FIOTEC
FIOCRUZ

POLÍTICA DE RISCOS

Sumário

Este documento pertence à Fiotec. As informações nele contidas possuem todos os direitos reservados. Nenhuma parte deste material deverá ser reproduzida, armazenada em cópias de segurança, transmitida sob qualquer forma ou por qualquer meio de impressão, seja ele físico ou eletrônico, sem autorização prévia e expressa da Fiotec.

1. Apresentação

Todas as organizações enfrentam riscos que podem afetar a realização da sua missão e o cumprimento de suas metas e objetivos. Esses, por sua vez, não podem ser eliminados, porém devem ser tratados e mitigados. As entidades do terceiro setor não possuem uma agenda de riscos diretamente correlacionada a geração de lucro, entretanto a ausência de uma política de riscos pode comprometer o alcance dos seus objetivos, colocando em risco a sua finalidade maior: o atendimento ao interesse público.

Desta forma, a análise de riscos na Fiotec é baseada na avaliação dos processos, ressaltando desta forma, a importância da gestão de processos como a base para identificar e mitigar riscos.

2. Finalidade

Estabelecer as diretrizes da gestão de riscos da Fiotec, como forma de atingir seus objetivos institucionais e apoiar o cumprimento de outras políticas, bem como inserir a visão de riscos no seu planejamento estratégico e nas tomadas de decisões. Neste contexto, visando garantir a conformidade nos processos executados pela Fundação, esta Política define princípios que visam observar as melhores práticas relacionadas à Gestão de Riscos.

3. Aplicabilidade

Esta política se aplica à todas as áreas da Fiotec, suas unidades de negócios descentralizadas e demais localidades que demandem atuação e execução de rotinas e processos desta fundação. Poderá haver ajustes para adequar as premissas de impacto e probabilidade, visando torná-las mais apropriadas às localidades de atuação.

4. Princípios

São princípios fundamentais desta política:

a) **Princípio da coerência -** A gestão de riscos deve ser coerente ao Planejamento Estratégico Participativo e à cadeia de valor da Fiotec, bem

como ser sistemática, racional, transparente, dinâmica, interativa, adaptável a mudanças e considerar também o risco como oportunidade de melhoria;

b) **Apreciação do risco na tomada de decisões -** Os riscos devem ser considerados em todas as decisões e sua gestão deve ser realizada de maneira integrada em todos os programas implementados na instituição, em diferentes níveis, respeitadas as normas internas;

c) **Razoabilidade -** A gestão de riscos deve levar em consideração as particularidades e fatos geradores que podem incidir no comportamento dos riscos identificados**;**

d) **Priorização –** Os planos de ação devem considerar as possíveis consequências de curto, médio e longo prazos e devem ser priorizadas de acordo com a agregação ou preservação de valor para a Fiotec e a sociedade.

5. Conteúdo

5.1. Diretrizes Gerais

As diretrizes apresentadas nesta Política definem e caracterizam macro etapas do processo de gestão de riscos e abrange somente os riscos inerentes às atividades relacionadas à missão da Fiotec, conforme a seguir:

- Revisar ordinariamente a cada dois anos, ou extraordinariamente quando se fizer necessário, as premissas estabelecidas no Programa de Gestão de Riscos e Controles Internos para classificação dos riscos.
- Realizar, com frequência mínima anual, a avaliação dos riscos institucionais considerados críticos para a Fundação, sob os aspectos de probabilidade e impacto.
- Possuir processo para identificar e avaliar riscos em novos projetos e programas, visando a necessidade de implantação de controles mínimos para seu funcionamento adequado.

- Priorizar a implementação da gestão de riscos nos processos de maior criticidade e relevância estratégica, tendo as deliberações do Planejamento Estratégico Participativo como instrumento norteador.
- Possuir uma estrutura dedicada à gestão de riscos, com autonomia e atuação independente, apoiada pela Diretoria Colegiada.
- Estruturar o seu sistema de controles internos de forma compatível com as necessidades decorrentes das premissas e diretrizes estabelecidas no Programa de Gestão de Riscos e Controles Internos.

5.2. O processo de gestão de riscos da Fiotec

A Gestão de Riscos tem como objetivo identificar, analisar, avaliar, monitorar e comunicar os riscos inerentes às atividades da Fundação, por meio do mapeamento e avaliação de riscos, identificação de oportunidades e apoiando os seus projetos no atingimento dos objetivos – conforme a ABNT NBR ISSO/IEC 31.000-2018 (Gestão de Riscos).

