



POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS



GOVERNO DO ESTADO
DO ESPÍRITO SANTO
Secretaria da Saúde



SUMÁRIO

1 Finalidade.....	3
2 Abrangência	4
3 Regulação.....	4
4 Definições Técnicas.....	4
5 Princípios.....	5
6 Responsabilidades.....	5
7 Etapas da Gestão De Riscos	8
8 Metodologia e Condução da Gestão de Riscos.....	8
9 Desenvolvimento das etapas da Gestão de Riscos	9
10 Sanções e Penalidades	13
11 Disposições Finais	13
12 Referências.....	144

POLÍTICA	
Título: Política de Gestão de Riscos Corporativos	Código: POL.017
	Revisão: 00

POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS

APROVAÇÃO PERANTE O CONSELHO CURADOR

A presente Política foi aprovada pelo Conselho Curador da Fundação Estadual de Inovação em Saúde - iNOVA Capixaba, em 22/09/2026 – ata da 5ª Reunião do Conselho Curador – em sessão Extraordinária.

1 FINALIDADE

Esta Política de Gestão de Riscos Corporativos define objetivos, princípios e diretrizes para as ações de gestão de riscos da Fundação iNOVA Capixaba, visando apresentar a estrutura de gerenciamento de riscos, definindo a metodologia e o processo de gestão de riscos, incorporando a visão de riscos à tomada de decisões gerenciais e estratégicas.

A Política de Gestão de Riscos Corporativos da iNOVA Capixaba é um dos mecanismos de promoção da integridade e, por meio dela, visa-se implementar rotinas e procedimentos para prevenir, detectar e remediar a ocorrência de riscos e desvios éticos.

Como objetivos específicos, esta Política institui:

- I. Aumentar a probabilidade de atingimento dos objetivos estratégicos e operacionais traçados, a fim de se garantir a prevalência do interesse da população na excelência da prestação de serviços de saúde, de forma digna, célere, humana, altruísta, qualificada e eficiente;
- II. Disseminar a cultura de gerenciamento de riscos a todo o corpo funcional da Fundação;
- III. Dar suporte à missão, à continuidade e à sustentabilidade institucional, pela garantia razoável de atingimento dos objetivos estratégicos;
- IV. Possibilitar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais a iNOVA está exposta, inclusive para determinar questões relativas à delegação, se for o caso;
- V. Agregar valor por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização;
- VI. Buscar a criação de suportes tecnológicos da informação para apoiar os processos de integridade, riscos e acompanhar a implementação dos controles internos da gestão;
- VII. Facilitar a identificação de oportunidades e ameaças;
- VIII. Prezar pela conformidade legal e normativa dos processos organizacionais;
- IX. Melhorar a governança e a gestão administrativa;
- X. Aprimorar os controles internos;
- XI. Alocar e utilizar de forma eficiente os recursos para o tratamento de riscos;
- XII. Aprimorar a alocação orçamentária;
- XIII. Melhorar a prevenção de perdas e a gestão de incidentes;
- XIV. Aumentar a capacidade da Fundação de se adaptar a mudanças.

2 ABRANGÊNCIA

A Política de Gestão de Riscos Corporativos aplica-se à Fundação Estadual de Inovação em Saúde - iNOVA Capixaba – em toda sua estrutura organizacional: hospital próprio, filiais, unidades gestoras, administrativas e assistenciais, escritórios, ou representações – aos gestores, empregados, colaboradores, servidores cedidos, prestadores de serviços e demais *stakeholders*.

3 REGULAÇÃO

A presente Política tem como principais referenciais legais:

ABNT NBR ISO 31000:2018;

Lei Federal nº 14.133/2021;

Lei Federal nº 12.846/2013;

Lei Federal nº 13.709/2018;

Lei Estadual nº 10.993/2019;

Lei Complementar Estadual nº 924/2019.

