O CONSELHO DE ADMINISTRAÇÃO DA COMPANHIA DE RECURSOS HÍDRICOS DO CEARÁ - COGERH, em atendimento ao Art. 32, do seu Estatuto Social, em conjunto com o Art. 18 da Lei n° 13.303, de 30 de junho de 2016, após deliberação, RESOLVE:

Art. 1º Aprovar e Instituir a Política de Gestão de Riscos Integrada da Companhia de Gestão dos Recursos Hídricos do Ceará - COGERH com abrangência a todas as suas unidades, independentes da localidade, nos termos desta Norma Interna.

Parágrafo único. Fica a atualização do regramento contido na Política de Gestão de Riscos da COGERH, aprovada na 154ª Reunião do Conselho de Administração, 11 de outubro de 2022, absorvida por esta Norma Interna.

Art. 2° Esta Política de Gestão de Riscos Integrada está fundamentada na Lei n° 13.303, de 30 de junho de 2016, no Estatuto Social da COGERH, no Manual de Gestão de Riscos do Tribunal de Contas da União, 2018, nas diretrizes do Committee of Sponsoring Organizations of the Treadway Commission – COSO e em boas práticas sobre o tema.

Art. 3° A Política de Gestão de Riscos da COGERH jamais deverá ser vista de forma isolada e sim deverá ser sempre utilizada de forma integrada.

§ 1º A integração da Política de Gestão de Riscos a que se refere o caput, se dará:

I – Na concepção e execução do Planejamento Estratégico;

II – No planejamento e execução das iniciativas de fortalecimento da Gestão da Integridade;

III – Nos procedimentos das análises e melhorias de processos de negócio;

IV – Nos processos de gestão de projetos; e

IV – Nas estratégias de comunicação e suas execuções.

§ 2º A presente Política de Gestão de Riscos Integrada comporá os mecanismos de fortalecimento da Governança da COGERH, subsidiando o processo de decisão da Companhia.

## CAPÍTULO
## DOS FUNDAMENTOS

### Seção
### Da Finalidade

Art. 4° A Política de Gestão de Riscos Integrada da COGERH tem por finalidade estabelecer diretrizes e comunicar os princípios, objetivos e estrutura que estará alicerçado o Sistema de Gestão de Riscos Integrada no âmbito da Companhia, bem como as competências, respectivas atribuições dos atores desse sistema e a metodologia que deverá ser aplicada.

Parágrafo único É também objetivo desta Política de Gestão de Riscos Integrada uniformizar as diretrizes e consolidar as regras gerais sobre o tema na COGERH.

Art. 5º Os processos que comporão o Sistema de Gestão de Riscos Integrada da COGERH deverão contribuir para a gestão dos riscos diante das incertezas inerentes ao negócio da Companhia, como também integrarão o processo de criação e preservação da geração de valor da instituição.

Parágrafo único A incorporação do gerenciamento de riscos na estrutura da COGERH deverá ser realizada de forma a contribuir diretamente na habilidade de implementar suas estratégias e de realizar a sua missão.

Art. 6° A Gestão de Riscos Integrada da COGERH deverá estar alinhada ao Programa de Integridade da Companhia, e esse com esta Política, contribuindo mutuamente para as ações de prevenção, detecção, punição e remediação de práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta.

Art. 7° As iniciativas de Gestão de Riscos Integrada da COGERH deverão observar também ações que possibilitem a gestão de continuidade dos negócios, a fim de se desenvolver uma resiliência organizacional que possibilite responder eficazmente e salvaguardar os interesses das partes interessadas, a imagem e a continuidade do valor público agregado da instituição, no caso da concretização dos eventos de riscos.

## Seção II
## Dos Conceitos Chave para a Gestão de Riscos Integrada da COGERH

Art. 8º Para os efeitos da Política de Gestão de Riscos Integrada da COGERH, considera-se:

I – Governança - conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

II – Gestão de Riscos Integrada - processo de natureza continuada, integrada ao planejamento estratégico, à gestão da integridade, à análise e melhoria de processos, à gestão de projetos e processo de comunicação, com estratégias formuladas para identificar, avaliar, gerenciar e controlar potenciais eventos que possam afetar a organização e destina-se a fornecer segurança razoável quanto ao alcance dos seus objetivos;

III - Integridade Pública: alinhamento consistente à adesão de valores, princípios e normas éticas comuns para sustentar e priorizar o interesse público sobre os interesses privados no Setor Público;

IV – Evento de Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos da COGERH;

V – Evento de Risco Inerente: evento a que a COGERH está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrênciaou ou seu impacto;

VI – Evento de Risco Residual: evento a que COGERH está exposta após a implementação de ações gerenciais para o seu tratamento;

VII – Evento de Riscos Estratégicos: Riscos que possam impactar no alcance de objetivos estratégicos e na execução da estratégia planejada.

VIII– Eventos de Riscos Operacionais: eventos que podem comprometer as atividades da COGERH, normalmente associados a falhas, deficiências ou inadequação de processos internos, pessoas, infraestruturas e sistemas;

IX – Eventos de Riscos de Imagem/Reputação da COGERH: eventos que podem comprometer a confiança da sociedade, dos sócios ou de parceiros, de clientes ou de fornecedores em relação à capacidade da COGERH em cumprir sua

missão institucional;

X – Evento de Risco para a Integridade: vulnerabilidade que pode favorecer ou facilitar a ocorrência de práticas de corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, podendo comprometer os objetivos da COGERH;

XI – Eventos de Riscos Financeiros/Orçamentários: eventos que podem comprometer a capacidade da COGERH de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades;

XII – Severidade ou Criticidade ou Nível de Risco: resultado da combinação da probabilidade e do impacto atribuídos ao evento de risco;

XIII – Apetite ao Risco: nível da criticidade do evento de risco que uma organização está disposta a aceitar;

XIV– Limite de exposição aos riscos: representa o nível de risco acima do qual é desejável o seu tratamento;

XV – Tolerância ao Risco: nível de variação aceitável a partir do limite de risco, quanto ao alcance de um determinado objetivo;

XVI – Tratamento do Risco: processo de planejamento e a realização de ações e identificação dos respectivos controles internos para modificar o nível do risco e trazê-lo paraum nível dentro do limite estabelecido pela COGERH;

XVII – Controles Internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de agentes públicos das organizações, destinados a enfrentar os riscos e a fornecer segurança razoável de que, na consecução da missão da entidade, serão alcançados os seus objetivos.

XVIII – Responsável pelo Risco: Agente Público responsável pelas ações de planejamento, implantação e monitoramento das execuções de tratamento dos eventos de risco.

XIX – Matriz de Risco - Representação gráfica da exposição dos eventos de riscos identificados pela COGERH, mensurando o nível de criticidade/severidade, a partir da combinação do impacto do risco, no caso de ele se concretizar e de sua probabilidade de se concretizar.