	ETAPAS	DESCRIÇÃO
1	Estabelecimento do contexto	Etapa de identificação e definição dos parâmetros internos e externos a serem levados em consideração ao gerenciar riscos e ao estabelecimento do escopo e das categorias de riscos;
2	Identificação de riscos	Etapa de busca, reconhecimento e descrição de riscos, mediante a identificação das fontes, eventos, suas causas e as consequências potenciais. Possui como produto uma lista abrangente de riscos baseada nos eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos da Fiotec;
3	Análise de riscos	Etapa de desenvolvimento da compreensão sobre o risco e a determinação do nível do risco. Nesta etapa são elaborados os mapas de riscos. Envolve a apreciação das causas e das fontes de risco, suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer.
4	Avaliação de riscos	Etapa de comparação entre o nível de risco encontrado, durante a etapa de análise, com o limite de tolerância estabelecido pela instituição. Nesta etapa são elaborados os planos de riscos. A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Compara o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado.
5	Tratamento	Etapa de implementação de uma ou mais ações para modificar o nível do risco, ou seja, é a execução dos planos de riscos.
6	Monitoramento	Etapa de verificação, supervisão, observação crítica ou identificação da situação de risco, realizadas de forma contínua, é nesta etapa que são elaborados os relatórios de riscos.
7	Comunicação	Etapa de comunicação contínua com as partes interessadas, que ocorre durante todas as etapas do processo de gestão de riscos.

A CIC (Coordenação Estratégica de Integridade e Compliance) deverá estruturar e garantir a existência de um processo desenhado para avaliação, monitoramento e direcionamento da gestão de riscos.

5.3. Definição dos tipos de Riscos

Risco é todo evento potencial que pode impactar negativamente o alcance dos objetivos da Fiotec ou de processos.

Não obstante a definição de risco como um evento negativo, as diretrizes e premissas do programa devem possibilitar a identificação de oportunidades na execução das atividades pertinentes à Fundação.

Os riscos são categorizados da seguinte forma:

I - Origem dos eventos: É determinante para a definição da abordagem a ser empregada na resposta ao risco.

a) **Riscos inerentes externos** são ocorrências associadas ao ambiente macroeconômico, político, social, natural ou setorial em que a Fundação atua, porém, em geral, não é possível intervir diretamente sobre estes eventos que terão, portanto, uma ação predominantemente reativa.

b) **Riscos inerentes internos** são eventos originados na própria estrutura da Fundação, pelos seus processos, seu quadro de pessoal ou de seu ambiente tendo como resposta uma ação proativa.

II - Natureza dos Riscos: É o que permite a consolidação dos riscos de uma forma organizada, tendo sido definido para o Programa de Gestão de Riscos e Controles Internos as seguintes naturezas: estratégica, operacional, financeira, conformidade, tecnológico, privacidade e segurança da informação.

Tendo em vista a possibilidade de o risco ser enquadrado em mais de uma natureza, fica estabelecido que será utilizada como premissa a natureza de maior relevância para a Fiotec.

a) **Riscos Estratégicos**: estão associados à tomada de decisão da Alta Direção e podem gerar perda substancial no valor econômico da organização.

b) **Riscos Operacionais:** estão associados à possibilidade de ocorrência de perdas (de projetos, ativos, receitas) resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas. Os riscos operacionais geralmente acarretam redução, degradação ou interrupção, total ou parcial, das atividades, com impactos negativos na Fundação, além do potencial geração de passivos contratuais, regulatórios e ambientais.

c) **Riscos Financeiros:** Impactos significativos em receitas, despesas ou investimentos podendo ocasionar distorções significativas nas demonstrações financeiras e/ou no fluxo de caixa da Fundação.

d) **Riscos de Conformidade (*Compliance*):** aqueles associados à exposição pelo não cumprimento de leis, contratos, convênios e regulamentos emitidos pelos governos centrais e locais, regularidade ambiental e social, assim como regulamentos emitidos por entidades reguladoras, fiscalizadoras ou mesmo de natureza interna.

e) **Risco de Tecnologia, Privacidade e Segurança da Informação:** aqueles associados ao não cumprimento das normas de segurança da informação e boas práticas de desenvolvimento e infraestrutura de tecnologia, podendo gerar paralisação das atividades suportadas pela tecnologia, acessos inadequados e/ou não autorizados, possibilitando o vazamento e/ou sequestro de informações privadas, confidenciais ou sigilosas da Fundação.

5.4. Análise do Risco

Para classificação efetiva dos riscos, é necessário identificar a possibilidade da sua ocorrência e, concomitantemente, os impactos decorrentes da materialização do risco.

A combinação das análises realizadas determinará o rating do risco que deve estar representado no mapa de calor (*heatmap*).

