrer dentro de um determinado período de tempo.
- ✓ **Impacto:** Consequência da ocorrência de um evento. Avaliação qualitativa e/ou quantitativa do efeito do risco na Companhia, se materializado;
- ✓ **Criticidade do Risco:** Grau de severidade do risco, baseado na combinação de impacto e probabilidade.
- ✓ **Matriz de Riscos:** É uma ferramenta que ajuda a avaliar e priorizar os riscos identificados, com base na criticidade (impacto x probabilidade).
- ✓ **Mapa de Riscos:** Representação gráfica que avalia riscos com base na criticidade (impacto x probabilidade).
- ✓ **Indicadores de Risco (KRIs):** Métricas utilizadas para monitorar e antecipar possíveis riscos, permitindo ações preventivas.

- ✓ **Apetite ao Risco:** Nível máximo de exposição ao risco que a organização está disposta a aceitar para alcançar seus objetivos estratégicos.
- ✓ **Tolerância ao Risco:** Limite aceitável de variação no nível de exposição ao risco antes de serem necessárias ações corretivas.
- ✓ **Resposta ao Risco:** Definição do tratamento que a Companhia dará ao risco residual.
- ✓ **Ação Mitigatória:** Medida adotada para reduzir a probabilidade de ocorrência e/ou o impacto de um risco.
- ✓ **Plano de Gerenciamento de Riscos:** Documento que define estratégias, responsáveis, cronogramas e recursos necessários para tratar e monitorar riscos.
- ✓ **Monitoramento e Controle de Riscos:** Processo contínuo de acompanhamento dos riscos para identificar mudanças na criticidade e efetividade das ações de mitigação.
- ✓ **Controle Interno:** Procedimentos implementados para garantir conformidade com normas, minimizar riscos e assegurar eficiência operacional.
- ✓ **Revisão Periódica de Riscos**: Atualização regular do processo de gestão de riscos para incorporar mudanças no ambiente interno e externo da organização.

ANEXO I

I - TIPOS DE CONTROLES QUE PODEM SER IMPLEMENTADOS (ROL EXEMPLIFICATIVO):

A lista a seguir apresenta, a título de exemplo, uma relação de controles internos que podem ser utilizados no tratamento dos riscos:

1 **Aplicação de checklists**: Elaboração e uso de listas de verificação para garantir que todas as etapas do processo foram cumpridas, com responsabilização formal do executor. *Exemplo:* checklist para concessão de licenças e outorgas.

2. Atribuição de autoridade e limites de alçada: Definição formal de quem tem autoridade para tomar decisões, com limites claramente estabelecidos. *Exemplo:* gestão de contratos a partir de determinado valor sob responsabilidade de Superintendentes.

3. Capacitação e treinamento: Programas de capacitação técnica e comportamental, voltados para assegurar a correta execução dos processos sob responsabilidade dos colaboradores.

4. Comunicação, publicidade e transparência: implantação de diretrizes voltadas para tornar públicas as ações e decisões gerenciais, de modo a assegurar a transparência dos atos e contribuir para o controle dos processos (p.ex.: parcerias celebradas; relação de processos administrativos disciplinares abertos e situação).

5. Estruturação adequada: Garantia de que a estrutura física, tecnológica e de pessoal seja compatível com a complexidade e o volume das atividades desenvolvidas.

6. Formalização de manuais e procedimentos: Documentação clara de processos, com regras definidas sobre como realizar as atividades, garantindo padronização e mitigação de erros operacionais. *Exemplo:* Procedimentos Operacionais Padrões (POPs) e fluxogramas.

7. Planos ou Programas de contingência: planejamento de ações a serem implementadas em caso de eventos que comprometam os objetivos estratégicos da organização, podendo a chegar à paralisação total ou parcial das atividades (p.ex.: apagões; bug de sistemas; pandemias; greves prolongadas etc.).

8. Relatórios de acompanhamento: Emissão periódica de relatórios que avaliem a conformidade dos processos, especialmente aqueles críticos para o alcance dos objetivos estratégicos.

9. Segregação de funções: Divisão clara de responsabilidades e etapas dos processos entre diferentes pessoas ou setores, evitando conflitos de interesse ou fraudes.

10. Sistemas informatizados: implantação de controles informatizados e, se for o caso, com mecanismos automáticos capazes de sinalizarem e até impedirem realização de operações atípicas, não conformes ou ilegais, de acordo com parâmetros previamente definidos.