## Seção III
## Dos Princípios

Art. 9º A Gestão de Riscos Integrada da COGERH deverá observar os seguintes princípios:

I – Gestão de riscos integrada de forma sistemática, estruturada, oportuna e documentada;

II – Integração e utilização da gestão de riscos à tomada de decisão, ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, à gestão da integridade e da comunicação, todos relevantes para a execução da estratégia e para o alcance dos objetivos institucionais;

III – Estabelecimento de níveis de exposição a riscos adequados;

IV – Estabelecimento de procedimentos de controle interno proporcionais ao risco, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício, destinados a agregar valor à organização, ao tempo em que protegeo ambiente interno da instituição;

V – Implementação por meio de ciclos de revisão e melhoria contínua do desempenho, controles e governança, a partir da utilização dos resultados da gestão de riscos;

VI – consideração da importância dos fatores humanos e culturais; e

VII – *Due diligence* de Integridade – DDI, visa a aumentar a segurança nas contratações de bens e serviços e mitigar eventuais riscos no relacionamento das contratações e demais parcerias, subsidiando a avaliação do Critério Integridade.

# CAPÍTULO II
# DA GESTÃO DE RISCOS INTEGRADA

## Seção I
## Do Modelo da Gestão de Riscos Integrada

Art. 10. Sem prejuízo dos fundamentos citados no Art. 2° desta Política de Gestão de Riscos Integrada, a estrutura que executará os controles internos para o tratamento dos eventos de riscos priorizados seguirá o Modelo das Três Linhas

do Instituto dos Auditores Internos – IIA.

Parágrafo único A estrutura contida no Modelo das Três Linhas da COGERH se dará da forma a seguir:

I – a Primeira Linha será composta pelos controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos, de suporte e de gestão;

II – a Segunda Linha será composta pela Assessoria de Governança, Riscos e Conformidade responsável por assessorar, formular, disseminar e coordenar as iniciativas corporativas referentes à gestão de riscos integrada, bem como verificar a aderência da estrutura organizacional, dos processos e dos serviços da Companhia às políticas e diretrizes internas que tratam da Gestão de Riscos Integrada; e

III – a Terceira Linha será constituída pela Auditoria Interna, responsável por aferir a adequação do controle interno e a efetividade do gerenciamento dos riscos integrado.

IV – Os Órgãos de Governança são as estruturas colegiadas que:

a) Delegam responsabilidades e oferecem recursos à primeira e segunda linha para facilitar o alcance dos objetivos da organização, inclusive pela Gestão de Riscos Integrada.

b) Estabelecem e supervisonam a terceira linha para oferecer clareza e confiança no progresso em direção ao atingimento dos objetivos.

c) Prestam contas às partes interessadas, inclusive no que se refere aos resultados obtidos pelo Sistema de Gestão de Riscos Integrada.

Art. 11. Os Órgãos de Governança da COGERH são compostos pelo Conselho de Administração e pela Diretoria Executiva.

§ 1º O Conselho de Administração será o responsável por aprovar e supervisionar o Sistema de Gestão de Riscos Integrada da COGERH.

§ 2º A Diretoria Executiva será responsável para propor o modelo do Sistema de Gestão de Riscos integrada e de controle interno da COGERH.

§ 3º A Diretoria Executiva será a responsável por liderar as ações de tratamento de riscos e contará com o assessoramento técnico da Assessoria de

Governança, Risco e Conformidade.

§ 4º A Assessoria de Governança, Riscos e Conformidade deverá apresentar à Diretoria Executiva os resultados do monitoramento dos Planos de Ação elaborados pelas áreas responsáveis pelos eventos de riscos, bem como os resultados do monitoramento de sua execução.

§ 5º A Diretoria executiva poderá expedir determinação para as áreas que estiverem em atraso com a elaboração ou execução dos Planos de Ação de que tratam o parágrafo anterior, solicitando e apreciando os cronogramas para a execução dessas atividades.

§ 6º A Assessoria de Governança, Riscos e Conformidade deverá, sempre que solicitada, assessorar o responsável pelo risco na elaboração do plano de ação, informando a estrutura e o conteúdo mínimo que deverá estar contido no plano.

§ 7º Nas vezes em que forem solicitadas prorrogações de prazo, deverá ser traçada uma linha de base e apresentada para a Diretoria Executiva sempre que for tratado da análise do plano de ação atualizado.

§ 8º A Assessoria de Governança, Riscos e Conformidade, deverá primar por uma comunicação clara de como se dá o Sistema de Gerenciamento do Riscos Integrado e de seus respectivos controles, esclarecendo para a Diretoria Executiva e quando for o caso para o Conselho de Administração, os papéis e responsabilidades de cada ator no Modelo das Três linhas.

§ 9º A Diretoria Executiva deverá expedir documento para as áreas, dando ciência de suas responsabilidades referente ao Sistema de Gestão de Riscos Integrada da COGERH.

Art. 12. A Auditoria interna funcionará de forma independente, no entanto, essa independência não impedirá que sejam prestadas orientações, contribuindo com o alinhamento sobre temas pertinentes a gestão de riscos, através da comunicação e colaboração com as duas primeiras linhas.

Parágrafo único. Na realização das ações citadas no caput, na relação da Auditoria Interna com as duas primeiras linhas, restará esclarecido que não haverá confusão dessas contribuições com a execução das ações que poderão ser posteriormente auditadas.

Art. 13. Sem prejuízo das responsabilidades dispostas no Art. 56 do Estatuto Social da Cogerh, o Comitê de Auditoria Estatutário será responsável por:

I – Supervisionar as ações relacionadas ao controle interno e desenvolvidas pela

Auditoria Interna, no que se refere ao papel da Terceira Linha.

II – Monitorar a qualidade e a integridade dos mecanismos de controle interno.

III – Avaliar e monitorar a exposição ao risco da COGERH e requerer informações detalhadas sobre as políticas de gestão de riscos integrada.

IV – Assessorar o Conselho de Administração na avaliação e monitoramento da matriz de riscos estratégicos da Companhia com os riscos priorizados, seus respectivos planos e respostas de contingência.

## Seção II
## Integração da Gestão de Riscos ao Processo de Planejamento Estratégico

Art. 14. Em conformidade com o que dispõe o Art. 32 do Estatuto Social da Cogerh, o Conselho de Administração será o responsável por aprovar e supervisionar o Sistema de Gestão de Riscos Integrada da COGERH.

Art. 15. A Gestão de Riscos Integrada da COGERH deverá contribuir com o processo de tomada de decisão durante a elaboração e execução do planejamento estratégico.

§ 1º A Identificação, avaliação, tratamento, monitoramento e à análise da gestão de riscos deverão levar em consideração também os riscos que possam impactar na implementação da estratégia e no alcance dos objetivos da organização no cumprimento da sua missão institucional.