5.4.1. Entendimento e formalização dos Processos

Visando suportar o processo de avaliação e gestão dos riscos é necessário realizar o levantamento dos processos, detalhando suas atividades, tarefas, artefatos e agentes envolvidos.

O registro e a manutenção dos processos institucionais visam, além da retenção do conhecimento, possibilitar a classificação mais assertiva dos riscos identificados.

5.4.2. Impacto do Risco

Para mensurar o impacto dos riscos, devem ser analisadas as dimensões financeiras, reputacional, legal, operacional, infraestrutura tecnologia, privacidade, social e ambiental para posterior classificação, conforme premissas abaixo apresentadas:

Dimensões	IMPACTO				
	Muito Baixo	**Baixo**	**Médio**	**Alto**	**Muito Alto**
Financeiro	Perdas financeiras de até R$ 100.000,00	Perdas financeiras acima de R$ 100.000,00 até R$ 200.000,00	Perdas financeiras acima de R$ 200.000,00 até R$ 300.000,00	Perdas financeiras acima de R$ 300.000,00 até R$ 500.000,00	Perdas financeiras acima de R$ 500.000,00
Reputação	Repercussã o negativa entre colaboradore s	Repercussão negativa entre Gestores e Coordenadore s	Repercussão negativa entre Coordenadores Fiocruz	Repercussão negativa no ambiente externos e entre Agentes Financiadores	Repercussão negativa no ambiente externos e entre Órgãos Reguladores
Legal	Eventos que não originam ações judiciais, arbitrais, multas regulatórias e contratuais	Eventos que podem gerar ações judiciais, mas devem originar multas regulatórias e contratuais	Eventos que devem gerar ações judiciais, arbitrais, e multas regulatórias e contratuais e podem gerar perda de financiadores	Eventos que devem gerar ações judiciais, arbitrais, multas regulatórias e contratuais e perda de financiadores e podem gerar intervenção do MP	Eventos que devem gerar ações judiciais, arbitrais, multas regulatórias e contratuais e perda de financiadores e intervenção do MP
Operacional	Não compromete	Eventos que podem	Eventos que podem	Eventos que podem gerar	Eventos que devem gerar

	Processos finalísticos e de suporte Organização	comprometer processos finalísticos e de suporte da Organização	suspender em curto período processos finalísticos e de suporte da Organização	paralisação temporária de processos finalísticos e de suporte da Organização	paralisação de processos finalísticos e de suporte da Organização
Infraestrutura Tecnológica	Degradação do serviço com até 1 hora de duração	Degradação do serviço com até 4 horas de duração	Indisponibilidade de sistemas não críticos OU degradação do serviço com mais de 4 horas de duração	Indisponibilidade de sistemas não críticos OU degradação do serviço com mais de 8 horas de duração	Indisponibilidade de sistemas críticos OU interrupção de serviços de correio eletrônico e acesso à internet
Proteção e Privacidade de Dados	Cumprimento incorreto de procedimento de segurança gerando acesso indevido de dados sem vazamento de informação	Não cumprimento de procedimento de segurança gerando acesso indevido de dados sem vazamento de informação	Vazamento /acesso indevido de informação pública de uso interno	Vazamento / acesso indevido a informação de uso restrito	Vazamento / acesso indevido a informação Confidencial ou Sensível
Social	Eventos que não geram impacto social negativo as partes interessadas	Eventos que podem gerar impacto social negativo as partes interessadas	Eventos que podem gerar impacto social negativo as partes interessadas e repercussão negativa,	Eventos que devem gerar impacto social negativo as partes interessadas e pode gerar repercussão negativa	Eventos que devem gerar impacto social negativo as partes interessadas e repercussão negativa
Ambiental	Eventos que não geram impacto Ambiental negativo	Eventos que podem gerar impacto Ambiental negativo, mas não gera repercussão negativa.	Eventos que podem gerar impacto Ambiental negativo e repercussão negativa	Eventos que podem gerar impacto Ambiental negativo e gerar riscos á saúde humana.	Eventos que devem gerar impacto Ambiental negativo e gerar riscos à saúde humana

