



Universidade
Federal
Fluminense



PLANO DE GESTÃO DE RISCOS 2026-2027

PRÓ REITORIA DE PLANEJAMENTO

COORDENAÇÃO DE PLANEJAMENTO E DESENVOLVIMENTO

DIVISÃO DE ACOMPANHAMENTO DE PROGRAMAS INSTITUCIONAIS

NITERÓI - RJ

1. Apresentação.....	4
2. Objetivo.....	4
3. Papéis e responsabilidades.....	5
4 . Estrutura da gestão de riscos na UFF.....	9
5. Identificação dos riscos.....	10
Riscos associados aos objetivos estratégicos.....	10
Riscos organizacionais.....	11
Riscos de Integridade.....	11
Riscos relacionados à proteção de dados pessoais (LGPD).....	12
Metodologia.....	12
Tipologia e origem dos riscos.....	15
CLASSIFICAÇÃO DO RISCO:.....	18
MATRIZ DE RISCOS.....	19
Priorização dos riscos.....	20
Análise de risco inerente e residual.....	20
Apetite a Risco.....	22
Opções de tratamento.....	22
PLANO DE AÇÃO.....	23
Validação e acompanhamento.....	23
6. Planejamento da Gestão de Riscos (2026/2027).....	25
7 . Considerações finais.....	26
8 . Referências bibliográficas.....	27
ANEXO I.....	28

Reitor

Antonio Claudio Lucas da Nóbrega

Pró-Reitor de Planejamento

Julio Cesar Andrade de Abreu

Organização e Execução**Equipe PLAD**

Coordenadora: Maria Leonor Veiga Faria

Angela Rocha Martins

Layana Nogueira Teixeira

Pamella Macedo Drummond

Vanessa Sol da S. Valle

1. Apresentação

O Plano de Gestão de Riscos (PGR) da Universidade Federal Fluminense (UFF) estabelece a metodologia, os procedimentos e as responsabilidades para a implementação da gestão de riscos no âmbito institucional, em conformidade com a Instrução Normativa Conjunta nº 01/MP/CGU/2016, o Decreto nº 9.203/2017 e a Política de Gestão de Riscos da UFF.

A gestão de riscos da UFF está estruturada em três instrumentos complementares: a Política de Gestão de Riscos, que define diretrizes e princípios; o Plano de Gestão de Riscos, que detalha a operacionalização, e o Relatório de Gestão de Riscos, destinado ao monitoramento e à avaliação das ações implementadas.

Este Plano estabelece a metodologia, define os papéis e responsabilidades dos atores envolvidos e apresenta os mecanismos de identificação, análise, avaliação, priorização, tratamento e monitoramento dos riscos.

A iniciativa está alinhada ao Plano de Desenvolvimento Institucional (PDI), especialmente no eixo de Governança e Gestão, que prevê a ampliação das ações de gestão de riscos e integridade na UFF.

A adoção da gestão de riscos contribui para o fortalecimento da governança institucional, ao apoiar a tomada de decisão, aprimorar os controles internos e aumentar a capacidade da Universidade de alcançar seus objetivos estratégicos com eficiência, eficácia e transparência.

2. Objetivo

Estabelecer a metodologia, os procedimentos, as responsabilidades e os instrumentos necessários para a implementação da gestão de riscos na UFF, de forma sistemática e contínua, apoiando a tomada de decisão e contribuindo para o alcance dos objetivos estratégicos.

3. Papéis e responsabilidades

Para a efetiva implementação da gestão de riscos na UFF, são estabelecidos os seguintes papéis e responsabilidades:



Figura 1: Pirâmide – Papéis e responsabilidades

I - Comitê de Governança, Integridade, Riscos e Controles - CGIRC (Portaria nº 68.259/2021):

- Aprovar políticas, diretrizes, metodologias e mecanismos relacionados à gestão de riscos, integridade e controles internos;
- Aprovar o método de priorização de temas, processos e macroprocessos para gerenciamento de riscos;
- Definir as prioridades institucionais para o gerenciamento de riscos.

II - Coordenação de Planejamento e Desenvolvimento (PLAD/PROPLAN)

- Elaborar e propor o Plano de Gestão de Riscos e suas atualizações;
- Fornecer metodologias, ferramentas e orientações em geral para apoiar os

gestores da 1ª linha de defesa na identificação e avaliação dos riscos;

- Propor e promover ações de capacitação em gestão de riscos, em articulação com a Escola de Governança em Gestão Pública da UFF (EGGP/PROGEPE/UFF), no âmbito de suas competências, destinadas aos responsáveis pela gestão de riscos, gestores e demais servidores da UFF;
- Apoiar os gestores (1ª linha) na identificação, análise e avaliação dos riscos dos processos organizacionais selecionados;
- Apoiar os gestores (1ª linha) na implementação e no monitoramento dos controles internos destinados a mitigar os riscos identificados;
- Requisitar aos responsáveis pela gestão de riscos as informações necessárias à consolidação dos dados e à elaboração de relatórios gerenciais;
- Consolidar as informações provenientes das diversas áreas em relatórios gerenciais e encaminhá-los ao CGIRC;
- Assegurar a disponibilização de informações sobre riscos em todos os níveis da Instituição.