11. Testes de conformidade: Execução de testes (por amostragem ou totalidade) em pontos críticos dos processos para validar a aderência a normas internas e externas.

12. Utilização de senhas individuais: atribuição de senhas individuais de acesso a sistemas e bancos de dados, de modo a evitar utilização por pessoas não autorizadas a manipular dados e informações dos processos; registrar trilha de acessos e identificar os responsáveis por alterações e atualizações.

13. Visitas e controle in loco: Realização de visitas periódicas aos locais de execução das atividades para verificar conformidade com normas contratuais e legais (p.ex.: visitar local da execução da prestação do serviço para atestar cumprimento de obrigações conforme contrato).

14. Reuniões periódicas: Encontros regulares com as áreas envolvidas para análise dos riscos, acompanhamento de planos de ação e reavaliação dos controles implementados.

15. Indicadores de Desempenho e Risco (KPIs e KRIs): Estabelecimento de métricas específicas para monitorar o desempenho de processos e antecipar riscos.

16. Auditorias Internas Regulares: Execução de auditorias sistemáticas para avaliar a efetividade dos controles internos e recomendar ajustes.

17. Simulações e Testes de Estresse: Realização de simulações de cenários de risco extremo para avaliar a capacidade de resposta da organização e a eficácia dos planos de contingência.

18. Painéis de Controle e Dashboards Gerenciais: Ferramentas visuais que consolidam informações críticas sobre os riscos, controles e ações mitigadoras, facilitando a tomada de decisão.

19. Registro e Análise de Incidentes

Implantação de mecanismos para registrar eventos de risco materializados, investigar causas, corrigir falhas e evitar recorrência.

20. Controles Comportamentais e Culturais: Adoção de medidas que reforcem a ética, a integridade e a cultura de conformidade, como canais de denúncia, campanhas de comunicação e programas de integridade.

21. Controle de Acesso Físico: Restrição e monitoramento do acesso a áreas sensíveis (ex. empregados, arquivos, almoxarifado, laboratórios, etc.) por meio de crachás, biometria ou registro manual.

22. Validação Independente: Revisão de documentos, cálculos ou decisões por uma pessoa ou área distinta daquela que os elaborou, antes da sua validação final. *Exemplo:* conferência independente de editais, planilhas orçamentárias ou análises técnicas.

23. Rastreabilidade de Processos: Criação de mecanismos para garantir que todas as etapas de um processo possam ser auditadas posteriormente. *Exemplo:* registros de protocolos, logs de sistema, registro de movimentação de documentos físicos.

24. Controle de Versões de Documentos: Gestão formal das versões de documentos normativos e técnicos para evitar uso de versões obsoletas e assegurar a rastreabilidade de alterações.

25. Gestão de Contrapartes e Fornecedores: Implantação de critérios e mecanismos de avaliação contínua de fornecedores, conveniados ou prestadores de serviço, incluindo análise de risco contratual.

Presidente do Conselho de Administração

Monique Souza de Assis

Membros do Conselho de Administração

Carlos Eduardo de Paula Monteiro

Fábio Augusto Carvalho Peixoto

Luiz Cavalcante Peixoto Neto

Maria Aparecida Torres dos Santos

Raquel Nadal César Gonçalves

Roney Presbítero de Arruda Nascimento

Rosa Maria Barros Tenório

Elaboração:	**Validação:**
Superintendência de Desenvolvimento Organizacional, Compliance e Gestão de Riscos - SUDEO **Revisão:** Comitê de Gestão de Riscos: Ordem de Serviço nº 10/2025 – DP	Diretoria Colegiada: Reunião da DIREX, realizada em 21/10/2025. Comitê de Auditoria Estatutária: 53ª Reunião Ordinária do CAE, realizada dia 18/11/2025. **Aprovação:** Conselho de Administração: 369ª Reunião Ordinária do Conselho de Administração, realizada em 28/01/2026.

HISTÓRICO DE MODIFICAÇÕES

Versões		**Data**	**Resumo Histórico de Revisões** (Motivo da Alteração)	**Nº. pg.**
V. 01		30/05/20219	Emissão Inicial	Todas
Última Revisão	V.02	28/01/2026	Revisão – Processo SEI E:19620.0000009497/2025	Todas