Art. 16. A Diretoria Executiva deverá apresentar, até a última reunião ordinária do Conselho de Administração do ano anterior, o plano de negócios para o exercício anual seguinte, bem como a estratégia de longo prazo atualizada com a análise de riscos e oportunidades para, no mínimo, os próximos 5 (cinco) anos.

§ 1º A análise e apresentação da evolução dos indicadores contidos no Plano de Negócios da COGERH, descrito no caput deste artigo, deverá ser realizada em conjunto com a evolução das medidas de tratamento dos eventos de riscos dos indicadores estratégicos.

§ 2º Caberá à Assessoria de Governança, Riscos e Conformidade assessorar a Diretoria Executiva no que se refere a análise dos riscos durante a atualização da estratégia de longo prazo e na apresentação da evolução das medidas de tratamento dos eventos de riscos e de seus impactos nos indicadores contidos no Plano de Negócio da COGERH.

Art. 17. A identificação dos eventos de riscos estratégicos deverá estar alinhada com as entregas finalísticas da Cadeia de Valor da COGERH que colaboram para o cumprimento da missão da Companhia.

Parágrafo único. No processo de priorização dos eventos de riscos, o Conselho de Administração deverá priorizar, no mínimo, dois eventos de riscos relacionados aos macroprocessos finalísticos.

Art. 18. Nas reuniões da Diretoria Executiva, a Assessoria de Governança, Riscos e Conformidade, ao informar dos planos de ação que estão em atraso, deverá apresentar também os impactos relacionados aos eventos de riscos envolvidos, bem como nas vezes em que for solicitada a prorrogação dos prazos nos cronogramas de implementação.

§ 1º A análise dos impactos levará em consideração o atraso da ação em relação à linha de base inicial para contribuir com futuras decisões de prorrogação de prazos.

§ 2º A informação dos impactos dos eventos de riscos cujo plano de ação estiver em atraso, ou mesmo quando solicitada a prorrogação de prazos, deverá constar em ata da reunião da Diretoria Executiva na qual foi tratado.

## Seção III
## Integração da Gestão de Riscos com o Planejamento e Execução das Iniciativas deFortalecimento da Gestão da Integridade

Art. 19 No esforço da identificação dos eventos de riscos da COGERH, deverá ser buscada também a identificação dos eventos de riscos para integridade.

1º Na análise, avaliação e elaboração das medidas de tratamento dos eventos de risco para integridade não deverão ser considerados de forma isolada e sim integrados aos processos que possuem relacionamento com os respectivos eventos de riscos.

§ 2º O Plano de Integridade da COGERH deverá considerar os eventos de riscos para integridade identificados no período de sua elaboração e os respectivos planos de ação.

Art. 20. No processo de priorização dos eventos de riscos, o Conselho de Administração deverá priorizar no mínimo dois eventos de riscos para integridade.

Art. 21. Conforme o inciso XVIII do Art. 32 do Estatuto Social da COGERH, a evolução das ações para tratamento dos eventos de riscos para integridade deverá ser apresentada ao Conselho de Administração para permitir a supervisão do Sistema de Gestão de Riscos Integrada no que se refere a quebra de integridade.

## Seção IV
## Integração da Gestão de Riscos com a Comunicação

Art. 22. A integração entre os processos e responsáveis pela gestão de riscos integrada, se dará, também, por uma comunicação eficaz que deverá percorrer toda a Companhia.

Art. 23. O Sistema de Gestão de Riscos Integrada se integrará com ações de comunicação a partir dos cinco princípios abaixo:

I - Formação de uma cultura de Governança.

II – Monitoramento, avaliação e, se necessário, solicitações de mudança nas estratégias de gestão de riscos integrada.

III - Apresentação da evolução das ações para tratamento dos eventos de riscos priorizados.

IV - Disseminação dos resultados das revisões e atualizações das Políticas de gestão de riscos integrada.

Art. 24. Em busca de atender ao Princípio que visa a estabelecer uma Cultura de Governança, as ações deverão girar em torno dos seguintes pontos:

I – Supervisão e monitoramento do Sistema de Gestão de Riscos Integrada pela alta gestão, a partir da comunicação da Segunda e Terceira Linha nas reuniões da Diretoria Executiva e do Conselho de Administração.

II – Estabelecimento de estruturas na COGERH com atribuições para planejar, executar, monitorar e supervisionar as ações que tratam da Gestão de Riscos Integrada da Companhia, a partir da comunicação dos Órgãos de Governança, regulamentando as estruturas das segunda e terceira linhas e comunicando o seu patrocínio ao desempenho das atribuições dessas instâncias nas reuniões da Diretoria Executiva e do Conselho Administrativo.

III – Definição das diretrizes em forma de Políticas para orientar o Sistema de

Gestão de Riscos Integrada, a partir da disseminação dessa política para a Primeira linha e o respectivo patrocínio dessas diretrizes pelos Órgãos de Governança.

IV – Demonstração do compromisso da alta gestão com os valores fundamentais previstos no Sistema de Gestão de Riscos Integrada, a partir da comunicação para os integrantes das três linhas do patrocínio e comprometimento dos Órgãos de Governança com o Sistema de gestão de Riscos Integrada, comunicação essa contida nas atas das reuniões, palavras de abertura de documentos de referência da Companhia, aparecimentos e materiais de divulgação interna reforçando o compromisso, dentre outras ações.

Art. 25. Na busca para atender ao Princípio que visa a estabelecer monitoramento, avaliação e, se necessário, solicitações de mudanças nas estratégicas de gestão de riscos integrada, as ações deverão girar em torno dos seguintes pontos:

I – Analisar o contexto do negócio da COGERH e as possíveis mudanças de cenários, com o surgimento ou desparecimento de oportunidades e ameaças.
a) A partir da inserção da análise do contexto e sua evolução inserida na comunicação realizada nas análises dos Planos de Negócios, na evolução dos indicadores estratégicos com a integração da gestão de riscos integrada com essas conclusões, nas reuniões da Diretoria Executiva e Conselho Administrativo.

II - Definição do apetite ao risco da Companhia.
a) A partir da definição do apetite a risco da Companhia e a comunicação com as partes interessadas.

III – Monitoramento e avaliações periódicas de suas estratégias e alternativas frente a eventuais mudanças de cenários.
a) A partir da comunicação realizada nas análises dos Planos de Negócios, da evolução dos indicadores estratégicos e da integração da gestão de riscos integrada com essas conclusões, nas reuniões da Diretoria e Conselho Administrativo.

IV - Formulação e monitoramento do Plano de Negócios da Companhia.

Art. 26. Em busca de atender ao princípio que visa a estabelecer a apresentação da evolução das ações para tratamento dos eventos de riscos priorizados, as ações deverão girar em torno dos seguintes pontos:

I – Identificar o evento de risco.

