CONSELHO REGIONAL DE MEDICINA DO ESTADO DO TOCANTINS

INSTRUÇÃO NORMATIVA Nº SEI-1/2023, DE 03 DE MARÇO DE 2023.

Institui no âmbito do Conselho Regional de Medicina do Estado do Tocantins, a Política de Gestão de Riscos.

O Presidente do CONSELHO REGIONAL DE MEDICINA DO ESTADO DO TOCANTINS, no uso das atribuições conferidas pela Lei nº 3.268, de 30/09/1957, publicada em 1º de outubro de 1957, regulamentada pelo Decreto nº 44.045, de 19/07/1958, publicado em 25/07/1958, Decreto-Lei nº 200, de 25/02/1967, Lei nº 11.000, de 15/12/2004, publicada em 16/12/2004 e Decreto nº 10.911, de 22/12/2021.

CONSIDERANDO o Decreto nº 9.203, de 22 de novembro de 2017 que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional; CONSIDERANDO o Decreto nº 10.756, de 27 de julho de 2021 artigo 5º que institui o Sistema de Integridade Pública do Poder Executivo Federal;

CONSIDERANDO a Instrução normativa conjunta nº 1 de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal;

CONSIDERANDO a Lei nº 14.129, de 29 de março de 2021 Capítulo VII que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública;

CONSIDERANDO a Lei nº 14.133, de 1º de abril de 2021 arts. 11, 18, 22, 43, 46, 72, 98, 103, 117, 133, 147 e 169, que dispõe sobre Lei de Licitações e Contratos Administrativos;

CONSIDERANDO que um dos princípios da boa governança consiste no gerenciamento de riscos e na instituição de mecanismos de controle interno necessários ao monitoramento e à avaliação do sistema, assegurando a eficácia e contribuindo para a melhoria do desempenho organizacional;

CONSIDERANDO que a gestão de riscos permite tratar com eficiência as incertezas, seja pelo melhor aproveitamento das oportunidades, seja pela redução da probabilidade ou do impacto de eventos negativos, a fim de melhorar a capacidade de gerar valor e fornecer garantia razoável ao cumprimento dos seus objetivos;

CONSIDERANDO as recomendações das melhores práticas internacionais que tratam da gestão de riscos corporativos, como o *Committee of Sponsoring Organizations of the Treadway Commission/ Enterprise Risk Management - Integrated Framework* (Coso/ERM) e a Norma Técnica ABNT NBR ISO 31000:2009 Gestão de riscos – Princípios e Diretrizes.

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º - Instituir a Política de Gestão de Riscos do Conselho Regional de Medicina do Estado do Tocantins – CRM/TO.

Art. 2º A Política de Gestão de Riscos (PGR) do CRM/TO tem por finalidade estabelecer os princípios e as diretrizes para o tratamento dos riscos, contribuindo para o alcance dos objetivos estratégicos da instituição.

Art. 3º A Política de Gestão de Riscos do CRM/TO tem por objetivo assegurar aos gestores o acesso tempestivo a informações referentes aos riscos aos quais a instituição está exposta, melhorando o processo de tomada de decisão e ampliando a possibilidade do alcance dos objetivos estratégicos expressos no Planejamento Estratégico Institucional (PEI) e no Plano de Desenvolvimento Institucional (PDI) esse quando houver.

Art. 4º Esta política aplica-se a todas os Setores e Delegacias do CRM/TO, na gestão dos riscos que impactam seu ambiente. Parágrafo único. Na implantação do Plano de Gestão de Riscos e de suas sucessivas revisões, serão adotadas abordagens incrementais com a definição gradativa dos objetivos e processos associados: começando pelos riscos vinculados aos objetivos estratégicos, depois pelos riscos dos processos institucionais, até que toda a instituição esteja integrada à gestão de riscos.