III - Gestor de riscos (Pró-reitores, superintendentes e diretores de unidades acadêmicas e administrativas):

- Promover o fortalecimento contínuo do ambiente de gestão de riscos em sua unidade;
- Indicar os processos prioritários para a gestão de riscos;
- Validar e monitorar, no seu âmbito de atuação, a execução do Plano de Gestão de Riscos e das iniciativas decorrentes da sua implementação;
- Manter atualizadas as informações relativas à gestão de riscos em sua unidade;
- Acompanhar os riscos mapeados e reportar informações à PLAD/PROPLAN;

- Designar formalmente o Gerente de Riscos da unidade e a equipe técnica envolvida, assegurando que os designados possuam conhecimento adequado sobre o objeto de análise (objetivo estratégico ou processo);
- Garantir a implementação das ações de tratamento e dos controles definidos para os riscos sob sua responsabilidade;
- Monitorar continuamente os riscos da unidade, avaliando a efetividade das medidas adotadas e assegurando sua manutenção em níveis adequados;
- Comunicar à PLAD/PROPLAN e ao CGIRC a ocorrência de situações relevantes ou alterações que possam impactar a gestão de riscos;
- Promover a integração da gestão de riscos aos processos de planejamento e gestão da unidade, especialmente ao Plano de Desenvolvimento da Unidade (PDU).
- Aprovar e acompanhar a execução dos Planos de Ação relativos aos riscos sob sua responsabilidade.

IV - Gerente de riscos

- Conduzir a identificação, análise e avaliação dos riscos, em conformidade com a Política e a metodologia de gestão de riscos da UFF;
- Apoiar os gestores na definição e na implementação de medidas de tratamento e controles para os riscos identificados;
- Identificar e comunicar, no seu âmbito de atuação, situações que possam representar riscos;
- Monitorar os níveis de risco e avaliar a efetividade dos controles adotados;
- Manter a PLAD/PROPLAN informada sobre alterações relevantes nos processos e nos riscos associados;
- Atender às demandas de informação e reporte relacionadas à gestão de

riscos;

- Assegurar a atualização das informações no sistema de gestão de riscos;
- Disponibilizar informações sobre riscos às partes interessadas, observadas as normas de sigilo e classificação da informação.
- Apoiar os gestores na elaboração e na atualização dos Planos de Ação relativos aos riscos sob sua responsabilidade;

V - Proprietário do risco:

- Contribuir para a identificação, análise e avaliação dos riscos dos processos sob sua responsabilidade;
- Comunicar tempestivamente ao Gestor de Riscos a ocorrência de eventos de risco ou mudanças relevantes nos processos;
- Executar as ações de tratamento dos riscos sob sua responsabilidade;
- Registrar e manter atualizadas as informações relacionadas aos riscos e às ações de tratamento nos sistemas institucionais;
- Elaborar informações e relatórios para subsidiar o monitoramento dos riscos.

Cabe a todos os servidores, no âmbito de suas atribuições, contribuir para a identificação e avaliação dos riscos inerentes aos processos sob sua responsabilidade, comunicar tempestivamente a ocorrência de eventos de risco, inclusive aqueles ainda não mapeados, e apoiar os gestores na definição e implementação de planos de ação para o tratamento dos riscos.

Caberá a cada unidade da UFF atuar, em articulação com a PLAD/PROPLAN, na elaboração e no monitoramento do Plano de Gestão de Riscos, a partir da identificação e análise dos riscos associados aos processos organizacionais sob sua responsabilidade.

Destaca-se que, conforme o objetivo estratégico ou processo organizacional em análise, poderão ser designadas equipes específicas para atuação na gestão de riscos. Nos casos relacionados a objetivos estratégicos, recomenda-se que a equipe seja composta por membros com responsabilidade direta sobre as respectivas ações estratégicas.

4 . Estrutura da gestão de riscos na UFF

A estrutura da gestão de riscos da UFF está baseada no modelo de três linhas de defesa, no qual os diferentes atores exercem papéis complementares na gestão de riscos e controles internos.

1ª Linha de defesa: Operacionalização

Gestores: responsáveis pela execução dos controles internos no âmbito dos processos sob sua responsabilidade, com o apoio técnico dos servidores, respondendo pela gestão dos riscos nas atividades operacionais.



2ª Linha de defesa: Supervisão e monitoramento

Comitê de Governança, Integridade, Riscos e Controles Da UFF (CGIRC): responsável por definir diretrizes e deliberar sobre políticas, estratégias e planos de ação relacionados à governança, gestão de riscos, controles internos e integridade.