4 DEFINIÇÕES TÉCNICAS

Risco: efeito da incerteza sobre os objetivos da Fundação, decorrente de evento que, caso ocorra, pode dificultar ou impossibilitar o cumprimento desses objetivos (ameaça) ou favorecer seu atingimento (oportunidade);

Ameaças: eventos de risco que podem influenciar de forma negativa o atingimento dos objetivos da iNOVA Capixaba;

Apetite a risco: nível máximo de risco que a Fundação iNOVA Capixaba está disposta a aceitar no cumprimento de seus objetivos, considerando sua missão institucional, capacidade operacional, recursos disponíveis e obrigações legais, sendo definida pela Diretoria Executiva em documento específico de Declaração de Appetite ao Risco;

Gerenciamento de riscos: processo para detectar, avaliar, administrar e controlar potenciais eventos ou situações, no intuito de fornecer segurança para o alcance dos objetivos da iNOVA Capixaba;

Grupo de trabalho: grupo temporário constituído exclusivamente para conduzir o ciclo de gestão de riscos de processo transversal, na forma dos itens 8.2.1 e 8.3;

Nível de risco: representação da magnitude do risco na matriz elaborada;

Oportunidades: eventos que podem influenciar de forma positiva o atingimento dos objetivos da Fundação;

Resposta ao risco: é a definição da estratégia com maior probabilidade de eficácia para cada risco;

Risco inerente: risco a que Fundação está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

Risco residual: risco remanescente a que a Fundação está exposta considerando os controles para o tratamento de risco inerente;

Matriz de Riscos: consiste na definição dos riscos em função da combinação das escalas de probabilidade e de impacto.

Processo transversal: processo cuja execução percorre etapas sob responsabilidade de mais de uma área, de modo que nenhum gestor detenha autoridade sobre a totalidade de suas etapas e controles;

Probabilidade: é a chance de o evento ocorrer, em distintos graus de intensidade, podendo ser mensurado de forma qualitativa ou quantitativa;

Impacto: é o resultado de um evento que afeta o objetivo ou resultado, podendo ser mensurado de forma quantitativa ou qualitativa;

Stakeholders: são as partes interessadas que podem ser afetadas por ações, projetos, processos e práticas de governança corporativa executadas pela Fundação, como, por exemplo, gestores, empregados, fornecedores e governo.

5 PRINCÍPIOS

Os princípios básicos da Política de Gestão de Riscos Corporativos são:

- Proteção do ambiente corporativo;
- Melhoria contínua da organização;
- Visão sistêmica;
- Transparência.

6 RESPONSABILIDADES

6.1 A gestão de riscos corporativos é uma função estratégica e transversal, cuja efetividade depende da atuação integrada de diferentes níveis da estrutura organizacional. Cada instância da Fundação possui responsabilidades específicas no processo de gestão de riscos, que vão desde a definição de diretrizes e alocação de recursos até a identificação, avaliação e tratamento dos riscos. Essa divisão de competências visa assegurar que os riscos sejam tratados de forma proativa, sistemática e alinhada aos objetivos institucionais, promovendo a integridade, a eficiência e a sustentabilidade das atividades desenvolvidas. Desse modo, no âmbito da Fundação iNOVA Capixaba, compete:

Conselho Curador – Compete ao Conselho Curador aprovar a Política de Gestão de Riscos Corporativos, bem como suas eventuais revisões e promover a integração das práticas de gestão de riscos e controles internos ao processo decisório;

Diretoria Executiva – Cabe à Diretoria Executiva assegurar a alocação dos recursos necessários à mitigação dos riscos identificados, além de estabelecer o apetite ao risco da Fundação;

Unidade de Gestão de Riscos – Responsável por coordenar a aplicação da metodologia de gestão de riscos, consolidar as informações recebidas e reportar os riscos classificados como críticos;

Gestores das Áreas – Compete aos gestores identificar, avaliar, tratar, revisar e monitorar os riscos inerentes às suas respectivas áreas de atuação, selecionar os processos de trabalho que serão objeto do ciclo de gestão de riscos, designar os responsáveis por cada risco e por cada controle, elaborar o Plano de Ação e monitorar sua execução até a finalização, observado, nos processos transversais, o disposto no item 6.13;

Todos os Colaboradores – Todos os colaboradores devem comunicar os riscos identificados ou potenciais e adotar práticas alinhadas aos princípios de boa governança.

6.2 A comunicação dos riscos deverá ocorrer de forma estruturada e tempestiva, por meio de relatórios de riscos elaborados pelos gestores das áreas e encaminhados à Unidade de Gestão de Riscos, contendo, no mínimo, os riscos classificados como muito alto, seus responsáveis, níveis de risco inerente e residual e o plano de ação. Nos processos transversais, o relatório será encaminhado pelo gestor coordenador do grupo de trabalho, com ciência dos gestores das demais áreas envolvidas.