Art. 5º Para efeitos desta Política, entende-se por:

I - accountability: conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações;

II - apetite a risco: nível de risco que o CRM/TO está disposta a aceitar;

III - auditoria interna: atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia a organização a realizar seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, de controlesinternos, de integridade e de governança. As auditorias internas no âmbito da Administração Pública se constituem na terceira linha ou camada de defesa das organizações, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa, executada por todos os níveis de gestão dentro da organização) e da supervisão dos controles internos (segunda linha ou camada de defesa, executada por instâncias específicas, como comitês de risco e controles internos). Compete às auditorias internas oferecer avaliações e assessoramento às organizações públicas, destinadas ao aprimoramento dos controles internos, de forma que controles mais eficientes e eficazes mitiguem os principais riscos de que os órgãos e entidades não alcancem seus objetivos;

IV - atividade: trata-se de uma parte do processo caracterizada pelos seguintes .. elementos: nome, descrição, diagrama de fluxo de tarefas, tarefas e respectivos responsáveis, condição para ser realizada, informações utilizadas, informações produzidas, condição para ser finalizada, e templates e exemplos;

V - componentes dos controles internos da gestão: são o ambiente de controle interno da entidade, a avaliação de risco, as atividades de controles internos, a informação e comunicação e o monitoramento;

VI - 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 servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os

seguintes objetivos gerais serão alcançados:

a) execução ordenada, ética, econômica, eficiente e eficaz das operações;

b) cumprimento das obrigações de accountability;

c) cumprimento das leis e regulamentos aplicáveis; e

d) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica.

VII - efeito: desvio positivo e/ou negativo em relação ao resultado esperado;

VIII - estrutura da gestão de riscos: conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria continua da gestão de riscos no CRM/TO;

IX - evento: ocorrência ou mudança em um conjunto específico de circunstâncias;

X - fraude: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência ou de força física;

XI - gerenciamento de riscos: processo para identificar, avaliar e controlar potenciais situações para fornecer razoável certeza quanto ao alcance dos objetivos das Unidades do CRM/TO;

XII - gestor de processos: responsável pelo gerenciamento de processos inerentes aos objetivos das Unidades do CRM/TO;

XIII - gestão de riscos: atividades para dirigir e controlar o CRM/TO no que se refere a riscos;

XIV - gestor de riscos: responsável por garantir, por meio da aplicação de controles internos de gestão eficiente, que determinado risco esteja de acordo com o nível previamente definido;

XV - governança: compreende mecanismos de liderança, estratégia e controle para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

XVI - governança no setor público: compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

XVII - impacto ou consequência: resultado de um evento que afeta os objetivos do processo ou das Unidades do CRM/TO;

XVIII - incerteza: estado, mesmo que parcial, da deficiência das informações relacionadas a um evento: compreensão, conhecimento, consequência ou probabilidade;

XIX - linhas de defesa da gestão para o gerenciamento de riscos: modelo que contempla a segregação de responsabilidades e papéis dos envolvidos na gestão de riscos em três linhas conceituais: a) primeira linha de defesa: refere-se à gestão operacional, ou seja, aos gestores de processos, responsáveis por colocar em prática os controles internos da gestão; b) segunda linha de defesa: exerce funções de gerenciamento de riscos por meio da definição e do monitoramento dos controles

internos da gestão; e c) terceira linha de defesa: é responsável por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa, executada por todos os níveis de gestão dentro da organização) e da supervisão dos controles internos (segunda linha ou camada de defesa, executada por instâncias específicas, como comitês de risco e controles internos).

