

Ministério da Saúde

FIOCRUZ

**Fundação Oswaldo Cruz**

# **Guia de Gestão de Riscos da Fiocruz**

Fevereiro  
2019

## **Aprovação e Elaboração da Minuta do Guia**

- Mario dos Santos Moreira – Vice-Presidente de Gestão e Desenvolvimento Institucional (VPGDI)
- Juliano de Carvalho Lima – Diretor Executivo VPGDI
- Simone A. Borges Oliveira – Assessora Executiva da VPGDI

## 1. INTRODUÇÃO

Todo gestor público, independentemente de seu nível de atuação, deve ter como compromisso a aplicação dos recursos públicos a partir dos objetivos estratégicos e prioridades estabelecidas pela Alta Administração para gerar resultados que criem valor para a sociedade. Estes resultados, também devem ser comunicados para os diversos públicos com base em informações integras e de forma transparente.

Entretanto, constitui um desafio definir o quanto de risco uma instituição pública que atua no campo complexo da ciência, tecnologia e inovação em saúde, como é o caso da Fiocruz, deve aceitar no processo de tomada de decisão, visando o melhor desempenho na prestação de serviços públicos à sociedade. Naturalmente, estas instituições estão mais expostas a riscos complexos e dinâmicos, dada as características intrínsecas dos processos de inovação e produção de conhecimento em saúde frente as necessidades ( muitas vezes urgentes) de saúde da população em um país em desenvolvimento, com sistema universal, grande desigualdade social e educacional, e de dimensão continental como o Brasil. E são inúmeras as disfunções burocráticas do aparato estatal executivo atual vis-à-vis a esta dinâmica da inovação em saúde. Superar este desafio, não se dá sem o alinhamento aos princípios de Governança Pública, essenciais a sustentabilidade das instituições públicas. Mas, principalmente não se dará, sem a modernização do aparato estatal e priorização do fortalecimento das capacidades estatais para gestão das políticas públicas de interesse social, semelhante ao investimento realizado pelo Estado para o desenvolvimento de capacidades estatais para o controle.

Com a publicação da Instrução Normativa Conjunta MP/CGU nº 01/2016 foram dispostas orientações para a sistematização da gestão de riscos e controles internos no âmbito do poder executivo, como processo estratégico chave para a governança. Portanto, a gestão de riscos passa a ter que ser realizada pelos gestores públicos não mais de forma intuitiva, mas de forma sistematizada.

O Congresso Interno da Fiocruz discute as teses e diretrizes que alimentam o planejamento estratégico institucional. Coube a VIII Congresso Interno estabelecer a Tese 8 e a Diretriz 5, descritas em relatório final:

*“Tese 8 - A Fiocruz conquistou integridade institucional ao longo de sua história pública e é patrimônio da sociedade brasileira, devendo aprimorar sua política de governança, reestruturar seu sistema de controle interno e de gestão de risco, instituir um modelo de gerenciamento por meio de plataformas colaborativas, reforçar a integração, com segurança e efetividade, e fazer frente ao desmonte do serviço público, em permanente diálogo com a sociedade.”*

*“Diretriz 05 - Implantar a Política de Gestão de Integridade, Riscos e Controles Internos da Fiocruz, integrando-a ao modelo de controle interno central”.*

O Conselho Deliberativo (CD Fiocruz) aprovou a Política de Gestão de Riscos da Fiocruz (PGR/Fiocruz) publicada na Portaria PR 787/2018 de 26.06.18 que estabeleceu parte da arquitetura (conceitos, princípios, objetivos, estrutura, competências e processo) necessária a gestão de riscos eficaz na Fiocruz. A Gestão de Riscos da Fiocruz objetiva, entre outros, o cumprimento destas deliberações congressuais e tem como fundamento a confiança em seus servidores e gestores.

Este manual foi elaborado com base nas metodologias de gestão de riscos da Controladoria Geral da União (CGU), do Ministério do Planejamento, Desenvolvimento e Gestão e Tribunal de Contas da União (TCU) e ABNT ISO 31000 pela Assessoria Executiva da VPGDI e tem como objetivo ser uma diretriz para os órgãos, unidade e as vice-presidências empreenderem a gestão de riscos na Fiocruz de forma orientada.

Sendo assim, este documento apresenta os 10 passos para a implantação do gerenciamento de riscos pelos órgãos, unidade e vice-presidências da Fiocruz. Considerando os diferentes níveis de maturidade em gerenciamento de riscos nos órgãos, a opção foi por uma metodologia de fácil compreensão e baixa complexidade. A metodologia poderá acolher adaptações no caso de um maior nível de maturidade ou

especificidade dos órgãos, mediante justificativa, sem perder de perspectiva o rigor, a qualidade e a integridade das informações levantadas, produzidas, registradas e monitoradas.

Acompanha o guia, o cronograma de entregas e anexos para que os órgãos possam operacionalizar, de forma célere, a realização das etapas de gerenciamento dos riscos.

## 2. FUNDAMENTOS DA GESTÃO DE RISCOS DA FIOCRUZ

Em novembro de 2017 foi publicado pelo poder executivo, o Decreto nº 9.203 que dispôs sobre a política de governança da administração pública federal direta, autárquica e fundacional. A política institui como dever a adoção da gestão de riscos pela administração pública fundacional, conforme abaixo:

*Art. 17 A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os seguintes princípios:*

*I - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;*

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

*III - estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e*

*IV - Utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.*

Um ano antes, a Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016 acabou para o regulamentar o art. 17 deste decreto.

A evolução da Gestão de Riscos na Fiocruz buscará alinhamento com a legislação vigente, publicações científicas e com os principais frameworks do mercado. São conceitos principais da Gestão de Riscos e Controles Internos na Fiocruz:

**Gestão de riscos:** arquitetura (conceitos, princípios, objetivos, estrutura, competências e processo) necessária para se gerir os riscos eficazmente.

**Gerenciamento de risco:** processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza no alcance dos objetivos institucionais.

**Processo organizacional:** sequência de atividades que transformam entradas (informações, materiais, instruções ou matérias-primas) em saídas (produtos, serviços ou decisões) predefinidas.

**Objetivo institucional:** situação que se deseja alcançar para evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da instituição.

**Evento:** um incidente ou uma ocorrência de fontes internas ou externas à organização, que podem impactar a realização de objetivos de modo negativo, positivo ou ambos.

**Risco:** possibilidade de ocorrência de um evento que venha a ter impacto negativo realização de objetivos. O risco é medido em termos de probabilidade e impacto.