Coordenação de Planejamento e Desenvolvimento

(PLAD/PROPLAN): responsável pela supervisão, acompanhamento, suporte e coordenação das atividades de implementação da Política de Gestão de Riscos da UFF.

3ª Linha de defesa:

Auditoria Técnica (AT/CUR): responsável por avaliar a efetividade dos controles internos, bem como a atuação da primeira e da segunda linhas de defesa.

A gestão de riscos deve ser integrada aos processos organizacionais e à governança institucional.

5. Identificação dos riscos

A implementação da gestão de riscos na UFF vem sendo realizada de forma progressiva, abrangendo as áreas administrativas e acadêmicas. Este Plano de Gestão de Riscos, com vigência no período de 2026 a 2027, tem como finalidade integrar a gestão de riscos aos objetivos institucionais e aos principais elementos da atuação da Universidade, tais como programas, processos, projetos e atividades, priorizando ações ao longo desse período.

Nesse contexto, até 2025, a gestão de riscos na UFF estava estruturada em três áreas principais: **objetivos estratégicos** delineados no Plano de Desenvolvimento Institucional (PDI), **processos organizacionais** e **integridade**.

A partir deste Plano, passa-se a incorporar, de forma explícita, os riscos relacionados à **proteção de dados pessoais**, os quais possuem natureza transversal e devem ser considerados no âmbito das demais categorias de risco.

Riscos associados aos objetivos estratégicos

A gestão de riscos estratégicos tem como finalidade apoiar a tomada de decisão e o planejamento institucional, por meio da identificação, análise e tratamento dos riscos que possam impactar o alcance dos objetivos definidos no Plano de Desenvolvimento Institucional (PDI).

Essa abordagem considera eventos que possam comprometer ou potencializar o alcance dos objetivos estratégicos e da visão de futuro da Universidade, devendo estar alinhada ao PDI vigente e aos demais instrumentos de planejamento institucional.

A priorização dos objetivos estratégicos a serem trabalhados deverá considerar critérios de relevância e criticidade, sendo subsidiada pela PLAD/PROPLAN, com base em informações fornecidas pelas unidades e nas análises institucionais relacionadas ao PDI, e submetida à aprovação do Comitê de Governança, Integridade, Riscos e Controles (CGIRC), cabendo à PLAD/PROPLAN o seu monitoramento.

Compete ao CGIRC indicar os responsáveis pelos riscos associados aos objetivos estratégicos, cabendo a estes a definição das equipes e a condução das atividades de identificação, análise e tratamento dos riscos.

Riscos organizacionais

A gestão de riscos nos processos organizacionais tem por objetivo aprimorar o desempenho institucional, por meio da identificação e tratamento de eventos que possam comprometer a execução das atividades da Universidade.

A seleção dos processos a serem priorizados deverá considerar sua relevância para o cumprimento da missão institucional e para o alcance dos objetivos estratégicos.

Cada unidade deverá identificar os processos sob sua responsabilidade que contribuem para esses objetivos, bem como os respectivos riscos associados, com o apoio metodológico da PLAD/PROPLAN. Essa atividade deverá ser conduzida pelos gestores e equipes técnicas responsáveis pelos processos. Recomenda-se a priorização dos processos mais críticos, sem prejuízo da autonomia das unidades para gerenciar outros riscos considerados relevantes.

Riscos de Integridade

A gestão de riscos de integridade consiste na identificação e no tratamento de vulnerabilidades que possam favorecer a ocorrência de fraudes e atos de corrupção, conforme diretrizes da Controladoria-Geral da União (CGU).

Entre os principais riscos de integridade, destacam-se:

- abuso de posição ou poder em favor de interesses privados;
- nepotismo;
- conflito de interesses;
- pressão interna ou externa ilegal ou antiética para influenciar agente público;
- solicitação ou recebimento de vantagem indevida;
- utilização de recursos públicos em favor de interesses privados.

Esses riscos podem impactar diretamente o cumprimento dos objetivos institucionais e, frequentemente, estão associados a outros tipos de risco, como operacionais, financeiros e de imagem.

Na UFF, o tratamento dos riscos de integridade está integrado ao Programa e Plano de Integridade.

Riscos relacionados à proteção de dados pessoais (LGPD)

Os riscos relacionados à proteção de dados pessoais devem ser considerados no âmbito dos riscos organizacionais e estratégicos, especialmente quanto aos aspectos legais, operacionais e de integridade, em conformidade com a Lei nº 13.709/2018 (LGPD).

A gestão desses riscos deve observar, quando aplicável, as diretrizes e recomendações constantes do Relatório de Impacto à Proteção de Dados da UFF (RIPD).