XX - mensuração de risco: significa estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência;

XXI - monitoramento: verificação, supervisão, observação crítica ou identificação da situação, executadas de forma continua, a fim de identificar mudanças no nível de desempenho requerido ou esperado da estrutura da gestão de riscos, do processo de gestão de riscos, dos riscos ou dos controles internos da gestão;

XXII - objetivo organizacional: situação que se deseja alcançar de forma a evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro;

XXIII - Política de Gestão de Riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos;

XXIV - probabilidade: frequência de ocorrência de um evento, a partir de séries históricas e/ou na percepção dos gestores;

XXV - processo: conjunto de ações e atividades inter-relacionadas que são executadas para alcançar produto, resultado ou serviço predefinido;

XXVI - processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e atividades de identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos;

XXVII - representantes da alta administração: responsáveis por prover os recursos necessários à gestão de riscos, identificar papéis e responsabilidades, iniciar as atividades e gestão de riscos, e aprovar pontos importantes relativos à gestão de riscos;

XXVIII - responsáveis por Unidades (ou responsáveis técnicos): responsáveis pelas áreas da organização nas quais a metodologia de gestão de riscos será implementada, ou aqueles que devem prover informações para a gestão de riscos. Têm o papel de coletar as informações necessárias à identificação e à estimação de riscos e realizar melhorias necessárias, quando as análises indicarem essa necessidade;

XXIX - risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;

XXX - risco-chave: risco que, em função do impacto potencial ao CRM/TO, deve ser conhecido pela alta administração;

XXXI - risco externo: risco associado ao ambiente no qual a organização opera. Em geral, a organização não tem controle direto sobre esse evento, mas, mesmo assim, ações podem ser tomadas quando necessário;

XXXII - risco interno: risco associado à própria estrutura da organização, seus processos, governança, quadro de pessoal, recursos ou ambiente de tecnologia;

XXXIII - risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

XXXIV - risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

XXXV - Sistema de Controle Interno do Poder Executivo Federal:

compreende as atividades de avaliação do cumprimento das metas previstas no plano plurianual, da execução dos programas de governo e dos orçamentos da União e de avaliação da gestão dos administradores públicos federais, utilizando como instrumentos a auditoria e a fiscalização, e tendo como órgão central a Controladoria-Geral da União. Não se confunde com os controles internos da gestão, de responsabilidade de cada órgão e entidade do Poder Executivo Federal;

XXXVI - subprocessos: definem conjuntos de atividades, estruturadas para que sejam atingidos os objetivos parciais específicos relacionados à gestão de riscos; e

XXXVII - tipologias de risco: classificação dos tipos de riscos que podem afetar o alcance dos objetivos estratégicos das Unidades do CRM/TO.

CAPÍTULO II

DOS OBJETIVOS, DOS PRINCÍPIOS E DAS DIRETRIZES DA POLÍTICA DE GESTÃO DE RISCO

Art. 6º Para a execução desta política, deverão ser considerados os objetivos, os princípios e as diretrizes do CRM/TO, estabelecidos em seu Estatuto e Regimento Interno, bem como o planejamento estratégico, missão e visão de futuro, estabelecidos no PEI e no PDI da instituição, esse quando houver.

Parágrafo único. A gestão de riscos do CRM/TO observará, em consonância com sua missão, visão de futuro, objetivos e diretrizes estratégicas, os seguintes princípios:

I - proteção e agregação de valor à gestão;

II - integração dos processos organizacionais;

III - subsídios a tomada de decisões;

IV - abordagem de forma explícita da incerteza;

V - gestão sistemática, estruturada e oportuna, subordinada ao interesse público;

VI - estabelecimento de níveis de exposição a riscos adequados;

VII - estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização;

VIII - utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico;

IX - apoio à melhoria continua dos processos organizacionais;

X - utilização de informações tempestivas, suficientes e confiáveis;

XI - aplicação de fatores humanos e culturais;

XII gestão transparente e inclusiva;

XIII - gestão dinâmica e capaz de reagir a mudanças; e

XIV - promoção da melhoria continua do CRM/TO.