**Oportunidade:** possibilidade de ocorrência de um evento que afete positivamente a realização de objetivos.

**Probabilidade:** chance de um evento de risco ocorrer.

**Impacto:** consequência caso o evento de risco ocorra.

**Risco inerente:** nível de risco antes da consideração de qualquer ação de tratamento.

**Medida de controle:** medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas institucionais estabelecidos sejam alcançados.

**Controles internos:** conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações destinados a enfrentar os riscos e fornecer segurança razoável para o alcance dos objetivos e realização da missão institucional da Fiocruz.

**Risco residual** – nível de risco após a implementação das ações adotadas pela gestão (por exemplo, controles internos) para tratar o risco inerente.

**Apetite a risco** – expressão ampla de quanto risco uma organização está disposta a enfrentar para implementar sua estratégia, atingir seus objetivos e agregar valor para as partes interessadas, no cumprimento de sua missão.

**Tolerância a risco** – nível de variação aceitável no desempenho em relação à meta para o cumprimento de um objetivo específico, em nível tático ou operacional.

**Resiliência:** capacidade adaptativa de instituição em um ambiente complexo, volátil, incerto, ambíguo e de mudanças.

**Accountability:** conjunto de procedimentos adotados pelas instituições públicas e pelos trabalhadores que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho.

São princípios e os objetivos da Gestão de Riscos na Fiocruz:

Quadro 1: Princípios da Gestão de Riscos da Fiocruz

Aderência à integridade e a valores éticos
Alinhamento aos objetivos estratégicos da instituição;
Respeito aos fundamentos basilares da Administração Pública da legalidade, impessoalidade, moralidade, publicidade e eficiência;
Alinhamento ao modelo de gestão participativa da Fiocruz;
Compromisso com a democratização das informações e transparência;
Respeito à diversidade organizacional.
Agregar valor e estabelecer controles internos proporcionais ao risco, observada a relação custo-benefício
Confiança como ativo relevante para o desempenho institucional
Compromisso com os resultados voltados para a melhoria das condições de vida e de saúde dos brasileiros e para o desenvolvimento da ciência e tecnologia no país

Quadro 2: Objetivos da Gestão de Riscos da Fiocruz

Contribuir para o cumprimento da missão e para o desenvolvimento da estratégia institucional
Contribuir para a eficiência, a eficácia e a efetividade institucional, mediante execução ordenada, ética e econômica dos processos de trabalho
Produzir informações íntegras e confiáveis à tomada de decisões, ao cumprimento das obrigações com a transparência pública e à prestação de contas
Assegurar a conformidade dos processos com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e as normas internas da Fiocruz
Aumentar resiliência institucional

### 3. ESTRUTURA DE GESTÃO DE RISCOS DA FIOCRUZ

A Gestão de Riscos da Fiocruz é gerida de forma integrada entre as instâncias apresentadas nesta seção. Para coordenar os papéis dos atores envolvidos na Gestão de Riscos, a IN CGU/MP nº 01/2016 apresenta a estrutura de três linhas de defesa, conforme proposto pelo The Institute of Internal Auditors (IIA) da seguinte forma:

Na Fiocruz, a 1ª linha de defesa é composta pelos gestores dos processos nos diversos níveis do órgão específico singular e unidade, os comitês de gestão de riscos e controles internos e pelos servidores. O Diretor do órgão específico singular ou unidade é o gestor responsável pela gestão de riscos e controles internos de todos os processos organizacionais do órgão ou unidade que dirige.

Na 2ª linha, atua a Executiva Técnica e demais instâncias típicas de supervisão e monitoramento de controles internos<sup>1</sup>. A executiva técnica é formada pela Diretoria Executiva da VPGDI e assessores designados por cada vice-presidência.

A 3ª linha de defesa é realizada pela Auditoria Interna Fiocruz.

A alta administração da Fiocruz, é formada pelo Presidente da Fiocruz, os Diretores dos órgãos específicos singulares e unidade descentralizada, Vice-presidentes e Coordenadores transversais. O CD da Fiocruz é órgão colegiado de deliberação integrado pelos membros da alta administração referidos acima, incluindo Chefe de Gabinete, Sindicato e coordenadores dos órgãos seccionais, conforme estatuto Fiocruz.

A figura abaixo mostra as linhas de defesa na Gestão de Riscos na Fiocruz:

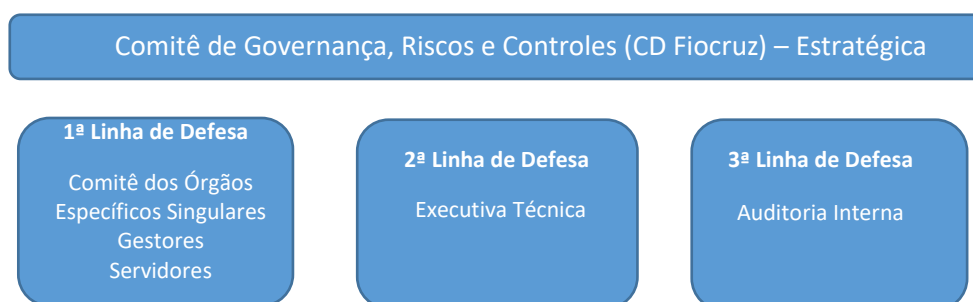


Figura 1 – Linhas de defesa na Gestão de Riscos e Controles Internos

#### 3.1. COMPETÊNCIAS DAS ESTRUTURAS

##### 3.1.1. Comitê de Governança, Gestão de Riscos e Controles (CGRC/CD Fiocruz)

- Definir e atualizar as estratégias de implementação da Gestão de Riscos, considerando os contextos externo e interno;
- Institucionalizar estruturas adequadas de governança, riscos e controles internos e garantir os recursos para sua implementação e capacitação de servidores;
- Garantir o alinhamento da gestão de riscos aos padrões de ética e de conduta, em conformidade com o Programa de Integridade da Fiocruz;
- Aprovar as políticas, manuais e normas de gestão de riscos e controles internos e suas revisões;
- Implementar e supervisionar os sistemas de gerenciamento de riscos e controles internos;
- Fomentar a inovação e a adoção de boas práticas de governança, gestão de riscos e controles internos;
- Definir o nível de apetite e exposição ao risco na condução dos programas, projetos e processos da Fiocruz considerando seus objetivos estratégicos;
- Aprovar os relatórios de gestão de riscos e controles internos;
- Aprovar o plano de gestão de riscos da Fiocruz e responsáveis;

<sup>1</sup> Por exemplo como a Controladoria, instância deliberada em Congresso Interno, a ser implantada.