6.3 Para coordenar os papéis e responsabilidades dos atores envolvidos na gestão de riscos, é apresentada a estrutura de três linhas, conforme preconizado pelo *The Institute of Internal Auditors (IIA)*.

6.4 O modelo das Três Linhas é uma referência internacionalmente adotada para estruturar as funções de governança, controle e auditoria dentro de uma organização, assegurando clareza nas responsabilidades relacionadas à gestão de riscos, controles internos e conformidade.

6.5 A Fundação INOVA Capixaba adota esse modelo como princípio orientador da sua estrutura de governança, garantindo que os riscos sejam gerenciados de forma coordenada e eficaz em todos os níveis da instituição.

6.6 Primeira Linha: áreas operacionais e assistenciais da Fundação, responsáveis diretamente pela execução das atividades, identificação e gestão de riscos em seus processos. Os gestores e equipes operacionais são incumbidos de:

- Realizar o mapeamento dos riscos inerentes aos seus processos;
- Implementar e manter controles internos operacionais;
- Monitorar indicadores de risco e desempenho;
- Comunicar tempestivamente qualquer situação que represente ameaça aos objetivos da Fundação.

6.7 Segunda Linha: representada pela Unidade de Gestão de Riscos, essa linha atua como articuladora do processo, apoiando os gestores na elaboração dos planos de ação e validação das matrizes de riscos. Tem como funções:

- Estabelecer metodologias de gestão de riscos;
- Consolidar e analisar os riscos reportados pela primeira linha;
- Promover apoio técnico, treinamentos, capacitações e disseminação da cultura de gestão de riscos;
- Apoiar a tomada de decisão estratégica com base em relatórios de riscos.

No tocante aos riscos assistenciais, o Núcleo de Segurança do Paciente (NSP) exerce função equiparada à segunda linha, atuando como instância técnica especializada na identificação, análise e tratamento desses riscos segundo a Política de Segurança do Paciente e a Política de Gestão de Riscos Assistenciais.

6.8 Terceira Linha: composta pela área de Controladoria e Integridade, subordinada diretamente ao Conselho Curador, essa linha é responsável por fornecer avaliação independente da eficácia da gestão de riscos, dos controles internos e da governança institucional. Ao fazê-lo, pode considerar a avaliação de outros prestadores internos e externos.

Suas atribuições incluem:

- Emitir recomendações para o aprimoramento de processos e controles;
- Realizar auditorias programadas e especiais;
- Verificar a efetividade das ações corretivas adotadas;
- Apoio aos órgãos de controle interno e externo.

6.9 A efetividade do modelo depende da colaboração contínua entre as três linhas, com comunicação fluida, compartilhamento de informações e atuação coordenada. O respeito a esse modelo fortalece a governança institucional, minimiza a ocorrência de falhas sistêmicas e assegura que os riscos sejam tratados de forma proativa e consistente.

6.10 Os achados oriundos de auditorias e fiscalizações externas deverão ser analisados pela área de Controladoria e Integridade e, quando aplicável, incorporados às matrizes de riscos e aos planos de ação.

6.11 Para fins de governança corporativa de riscos e sem prejuízo da metodologia assistencial aplicável, os riscos assistenciais classificados em seu maior nível de criticidade pelas metodologias das Políticas de Segurança do Paciente e de Gestão de Riscos Assistenciais deverão ser informados pelo NSP à Unidade de Gestão de Riscos.

6.12 A integração de que trata o item 6.11 não transfere à Unidade de Gestão de Riscos a coordenação operacional da gestão de riscos assistenciais, que permanece com as estruturas definidas na Política de Segurança do Paciente e na Política de Gestão de Riscos Assistenciais.

6.13 Nos processos transversais, a condução do ciclo de gestão de riscos cabe à grupo de trabalho, constituído na forma dos itens 8.2.1 e 8.3, ao qual competem a identificação, a análise e a avaliação dos riscos das etapas abrangidas e a proposição do respectivo tratamento.