Art. 7º A gestão de riscos do CRM/TO tem como objetivos:

I - prover razoável garantia de atingimento dos objetivos institucionais;

II - encorajar a gestão proativa;

III - atentar para a necessidade de identificação e tratamento de riscos em todo CRM/TO;

IV - melhorar a identificação de oportunidades e ameaças;

V - melhorar o fluxo de informações tempestivas, suficientes e confiáveis;

VI - melhorar a governança e promover a integridade pública;

VII - prover confiança para a tomada de decisão dos gestores;

VIII - melhorar os controles internos da gestão;

IX - alocar e utilizar eficazmente os recursos para o tratamento de riscos;

X melhorar a eficácia e a eficiência operacionais;

XI - melhorar a prevenção de perdas e a gestão de incidentes;

XII - assegurar que os responsáveis pela tomada de decisão, em todos os níveis do CRM/TO, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso;

XIII - aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis;

XIV - agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos bem como dos impactos negativos decorrentes de sua materialização;

XV - melhorar a aprendizagem organizacional; e

XVI aumentar a capacidade de adaptação a mudanças.

Art. 8º A gestão de riscos do CRM/TO tem como diretrizes:

I - a gestão de riscos será integrada ao planejamento estratégico estabelecido no PEI e no PDI, esse quando houver, em consonância com os processos do CRM-TO;

II - os riscos serão divididos em riscos estratégicos e riscos de processos organizacionais, classificados conforme a tipologia a seguir:

a) riscos estratégicos: são aqueles cuja ocorrência interfere diretamente na consecução dos objetivos estratégicos ou de planos/metas descritos no PEI e no PDI do CRM/TO;

b) riscos operacionais: têm origem nos processos internos e rotineiros do CRM/TO. Estão diretamente conectados com os servidores que executam a função, são mais fáceis de serem detectados e atenuados. Também podem estar relacionados a casos fortuitos;

c) riscos financeiros/orçamentários: são aqueles relacionados à disponibilidade (ou à falta)de recursos para a consecução dos objetivos do CRM/TO;

d) riscos de comunicação/imagem/reputação: são aqueles relacionados à confiabilidade e consistência das informações disponibilizadas ao público interno e externo e aos eventos que possam comprometer a confiança da sociedade em relação à capacidade do CRM/TO em cumprir sua missão institucional;

e) riscos de integridade: são aqueles oriundos de ações relativas à alta administração que refletem negativamente na imagem do Conselho perante a sociedade;

f) riscos legais/de conformidade: são aqueles relacionados ao

descumprimento de uma exigência legal/regulamentar do CRM/TO, ou recomendações dos controles interno e externo; e

g) riscos ambientais: resultam da associação entre os riscos naturais e os riscos decorrentes de processos naturais agravados pela atividade humana e pela ocupação do território.

III - a identificação dos riscos deverá ser realizada a partir do mapeamento dos processos.

IV - a análise e avaliação dos riscos deverá seguir a seguinte metodologia:

a) abordagem qualitativa e quantitativa de avaliação dos riscos, baseada na probabilidade e no impacto da sua ocorrência;

b) a probabilidade de ocorrência será definida a partir de categorias, em razão de suas especificidades e de sua complexidade;

c) o impacto será analisado e considerado sob as seguintes perspectivas:

1. impacto financeiro/orçamentário;

2. impacto temporal;

3. impacto social; e

4. outros impactos pertinentes ao evento de risco analisado.

V - definição de indicadores que permitam a análise do desempenho da gestão de riscos, tendo como base o número de riscos previstos, mapeados e ocorridos, a eficácia das medidas de tratamento e monitoramento adotadas, entre outras;

VI - definição dos responsáveis diretos por cada risco, com competência de implantar as medidas de tratamento e monitoramento e obrigação de se reportar diretamente ao Comitê de Governança, Integridade, Riscos e Controles (CGIRC) bem como ao seu gestor;

VII - política de capacitação institucional, com foco no desenvolvimento de formações específicas em gestão de riscos voltadas para todos os atores envolvidos;

VIII - atualização sistemática por meio de monitoramento que promova, em períodos previamente determinados, revisão de hierarquização e priorização de processos e a respectiva identificação, análise, avaliação, hierarquização, priorização, tratamento e monitoramento dos riscos.