- Garantir o alinhamento da gestão de riscos aos padrões de ética e de conduta, em conformidade com o Programa de Integridade da Fiocruz;
- Realizar avaliações periódicas para verificar a eficácia da gestão de riscos e dos controles internos da gestão, comunicando o resultado aos responsáveis pela adoção de ações corretivas;
- Definir a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;
- Monitorar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas;
- Avaliar o desempenho da arquitetura de Gestão de Riscos e fortalecer a aderência dos processos à conformidade normativa;
- Definir indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho da CGU;
- Supervisionar a atuação das demais instâncias da Gestão de Riscos e Controles Internos

### **3.1.2. Executiva Técnica**

- Identificar e gerenciar os riscos dos processos organizacionais que gerenciam;
- Realizar os objetivos estratégicos, políticas, diretrizes, metodologias e mecanismos para a comunicação e institucionalização do gerenciamento dos riscos e controles internos da gestão;
- Propor aprimoramentos em políticas, diretrizes e normas complementares para o gerenciamento de integridade, riscos e controles internos da gestão ao CGRC;
- Monitorar os riscos estratégicos ao longo do tempo, de modo a permitir que as respostas adotadas resultem na manutenção do risco em níveis adequados;
- Assegurar que as informações adequadas sobre gerenciamento de integridade, riscos e controles internos da gestão estejam disponíveis em todos os níveis, no âmbito das unidades;
- Disseminar a cultura do gerenciamento de integridade, riscos e de controles internos;
- Estimular e promover condições à capacitação dos gestores, no exercício do cargo, e dos trabalhadores no gerenciamento de riscos e controles internos da gestão;
- Assegurar o cumprimento das recomendações e orientações emitidas pelo CGRC/ CD Fiocruz;
- Assegurar o cumprimento das regulamentações, leis, códigos, normas e padrões na condução das políticas e na prestação de serviços de interesse público;
- Assegurar o cumprimento de práticas que institucionalizem a responsabilidade de todos os envolvidos na prestação de contas, transparência e efetividade das informações;
- Promover a integração dos trabalhadores responsáveis pelo gerenciamento de integridade, riscos e controles internos da gestão;
- Promover a implementação de metodologias e instrumentos no gerenciamento de integridade, riscos e controles internos da gestão;
- Coordenar os processos de identificação, classificação e avaliação dos riscos estratégicos a que a Fiocruz está sujeita;
- Emitir relatórios periódicos de gestão de riscos e controles internos;
- Viabilizar suporte de tecnologia da informação para apoiar os processos de integridade, riscos e a implementação dos controles internos da gestão nas unidades.

### **3.1.3. Comitês dos órgãos específicos singulares (CGRCO)**

- Elaborar e submeter ao conselho deliberativo da unidade o Plano de Gestão de Riscos e Controles Internos;
- Indicar um representante para atuar como ponto focal para gestão de integridade, riscos e controles internos;
- Manter controles internos eficazes, conduzindo procedimentos de resposta aos riscos;
- Gerenciar os riscos dos processos de trabalho de acordo com essa política e as correlacionadas, bem como, garantir a implantação do modelo de gerenciamento de risco adotado pela Fiocruz;
- Submeter, após aprovação do conselho deliberativo da unidade, o Plano de Implementação de Controles à aprovação da CGRC;
- Implementar e gerenciar as ações contidas no Plano de Implementação de Controles e avaliar os resultados;

- Apoiar no monitoramento dos riscos de seus processos ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com o modelo de gerenciamento de riscos aprovado e com esta Política;
- Gerar e reportar informações adequadas sobre o gerenciamento de integridade, riscos e controles internos à CGRC;
- Disseminar preceitos de comportamento íntegro e da cultura de gerenciamento de riscos e controles internos da gestão, em sua área de atuação;
- Observar a inovação e a adoção de boas práticas no gerenciamento de integridade, riscos e controles da gestão;
- Cumprir as recomendações e observar as orientações emitidas pelo CGRC;
- Adotar princípios de conduta e padrões de comportamento estabelecidos nas diretrizes de integridade desta Política;
- Cumprir as regulamentações, leis e códigos, normas e padrões instituídos;
- Cumprir as práticas institucionalizadas na prestação de contas, transparência e efetividade das informações.
- Enviar relatórios periódico sobre o gerenciamento dos riscos e controles internos
- informar o Unidade de Gestão da Integridade (UGI) sobre mudanças significativas nos processos organizacionais sob sua responsabilidade;
- Responder às requisições da Unidade de Gestão da Integridade (UGI);

#### **3.1.4. Responsáveis pelo gerenciamento de riscos dos processos organizacionais (gestores)**

- Identificar, analisar e avaliar os riscos dos processos sob sua responsabilidade, em conformidade ao o definido pela Fiocruz;
- Propor respostas e respectivas medidas de controle a serem implementadas nos processos organizacionais sob sua responsabilidade;
- Monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas nos processos organizacionais sob sua responsabilidade;
- 

#### **3.1.5. SERVIDORES E DEMAIS COLABORADORES DA FIOCRUZ**

- Monitoramento da evolução dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento.

### **4. GERENCIAMENTO DE RISCOS NA FIOCRUZ**

O gerenciamento de riscos e controles internos corporativo passa a ser uma prática permanente em cada órgão específico singular e unidade da Fiocruz, sendo esperada evolução da maturidade a cada ciclo anual.

Nesta fase inicial, a opção foi por uma abordagem simplificada, que será aprimorada continuamente.

São dez os passos que devem ser realizados por todos os órgãos e unidade da Fiocruz, conforme prazos de monitoramento abaixo:

#### **PASSO 1: INSTITUA O COMITÊ DE GERENCIAMENTO DE RISCOS E CONTROLES INTERNOS (CGRCO)**

**Cada órgão específico singular e unidade da Fiocruz deverá instituir um Comitê de Gestão de Riscos e Controles Internos (CGRCO)<sup>2</sup> por meio de portaria, designando coordenador (a) e secretário (a) executivo (a) e enviar para gestaoderiscos@fiocruz.br até 31 de março de 2019.**

Todos os integrantes do Comitê, em especial o coordenador deverão ser servidores<sup>3</sup> e com fácil acesso a Diretoria e áreas do órgão. Os integrantes deverão ser os responsáveis pelas áreas de supervisão dos

<sup>2</sup> Trata-se do Comitê previsto do art. 18 e 22 na Portaria PR 787/2018.

<sup>3</sup> Conforme previsto do art. 18 na Portaria PR 787/2018.



processos finalísticos e de gestão pública do órgão, tais como gestão de qualidade, biossegurança, gestão de projetos, gestão financeira, gestão de recursos humanos, gestão operacional entre outras.