6.13.1 Ao gestor indicado para coordenar o grupo de trabalho compete selecionar as etapas objeto do ciclo, coordenar e monitorar as atividades do grupo, observar a periodicidade das reuniões, subsidiá-lo com as informações relevantes, encaminhar o relatório de que trata o item 6.2 e monitorar a execução do Plano de Ação até sua finalização.

6.13.2 A matriz de riscos e o Plano de Ação propostos pelo grupo de trabalho serão aprovados conjuntamente pelos gestores das áreas envolvidas, ficando cada um deles responsável pelos riscos e pelos controles das etapas sob sua autoridade.

6.13.3 O encerramento das atividades do grupo de trabalho não transfere essa responsabilidade, que permanece com os gestores das áreas envolvidas. Nos ciclos subsequentes de que trata o item 9.17, o grupo de trabalho será novamente constituído.

6.13.4 A Unidade de Gestão de Riscos presta apoio metodológico ao grupo de trabalho, sem participação na decisão quanto à resposta ao risco.

7 ETAPAS DA GESTÃO DE RISCOS

7.1 Sem prejuízo da utilização de outros documentos técnicos complementares, a INOVA Capixaba adotará o seguinte processo de gestão de riscos, baseado nas orientações da “Associação Brasileira de Normas Técnicas – NBR ISO 31000:2018, Gestão de Riscos: Diretrizes”:

- I. Estabelecimento do contexto: relacionado à definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, bem como à determinação do escopo e dos critérios de risco;
- II. Identificação dos riscos: consistente na busca, reconhecimento e descrição de riscos, mediante a identificação das fontes de risco, dos eventos, de suas causas e suas consequências potenciais;
- III. Classificação dos riscos: auxilia os gestores na organização dos riscos em grupos/categorias com propósitos específicos;
- IV. Análise e avaliação dos riscos: referente à compreensão da natureza do risco e à determinação do respectivo nível de risco mediante a combinação da probabilidade de sua ocorrência e dos impactos possíveis;
- V. Tratamento dos riscos: consistente na seleção e adoção de uma ou mais ações de tratamento para alterar os riscos;
- VI. Monitoramento e análise crítica: relacionados à verificação, supervisão, observação crítica ou identificação da situação de risco, realizadas de forma contínua, a fim de determinar a adequação, suficiência e eficácia dos controles internos para atingir os objetivos estabelecidos;
- VII. Comunicação e consulta: consistente na manutenção de fluxo regular e constante de informações com as partes interessadas, durante todas as fases do processo de gestão de riscos.

8 METODOLOGIA E CONDUÇÃO DA GESTÃO DE RISCOS

8.1 A aplicação da metodologia de gestão de riscos deverá observar o nível de complexidade, criticidade e maturidade dos processos, podendo ser adotadas abordagens simplificadas para processos de menor risco, sem prejuízo da aplicação integral da metodologia nos processos estratégicos e críticos.

8.2 A gestão de riscos será conduzida pelo gestor da área responsável pelo processo, a quem competem a identificação, a avaliação, o tratamento, a revisão e o monitoramento dos riscos, nos termos do item 6.

8.2.1 Constituir-se-á grupo de trabalho exclusivamente quando se tratar de processo transversal, hipótese em que a responsabilidade pelas etapas do ciclo não é atribuível a um único gestor.

8.2.2 Não caracteriza processo transversal, para os fins desta Política, o processo executado integralmente por uma área que apenas receba insumos ou preste informações a outras, permanecendo sob a autoridade de um único gestor a totalidade de suas etapas e controles.

8.3 O grupo de trabalho será constituído mediante proposta de qualquer dos gestores das áreas envolvidas ou da Unidade de Gestão de Riscos, por ato: (a) – do Diretor da área, quando o processo for da Sede Corporativa; (b) – do Diretor da área da unidade hospitalar, quando o processo for da unidade hospitalar, e observará:

I – a indicação, no ato de constituição, do gestor responsável por sua coordenação, escolhido entre os gestores das áreas envolvidas, preferencialmente o responsável pela etapa de maior criticidade do processo;

II – composição mínima: os gestores de todas as áreas envolvidas, ou seus representantes formalmente designados, e ao menos um empregado com atuação direta nas etapas avaliadas;

III – a delimitação expressa do processo e das etapas abrangidas e o prazo de conclusão dos trabalhos.