Na avaliação dos riscos, devem ser considerados os possíveis impactos aos titulares dos dados, incluindo violações de confidencialidade, integridade e disponibilidade das informações, bem como outros efeitos decorrentes de tratamento inadequado ou ilícito de dados pessoais.

Metodologia

A metodologia de gestão de riscos da UFF tem por finalidade estabelecer as etapas para a operacionalização da gestão de riscos no âmbito institucional, estando alinhada à ABNT NBR ISO 31000 e às diretrizes da Controladoria-Geral da União (CGU).

O processo de gestão de riscos compreende as seguintes etapas:

- I. **Entendimento do contexto:** etapa em que são definidos os contextos interno e externo, bem como identificados os objetivos relacionados aos processos organizacionais;
- II. **Identificação dos riscos:** etapa em que são identificados os eventos de risco que podem impactar o alcance dos objetivos;
- III. **Análise dos riscos:** etapa em que são examinadas as causas e as possíveis consequências dos riscos identificados;
- IV. **Avaliação e priorização dos riscos:** etapa em que são estimados os níveis de risco, com base na probabilidade de ocorrência e no impacto, e definidos os riscos que demandam tratamento prioritário.
- V. **Tratamento dos riscos:** etapa em que são definidas as respostas aos riscos e as respectivas medidas de controle;
- VI. **Comunicação e monitoramento:** etapa contínua, realizada ao longo de todo o processo, responsável pela disseminação de informações e pelo acompanhamento dos riscos e das ações implementadas.

A figura a seguir representa o fluxo do processo de gestão de riscos adotado pela UFF:



Figura 2: Processo de Gestão de Riscos da ISO 31000(ABNT,2009) – Adaptado

1 ESTABELECIMENTO DO CONTEXTO

O **entendimento do contexto** consiste na análise dos ambientes interno e externo nos quais a UFF atua, com o objetivo de identificar fatores que possam influenciar o alcance dos objetivos institucionais.

O **contexto interno** abrange a estrutura de governança, a organização institucional, as atribuições e responsabilidades, os recursos disponíveis, os processos de trabalho, os fluxos de informação, a cultura organizacional e as diretrizes institucionais.

O **contexto externo** compreende fatores políticos, legais, regulatórios, econômicos, sociais e tecnológicos, bem como as relações com as partes interessadas externas e suas expectativas.

Essa etapa tem como finalidade compreender o objeto de análise, seja um objetivo estratégico ou um processo organizacional, e estabelecer uma base adequada para a identificação dos riscos.

A identificação dos riscos consiste em reconhecer e descrever os eventos que possam impactar o alcance dos objetivos definidos na etapa anterior, incluindo suas possíveis causas e consequências.

Essa etapa envolve a identificação das fontes de risco, dos eventos associados e dos efeitos potenciais sobre os objetivos analisados.

A equipe responsável deverá identificar, de forma abrangente, os eventos que possam comprometer o alcance dos objetivos do processo ou do objetivo estratégico, considerando situações que possam impedir, dificultar ou atrasar sua realização.

Como apoio à identificação dos riscos, podem ser utilizadas questões orientadoras, tais como:

Quais eventos podem impactar negativamente o alcance dos objetivos institucionais ou do processo analisado?

Na identificação dos riscos, deve-se considerar a tipologia de riscos adotada pela UFF, conforme apresentado no Quadro a seguir.

Tipologia e origem dos riscos

Tipologia de risco	Descrição	Exemplos
Estratégico	Riscos que impactam o alcance dos objetivos estratégicos da instituição.	Planejamento inadequado, mudanças no ambiente externo, falhas na definição de prioridades.
Operacional	Riscos relacionados a falhas, deficiências ou inadequações em processos, pessoas, sistemas ou infraestrutura.	Erros de execução, falhas de sistemas, insuficiência de pessoal, processos mal definidos.

Legal/ Regulatório	Riscos decorrentes do descumprimento de leis, normas ou regulamentos aplicáveis.	Não conformidade com legislação, mudanças normativas, falhas em contratos.
Integridade	Riscos relacionados a fraudes, corrupção ou desvios éticos.	Conflito de interesses, nepotismo, uso indevido de recursos, favorecimento indevido.
Financeiro/ Orçamentário	Riscos que afetam a disponibilidade ou a execução de recursos financeiros e orçamentários.	Contingenciamento, falhas na execução orçamentária, atrasos em repasses.
Imagem/ Reputação	Riscos que afetam a confiança da sociedade na instituição.	Divulgação negativa, falhas na prestação de serviços, crises institucionais.

Quadro 1: Tipologia e origem dos riscos

3

ANÁLISE DO RISCO

A análise de riscos consiste em compreender a natureza dos riscos identificados, por meio da identificação de suas causas e consequências, de forma a subsidiar a etapa de avaliação e a tomada de decisão quanto ao seu tratamento.