A **CGRCO** deve aprovar a agenda de reuniões do ano, possibilitando aos integrantes a reserva da agenda de trabalho. As pautas, atas e todo o material de trabalho produzido por pelos CGRCOs devem ser registradas e armazenadas em [drive.fiocruz.br](http://drive.fiocruz.br). As competências desta instância em âmbito corporativo estão previstas no item 3.1.3.

## **PASSO 2: PRIORIZE OS PROCESSOS ORGANIZACIONAIS**

Instituído o CGRCO, devem ser estabelecidas as prioridades para o levantamento e gerenciamento de riscos, classificando os processos organizacionais do órgão por seu grau de exposição aos riscos. Para tal, deve ser realizada a análise qualitativa e quantitativa dos processos organizacionais do órgão com base nos seguintes fatores especificados no anexo VI:

- Análise quantitativa - fatores: materialidade, necessidade de Recursos Humanos (qualificação técnica especializada) e os Recursos Tecnológicos necessários para a execução do processo;
- Análise qualitativa – fatores: processo estratégico, demandas do TCU, demandas da CGU, relevância do processo, valores não orçamentários e reclamações e denúncias registradas na ouvidoria.

Necessariamente, processos do macroprocesso finalístico operado pelo órgão específico singular deve estar entre os priorizados para análise neste primeiro ciclo. As análises permitirão a classificação dos processos nas categorias: essencial (E), relevante (R) e necessário (N). Os prazos para o levantamento de riscos dos processos do órgão, unidade ou vice-presidência são de 2 anos para os classificados como essenciais, até 3 anos para os classificados como relevantes e de até 05 anos para os necessários.

## **CLASSIFICAÇÃO FINAL DO PROCESSOS ORGANIZACIONAIS**

Após a aplicação do anexo VI, a classificação final dos processos será a média ponderada da NOTA DA AVALIAÇÃO QUANTITATIVA FINAL e da NOTA DA AVALIAÇÃO QUALITATIVA FINAL, conforme abaixo:

$$CF = (\text{nota da avaliação quantitativa}) + (\text{nota da avaliação qualitativa}) / 2$$

Ao final os processos organizacionais poderão ser classificados como:

<b>Classificação</b>	<b>Resultado Final</b>
Essencial	Resultado maior ou igual a 2,2
Relevante	Resultado maior ou igual a 1,6 e menor que 2,2
Necessário	Resultado menor que 1,6

- Essencial (E): processos que mobilizam mais recursos institucionais e estão mais expostos ao risco deverão ter prioridade sobre os demais no gerenciamento de riscos.
- Relevante (R): processos de grande importância ou que merecem destaque, e que deverão ter uma prioridade média sobre os demais no gerenciamento de riscos.
- Necessário (N): processos de menor importância, que deverão ter prioridade baixa sobre os demais no gerenciamento de riscos.

A unidade com o assessoramento do CGRCO deve identificar e priorizar os processos organizacionais que comporão o Plano de Gerenciamento de Riscos e Controles Internos<sup>4</sup> do seu órgão. O gerenciamento de riscos deverá ser implementado de forma gradual, sendo priorizados os processos organizacionais classificados como essenciais e que impactam diretamente no atingimento dos objetivos ou diretrizes estratégicas definidas do planejamento estratégico.

<sup>4</sup> Trata-se do plano previsto no inciso II do art. 22 na Portaria PR 787/2018.

### PASSO 3: ESTUDE O PROCESSO PRIORIZADO

A CGRCO deve selecionar os processos classificados como essenciais, o que definirá o escopo da gestão de riscos do órgão, estudar e documentá-los da seguinte forma:

- Nome do processo;
- As leis e normas aplicáveis;
- Descrição resumida com as principais etapas, atividades, produtos, atores envolvidos (caso tenha o fluxo mapeado no bizagi apresentar), periodicidade e média de duração em dias, semanas ou meses.
- Pontos fortes e fracos, oportunidades e ameaças ao processo (use a matriz SWOT);
- Objetivo geral e específico (alinhar com os objetivos estratégicos do órgão);
- Responsável pelo gerenciamento de risco do processo (esse gestor deve ter alçada suficiente para orientar e acompanhar as etapas de identificação, análise, avaliação e implementação das respostas aos riscos e terá auxílio do Coordenador(a) ou secretário(a) executivo(a) da CGRCO para tal); e
- Equipe técnica que participará do processo de gerenciamento de riscos (pessoas que conhecem o processo selecionado, seus controles, suas interfaces e resultados)

O anexo II deve ser usado para documentar as informações acima, integrando o Plano de Gerenciamento de Riscos e Controles Internos (PGRCO) do órgão.

### PASSO 4: IDENTIFIQUE E ANALISE OS RISCOS

Definido o escopo do gerenciamento de riscos, a CGRCO, o gestor e a equipe técnica devem identificar os riscos dos processos selecionados. Para tal, orientamos o uso do anexo III.

A identificação dos riscos é o processo de busca, reconhecimento e descrição dos riscos que potencialmente possam vir a impactar negativamente no alcance dos objetivos organizacionais do órgão. Uma das técnicas utilizada nesta etapa é o Brainstorming<sup>5</sup>.

Os integrantes são incentivados a contribuir com o máximo possível com as ideias que conseguirem, sem prejulgamento.

Após a identificação do risco, deverão ser apontadas todas as suas causas e consequências significativas, associadas ao evento de risco identificado;

- Causa - é o motivo que pode promover a ocorrência do risco.
- Consequência - é o resultado de um evento que afeta os objetivos.

Os riscos identificados nesta etapa são os chamados riscos inerentes. São os riscos aos quais uma organização está exposta sem considerar quaisquer ações gerenciais (leia-se: controles internos) que possam reduzir a probabilidade da ocorrência ou impacto dos riscos.

#### **As categorias de riscos a ser utilizadas pelos órgãos, unidade e vice-presidência são no mínimo:**

- **Riscos operacionais:** eventos que podem comprometer as atividades do órgão específico singular ou da unidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.
- **Riscos financeiros/orçamentários:** eventos que podem comprometer a capacidade do órgão ou unidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.
- **Riscos de integridade:** eventos que possam favorecer a ocorrência de fraudes, atos de corrupção ou violações dos princípios de governança<sup>6</sup> comprometendo a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou unidade em

<sup>5</sup> Para conhecer outras técnicas consulte a ABNT NBR 31010 Gestão de Riscos – Técnicas para a avaliação de gestão de riscos.

<sup>6</sup> Saiba mais sobre os princípios da governança aqui <http://www.cgu.gov.br/noticias/2018/12/governo-federal-lanca-guia-sobre-a-politica-de-governanca-publica/guia-politica-governanca-publica.pdf>

cumprir sua missão institucional e entregar resultados. São “quebras de integridade” que desviam ou negam a finalidade pública ou do serviço público a ser entregue ao cidadão.