II - Identificar a criticidade/severidade do evento de risco.

III – Priorizar os eventos de riscos.

IV – Desenvolver uma visão de portfólio dos eventos de riscos.

V – Realizar o planejamento do tratamento dos eventos de riscos.

VI – Revisão das medidas de tratamento dos eventos de risco a partir da identificação de mudança nos cenários interno e externo em que a COGERH está inserida.

VII – Buscar a Melhoria contínua do Sistema de Gestão de Riscos Integrada.

a) Para os itens I a IV, a partir da comunicação realizada entre a segunda linha e os Órgãos de Gestão na comunicação da importância dos papéis e responsabilidades para os atores da primeira linha, durante a reunião da Diretoria Executiva e do Conselho Administrativo.
b) A partir da comunicação realizada pela terceira linha com os órgãos de Governança informando da análise da gestão de riscos integrada da Companhia e com a Segunda Linha no assessoramento para o aperfeiçoamento das medidas de tratamento dos eventos de riscos.

Art. 27. Em busca de atender ao princípio que visa a estabelecer a disseminação dos resultados das revisões e atualizações das Políticas de gestão de riscos integrada, as ações deverão girar em torno dos seguintes pontos:

I – Comunicar as informações referentes ao tratamento de eventos de risco:

a) A partir da comunicação dos Órgãos de Governança com as três linhas, destacando o compromisso e patrocínio com o Sistema de Gestão de Riscos Integrada da COGERH.

b) A partir da disseminação para a primeira linha de suas funções e responsabilidades na Gestão de Riscos Integrada da COGERH.

## CAPÍTULO III
## DO MONITORAMENTO E AVALIAÇÃO DAS AÇÕES DA GESTÃO DE RISCOS INTEGRADA

### Seção I
### Da Periodicidade em que Serão Identificados, Avaliados, Tratados e

## Monitorados os Eventos de Riscos

Art. 28. O processo de gerenciamento de riscos integrado da COGERH deverá ser realizado iterativamente.

Parágrafo único. A Assessoria de Governança, Riscos e Conformidade deverá realizar o monitoramento a partir das informações contidas nas fichas de riscos e verificará, de forma contínua, o percentual de execução das ações estratégicas relacionadas aos eventos de riscos corporativos e se esse percentual está alinhado com o prazo estabelecido.

Art. 29. A periodicidade de monitoramento dos eventos de riscos deverá ser realizada no âmbito do ciclo de vida de cada processo ou projeto.

§ 1º A exemplo da periodicidade descrita no *caput*, os ciclos de vidas estão exemplificados em alguns processos, conforme a seguir:

I - Processos relacionados a contratações e aquisições, o ciclo de vida se dá desde a formalização da demanda até o recebimento e o respectivo último pagamento.

II – Em processos relacionados à execução de obras, o ciclo de vida se dá desde o planejamento até a entrega da obra com o respectivo último pagamento. Nesses casos o período após a finalização do ciclo de vida deverá ser abarcado por processos de inspeção e manutenção, por exemplo.

III - O Ciclo de Vida dos projetos, terá início com o Termo de Abertura do Projeto (TAP) e findará com o Termo de Encerramento do Projeto (TEP).

§ 2º No final do processo de monitoramento, a Assessoria de Governança, Riscos e Conformidade, para os eventos de riscos corporativos, e o Escritório de Projetos Corporativos, para os eventos de riscos dos projetos, deverão elaborar relatório contendo a compilação das lições aprendidas e as respectivas conclusões de oportunidades de melhorias.

§ 3º O relatório de monitoramento deverá ser apresentado à Diretoria Executiva, sempre que finalizado.

§ 4º A Assessoria de Governança, Riscos e Conformidade terá o prazo de 12(doze) meses, a partir da vigência dessa Política de Gestão de Riscos Integrada, para iniciar a priorização dos processos para monitoramento das ações mitigatórias dos eventos de riscos.

§ 5º O Escritório de Projetos Corporativos terá o prazo de 12(doze) meses para

organizar a sua metodologia de monitoramento e avaliação dos eventos de riscos dos projetos, a partir de então, deverá ser realizada essa ação em pelo menos todos os projetos considerados estratégicos.

Art. 30. O portfólio dos eventos de riscos, bem como a avaliação dos planos de ação e sua implantação, ou mesmo o alcance dos seus resultados, deverão ser revisitados, atualizados e verificada a necessidade de serem trabalhadas novas prioridades, no maximo a cada quatro anos.

§ 1º O período indicado no *caput* compreende as etapas de planejamento e identificação dos eventos de riscos, sua priorização, o planejamento das ações de tratamento e a elaboração dos seus respectivos planos, as suas implantações ou implementações, a avaliação das ações com a identificação das oportunidades de melhoria e as respectivas implementações dos ajustes identificados, fechando o Ciclo PDCA.

Art. 31. No processo de monitoramento das ações da gestão de riscos integrada, a Assessoria de Governança, Riscos e Conformidade deverá fazer uso de indicadores Chave de desempenho.

Art. 32. O resumo das principais conclusões dos resultados dos monitoramentos e avaliações de todas as ações deverão ser apresentados para a Diretoria Executiva no final dos quatro anos, para subsidiar a nova atualização da Política de Gestão de Riscos Integrada.

Parágrafo único. A apresentação do relatório final não exclui a necessidade das apresentações dos relatórios individuais sobre as ações dos eventos de riscos dos processos priorizados.

Art. 33. A Diretoria executiva deverá expedir recomendações ou determinações, quando necessário, sempre que as áreas que possuam responsáveis pelos eventos de riscos ou que participem de algum dos processos sobre o tema estiverem com dificuldades em priorizar as ações para o tratamento desses eventos de riscos.

## Seção II
## Da Medição do Desempenho da Gestão de Riscos Integrada

Art. 34. A medição do desempenho da gestão de riscos integrada será realizada pela Auditoria Interna, com a periodicidade de pelo menos um ano e apresentada para o Conselho de Administração.

§ 1º A avaliação do desempenho da gestão de riscos integrada será realizada

de forma a verificar o funcionamento desse gerenciamento dos eventos de riscos, a partir de sua eficácia e a manutenção dessa eficácia ao longo do tempo.

§ 2º Na avaliação do desempenho da gestão de riscos integrada, a Auditoria Interna abordará também sobre o impacto dos atrasos na implantação dos planos de ação no alcance dos objetivos da gestão de riscos integrada da COGERH, tomando por referência as distâncias de prazos contidas inicialmente nas linhas de base e o prazo atualizado.

Art. 35. O Comitê de Auditoria Estatutário deverá supervisionar as atividades da Auditoria Interna no que se refere à medição do desempenho da gestão de riscos integrada da COGERH, emitindo parecer sobre essa atividade e recomendações para subsidiar o Conselho de Administração no exercício de avaliação da gestão de riscos integrada.