8.4 O grupo de trabalho registrará em ata as reuniões realizadas, as técnicas de identificação empregadas, os participantes e as conclusões alcançadas, e encerrará suas atividades com a entrega da matriz de riscos e da proposta de Plano de Ação aos gestores das áreas envolvidas, para aprovação na forma do item 6.13.2, e à Unidade de Gestão de Riscos, para consolidação corporativa.

8.4.1 As divergências entre os gestores das áreas envolvidas quanto à classificação do risco ou à resposta a ser adotada serão registradas em ata e submetidas à decisão do Diretor que constituiu o grupo de trabalho, podendo contar com apoio metodológico da Unidade de Gestão de Riscos, registrando-se na matriz de riscos a decisão adotada e as posições divergentes.

9 DESENVOLVIMENTO DAS ETAPAS DA GESTÃO DE RISCOS

9.1 Na etapa de identificação dos riscos, as causas são fontes de vulnerabilidades que viabilizam a concretização do evento de risco, por sua vez, as consequências são os impactos nos objetivos.

9.2 Para fins de identificação do risco, poderão ser adotados questionários, entrevistas com os empregados envolvidos no processo de trabalho selecionado, análise do mapeamento do fluxo de trabalho, *brainstorming*, *SWOT*, *PDCA*, *Diagrama de Ishikawa*, *5W2H*, *What if*, dentre outras técnicas.

9.3 Na fase de análise de riscos a cada evento de risco deve ser atribuído o grau de probabilidade e o grau de impacto.

9.4 O grau de probabilidade deverá variar das métricas “muito baixo” ao “muito alto”, a depender do histórico de ocorrência levantado por meio de documentos, entrevistas e relatos, histórico e recomendações de auditoria, por exemplo.

Probabilidade	Descrição da probabilidade, desconsiderando os controles	Grau
Muito baixo	Improvável. O evento poderá ocorrer, mas as circunstâncias não indicam essa possibilidade	1
Baixo	Raro. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade	2
Médio	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade	3
Alto	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade	4
Muito alto	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	5

Quadro 1: Escala de probabilidades
Fonte: Adaptado TCU (2018)

9.5 O grau de impacto deverá variar das métricas “muito baixo” ao “muito alto”, a depender da forma que os objetivos poderão ser afetados.

Impacto	Descrição do impacto, caso o evento ocorra	Grau
Muito baixo	Mínimo impacto nos objetivos	1
Baixo	Pequeno impacto nos objetivos	2
Médio	Moderado impacto nos objetivos, porém recuperável	3
Alto	Significativo impacto nos objetivos, de difícil reversão	4
Muito alto	Catastrófico impacto nos objetivos, de forma irreversível	5

Quadro 2: Escala de impacto
Fonte: Adaptado TCU (2018)

9.6 O NRI (Nível de Risco Inerente) advém do produto do grau de probabilidade pelo grau de impacto atribuído a cada evento de risco identificado, $NRI = GP \times GI$, onde GP corresponde ao grau de probabilidade e GI ao grau de impacto, variando seu resultado entre nível baixo, médio, alto e muito alto, como demonstrado na Figura 1 abaixo.

Nível baixo	Nível médio	Nível alto	Nível muito alto
1 a 4	5 a 9	10 a 19	20 ao 25

Figura 1: Valores do NRI

9.7 A combinação entre os graus de impacto e de probabilidade resultará na matriz de nível de risco, conforme Figura 2, por meio da qual se determinará o nível de risco do evento.

		MATRIZ DE RISCOS				
IMPACTO	MUITO ALTO	5	10	15	20	25
	ALTO	4	8	12	16	20
	MÉDIO	3	6	9	12	15
	BAIXO	2	4	6	8	10
	MUITO BAIXO	1	2	3	4	5
		MUITO BAIXO	BAIXO	MÉDIO	ALTO	MUITO ALTO
		PROBABILIDADE				

Figura 2: Matriz de nível de riscos

9.8 Em seguida, deve-se avaliar a eficácia dos controles internos existentes em relação aos processos, para avaliação do Risco Residual (RR), na forma do item 9.9.