Para cada risco identificado, devem ser analisados:

Consequências: efeitos ou impactos decorrentes da materialização do risco, que possam comprometer o alcance dos objetivos institucionais ou dos processos analisados.

Causas: fatores que contribuem para a ocorrência do risco, podendo estar relacionados a processos, pessoas, sistemas, infraestrutura ou ao ambiente externo.

A identificação das causas deve considerar, entre outros aspectos:

- **características do processo** (métodos, procedimentos, regulamentações, formalização, execução, controle e monitoramento);
- **fatores humanos** (competências, condutas e capacitação);

- **condições externas** (cenário político, econômico e relação com fornecedores);
- **infraestrutura física e tecnológica**, incluindo sistemas de informação.

A partir dessa análise, serão obtidas as informações necessárias para a avaliação dos riscos, especialmente quanto à probabilidade de ocorrência e ao impacto associado.

4

AVALIAÇÃO DO RISCO

A avaliação de riscos tem por objetivo estimar o nível de risco, a partir da combinação entre a probabilidade de ocorrência e o impacto associado, de modo a subsidiar a priorização e a definição das respostas aos riscos.

Nesta etapa, todos os riscos identificados devem ser avaliados com base em critérios previamente definidos, considerando o contexto institucional, os objetivos organizacionais e os requisitos legais e normativos aplicáveis

Os principais componentes da avaliação são:

- **Probabilidade:** chance de ocorrência do evento de risco;
- **Impacto:** magnitude dos efeitos do risco sobre os objetivos institucionais;
- **Risco inerente:** nível de risco na ausência de controles;
- **Risco residual:** nível de risco após a implementação de medidas de controle.

A combinação entre probabilidade e impacto determina o nível de risco, permitindo sua classificação em diferentes graus de criticidade, conforme matriz de riscos adotada.

As escalas de probabilidade e impacto são apresentadas a seguir:

ESCALA DE PROBABILIDADE		
Probabilidade	Descrição da probabilidade	Peso
Muito baixa	Improvável. Em situações excepcionais o evento poderá ocorrer, mas nada nas circunstâncias indica essa possibilidade	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	3
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	4
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá. As circunstâncias indicam claramente essa possibilidade.	5

Quadro 2: Escala de Probabilidade/ Fonte: Metodologia de Gestão de Riscos (CGU, 2021)

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

Quadro 3: Escala de impacto/ Fonte: Metodologia de Gestão de Riscos (CGU, 2021)

A multiplicação entre os valores de probabilidade e impacto define o nível do risco inerente, ou seja, o nível de risco antes da consideração dos controles existentes.

RISCO INERENTE = Probabilidade X Impacto

CLASSIFICAÇÃO DO RISCO:

Com base no resultado obtido, os riscos são classificados em níveis de criticidade, conforme faixas previamente definidas.

Classificação	Faixa
Risco Baixo - RB	1 - 4
Risco Médio - RM	5 - 11
Risco Alto - RA	12 - 19
Risco Extremo - RE	20 - 25

Quadro 4: Classificação do Risco/ Fonte: adaptado da Metodologia de Gestão de Riscos: CGU/2018

MATRIZ DE RISCOS

A matriz de riscos representa graficamente a combinação entre probabilidade e impacto, permitindo visualizar o nível de criticidade dos riscos e apoiar sua priorização.

Quanto maiores os valores de probabilidade e impacto, maior será o nível de risco e, conseqüentemente, maior a necessidade da adoção de medidas de tratamento.

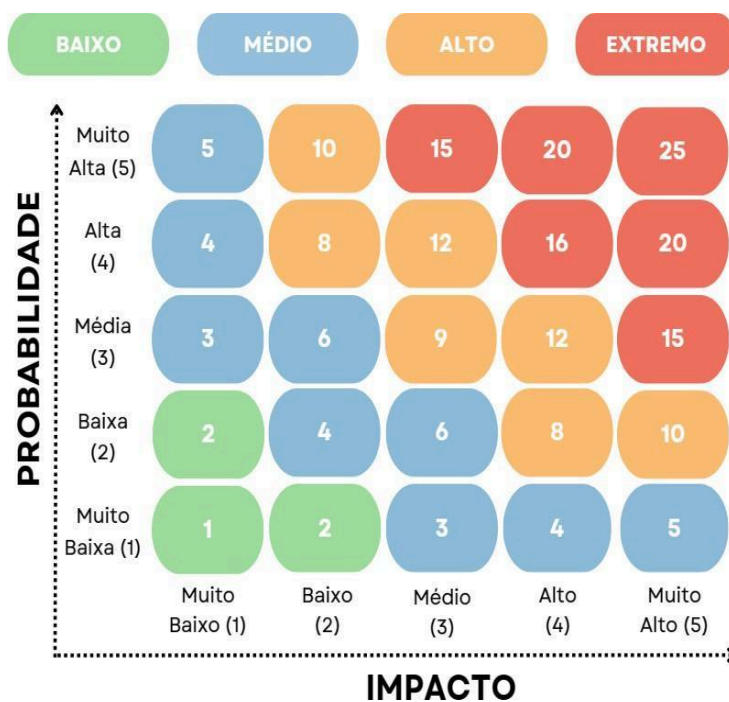


Figura 3: Representação visual da matriz de riscos Probabilidade x Impacto/ Fonte: Plataforma FORRISCOS

Priorização dos riscos

Com base nos resultados da avaliação, os riscos são priorizados conforme seu nível de criticidade, orientando a definição e a implementação de Planos de Ação.