Art. 36. O processo da medição do desempenho da gestão de riscos integrada deverá, abordar dentre outros que possam surgir, os seguintes aspectos:

I – análise do desenho do processo de gestão de riscos integrada, com vista a verificar possíveis oportunidades de aperfeiçoamento, que deverá observar:

a) o modo de funcionamento do sistema;
b) se há necessidade ao longo do tempo de ajustar os procedimentos de rotina do sistema;
c) se há necessidade de eliminar ou inserir novos componentes;
d) se está ocorrendo aderência às rotinas de gestão de riscos; e
e) Se as solicitações de prorrogações de prazos estão prejudicando o alcance dos objetivos da gestão de riscos integrada.

§ 1º A análise do Sistema de Gestão de Riscos Integrada descrita no inciso I poderá ser realizada a partir de análise de documento, realização de reuniões ou aplicação de listas de verificações com os agentes que executam essas rotinas, bem como aqueles que serão afetados pelas mesmas, a fim de verificar seu desempenho.

## CAPÍTULO IV
## DA METODOLOGIA E FERRAMENTAS PARA O APOIO À GESTÃO DE RISCOSINTEGRADA

### Seção I – Da Metodologia

Art. 37. A metodologia e as ferramentas a serem aplicadas no processo de Gestão de Riscos Integrada na COGERH compreendem a aplicação sistemática

de políticas, as práticas de gestão e as ações direcionadas ao gerenciamento de riscos, objetivando apoiar o processo de tomada de decisão e o alcance dos objetivos da instituição.

Art. 38. O mapeamento e a avaliação dos riscos, considerará, pelo menos, as seguintes tipologias de eventos de riscos:

I – Riscos Estratégicos;

II – Riscos Operacionais;

III – Riscos de Conformidade;

IV – Riscos de Imagem/Reputação da Instituição;

V – Riscos para a Integridade; e

VI – Riscos Financeiros/Orçamentários.

Art. 39. O Plano de Gestão de Riscos Integrada da COGERH será elaborado a partir:

I – da priorização dos eventos de riscos corporativos, realizada pela Diretoria Executiva; e

II – dos projetos planejados e executados na companhia.

Parágrafo único. Para os eventos de riscos finalísticos, esses devem ter, no Plano de Gestão de Riscos Integrada, a evidência e a localização do macroprocesso priorizado na estrutura da Cadeia de Valor da COGERH.

Art. 40. Os processos da Gestão de Riscos Integrada da COGERH são os descritos a seguir:

I – Análise do contexto que envolve os eventos de riscos;

II – Fixação de objetivos;

III– Identificação de riscos;

IV – Análise e avaliação de riscos;

V – Respostas aos riscos;

VI – Identificação dos controles internos;

VII – Informação e Comunicação; e

VIII – Monitoramento.

Art. 41. No resultado da análise do contexto deverá conter as seguintes informações:

I – em se tratando de processo de trabalho, a sua localização na estrutura da cadeia de valor da COGERH;

II – Vulnerabilidades identificadas;

III – Apetite ao risco da instituição;

IV – Tolerância ao risco do macroprocesso; e

V – A estrutura de atribuições das responsabilidades da gestão de risco integrada.

§ 1º O Anexo apresenta a descrição das ferramentas utilizadas para a gestão de riscos consideradas pela COGERH, bem como o limite do nível de riscos.

§ 2º O apetite a risco e a respectiva tolerância, considerados pela COGERH, serão descritos no Documento Declaração de Apetite a Risco.

§ 3º Caberá a Diretoria Executiva apoiada pela Assessoria de Governança, Riscos e Conformidade propor o limite do apetite a risco e a sua respectiva tolerância.

§ 4º Caberá ao Conselho Administrativo aprovar o limite do apetite a risco e a sua respectiva tolerância proposta pela Diretoria executiva.

§ 5º A gestão de riscos integrada da COGERH referente a Projetos será realizada conforme o Project Management Body of Knowledge - PMBOK.

Art. 42. Os objetivos deverão ser definidos como forma de contribuírem com a identificação e avaliação dos riscos no que se refere ao seu alcance, bem como possibilitarem a adoção de medidas necessárias para administrá-los.

Art. 43. Na fixação dos objetivos, serão consideradas pelo menos as seguintes categorias, sem prejuízo de outros que possam ser identificados:

I – Estratégicos ou de negócios;

II – Financeiros;

III – Custos;

IV – Prazos;

V – Escopo;

VI – Qualidade;

VII – Comunicação;

VIII – Conformidade; e

IX – Integridade.

Art. 44. A saída do processo de identificação de riscos deverá conter os riscos inerentes à própria atividade da organização, em seus diversos níveis.

Art. 45. No processo de identificação dos riscos deverão ser identificados eventos em potencial, que, se ocorrerem, afetarão os objetivos impactando-os positivamente ou negativamente.

Parágrafo único. No processo de identificação dos eventos, deverá ser realizado esforço para identificar potenciais eventos interdependentes que possam ser desencadeados pelo evento principal.

Art. 46. Na identificação de riscos para integridade deverão ser considerados, além de infrações de leis e normas, também, as quebras de integridade.

Parágrafo único. Entende-se como quebra de integridade os atos como: recebimento/oferta de propina, desvio de verbas, fraudes, abuso de poder/influência, nepotismo, conflito de interesses, uso indevido e vazamento de informação sigilosa e práticas antiéticas.

Art. 47. No processo de Avaliação de Riscos, os riscos deverão ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência, bem como da

severidade ou criticidade que reflete a combinação entre os dois primeiros.

§ 1º A avaliação de riscos deve ser feita por meio de análises qualitativas, quantitativas ou da combinação de ambas.

§ 2º Os riscos devem ser avaliados quanto à sua condição de inerentes e residuais.

§ 3º A probalidade, o impacto e a severidade analisados no Processo de Avaliaçãode Riscos deverão ter o foco nos objetivos definidos.

§ 4º Na análise de probabilidade e impacto do risco, a equipe deverá estar atenta ao tempo para produzir uma resposta ao risco.

§ 5º A avaliação da criticidade dos riscos deve ser realizada considerando critérios de impacto e probabilidade estabelecidos.

§ 6º Para a realização da análise dos eventos de riscos, será utilizada a Régua de Impacto e Probabilidade, consolidando os critérios apropriados acerca dos efeitos dos riscos, presumindo o cenário da sua materialização, bem como a probabilidade e frequência dessa materialização, tomando como base os dados históricos e a percepção e/ou julgamento da Diretoria Executiva, Gerência e pessoa chave.

Art. 48. O horizonte de tempo empregado para avaliar riscos, deverá ser consistente com o tempo das estratégias e objetivos relacionados a esses riscos.