CAPÍTULO III

DOS MACROPROCESSOS, PROCESSOS E SUBPROCESSOS DA POLÍTICA DE GESTÃO DE RISCO

Art. 9 A identificação dos macroprocessos, processos e subprocessos deverá ser realizada considerando a competência institucional de cada setor do CRM/TO, e os riscos identificados deverão ser atribuídos a um servidor ou setor (proprietário de risco), que serão designados e supervisionados pelo gestor do risco.

Art. 10 A operacionalização da Gestão de Riscos deverá contemplar, no mínimo, as seguintes etapas:

I - estabelecimento do contexto: consiste na definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos e

estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos;

II - identificação dos riscos: etapa que compreende o reconhecimento abrangente dos riscos aos quais a instituição está exposta;

III - análise dos riscos: etapa que se refere à identificação das possíveis causas e consequências dos riscos;

IV - avaliação dos riscos: etapa que se refere à estimativa dos níveis dos riscos identificados bem como dos resultados obtidos com a adoção de estratégias de mitigação dos riscos;

V - tratamento dos riscos: etapa na qual se identificam as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido, além da escolha das medidas de controle associadas a essas respostas;

VI - comunicação e monitoramento: etapa que ocorre durante todo o processo de gerenciamento de riscos, responsável pela integração de todas as instâncias envolvidas bem como pelo monitoramento continuo da própria Gestão de Riscos, com vistas a sua melhoria.

Parágrafo único. O tratamento e o monitoramento dos riscos devem ser contínuos e realizados anualmente, por meio de identificação, análise, avaliação e priorização.

Art. 11 A priorização dos processos no gerenciamento de riscos será determinada pelo "grau de cada risco", com base em uma matriz dada pela combinação do impacto e da probabilidade de ocorrência do risco.

§ 1° Probabilidade da ocorrência do risco identificado: corresponde ao nível de probabilidade de que as ameaças se concretizem e provoquem danos na instituição, em seus ativos ou pessoas, sendo classificada para efeitos desta política, de acordo com seus aspectos .. históricos, estruturais e conjunturais, como:

I peso 1 - probabilidade muito baixa: somente pode ocorrer em circunstâncias excepcionais;

II peso 2 - probabilidade baixa: pode ocorrer sob certas circunstâncias, diferentes das atuais;

III peso 3 - probabilidade média: pode ocorrer nas circunstâncias atuais;

IV peso 4 - probabilidade alta: deve ocorrer em algum momento, pois as circunstâncias corroboram; e

V peso 5 - probabilidade muito alta: é quase certo que ocorra, uma vez que as circunstâncias corroboram e há sinais que apontam uma tendência.

§ 2° Impacto: avalia o impacto do risco no alcance dos objetivos institucionais, sendo classificado para efeito desta política como:

I peso 1 - impacto muito baixo: quando ocorrer, causará impactos mínimos;

II peso 2 - impacto baixo: quando ocorrer, causará impactos pequenos;

III peso 3 - impacto médio: quando ocorrer, causará impactos significativos, porém recuperáveis;

IV - peso 4 - impacto alto: quando ocorrer, causará impactos de reversão muito difícil; e

V peso 5 - impacto extremo: quando ocorrer, causará impactos irreversíveis.

§ 3° As classes de probabilidade e impacto, bem como seus descritivos, poderão ser reavaliadas, a qualquer momento, pelo Comitê de Governança,

Integridade, Riscos e Controles do CRM/TO.

Art. 12 A partir da multiplicação entre as classes de probabilidade e impacto de cada risco, é possível classificar o "grau de risco" de cada processo mapeado, de acordo com as matrizes de classificação de riscos constante no Anexo I.