- **Riscos legais:** eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou unidade;
- **Riscos políticos:** eventos relacionados as ações ou reorientações de governo que poderiam vir a impactar políticas públicas de estado relacionadas a saúde, a ciência, tecnologia e inovação e consequentemente a sociedade o Sistema Único de Saúde (SUS)

Devem ser levantados também os riscos com baixa probabilidade, mas alto impacto caso ocorram, os chamados de “Cisnes Negros”.<sup>7</sup>

## PASSO 5: AVALIE OS RISCOS E OS CONTROLES INTERNOS

Com a lista dos riscos identificados, o próximo passo é quantificar o nível de risco inerente - o nível de riscos, sem considerar quaisquer controles internos realizados pelo órgão ou unidade que reduzem ou podem reduzir a probabilidade de sua ocorrência ou sem impacto e o risco residual, nível de risco considerando os controles internos realizados pelo órgão ou unidade.

Nesta etapa, são calculados os níveis dos riscos identificados pela CGRCO pela equipe técnica designada, a partir de critérios de probabilidade e impacto definidos.

Para cada um dos riscos da lista, considerando todas as informações coletadas nos passos anteriores e as descrições das escalas abaixo, escolha na escala a probabilidade e o impacto no qual o risco identificado melhor se enquadra. Os quadros 3 e 4 trazem as escalas de probabilidade e impacto, respectivamente, com os pesos para cada uma das descrições:

### Quadro 3 – Escala de Avaliação da Probabilidade do Risco identificado

Probabilidade				
Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias atuais indica essa possibilidade.	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	Possível. De alguma forma, o evento poderá até ocorrer, pois as circunstâncias indicam moderadamente esta possibilidade.	Provável. De forma até esperada o evento poderá ocorrer, pois as circunstâncias indicam fortemente esta possibilidade.	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente esta possibilidade.
1	2	5	8	10
<b>Muito baixa</b>	<b>Baixa</b>	<b>Média</b>	<b>Alta</b>	<b>Muito alta</b>

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) e Metodologia de Gestão de Riscos (CGU, 2018)

<sup>7</sup> Termo popularizado por Nassim Nicholas Taleb em seu livro “A lógica do cisne negro”. Acreditava-se, na Europa, que todos os cisnes eram brancos. Bastou a descoberta de um único cisne negro na Austrália para derrubar essa teoria. Acontecimentos de baixa probabilidade e alto impacto, praticamente impossíveis de prever, são comuns num sistema complexo, como o mundo atual.

#### Quadro 4 – Escala de Avaliação do Impacto do Risco identificado

Impacto				
Mínimo Impacto sobre os objetivos (estratégicos, operacionais, outros)	Pequeno impacto sobre os objetivos	Moderado impacto nos objetivos, porém recuperável.	Significativo Impacto nos objetivos, de difícil reversão.	Catastrófico impacto nos objetivos, de forma irreversível.
1	2	5	8	10
<b>Muito Baixo</b>	<b>Baixo</b>	<b>Médio</b>	<b>Alto</b>	<b>Muito alto</b>

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) e Metodologia de Gestão de Riscos (CGU, 2018)

O nível do risco inerente é expresso pela multiplicação entre a probabilidade de sua ocorrência e o impacto, em termos de possíveis consequências negativas aos objetivos organizacionais, da seguinte forma:

$$\text{NÍVEL DE RISCO INERENTE (RI)} = \text{NÍVEL DE PROBABILIDADE (NP)} \times \text{NÍVEL DE IMPACTO (NI)}$$

Após encontrar o resultado do cálculo, o risco pode ser identificado dentro das seguintes faixas:

#### Quadro 5 – Classificação do risco

Classificação	Faixa
<b>Risco Baixo</b>	<b>0 – 9,99</b>
<b>Risco Médio</b>	<b>10 – 39,99</b>
<b>Risco Alto</b>	<b>40 - 79,99</b>
<b>Risco Muito Alto/ Estratégico</b>	<b>80-100</b>

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) e Metodologia de Gestão de Riscos (CGU, 2018) adaptado.

Os possíveis resultados da combinação entre probabilidade e impacto são apresentados na matriz abaixo.

#### Quadro 6 – Matriz de Riscos

IMPACTO	Muito Alto 10	10 RM	20 RM	50 RA	80 RE	100 RE
	Alto 8	8 RB	16 RM	40 RA	64 RA	80 RE
	Médio 5	5 RB	10 RM	25 RM	40 RA	50 RA
	Baixo 2	2 RB	4 RB	10 RM	16 RM	20 RM
	Muito Baixo 1	1 RB	2 RB	5 RB	8 RB	10 RM
		<b>Muito Baixa 1</b>	<b>Baixa 2</b>	<b>Média 5</b>	<b>Alta 8</b>	<b>Muito Alta 10</b>
		<b>PROBABILIDADE</b>				

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) e Metodologia de Gestão de Riscos (CGU, 2018)

Avaliado o nível de risco inerente, a equipe deve avaliar o quanto os controles internos existentes têm auxiliado no tratamento do risco, em relação aos objetivos do processo organizacional.

**Quadro 7 – Escala de Avaliação da eficácia dos Controles Internos existentes**

Controles Internos				
Controles Inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	Controles têm abordagem ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	Controles implementados mitigam alguns aspectos do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	Controles implementados e sustentados por ferramentas adequadas e embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Controles implementados podem ser considerados a "melhor prática" mitigando todos os aspectos relevantes do risco
1	0,8	0,6	0,4	0,2
Inexistente	Fraco	Mediano	Satisfatório	Forte

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) e Metodologia de Gestão de Riscos (CGU, 2018)

O valor encontrado para o nível de risco inerente de cada risco, multiplicado pelo fator de avaliação dos controles internos existentes, corresponde ao nível de risco residual.

**NÍVEL DE RISCO RESIDUAL (RR) =**  
**NÍVEL DE RISCO INERENTE (RI) X FATOR DE AVALIAÇÃO DO CONTROLE (FC)**

A avaliação dos controles internos, pode fazer com que o risco inicialmente avaliado em uma determina faixa de classificação altere sua faixa.

**PASSO 6: PRIORIZE OS RISCOS**

Classificados os riscos residuais para cada um dos riscos identificados, deve ser definida a atitude do órgão ou unidade perante ao risco, priorizando-os para tratamento.