Art. 49. No processo de tratamento dos eventos de riscos com eventos que gerem impactos negativos, na definição das respostas para os mesmos, deverão ser adotadas algumas das estratégias a seguir:

I – Evitar ou Eliminar;

II – Mitigar ou Minimizar;

III – Compartilhar; ou

IV – aceitar.

§ 1º A estratégia evitar ou eliminar, ocorre quando a atuação tem como finalidade eliminar a ameaça ou proteger o objetivo de seu impacto. Pode ser apropriado para ameaças de alta prioridade com alta probabilidade de ocorrência e um impacto negativo importante.

§ 2º A estratégia Evitar ou Eliminar poderá implicar na descontinuação das atividades que geram os eventos de riscos.

§ 3º Na estratégia Mitigar ou Minimizar, são adotadas medidas para reduzir a probabilidade ou o impacto dos eventos de riscos, ou, até mesmo, ambos.

§ 4º A estratégia Compartilhar implica na redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco.

§5º O compartilhamento envolve transferir a responsabilidade por uma oportunidade a terceiro para que este compartilhe de obrigações e consequentemente de alguma medida dos benefícios, caso a oportunidade ocorra.

§6 º A estratégia Compartilhar é uma estratégia relacionada à formação de parcerias, acordos de cooperação técnica dentre outros institutos.

§7º Na estratégia Aceitar, nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos. No entanto os eventos de riscos para integridade não serão objeto da estratégia aceitar.

§ 8º Na estratégia Minimizar, deverá ser buscada a redução do evento de risco inerente até que o nível residual seja compatível pelo menos com faixa de tolerância da COGERH, no que se refere aos eventos de riscos.

Art. 50. No processo de tratamento dos eventos de riscos com eventos que gerem impactos positivos, na definição das respostas para os mesmos, deverão ser adotas alguma das estratégias a seguir:

I – escalar;

II – explorar;

III – melhorar;
ou

IV – aceitar.

§ 1º A estratégia escalar significa o encaminhamento da tomada de decisão para o gerenciamento no nível da alta gestão, e não no nível do operacional.

§ 2º A estratégia explorar é utilizada para oportunidades de alta prioridade, quando a organização deseja garantir que a oportunidade seja realizada, alocando mais recursos para ações prioritárias.

§ 3º A estratégia Melhorar busca potencializar essa oportunidade para que ela traga o máximo de benefícios possível.

§ 4º A aceitação de uma oportunidade reconhece a sua existência, mas nenhuma ação proativa é tomada. Essa estratégia pode ser apropriada para oportunidades de baixa prioridade e também pode ser adotada quando não há recursos disponíveis para agir diante de uma oportunidade.

Art. 51. A escolha da estratégia para o tratamento dos eventos riscos dependerá do nível de exposição a riscos previamente estabelecidos pela organização, em confronto com a avaliação que se fez do risco.

Art. 52. O Processo de Controle constitui nos procedimentos estabelecidos e executados para a gestão dos riscos, que a organização tenha optado por tratar.

§ 1º As atividades de controle interno devem estar distribuídas por toda a organização, em todos os níveis e em todas as funções. Incluem uma gama de controles internos da gestão, preventivos e detectivos, bem como a preparação prévia de planos de contingência e resposta à materialização dos riscos.

§ 2º Dependendo das circunstâncias, uma determinada atividade de controle pode ajudar a atender aos objetivos da organização em mais de uma categoria.

Art. 53. Na identificação das atividades de controle, deverá ser pensada na sua integração com as respostas aos riscos, a fim de buscar sua execução de forma adequada e oportuna.

Art. 54. A Unidade que possui em suas atribuições a responsabilidade de desempenhar os serviços de tecnologia da informação deverá em conjunto com o Data Protection Officer – DPO ou Encarregado de proteção de dados pessoais, elaborar Política de Proteção de Dados, abarcando a proteção de dados pessoais, e submeter à Diretoria Executiva e, em segunda instância, para a provação do Conselho de Administração.

§ 1º O Data Protection Officer – DPO ou Encarregado de proteção de dados pessoais será a instância executiva que tratará do Sistema de Gestão de Riscos relacionado à proteção de dados pessoais junto à Diretoria Executiva e ao Conselho de Administração.

§ 2º A Gerência de Tecnologia da Informação será a instância executiva que tratará do Sistema de Gestão de Riscos relacionado à gestão de incidentes e proteção de dados junto à Diretoria Executiva e ao Conselho de Administração e deverá atuar em conjunto como Data Protection Officer – DPO ou Encarregado de proteção de dados

Art. 55. O Processo de Informação e Comunicação deverá ser capaz de identificar, coletar e comunicar informações relevantes, a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de eventos de riscos e a tomada de decisão.

§ 1º A comunicação das informações produzidas deve atingir todos os níveis, por meio de informações produzidas, por meio de canais claros e abertos que permitam que a informação flua em todos os sentidos.

§ 2º Sempre que possível, deverá ser inserido no processo de monitoramento o acompanhamento dos Indicadores Chaves de risco.

Art. 56. Durante o processo de monitoramento da gestão de riscos, as oportunidades de melhoria serão relatadas à Diretoria Executiva.

Art. 57. No escopo do monitoramento da Gestão de Riscos Integrada, ao serem identificadas as fraquezas em potencial, deverão ser recomendadas as respectivas medidas alternativas à administração, acompanhadas de informações úteis na realização de determinações de custo-benefício.

Art. 58. Os responsáveis pelos riscos serão identificados e aprovados pela Diretoria Executiva, apoiada pela Assessoria de Governança, Riscos e Conformidade.

§ 1º Os responsáveis pelos riscos serão designados formalmente e cientificados a partir da ato da Diretoria Executiva.

§ 2º Os responsáveis pelos riscos deverão reportar à Assessoria de Governança, Riscos e Conformidade, a evolução do planejamento e implantação das medidas de tratamento dos eventos de riscos, bem como apresentar informação sobre a execução dessas ações.

## CAPÍTULO V
## DAS DISPOSIÇÕES FINAIS

Art. 59. Os Administradores deverão participar anualmente de capacitações sobre a Política de Gestão de Riscos Integrada da COGERH.

§ 1º A Assessoria de Governança, Riscos e Conformidade será a responsável por coordenar os treinamentos de que trata o *caput* desse artigo, identificando os temas necessários que serão abordados nas capacitações.

Art. 60. Essa Norma Interna entra em vigor na data de sua publicação.

## ANEXO I
## INSTRUMENTOS DE SUPORTE À GESTÃO DE RISCOS INTEGRADA DA COGERH

**Matriz de Probabilidade e Impacto.**

| **Probabilidade** | | | | | | |
|---|---|---|---|---|---|---|
| **Muito Alta** | 5 | **5** | **10** | **15** | **20** | **25** |
| **Alta** | 4 | **4** | **8** | **12** | **16** | **20** |
| **Moderada** | 3 | **3** | **6** | **9** | **12** | **15** |
| **Baixa** | 2 | **2** | **4** | **6** | **8** | **10** |
| **Muito Baixa** | 1 | **1** | **2** | **3** | **4** | **5** |
| | | 1 | 2 | 3 | 4 | 5 |
| | | **Muito Baixo** | **Baixo** | **Moderado** | **Alto** | **Muito Alto** |
| | | **Impacto** | | | | |

**Limite do Nível de Riscos**

4 => Baixo. 4 < Moderado =< 9.