Os riscos classificados como mais elevados, especialmente aqueles considerados **críticos** (com nível de risco alto ou extremo) devem ser priorizados para tratamento, sem prejuízo do monitoramento contínuo dos demais riscos.

Na priorização, devem ser considerados, ainda, o contexto institucional, a capacidade operacional das unidades e o custo-benefício das medidas de controle.

Análise de risco inerente e residual

CRITICIDADE DOS RISCOS	
RISCO NO QUADRANTE VERMELHO	Risco inaceitável, que possui alta probabilidade de ocorrência e poderá resultar em impacto extremamente severo, caso ocorra; exige tratamento imediato, colocando-se em execução um plano de ação composto por controle preventivo (para eliminar suas causas ou reduzir sua frequência), controle concomitante e plano de contingência para reduzir sua severidade.
RISCO NO QUADRANTE AMARELO	Pode ser tanto um risco provável, que possui alta probabilidade de ocorrência e baixo impacto na consecução dos objetivos, bem como um risco inesperado, que possui baixa probabilidade de ocorrência e alto impacto na consecução dos objetivos. Estas ameaças exigem respostas rápidas ao serem detectadas – portanto, devem ter sido planejadas e testadas em um plano de contingência –, além de ações preventivas. Diferem-se dos riscos do quadrante vermelho por terem ações de tratamento implementadas com mais planejamento e tempo. São eventos que devem ser constantemente monitorados.
RISCO NO QUADRANTE AZUL	Devem ser quantificados e monitorados de forma rotineira e sistemática, porque suas consequências são gerenciáveis; também podem possuir planos de contingência.
RISCO NO QUADRANTE VERDE	Risco que representa pequeno problema e causa pouco prejuízo, portanto controlável, devendo ser somente gerenciado.

Figura 4: Grau de risco = Probabilidade x Impacto

Os riscos devem ser analisados quanto à sua condição de inerentes (antes da implementação de controles) e residuais (após a adoção de medidas de controle), de forma a avaliar a efetividade dos controles existentes e a necessidade de sua melhoria ou da implementação de novos controles.

5

TRATAMENTO DO RISCO

Nesta etapa, são definidas as respostas aos riscos, considerando os níveis de risco apurados na etapa de avaliação.

Os riscos classificados como **alto** e **extremo**, por estarem fora do apetite a risco da UFF, devem ser priorizados para tratamento e monitoramento. Já os riscos classificados como **baixo** e **médio** podem ser aceitos, sem prejuízo da adoção de medidas de tratamento, a critério do gestor, devendo, em todos os casos, ser monitorados.

A definição da estratégia de tratamento deve considerar o nível de risco, o custo-benefício das medidas a serem adotadas e a capacidade operacional da unidade, podendo envolver a participação de diferentes áreas.

Atitude perante o risco para cada classificação		
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 pela unidade e aprovada pelo seu dirigente máximo.
RISCO MÉDIO	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é 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.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
RISCO ALTO	Nível de risco além do apetite a risco. Qualquer risco neste 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 da unidade.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
RISCO EXTREMO	Nível de risco muito além do apetite a risco. Qualquer risco neste nível deve ser comunicado ao Comitê de Governança Interna e ao dirigente máximo da unidade e ter uma resposta imediata. Postergação de medidas só com autorização do CGIRC.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo e pelo CGIRC.

Figura 5: Opções de Tratamento ao Risco/ Fonte: CGU – Metodologia de Gestão de Riscos.

Apetite a Risco

O apetite a risco representa o nível de risco que a instituição está disposta a aceitar para o alcance de seus objetivos.

No âmbito da UFF, consideram-se dentro do apetite a risco os riscos classificados como **baixo** e **médio**, conforme critérios estabelecidos neste Plano.

Os riscos classificados como **alto** e **extremo** devem ser tratados, sendo necessária justificativa formal nos casos em que não houver adoção de medidas.