O quadro 8, define quais ações devem ser adotadas em relação a classificação dos riscos e suas exceções

**Quadro 8- Atitude perante ao Risco Residual**

Classificação	Ação necessária	Exceção
Risco Baixo	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pelo órgão ou unidade e aprovada pelo seu Diretor e CD do órgão.
Risco Médio	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é	Caso o risco seja priorizado para implementação de medidas de

	necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo, sem custos adicionais.	tratamento, essa priorização deve ser justificada pelo órgão ou unidade e aprovada pelo seu Diretor e CD do órgão.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo do órgão ou unidade	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo órgão ou unidade e aprovada pelo seu Diretor e CD Fiocruz.
Risco Muito Alto/Estratégico	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser objeto de Avaliação Estratégica da Executiva Técnica (Parecer) , após comunicado ao CD Fiocruz e ao dirigente máximo do órgão ou unidade e ter uma resposta imediata. Postergação de medidas só com autorização do CD Fiocruz	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo órgão ou unidade e aprovada pelo seu Diretor e CD Fiocruz.

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) e Metodologia de Gestão de Riscos (CGU, 2018) adaptado.

Portanto, dadas as exceções que devem ser justificadas, os riscos classificados como muito alto/estratégicos e altos pelos órgãos, unidade e vice-presidências são os prioritários para tratamento.

## PASSO 7: DEFINA AS AÇÕES E O PLANO DE TRATAMENTO DOS RISCOS

Priorizados os riscos, a equipe deve definir as ações de tratamento com base no Anexo VI. Ao definir as ações do plano de tratamento é importante realizar uma análise do custo-benefício das medidas/controles em relação a sua aplicabilidade, bem como os benefícios que poderão ser agregados ao processo. Nem sempre o custo financeiro da implementação de uma ação poderá ser maior do que o valor do processo, atividade ou objeto analisado na instituição.

As opções de tratamento são as seguintes.

- **Mitigar:** um risco normalmente é mitigado quando classificado como muito alto/estratégico ou alto pelo órgão, unidade e vice-presidência. A implementação de controles, neste caso, apresenta um custo/benefício adequado. Mitigar riscos significa implementar controles internos que diminuam as causas ou consequências dos riscos, identificadas no passo 4 de identificação e análise dos riscos.
- **Compartilhar/Transferir:** Um risco normalmente é compartilhado quando é classificado como Alto ou Muito Alto/Estratégico, mas a implementação de controles não apresenta um custo/benefício adequado. Na Fiocruz, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
- **Evitar:** Um risco normalmente é evitado quando é classificado como Alto ou Muito Alto/ Estratégico, e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a Fiocruz. Na Fiocruz, evitar o risco significa encerrar ou alterar o processo ou serviço. Nesse caso, essa opção deve ser aprovada pelo CD da Fiocruz.
- **Aceitar:** Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco. Pois sua probabilidade e impacto são tão baixos que não justificam a criação de controles para mitigação, ou os controles existentes já resguardam boa parte de suas consequências.

Caso as opções de tratamento sejam mitigar, compartilhar ou evitar devem ser definidas medidas de tratamento para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou mais próximo possível das faixas de apetite a risco (risco “Baixo” ou “Médio”).

O Plano de Tratamento gerado pelo processo de gerenciamento de riscos do processo organizacional é um plano de ação para a implementação das medidas de tratamento dos riscos desse processo organizacional e deve conter todos os itens previstos no anexo III.

## **PASSO 8 – VALIDE OS RESULTADOS DO GERENCIAMENTO DOS RISCOS**

As CGRCO devem apresentar o Plano de Gerenciamento dos Riscos e Controles Internos para os gestores e aprová-lo em sessão do CD do órgão.

**Após a aprovação dos resultados o coordenador do CGRCI ou Diretor do órgão específico singular ou unidade deve:**

- **Encaminhar o PGRCI completo digitalizado junto com as cópias das atas da sessão do CD que aprovou o plano para gestaoderiscos@fiocruz.br, até 31 de maio de 2019; e**
- **Encaminhar o plano de tratamento de riscos para as áreas co-responsáveis;**

## **PASSO 9: IMPLANTE E MONITORE O PLANO DE TRATAMENTO DOS RISCOS**

A implementação do PGRCI envolve a participação do CGRCO, da área organizacional responsável pelos processos organizacionais priorizados e das áreas corresponsáveis em cada ação prevista no plano.

Cabe ao coordenador(a) da CGRCO monitorar e reportar a evolução das iniciativas ao Diretor do órgão, unidade ou Vice-Presidente. A responsabilidade primária permanece com o responsável pelo processo priorizado e em última instância pelo Diretor do órgão, unidade ou Vice-Presidente.

Em relação ao risco, devem ser monitoradas e analisadas criticamente, de forma regular, as seguintes mudanças:

- Um determinado contexto sofreu alteração;
- A probabilidade de um evento negativo era baixa e agora é alta;
- Um risco que era aceito, agora será tratado
- Surgimento de novos riscos.

A fase de monitoramento contínuo também é responsável por garantir:

- Se o tratamento do risco está sendo realizado conforme planejado;
- Se foram realizadas alterações no contexto;
- Se as ações implementadas estão sendo eficazes na redução dos riscos encontrados;
- A Gestão de Riscos está sendo realizado de forma adequada.

**Após a aprovação dos resultados de monitoramento o coordenador do CGRCO ou Diretor do órgão ou unidade ou vice-presidente deve:**

- Encaminhar o relatório conforme anexo I até o último dia dos meses de junho e dezembro de 2019 para a VPGDI.

## **PASSO 10: COMUNIQUE OS RISCOS**

A comunicação do risco é uma etapa que deve ocorrer paralelamente a todo o processo de Gerenciamento de Riscos. Deve haver uma troca interativa, formalmente documentada, intencional e contínua, de conhecimentos, informações e percepções sobre os riscos que devem ser gerenciados. Através desta etapa devem ser transmitidas as informações sobre o desenvolvimento das atividades, modificações no contexto e os resultados alcançados as partes interessadas e com base na matriz de responsabilidades.

O CGRGO deve comunicar semestralmente ao CD do órgão e anualmente para todo o órgão específico e unidade os resultados do monitoramento da gestão de riscos.

Mudanças identificadas durante o monitoramento devem ser encaminhadas a UGI e Executiva Técnica, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos já realizados nos processos organizacionais da Fiocruz

Semestralmente, o Executiva Técnica produzirá um boletim com o resultado do acompanhamento das ações relacionadas ao Plano de Gestão de Riscos de cada unidade, que será enviado ao CD Fiocruz.

Além disso, a Executiva Técnica e a UGI elaborarão o Relatório de Monitoramento da Gestão de Riscos da Fiocruz com a consolidação desses resultados, que deve ser encaminhado, no mínimo, uma vez por ano ao CD Fiocruz.