9 < Alto +=< 19. 19 < Muito Alto.

## Critérios de avaliação dos controles.

| Desenho do Controle | | Operação do Controle | |
|---|---|---|---|
| **Risco de Control e RCD** | **Critérios** | **Critérios** | **Risco do Controle RCO** |
| Muito Alto 1 | Não há procedimento de controle. | Não há procedimentos de controle. | Muito Alto 1 |
| Alto 0,8 | Há procedimento de controle, mas não são adequados, nem estão formalizados. | Há procedimentos de controle, mas não são executados. | Alto 0,8 |
| Médio 0,6 | Há procedimentos de controle formalizados, mas não estão adequados o suficiente. | Os procedimentos de controle estão sendo parcialmente executados. | Médio 0,6 |
| Baixo 0,4 | Há procedimentos de controle, adequados, suficiente, mas não estão formalizados. | Os procedimentos de controle estão sendo executados, mas sem evidência de sua realização. | Baixo 0,4 |
| Muito Baixo 0,2 | Há procedimentos de controle formalizados, adequados, suficiente e estão formalizados. | Procedimentos de controle são executados e com evidência de sua realização. | Muito Baixo 0,2 |

NRI = Nível de Riscos Inerentes. NRR = Nível de Riscos Residual.

RC = Resultado do Controle. RC = (RCD + RCO)/2 NRR = NRI x RC

**Análise de Probabilidade e Frequência estimada de materialização do Risco**

| Escala | Probabilidade | Frequência | Descrição |
|---|---|---|---|
| **Quase Certo 5** | 90% < 100% | Mais de 1 vez por mês | Esperado ocorrer na maioria dasvezes<br><br>Mais de 60 vezes a cada 5 anos |
| **Provável 4** | 70% < 90% | Mais de 1 vez por semestre até 1 vez por mês | Provável que ocorra em grande partedas vezes<br><br>De 11 a 60 vezes a cada 5 anos |
| **Possível 3** | 30% < 70% | 1 vez por ano a umavez por semestre | Pode ocorrer em algum momento<br><br>De 5 a 10 vezes a cada 5 anos |
| **Baixa 2** | 10% < 30% | Menos de uma vez por ano | Poderia ocorrer em circunstâncias excepcionais<br><br>De 3 ou 4 vezes a cada 5 anos |
| **Raro 1** | < 10% | Menos de uma vez em 5 anos | Poderia acontecer em circunstâncias raras<br><br>Nenhuma vez em 5 anos |

Fonte: Política de Gestão de Riscos - COGERH – V2.

## A Avaliação de Impacto dos Riscos Inerentes e Residuais

| Escala Impacto | Continuidade & Perenidade | Operação | Conformidade | Imagem & Reputação | Meio Ambiente & Comunidade | Saúde & Segurança |
|---|---|---|---|---|---|---|
| **Muito Alto 5** | • Continuidade do negócio afetada<br>• Perda de conhecimento estratégico | • Interrupção acima de 50% do serviço de abastecimento de água destinado à indústria e/ou ao abastecimento humano, a partir de 3dias | • Eventos/processos relacionados ao descumprimento de regulamentação e/ou de legislação, de larga escala (quantidade e/ou montante financeiro) movidos contra a empresa resultando em grandes penalizações, multas e/ou interrupção das operações<br>• Desvio nos valores e nos princípios éticos e de integridade da COGERH<br>• Penalizações pessoais a administradores da COGERH | • Exposição negativa a nível nacional ou internacional | • Impacto severo e irreversível ao solo, biodiversidade, recursos hídricos, are/ou comunidade<br>• Impacto adverso ao solo, biodiversidade, recursos hídricos, ar e/ou comunidade que demandem tempo de resposta acima de 3anos | • Perda de vida humana<br>• Invalidez/ deficiência permanente |
| **Alto 4** | • Continuidade donegócio pode ser afetada<br>• Perda de conhecimento técnicoespecializado | • Interrupção abaixo de 50% do serviço de abastecimento de água destinado à indústria e/ou ao abastecimento humano, a partir de 3 dias<br>• Interrupção acima de 50% do serviço de abastecimento de água destinado à irrigação e/ou ao serviço e comércio, a partir de 3 dias | • restrições na operação<br>Parecer da Auditoria Externa sobre as demonstrações financeiras adverso, com ressalvas ou com abstenção de opinião | • Exposição negativa a nível estadual | • Impacto adverso ao solo, biodiversidade, recursos hídricos, ar e/ou comunidade que demandem tempo de resposta de 1 a 3 anos | • Ferimentos gravesou doenças ocupacionais que gerem invalidez temporária<br>• Lesões que gerem afastamento por período a partir de30 dias |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Moderado 3** | • Continuidade de projetos afetada<br>• Perda de conhecimento técnico | • Interrupção abaixo de 50% do serviço de abastecimento de água destinado à indústria e/ou abastecimento humano, por até 2 dias<br>• Interrupção acima de 50% do serviço de abastecimento de água destinado à irrigação e/ou ao serviço e comércio, por até 2 dias<br>• Interrupção abaixo de 50% do serviço de abastecimento de água destinado à irrigação e/ou ao serviço e comércio, a partir de 3 dias | • Notificações/advertências com necessidade de estabelecer provisão para penalizações e multas dos órgãos fiscalizadores/reguladores | • Exposição negativa a nívelmunicipal | • Impacto adverso ao solo, biodiversidade, recursos hídricos, ar e/ou comunidade que demandem tempo de resposta menor que 1 ano | • Ferimentos graves ou doenças ocupacionais que não gerem invalidez<br>• Lesões que gerem afastamento por período de 15 a 30 dias |
| **Baixo 2** | • Continuidade de projetos pode ser afetada<br>• Perda de conhecimento operacional | • Interrupção abaixo de 50% do serviço de abastecimento de água destinado à irrigaçãoe/ou ao serviço e comércio, por até 2 dias<br>• Interrupção acima de 50% do serviço de abastecimento de água destinado aos demaisusos, a partir de um dia | • Notificações/advertências sem necessidade de estabelecer provisão para penalizações e multas dos órgãos fiscalizadores/reguladores | • Exposição negativa junto a fornecedores e parceiros estratégicos (partes envolvidas) | • Impacto mínimo ao solo, biodiversidade, recursos hídricos e/ou ar que não demandem resposta da empresa | • Ocorrências com ferimentos leves<br>• Lesões que gerem afastamento por período menor que 15 dias |
| **Muito Baixo 1** | • Impacto interno em atividade relacionada a processo<br>• Perda de conhecimento administrativo | • Interrupção abaixo de 50% do serviço de abastecimento de água destinado aos demais usos, a partir de um dia<br>• Interrupção operacional que não gere impactono serviço de abastecimento | • Recomendações pelo não atendimento às leis e normas estabelecidas pelos órgãos fiscalizadores/reguladores | • Exposição negativa exclusiva junto o público interno (empregados) | • Incômodo às pessoas/ comunidades (odor, barulho, poeira, etc.) | • Ocorrências sem danos físicos ou pequenos incidentes |