Níveis de avaliação dos controles internos existentes		
Nível	Descrição	Fator de avaliação dos controles (FAC)
Inexistente	Controles inexistentes, mal desenhados ou mal implementados	1
Fraco	Controles tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente	0,4
Forte	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco	0,2

Quadro 3: Avaliação dos Controles Internos
Fonte: Adaptado TCU (2018)

9.8.1 A atribuição do FAC (Fator de Avaliação dos Controles) será acompanhada da identificação do controle avaliado, do responsável por sua execução e da evidência de seu desenho e de sua operação regular. Na ausência de evidência documental do desenho e da operação do controle, este será avaliado, no máximo, no nível "Fraco" (Fator 0,8), vedada sua classificação nos níveis "Mediano", "Satisfatório" ou "Forte".

9.9 Com essa avaliação, para cada risco identificado calcula-se o risco residual, que é representado pela multiplicação do Nível de Risco Inerente (NRI) e Fator de Avaliação dos Controles (FAC), conforme a fórmula: $RR = NRI \times FAC$.

9.9.1 Considerando que o FAC pode assumir valores fracionários, o Risco Residual poderá resultar em número não inteiro. Nessas hipóteses, para fins de enquadramento nas faixas de classificação da Figura 1, o valor será arredondado para o número inteiro imediatamente superior, adotando-se o critério conservador que privilegia a faixa de maior severidade.

9.10 O valor do risco residual pode fazer com que o risco se enquadre em uma faixa de classificação diferente da faixa definida para o risco inerente (Figura 1).

9.11 Os riscos serão identificados com base nas categorias a seguir:

- (i) Riscos Estratégicos: decisões que podem afetar negativamente o alcance dos objetivos da Fundação;
- (ii) Riscos de Conformidade: não cumprimento de princípios constitucionais, legislações específicas ou regulamentações externas aplicáveis, bem como normas e procedimentos internos;

- (iii) Riscos Operacionais: perdas resultadas por falhas, deficiências ou inadequação de processos internos, estrutura, pessoas, sistemas, tecnologia, assim como de eventos externos;
- (iv) Riscos de Reputação: comprometimento da confiança da sociedade em relação à capacidade da iNOVA Capixaba em cumprir sua missão institucional e interferência direta na imagem da Fundação;
- (v) Riscos de Comunicação: eventos que podem impedir ou dificultar a disponibilidade de informações para a tomada de decisões para o cumprimento das obrigações de prestação de contas às instâncias controladoras e à sociedade;
- (vi) Riscos de Integridade: desvios éticos e de conduta incongruentes com os padrões estabelecidos pelo iNOVA Capixaba;
- (vii) Riscos Orçamentários e Financeiros: comprometimento dos recursos orçamentários e financeiros necessários à realização das atividades da iNOVA Capixaba;
- (viii) Riscos Cibernéticos: possibilidade de que uma ameaça virtual possa explorar vulnerabilidades de ativos, impactando assim na confidencialidade, integridade e disponibilidade das informações;
- (ix) Riscos Ambientais: monitoramento de potenciais efeitos negativos causados pelas atividades hospitalares, tais como contaminação do solo, acidentes biológicos, não conformidades no tratamento de resíduos hospitalares, entre outros.

9.12 A identificação por categorias de riscos deverá auxiliar a definição do grau de impacto do evento de riscos e possível priorização em seu tratamento, como descrito na Figura 3 abaixo.

Nível de risco	Critérios para priorização e tratamento de riscos
Risco muito alto	Qualquer risco nesse nível deve ser comunicado à Direção e ter resposta imediata. Postergação de medidas só com autorização do Diretor-Geral
Risco alto	Qualquer risco nesse nível deve ser comunicado à Direção e ter uma resposta em um tempo determinado. Postergação de medidas apenas com autorização do Diretor de área
Risco médio	Geralmente nenhuma ação especial é necessária, porém requer atividades de monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais
Risco baixo	Não há necessidade de promover nenhuma ação.

Figura 3: Critérios de categorização de riscos

9.13 O tratamento dos riscos será feito mediante as seguintes respostas, a depender do apetite de risco definido e dos controles existentes:

- Evitar o risco, pela decisão de não iniciar ou descontinuar a atividade que dá origem a ele;
 - Acolher o risco, assumindo a exposição atual;
 - Mitigar o risco, minimizando o impacto e/ou probabilidade.
 - Compartilhar e/ou transferir o risco para terceiros, evitando exposição própria.