## **6. PROTEÇÃO INFORMAÇÃO**

As informações sobre o gerenciamento de riscos são documentos preparatórios que serve para fundamentar tomada de decisão futura, portanto informação estratégica e de caráter reservado.

A Lei de Acesso a Informação (LAI) não proíbe a entrega deste tipo de documento, mas garante o seu acesso após a edição do ato relativo à tomada de decisão que os utilizou como fundamento. Entende-se, portanto, haver relativa discricionariedade da Administração ao conceder acesso a tais documentos antes que o processo de tomada de decisão seja concluído.

Desta forma, a negativa de acesso é discricionária e deverá estar acompanhada da justificativa sobre o prejuízo que a publicidade da informação solicitada poderá causar à efetividade da decisão futura fundamentada no art. 7 parágrafo 3º da LAI ( Lei nº 12.527/2011) e no art. 3º inciso XII do Decreto nº 7.724/12.

## **7. CAPACITAÇÃO**

Será lançado um plano de capacitação pela Escola Corporativa em breve.

Entretanto, não é necessário aguardar esta divulgação pois todas as dúvidas devem ser sanadas por meio da secretaria executiva da Executiva Técnica.

Orientamos que os órgãos e unidades realizem os cursos on line e gratuitos sobre gestão de riscos e controles internos disponíveis nos seguintes sites:

<https://www.escolavirtual.gov.br/>

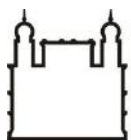
<https://www.enap.gov.br>

<https://portal.tcu.gov.br/educacao-corporativa/>

<https://ead.cgu.gov.br/>



ANEXO I – MODELO DO RELATORIO SEMESTRAL DOS COMITÊS DE GERENCIAMENTO DE RISCO E CONTROLES INTERNOS DOS ÓRGÃOS DA FIOCRUZ



Ministério da Saúde

FIOCRUZ

**Fundação Oswaldo Cruz**

Nome do Órgão Singular, unidade ou vice-presidência	
Nome do Coordenado(a) do Comitê de Gestão de Riscos e Controles Internos	
Nome do Secretário(a) Executivo(a) do Comitê	

Atividades de Gerenciamento de Risco e Supervisão de Risco

1. Reuniões do Conselho de Gestão de Risco e Controles Internos (Datas da última reunião / próxima reunião e ações significativas surgidas também em relação a disseminação de boas práticas para a mudança de cultura)

--

2. Riscos Identificados como alto ou muito altos e plano de ação para estabelecimentos de controles internos (especificar também os relatórios utilizados no processo de identificação de riscos)

--

3. Reunião do Conselho Deliberativo do órgão em que foi discutido e aprovado do Plano de Gerenciamento de Riscos e principais posicionamentos e recomendações dos membros

--

4. Atividades de Gerenciamento de Riscos (por exemplo, como é realizado o monitoramento e comunicação dos riscos, riscos novos ou emergentes, etc.)

5. Resumo dos principais problemas e violações / violações da conformidade (política, requisitos regulamentares / setoriais)

6. Mudanças legislativas ou normativas significativas que impactaram os processos e projetos do órgão e as relacionadas ao cumprimento / mudanças nas atividades do governo (incluindo inspeções). Explicitar se houveram ações proativas do órgão para a melhoria das leis em elaboração que impactam seus processos e projetos.

7. Iniciativas e aprimoramentos significativos de conformidade (por exemplo, funções-chave recrutadas, principais programas de treinamento nos processos estratégicos e de apoio)

8. Diversos (Outras atividades dignas de nota, incluindo a participação em conferências externas)

--

Assinaturas

Coordenador(a) do Comitê de Gestão de Riscos e Controle Interno

Diretor(a) do Órgão Singular ou unidade ou Vice-Presidente

## ANEXO II – Estudo do Processo Institucional

<b>Tese:</b>	
<b>Diretriz:</b>	
<b>Macroprocesso:</b>	
<b>Nome do Processo:</b>	
<b>Objetivos Estratégicos da Fiocruz alcançados pelo processo:</b>	
<b>Objetivo(s) do processo:</b>	
<b>Leis e normas aplicáveis</b> <b>Matriz SWOT</b> <b>Responsável pelo gerenciamento do processo:</b>	

Nota: Acrescentar fluxo mapeado do processo

ANEXO III – Planilha de Identificação e avaliação dos riscos e controles internos

Área	Processo	Causas	Eventos / Riscos	Consequências / Impactos	Descrição do Risco	Nível de Risco Inerente	Controles Existentes	Avaliação dos Controles Existentes	Nível de Risco Residual	Tipo de Tratamento
Gestão de Pessoas	Gestão de Conflitos	Diferenças entre as gerações e na formação impactam no entendimento do que é gerir atividades públicas Tensões resultantes de reivindicações Disputas políticas fruto do processo eleitoral interno Disputas dos recursos escassos Disputas dos espaços de liderança e DASs Abuso de poder	Assédio moral e sexual	Piora do clima organizacional Queda de produtividade Inassiduidade no trabalho aumento da solicitação de remoção e dos afastamentos Alteração do comportamento com consequente queda de desempenho individual Adoecimento da força de trabalho Custos para tratamento e reabilitação da saúde	A inabilidade na gestão de conflitos por parte dos gestores pode escalonar conflitos em formas mais graves de violência como o assédio moral e sexual.	MUITO ALTO Probabilidade (8) X Impacto (8) = 64	Política de prevenção e enfrentamento do assédio moral por sistema de acolhimento multiportas divulgadas por meio de Cartilha, pela Comissão criada para este fim ( Portaria PR 340/2013)	Satisfatório (0,4) Controles implementados e sustentados por ferramentas adequadas e embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	MÉDIO 64 x 0,4 = 25,6	MITIGAR

**ANEXO IV – Plano de tratamento dos Riscos**

Medidas de Tratamento	Ação	Responsável	Áreas Co-Responsáveis	Prazo	Situação	Custo estimado
Programa de Desenvolvimento de Líderes - teoria e prática da gestão de conflitos	Aperfeiçoar o conteúdo prático dos cursos de gestão de conflitos, com base nos casos reais tratados pela Ouvidoria, anonimizados simulando como o gestão trataria aquele conflito para evitar escalonamento e fortalecer ações junto aos gestores em período de transição de Direção e pós eleitoral	Coordenadora da COGEPE	Escola Corporativa e UGI	Atividade contínua	Em andamento	