5.4.3. Probabilidade do risco

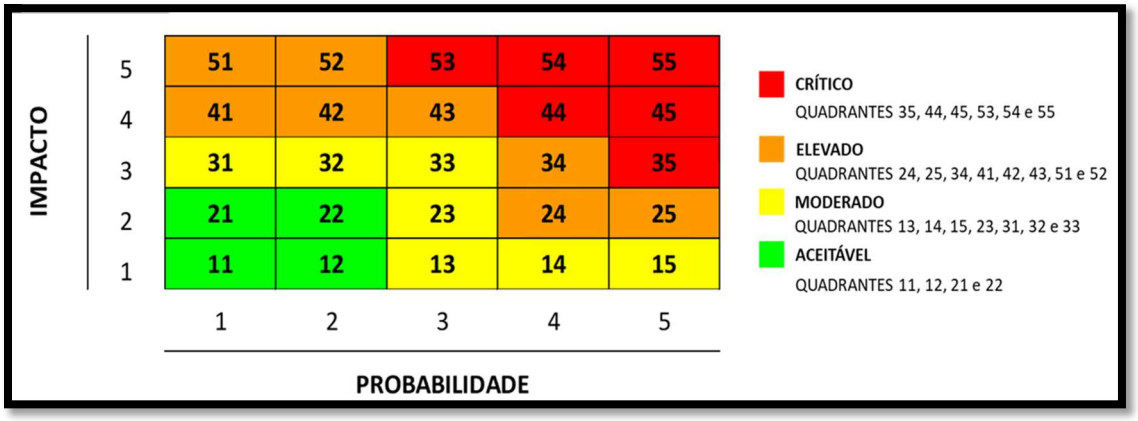
Para que possamos definir a possibilidade da ocorrência de um evento foram definidas as premissas abaixo apresentadas:

Probabilidade	Situação
Muito baixo	Chance remota de que o evento ocorra e/ou histórico raro de ocorrências ou não possuir histórico de materialização do risco.
Baixo	É mais provável que o evento não ocorra do que ocorra e/ou histórico de baixa frequência de materialização do risco.

Médio	É possível que o evento ocorra e/ou histórico de moderada frequência de materialização do risco.
Alto	É mais provável que o evento ocorra que não ocorra e/ou histórico de alta frequência de materialização do risco.
Muito Alto	É quase certo que o evento irá ocorrer e/ou histórico de intensa frequência de materialização do risco.

5.4.4. Grau do Risco

Visando definir a classificação final do evento (*rating* do risco) é preciso considerar as classificações anteriormente realizadas (impacto e probabilidade) e compará-la com as premissas pré-estabelecidas de *rating* abaixo apresentadas:



As respostas e ações de monitoramento que serão associadas aos riscos estão diretamente relacionadas ao seu *rating*. Quanto maior a severidade do risco, maior robustez serão implementadas nas suas atividades de controle.

5.5. Tratamento do risco

O risco nunca pode ser eliminado por completo, no entanto, para definição das tratativas, a avaliação dos riscos é feita de forma conjunta, pelo proprietário do risco. Entende-se como proprietário dos riscos, os envolvidos no processo sob o apoio da CIC, visando estabelecer ações de controle mais assertivas, que podem ser:

I. **Evitar**: Quando se elimina o fato gerador do risco, por exemplo, descontinuando determinado processo ou saindo de mercado específico. Dessa forma, são estabelecidas ações que eliminam a probabilidade do risco se materializar.

II. **Gerenciar:** Quando são aplicáveis os controles internos (ex.: aprovação, revisão, segregação de funções, reconciliação, perfis de acesso etc.) ou barreiras para que o dano potencial e/ou probabilidade do risco sejam substancialmente reduzidos.

III. **Transferir**: Quando o risco é dividido ou transferido para uma contraparte externa à Fundação. Exemplos de compartilhamento de riscos são as operações de hedge (moeda estrangeira, preços, juros) e apólices de seguro etc.

IV. **Assumir:** Quando o impacto versus probabilidade do risco é considerado irrelevante, toma-se a decisão de aceitar o risco, pois o custo da ação de controle seria maior do que o próprio risco potencial envolvido.

Os Riscos identificados nas rotinas de avaliação e gestão de riscos serão armazenados em repositório específico e reportados as partes interessadas com tempestividade e acuracidade requeridas.

5.6. Matriz de Responsabilidade

5.6.1. Conselho Curador

- Aprovar o Conteúdo dessa Política.

5.6.2. Diretoria Colegiada

- Garantir que toda Fiotec conheça a leitura e a aplicação do conteúdo desta Política.

- Atuar de forma comprometida no gerenciamento e cultura de riscos, através do engajamento, conhecimento, compreensão e acompanhamento dos principais riscos da Fundação.

- Ratificar a priorização dos riscos a serem tratados/gerenciados.
- São responsáveis por patrocinar a implantação do Programa de Gestão de Riscos e Controles Internos e devem informar à CIC sobre a identificação de novos riscos críticos ou eventos que sejam relevantes e suas respectivas evoluções.