Art. 13 Em conformidade com a matriz de classificação dos riscos, será definida a estratégia de tratamento para cada grau de risco, de acordo com a classificação abaixo:

I - muito baixo e baixo - Estratégia de aceitar: neste caso, deve-se conviver com o evento de risco, mantendo os procedimentos e práticas atualmente adotados. O risco é considerado baixo e não será necessário nenhuma ação imediata, porém deve ser monitorado;

II - médio - Estratégia de reduzir ou compartilhar: medidas para reduzir a probabilidade ou o impacto do risco devem ser adotadas como, por exemplo, o compartilhamento do risco ou parte dele. É aconselhável que o risco seja tratado em médio prazo e que seja monitorado frequentemente. As restrições (como custo e esforço de tratamento) podem ser consideradas na priorização do tratamento de riscos dessa classe; e

III - alto e extremo - Estratégia para evitar: o risco é considerado extremo e requer grande preocupação. Ações imediatas devem ser implementadas para gerenciar o risco e limitar a exposição da instituição, e os resultados devem ser monitorados, frequentemente, para avaliar a efetividade das ações.

Art. 14 O Comitê de Governança, Integridade, Riscos e Controles do CRM/TO é o responsável pela aplicação e revisão desta política, e suas competências estão definidas na Portaria CRM/TO nº19, de 18 de abril de 2022.

CAPÍTULO IV

DOS AGENTES ENVOLVIDOS E DE SUAS RESPONSABILIDADES

Art. 15 Para a efetivação da gestão de riscos no âmbito da instituição, ficam estabelecidas as responsabilidades dos diversos agentes envolvidos:

I - Plenário:

a) Homologar a Política de Gestão de Riscos e suas alterações e o Plano de Gestão de Riscos.

II - Diretoria

a) Aprovar a Política e o Plano de Gestão de Riscos, e suas alterações, e a indicação dos gestores dos riscos; avaliar e aprovar a priorização dos riscos.

III - Presidente:

a) garantir a continuidade e aperfeiçoamento da Política de Gestão de Riscos.

IV - Comitê de Governança, Integridade, Riscos e Controles (CGIRC):

a) analisar, avaliar, aprovar e acompanhar o Plano de Gestão de Riscos;

b) promover práticas e princípios de conduta e padrões de comportamentos;

c) institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos;

d) promover o desenvolvimento continuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de riscos e de controles internos;

e) garantir a aderência a regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;

f) promover a integração dos agentes responsáveis pela governança, integridade, gestão de riscos e pelos controles internos;

g) promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, transparência e efetividade das informações;

h) aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;

i) supervisionar o mapeamento e avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público;

j) liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no CRM/TO;

k) estabelecer limites de exposição a riscos globais do CRM/TO bem como os limites de alçada ao nível de unidade, política pública, ou atividade;

l) aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão; e m)emitir recomendação para o aprimoramento da governança, da integridade, da gestão de riscos e dos controles internos.

V- Comitê Assessor de Governança, Integridade, Riscos e Controles (CAGIRC) (quando instituído):

a) propor ao CGIRC do CRM/TO:

1. revisão da política de gestão de riscos;

2. definição de limites de exposição aos riscos identificados;

3. relação dos riscos-chave;

4. políticas, diretrizes, metodologias e mecanismos para comunicação; e

5. institucionalização da gestão de riscos e dos controles internos da gestão.