## ANEXO V - Matriz de Responsabilidades no Processo de Gestão de Riscos na Fiocruz

Instâncias	CD Fiocruz	Câmara Técnica de Gestão	Executiva Técnica	Assessoria Executiva VPGDI	Comitê do órgão específico singular ou unidade	CD do órgão específico singular ou unidade	Diretor do órgão ou unidade	Gestor do processo	Responsável pela implementação da ação de tratamento	Servidores e demais trabalhadores do órgão ou unidade
<b>Ações</b>										
Definir plano de gestão de riscos e controles internos do órgão					R		A	R	C	I
Definir metodologia de gestão de riscos	A	C	A	R						I
Selecionar processos organizacionais										I
Realizar entendimento do contexto					R					C
Realizar identificação de análise de riscos					R			C		C
Realizar a avaliação dos riscos					R			C		C
Realizar a priorização dos riscos					R			C		I
Realizar a definição de respostas aos riscos					R			C		I
Validar os riscos levantados					R	A		C		I
Implementar o plano de tratamento					R		A	A	R	I
Monitorar a implementação do plano de tratamento			R		R			A	R	I
Definir Apetite de Risco Corporativo	A					A		C		C
Aprovar o plano de gestão de riscos e controles internos corporativo	A					C		C		I
Realizar avaliação estratégica corporativa	A		R							I

R - Responsável: quem executa a atividade.

A - Autoridade: quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade.

C - Consultado: quem pode agregar valor ou é essencial para a implementação.

I - Informado: quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

## ANEXO VI – Método para a avaliação de processos

### AVALIAÇÃO QUANTITATIVA

Deve ser realizada com base em três critérios: Materialidade, Recursos Humanos e Recursos Tecnológicos.

**Materialidade - é o valor de referência definido para avaliar a relevância da previsão orçamentária do processo.**

O critério de materialidade é verificando qual o percentual de recursos orçamentários que o processo mobiliza considerando o volume total do orçamento previsto para o órgão. A partir do percentual mobilizado, sendo o valor maior ou menor a 20% de recursos atribui-se nota de 1 a 3, conforme abaixo.

Níveis de Materialidade	Nota
>ou = a 20% do orçamento do órgão ou unidade ou vice-presidência	3
>ou = 10% < 20% do orçamento do órgão ou unidade ou vice-presidência	2
< ou = 10% do orçamento do órgão ou unidade ou vice-presidência	1

**Recursos Humanos (qualificação técnica) - valor atribuído ao grau de dependência de servidores com qualificação técnica específica para a execução do processo.**

Ao critério de Recursos Humanos podem ser atribuídos os valores:

Níveis de dependência de RH	Nota
A execução do processo é totalmente depende de servidores com qualificação técnica específica	3
A execução do processo é parcialmente depende de servidores com qualificação técnica específica	2
A execução do processo não depende de servidores com qualificação técnica específica	1



**Recursos Tecnológicos (qualificação técnica) - valor atribuído ao grau de dependência de recursos tecnológicos para a execução do processo.**

Ao critério de Recursos Tecnológicos podem ser atribuídos os valores:

<b>Níveis de dependência de RH</b>	<b>Nota</b>
A execução do processo é totalmente dependente de recursos tecnológicos.	<b>3</b>
A execução do processo é parcialmente depende de dependente de recursos tecnológicos.	<b>2</b>
A execução do processo não depende dependente de recursos tecnológicos.	<b>1</b>

**A nota final da AVALIAÇÃO QUANTITATIVA será a média aritmética<sup>8</sup> simples das notas obtidas nos três critérios acima.**

A depender do nível de maturidade do órgão ou unidade ou vice-presidência poderão ser atribuídos pesos para cada um dos critérios, com justificativa. Neste caso a nota final deverá ser a média aritmética ponderada das notas dos três critérios acima.

**AVALIAÇÃO QUALITATIVA**

Deve ser realizada com base em sete critérios: Processo Estratégico, Demandas dos Tribunais de Contas da União (TCU), Demandas do Ministério da Transparência e Controladoria Geral da União (CGU), Relevância do Processo, Valores não-Orçamentários, Reclamações Registradas na Ouvidoria

***Processo Estratégico - processo objeto de análise está vinculado ou não as diretrizes estratégicas do órgão e da Fiocruz.***

Ao critério podem ser atribuídos os valores:

<b>Níveis</b>	<b>Nota</b>
Processo vinculado aos objetivos de contribuição do órgão, unidade ou vice-presidência ao alcance dos objetivos, diretrizes estratégicas e teses da Fiocruz	<b>3</b>
Processo não vinculado aos objetivos de contribuição do órgão, unidade ou vice-presidência ao alcance dos objetivos, diretrizes estratégicas e teses da Fiocruz	<b>1</b>

<sup>8</sup> Cálculo da média aritmética simples -  $M = \frac{C_1 + C_2 + C_3}{n}$  Onde Ms: média aritmética simples; c1+c2+c3: valores encontrados para cada um dos critérios; e n: número de critérios

***Demandas do TCU - processo objeto de análise possui ou não apontamentos do TCU.***

Ao critério podem ser atribuídos os valores:

<b>Níveis</b>	<b>Nota</b>
Existe determinação e recomendação do TCU ao processo.	3
Existe recomendação do TCU ao processo.	2
Não existe recomendação ou determinação do TCU ao processo.	1

***Demandas do CGU - processo objeto de análise possui ou não apontamentos do CGU.***

Ao critério podem ser atribuídos os valores:

<b>Níveis</b>	<b>Nota</b>
Existe recomendação do CGU ao processo vencida e a vencer.	3
Existe recomendação do CGU ao processo a vencer.	2
Não existe recomendação do CGU ao processo.	1

***Relevância do Processo - processo objeto de análise trata-se ou não de processo finalístico.***

Ao critério podem ser atribuídos os valores:

<b>Níveis</b>	<b>Nota</b>
Trata-se de processo finalístico	3
Trata-se de processo de apoio.	1

***Valores não orçamentários - processo objeto de análise possui ou não possui recursos não orçamentários para sua execução.***

Ao critério podem ser atribuídos os valores:

<b>Níveis</b>	<b>Nota</b>
Processo com recursos não orçamentários	3
Processo sem recursos não orçamentários	1

***Reclamações registradas na Ouvidoria - processo objeto de análise possui ou não reclamação registrada na ouvidoria.***

Ao critério podem ser atribuídos os valores:

<b>Níveis</b>	<b>Nota</b>
Existe registro de reclamação registrada na Ouvidoria	3
Não existe registro de reclamação registrada na Ouvidoria	1

**A nota final da AVALIAÇÃO QUALITATIVA será a média aritmética simples das notas obtidas nos três critérios acima.**

A depender do nível de maturidade do órgão ou unidade ou vice-presidência poderão ser atribuídos pesos para cada um dos critérios, com justificativa. Neste caso a nota final deverá ser a média aritmética ponderada das notas dos três critérios acima.