5.6.3. Gestores e Líderes da Fiotec

- Garantir na sua equipe a leitura e a aplicação do conteúdo desta Política.
- São responsáveis por identificar, mensurar, avaliar e gerenciar os eventos de risco, que podem influenciar o cumprimento dos objetivos de suas áreas e negócios.
- Possuem as atribuições de avaliar e propor melhorias dos mecanismos de gestão de riscos em sua área/negócio, além de garantir os recursos necessários para a implantação dos planos de ação para mitigação dos riscos identificados.

5.6.4. CIC (Coordenação Estratégica de Integridade e Compliance)

- Implementar as diretrizes e premissas do Programa de Gestão de Riscos e Controles Internos, bem como gerenciar as rotinas operacionais definidas no Programa.
- Elaborar e revisar periodicamente as Políticas do Programa de Gestão de Riscos e Controles Internos, visando a melhoria contínua dos processos e ou rotinas estabelecidas no Programa.
- Aprimorar a capacitação técnica e a infraestrutura da estrutura de gestão de riscos, visando propiciar a melhoria contínua do Programa de Gestão de Riscos e Controles Internos.
- Promover e capacitar, por meio de treinamentos periódicos sobre a Política de Riscos, todas as partes interessadas ao negócio;

- Definir os indicadores de performance do Programa de Gestão de Riscos e Controles Internos, monitorá-los notificando à Diretoria Colegiada quaisquer alterações no rating dos riscos priorizados.

5.6.5 Todos os Colaboradores

- Conhecer e cumprir as diretrizes desta Política;
- Atuar em defesa da Fiotec identificando e comunicando potenciais riscos e não conformidades.

6. Disposições gerais

Esta política deve ser considerada conjuntamente com outras temas institucionais, visando identificar eventuais conflitos acerca das diretrizes predefinidas para gestão de riscos da Fiotec.

A abordagem aos riscos não apenas sublinha a relevância dos processos internos na identificação, mas também assegura que todos compreendam a fundamentação da política e se engajem ativamente na sua execução,

Além disso, esta política pode requerer a elaboração de outros instrumentos normativos, possibilitando o pleno entendimento do respectivo tema.

6.1. Exceções, eventuais violações e casos omissos

As exceções, eventuais violações e casos omissos a esta Política devem ser submetidos à apreciação da avaliação dos riscos institucionais considerados críticosavaliação dos riscos institucionais considerados críticose encaminhados para posterior decisão pela Diretoria Colegiada, conforme a gravidade do evento.

7. Referência Normativa

Código de Conduta Ética Fiotec

ABNT NBR ISO/IEC 31000:2018 Gestão de riscos – Diretrizes

COSO ERM 2017

8 Controle de Revisões

Revisão	Data	Resumo da Alteração
0	30/09/2019	Versão Inicial aprovada pela Diretoria e Conselho Curador
01	24/10/2024	Revisão do texto inicial aprovada pela Diretoria e Conselho Curador. Foi inserido os papéis e responsabilidades da estrutura responsável pela Gestão de Riscos da Fiotec, além da revisão da metodologia de gestão de riscos e o mapa de riscos.
02	06/04/2026	Atualização da nova estrutura da área de Integridade e Compliance, onde era: Gerência de Integridade e Compliance (GIC), para: Coordenação Estratégica de Integridade e Compliance (CIC). Texto nos itens: 5.2; 5.5; 5.6.2; 5.6.4 e 6.1 Alteração da revisão da avaliação dos riscos institucionais considerados críticos, onde era: com frequência mínima de semestral, para: anual. Texto no item: 5.1 Aprovação realizada na reunião com o Conselho Curador de Ata nº 141.

9 Termos e definições

As definições dos termos e expressões utilizados neste documento, estão listados abaixo:

Conceito de Risco: Risco é o efeito das influências e fatores externos e internos que torna incerto o atingimento dos objetivos de uma empresa. Aplicado ao conceito de valor, além da geração do retorno pelo trabalho, uma empresa deve saber gerenciar os seus riscos.

Fonte do Risco: Elemento que individualmente ou combinado, tem potencial de dar origem ao risco.

Evento: Ocorrência ou mudança em um conjunto específico de circunstâncias.

Controle: Medida que mantém ou modifica o risco.

***Heatmap*:** Um mapa de calor é uma técnica de visualização de dados que mostra a magnitude de um fenômeno por meio de cor em duas dimensões. A variação de cor pode ser por matriz ou intensidade.

***Rating*:** O Rating é um termo em inglês que, traduzido, significa classificação.

Apetite ao Risco: É a exposição a diferentes riscos que a Fundação está disposta a assumir, visando atingir aos seus objetivos estratégicos.

10 Anexos

Não se aplica.