Fonte: Política de Gestão de Riscos - COGERH – V2

**Ações para os respectivos níveis de Escala de Severidade/Criticidade**

| Escala de Severidade | Descrição da Escala |
|---|---|
| **Baixa** | Dentro do apetite a riscos da instituição. No entanto, deverão ser observados todos os aspectos identificados referente a prevenção dos riscos para a integridade. |
| | Realizar monitoramento periódico de rotina. |
| | Devem ser mitigados, salvo no caso de não ser possível a partir da relação custo e benefício. |
| **Moderada** | Acima do apetite ao risco da instituição. |
| | Dentro do limite de tolerância a risco da instituição. No entanto, deverão serobservados todos os aspectos identificados referente a prevenção dos riscos para a integridade. |
| | Planejar e executar ações para redução da severidade. |
| | Se possível, além de ações corretivas, identificar ações preventivas de mitigação da severidade. |
| | Se for possível identificar gatilhos existentes, reforçar o seu monitoramento por procedimentos de rotinas. |
| **Alta** | Acima do apetite e tolerância ao risco da instituição. |
| | Planejar e executar ações para redução da severidade. |
| | Se for possível identificar gatilhos existentes, aumentar a frequência de seu monitoramento. |
| | Se possível, além de ações corretivas, identificar ações preventivas de mitigação da severidade. |
| | Recomendação de não seguir com a ação, salvo por decisão registrada em ata da Diretoria Executiva. Na ata deve indicar aumento na frequência dos controles. A ressalva não cabe para riscos para integridade. |
| **MuitoAlta** | Acima do apetite e tolerância ao risco da instituição. |
| | Planejar e executar ações para redução da severidade. |
| | Necessariamente identificar gatilhos existentes, aumentar a frequência de seu monitoramento. |
| | Necessariamente, além de ações corretivas, realizar ações preventivas de mitigação da severidade. Na ata deve indicar quais serão as unidades responsáveis para reforçar o tratamento dos eventos de riscos. A ressalva não cabe para riscos para integridade. |
| | Recomendação de não seguir com a ação, salvo por decisão registrada em ata do Conselho de Administração. Na ata deve indicar quais serão as unidades responsáveis para reforçar o tratamento dos eventos de riscos. A ressalva não cabe para riscos para integridade. |

**Classificação dos Riscos Por Natureza, Categorias e Subcategorias Definidas do Dicionário de Riscos da COGERH**

| |
|---|
| **ESTRATÉGICO** |
| **Governança** |
| Comunicação e Divulgação |
| Estrutura Organizacional |
| Social |
| Partes Relacionadas |
| Gestão de Riscos e Monitoramento |
| Sucessão |
| Relacionamento com Poder Concedente e Acionistas |
| **Gestão Estratégica e Modelo de Negócio** |
| Planejamento Estratégico e Orçamento |
| Projetos e Investimentos |
| Alianças e Estratégias |
| Satisfação dos Usuários |
| Alocação de Recursos Hídricos |
| Inovação |
| Continuidade dos Négocios |
| **Político/Econômico** |
| Cenário Econômico |
| Políticas Públicas |
| Reputação e Imagem |
| Reputação |
| Recursos Públicos |
| **Desastres** |
| Biológicos |
| Segurança de Barragens |
| Contaminação por Atividades Agrícolas, Mineradoras e Industriais |
| **INTEGRIDADE** |
| **Quebras de Integridade** |
| Fraudes |
| Abuso de Poder |
| **Influência** |
| Nepotismo |
| Conflito de Interesses |
| **Conduta** |
| Uso Indevido e Vazamento de Informação Sigilosa |
| Práticas Antiéticas |
| **CONFORMIDADE** |
| **Regulamentos e Legislações** |
| Aderência ás Regras |
| Ambiental |
| Jurídico/Legal |
| Societário |
| Tributário/Fiscal |
| Trabalhista |
| Acordos. Judiciais/Extrajudiciais |
| Regulatório |
| Corrupção e Lavagem de Dinheiro |

| |
|---|
| Licenças e Alvarás |
| **FINANCEIRO** |
| **Gestão de Liquidez e Capital** |
| Fluxo de Caixa |
| Disponibilidade de Capital |
| **Crédito** |
| Custo de Oportunidade |
| Garantia |
| Inadimplência da Companhia |
| **Mercado** |
| Taxa de Juros |
| **OPERACIONAL** |
| **Operacional** |
| Capacidade Operacional |
| Efetividade e Eficiência |
| Fornecedores |
| Gestão de Estoque |
| Medição |
| Apoio à Fiscalização |
| Limites de Autoridade e Alçada |
| Gestão de Conteúdo e Propriedade Intelectual |
| Licitações |
| Terceirização |
| Outorga |
| Gestão Patrimonial |
| CálculoTarifário |
| Segurança Patrimonial |
| Segregação de Função |
| Segurança Hídrica |
| Manutenção |
| Monitoramento Qualitativo e Quantitativo (Água Subterrânea e Água Superficial) |
| **Contábil** |
| Registros das Informações |
| Publicações das Informações |
| **Contratos** |
| Gestão de Contratos |
| Obrigação Contratual |
| **Tecnologia da Informação** |
| Dependência de TI |
| Disponibilidade e Desempenho |
| Gestão de Mudança |
| Sistemas de Informação |
| Segurança da Informação (Confidencialidade, Integridade e Disponibilidade) |
| Obsolescência Tecnológica |
| Ativos Tecnológicos |
| Automação de Processos |
| **PESSOAL** |
| **Gestão de Conhecimento** |
| Capacitação e Desenvolvimento |
| Retenção e Atração de Talentos |
| Gestão de Mudança |

| |
|---|
| Liderança |
| Comprometimento e Engajamento |
| Competências e Desempenho |
| **Saúde e Segurança** |
| Clima Organizacional |
| Dependência de Pessoal |
| Contaminação por Trabalho e Campo |
| **MEIO AMBIENTE** |
| **Intempérie Climática** |
| Acidente Ambiental |
| Proteção de Aquíferos |
| Inventário de Reservatórios |

Fonte: Política de Gestão de Riscos – COGERH – V2. Acrescenta a Natureza Integridade.