b) supervisionar, orientar e monitorar a hierarquização e priorização de processos bem como a identificação, análise, avaliação, hierarquização, priorização, tratamento e monitoramento dosriscos no CRM/TO;

c) definir apetite aos riscos não considerados chave;

d) consolidar e manter controle atualizado referente aos processos hierarquizados e priorizados e aos riscos identificados, analisados, avaliados, hierarquizados, priorizados, tratados e monitorados;

e) opinar sobre a alocação dos recursos orçamentários destinados a Tecnologias da Informação e Comunicação (TIC) bem como sobre alterações posteriores que provoquem impacto significativo sobre a alocação inicial;

f) assessorar na implementação das ações de segurança da informação e comunicação;

g) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicação;

h) propor alterações na Política de Segurança da Informação e Comunicação;

i) propor normas relativas à segurança da informação e comunicação;

j) propor políticas e normas relativas à governança de TIC;

k) identificar e disseminar boas práticas de gestão de riscos a todas as Unidades do CRM/TO;

l) incentivar a capacitação continua de todos os agentes públicos das Unidades do CRM/TO; e

m)garantir que os gestores de processos e de riscos e os demais envolvidos, direta ou indiretamente, na gestão de riscos cumpram e observem a política aprovada pelo CGIRC do CRM/TO.

VI – Coordenadores, Chefes de Departamentos/Setores do CRM/TO:

a) promover o planejamento de atividades sistematizadas, apoiando estudos, projetos e programas para o desenvolvimento institucional;

b) propor políticas e normas de planejamento, de desenvolvimento e das relações institucionais;

c) coordenar a elaboração, execução e monitoramento da gestão de riscos e do plano de integridade institucional, em consonância com os instrumentos legais e com as políticas institucionais do Comitê de Governança, Integridade, Riscos e Controles;

d) propor a melhoria continua dos processos e fluxos, resultantes de propostas institucionais e de grupos de trabalho; e

e) monitorar e publicar no portal do CRM/TO a execução do Plano de Gestão de Riscos e do Plano de Integridade em nível institucional.

f) fundamentar a implantação da Gestão de Riscos por meio do mapeamento de processos;

g) disseminar o conhecimento sobre gestão por processos e o conhecimento institucional, contribuindo para a gestão do conhecimento e otimizando a capacitação dos servidores na área; e

h) elaborar proposta de capacitação para os responsáveis pela gestão de riscos: gestores e proprietários de riscos.

VII- Gestor de Risco:

a) assegurar que o risco seja gerenciado de acordo com a PGR;

b) monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na redução das chances de ocorrência ou na manutenção do risco em níveis adequados, de acordo com a PGR;

c) garantir que as informações adequadas sobre os riscos da sua área de gestão estejam disponíveis em todos os níveis da Instituição;

d) elaborar e assegurar a implementação do plano de ação (respostas aos riscos) definido para tratamento dos riscos sob sua responsabilidade;

e) operacionalizar as respostas aos riscos;

f) identificar e comunicar situações de riscos, quando pertinentes; e

g) primar pela inovação e adoção de boas práticas à gestão.

VIII - Proprietário de Risco:

a) contribuir nas atividades de identificação, análise e avaliação dos riscos inerentes aos processos sob sua responsabilidade;

b) comunicar tempestivamente ao Gestor de Risco riscos inerentes aos processos sob sua responsabilidade;

c) executar os planos de tratamento e respostas aos riscos;

d) participar das oficinas promovidas pela instituição sobre Gestão de Risco; e

e) praticar outros atos de natureza técnica e/ou administrativa necessários ao exercício de suas responsabilidades.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