Opções de tratamento

As principais opções de tratamento de riscos são apresentadas no Quadro 4:

OPÇÕES DE TRATAMENTO DO RISCO	
Opção de tratamento	Descrição
ACEITAR	Aplicável quando o risco se encontra dentro do apetite a risco. Não exige novos controles, devendo ser monitorado.
MITIGAR	Aplicável, em geral, a riscos classificados como “alto” ou “extremo”, quando a implementação de controles apresenta relação custo-benefício adequada. Consiste na adoção de medidas para reduzir a probabilidade de ocorrência e/ou o impacto do risco.
COMPARTILHAR	Aplicável, em geral, a riscos classificados como “alto” ou “extremo”, quando a implementação de controles não apresenta relação custo-benefício adequada. Consiste na transferência parcial do risco a terceiros, por meio de instrumentos como contratos ou seguros.
EVITAR	Aplicável, em geral, a riscos classificados como “alto” ou “extremo”, quando a mitigação se mostra inviável em razão de custo elevado ou da impossibilidade de compartilhamento. Consiste na eliminação do risco por meio da descontinuidade da atividade ou processo, mediante decisão institucional, a ser submetida ao CGIRC.

Quadro 5: Opções de tratamento do risco/ Fonte: Adaptado de Metodologia de Gestão de Riscos – Opções de tratamento do risco (CGU,2018).

PLANO DE AÇÃO

Quando a estratégia adotada for **mitigar**, devem ser definidas medidas de tratamento, formalizadas em Plano de Ação. Essas medidas devem ser capazes de reduzir os níveis de probabilidade e/ou de impacto do risco, de modo a enquadrá-lo o mais próximo possível das faixas de apetite a risco (classificação “Baixo” ou “Médio”).

O Plano de Ação deve conter, no mínimo:

- identificação do risco;
- medidas de tratamento (preventivas e/ou corretivas);
- resultados esperados com a implementação das medidas;
- responsável pela implementação;
- prazos para início e conclusão da implementação;

Antes da proposição de novos controles, deve-se avaliar a necessidade de aprimorar ou eliminar controles existentes, com base na análise realizada. Somente após essa avaliação, e caso ainda seja necessário reduzir o nível de risco, poderão ser propostas novas medidas, observando critérios de eficiência e eficácia.

Quando o Plano de Ação envolver mais de uma unidade, sua proposta deverá ser submetida às áreas envolvidas para validação das respectivas iniciativas.

A PLAD/PROPLAN disponibilizará modelo padrão de Plano de Ação, com orientações para seu preenchimento, a fim de apoiar a elaboração e a padronização das informações pelas unidades. O modelo poderá ser acessado no site da PROPLAN, em seção específica destinada à gestão de riscos.

Validação e acompanhamento

Os resultados da avaliação de riscos e os respectivos Planos de Ação devem ser aprovados pelo dirigente máximo da unidade.

Quando o Plano de Ação envolver outras unidades, a articulação e a validação das ações deverão ser realizadas previamente à sua aprovação, sob responsabilidade do gestor do processo.

Após a aprovação, as ações devem ser incorporadas aos instrumentos de planejamento da unidade (PDU) e acompanhadas quanto à sua execução.

A comunicação e a consulta consistem em processos contínuos de compartilhamento de informações e diálogo com as partes interessadas, internas e externas, devendo ocorrer ao longo de todas as etapas da gestão de riscos, observada a classificação da informação quanto ao sigilo.

A adoção de abordagem consultiva contribui para o adequado entendimento do contexto, a identificação e análise dos riscos, a consideração de diferentes perspectivas e o fortalecimento do apoio às ações de tratamento.

A Política e o Plano de Gestão de Riscos devem ser amplamente divulgados no âmbito da Universidade, com destaque para os papéis e responsabilidades dos agentes envolvidos na gestão de riscos.

Compete à Coordenação de Planejamento e Desenvolvimento (PLAD/PROPLAN) articular-se com a Superintendência de Comunicação (SCS), no âmbito de suas competências, para apoiar a divulgação das ações de gestão de riscos e colaborar na elaboração e atualização dos planos de comunicação institucionais sobre o tema.

O monitoramento consiste no acompanhamento contínuo dos riscos e dos controles implementados, com o objetivo de verificar sua efetividade e identificar a necessidade de ajustes, em decorrência de mudanças no contexto interno e externo.

Essa etapa deve ocorrer ao longo de todo o processo de gestão de riscos, permitindo a identificação de novos riscos, a análise de eventos ocorridos, incluindo quase incidentes, e o aperfeiçoamento contínuo das práticas adotadas.

No âmbito operacional, compete aos proprietários dos riscos realizar o

acompanhamento dos riscos e das ações de tratamento, incluindo a atualização das informações nos sistemas institucionais, sob a supervisão dos gestores das unidades.

Cabe ao Comitê de Governança, Integridade, Riscos e Controles (CGIRC) acompanhar a evolução dos níveis de risco e avaliar a efetividade das medidas de controle implementadas na instituição.