9.14 O gestor da área elaborará o 'Plano de Ação' para o tratamento dos riscos ou, nos processos transversais, o grupo de trabalho o proporá, aprovado na forma do item 6.13.2. O Plano de Ação conterá as razões que levaram à escolha de evitar, mitigar, compartilhar ou aceitar o evento de

risco, os responsáveis pela implementação do plano; as ações propostas; os recursos requeridos; medidas de desempenho e restrições; requisitos para a apresentação de informações e de monitoramento e cronograma.

9.15 O apetite a risco constituirá referência obrigatória para a classificação, priorização e tratamento dos riscos, devendo orientar a definição de respostas e a alocação de recursos.

9.16 A execução do Plano de Ação para o tratamento do risco pode gerar novos controles ou determinar a modificação dos controles existentes.

9.17 De modo geral, nos ciclos subsequentes do processo de gestão de riscos, a área deverá levar em consideração o nível de risco inerente apurado no primeiro ciclo e proceder à reavaliação dos controles para a mensuração do risco residual. A confrontação entre os níveis de riscos residuais de ciclos distintos tem por finalidade verificar se os controles estabelecidos nos Planos de Ação estão se mostrando eficazes na mitigação dos riscos.

10 SANÇÕES E PENALIDADES

10.1 Sem prejuízo das sanções cíveis, penais e administrativas previstas na legislação vigente, a serem aplicadas pela autoridade competente, a violação dos termos desta política sujeitará os responsáveis às medidas disciplinares cabíveis, conforme o regime disciplinar interno desta Fundação e a legislação trabalhista aplicável.

11 DISPOSIÇÕES FINAIS

11.1 O gerenciamento de riscos deverá ser implementado em todas as áreas da iNOVA Capixaba, de forma gradual, respeitando a aprendizagem e a maturidade organizacionais, com priorização incidente sobre os processos organizacionais que impactam diretamente no atingimento dos objetivos estratégicos definidos pela iNOVA Capixaba.

11.2 A matriz de riscos e os respectivos planos de ação deverão ser revisados, no mínimo, anualmente, ou sempre que ocorrerem eventos relevantes que possam alterar significativamente o perfil de riscos da Fundação.

11.3 Os riscos classificados como “muito alto” deverão ser reportados tempestivamente à Unidade de Gestão de Riscos, que, após avaliação interna, reportará à Diretoria Executiva e, caso necessário, ao Conselho Curador.

11.4 Constitui diretriz desta Política a progressiva incorporação das informações de riscos aos instrumentos de planejamento e decisão da Fundação, especialmente ao planejamento estratégico, à proposta orçamentária e ao programa de investimentos, aos contratos e planos operativos firmados com a Secretaria de Estado da Saúde, à definição e avaliação de metas e indicadores institucionais e ao planejamento das contratações, à gestão contratual e à gestão de fornecedores, observado o disposto no art. 11, parágrafo único, e no art. 169 da Lei nº 14.133/2021 e no Regulamento de Compras e Contratações da Fundação.

11.5 Os riscos relacionados a informações institucionais, dados pessoais e dados pessoais sensíveis, especialmente os referentes à saúde e aos prontuários, serão gerenciados de forma integrada com a Política de Gestão e Proteção da Informação e com a Política de Gestão Institucional de Prontuário.

12 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 31000: Gestão de Riscos: Princípios e Diretrizes. Rio de Janeiro, 2018;

BRASIL. Controladoria Geral da União - CGU. Gestão de riscos corporativos: Orientações para o setor público. Brasília - DF. 2021.

_____. Controladoria Geral da União - CGU. Metodologia de Gestão de Riscos. Brasília – DF. 2021.

_____. Tribunal de Contas da União - TCU. Manual de Gestão de Riscos do TCU. Segepres/Seplan – Brasília - DF. 2018.

_____. Tribunal de Contas da União - TCU. Manual de Gestão de Riscos do TCU – Um passo para a eficiência. 2ª edição – Brasília - DF. 2020.

IIA. The Institute of Internal Auditors. Modelo das 3 três linhas do IIA – Uma atualização das três linhas de defesa. 2020.