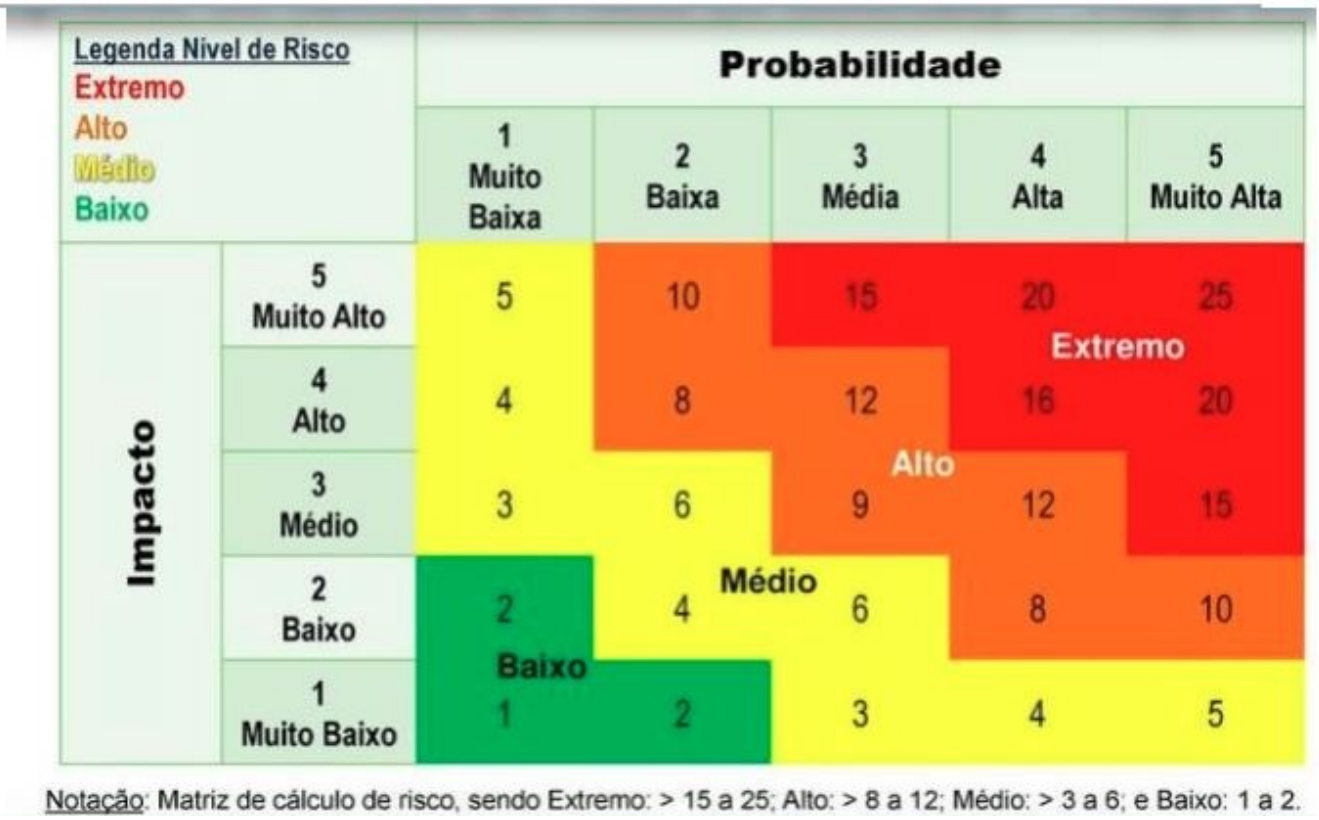
Art. 16 Os casos omissos ou as excepcionalidades serão resolvidos pelo CGIRC do CRM/TO.

Art. 17 Esta Instrução Normativa entra em vigor na data de sua publicação.

Palmas/TO, 03 de Março de 2023.

Dr. Jorge Pereira Guardiola
Presidente do CRM-TO

ANEXO I
MATRIZ DE CLASSIFICAÇÃO DE RISCOS



Notação: Matriz de cálculo de risco, sendo Extremo: > 15 a 25; Alto: > 8 a 12; Médio: > 3 a 6; e Baixo: 1 a 2.

Documento assinado eletronicamente por **Jorge Pereira Guardiola**, **Presidente**, em 07/03/2023, às 14:53, com fundamento no art. 5º da RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022.

A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0102922** e o código CRC **8B785534**.

ACSV 71 (704 Sul), Av. LO 15, Lote 18, 1° piso - Bairro Plano Diretor Sul | CEP 77022-322 | Palmas/TO - http://www.crmto.org.br/