A PLAD/PROPLAN disponibilizará orientações complementares, por meio de um guia prático para apoiar a implementação da gestão de riscos pelas unidades, disponível em: <https://www.uff.br/proplan/gestao-de-riscos/>

6. Planejamento da Gestão de Riscos (2026/2027)

O planejamento contempla ações voltadas ao fortalecimento da gestão de riscos na Instituição, com ênfase na operacionalização do Subcomitê de Gestão de Riscos, conforme previsto na Política institucional, bem como no aprimoramento da gestão de riscos relacionados à proteção de dados pessoais, em conformidade com a Lei nº 13.709/2018 (LGPD).

A operacionalização do Subcomitê poderá se dar por meio da instituição de instância técnica de apoio, de caráter consultivo, composta, inicialmente, por representantes das unidades administrativas, com ampliação progressiva para inclusão das unidades acadêmicas, conforme a evolução da maturidade da gestão de riscos na UFF.

As ações previstas abrangem:

- riscos associados aos objetivos estratégicos;
- riscos relacionados aos processos organizacionais;
- riscos de integridade;
- riscos relacionados à proteção de dados pessoais.

Essas iniciativas priorizam o fortalecimento da governança, a integração entre unidades e a melhoria contínua dos processos institucionais, sendo seu acompanhamento realizado periodicamente pela PLAD/PROPLAN, com reporte ao CGIRC.

O detalhamento das ações, responsáveis e prazos consta no **Anexo I – Plano de Ação da Gestão de Riscos (2026–2027)**.

7 . Considerações finais

Destaca-se a importância do Relatório de Gestão de Riscos como instrumento de monitoramento e aprimoramento contínuo das práticas institucionais, contribuindo para a evolução dos métodos, ferramentas e processos adotados.

As informações registradas ao longo do ciclo de gestão de riscos subsidiam o planejamento das respostas aos riscos, com base nos registros existentes, no mapa de riscos institucionais e nas lições aprendidas, reforçando a cultura de aprendizado contínuo e a reutilização de informações para fins de gestão.

Informações relevantes devem ser identificadas, coletadas e comunicadas de forma tempestiva, de modo a apoiar o cumprimento das responsabilidades institucionais, considerando tanto dados internos quanto informações relacionadas ao ambiente externo. A comunicação deve ocorrer de forma clara e acessível, alcançando todos os níveis da Instituição.

Considerando a complexidade e a diversidade da UFF, este Plano não se configura como instrumento definitivo, devendo ser continuamente aprimorado, de modo a fortalecer a gestão de riscos e a governança institucional.

8 . Referências bibliográficas

ABNTNBR ISO 31000:2009. *Gestão de Riscos – Princípios e Diretrizes*. Associação Brasileira de Normas Técnicas. Rio de Janeiro, RJ, 2009.

BRASIL. *Instrução Normativa Conjunta 01/2016 (MP/CGU)*. Disponível em:

http://www.cgu.gov.br/sobre/legislacao/arquivos/instrucoes-normativas/in_cgu_mpog_01_2016.

BRASIL. CGU. *Metodologia de Gestão de Riscos da CGU- versão 2.0*. Disponível em:

<https://repositorio.cgu.gov.br/bitstream/1/74049/1/Metodologia_de_riscos_2_0.pdf>

PROJETO ForRISCO. Disponível em:

<http://www.forplad.andifes.org.br/sites/default/files/Painel3-ForRiscomguiapraticoparagestao_de_riscos_em_instituicoes_publicas_-_UNB_-_Paulo_-_Poçosde_Caldas.pdf>

UNIVERSIDADE FEDERAL DO CEARÁ. Plano Gestão de Riscos. Fortaleza, CE, 2022. Disponível em:

<<https://secretariadegovernanca.ufc.br/wp-content/uploads/2022/12/plano-de-gestAo-de-riscos-2a-edicao-2023-2027.pdf>>

UNIVERSIDADE FEDERAL DO PARÁ. Planos de Gestão de Riscos UFPA. Belém, PA. Disponível em:

<<https://proplan.ufpa.br/index.php/documentos-digest/2-uncategorised/253-planos-riscos-ufpa>>

UNIVERSIDADE FEDERAL FLUMINENSE. Política de Gestão de Riscos. Disponível em:

<https://www.uff.br/proplan/gestao-de-riscos/>

UNIVERSIDADE FEDERAL FLUMINENSE. Plano de Gestão de Riscos 2025-2026. Disponível em:

<https://www.uff.br/proplan/gestao-de-riscos/>

ANEXO I

PLANO DE AÇÃO – 2026-2027

AÇÕES	RESPONSÁVEIS	PRAZO
Operacionalizar o Subcomitê de Gestão de Riscos	<i>CGIRC</i>	2027
Identificar e atualizar riscos estratégicos	<i>PLAD/PROPLAN</i>	2027
Atualizar os riscos de integridade	<i>PLAD / Comitê de Integridade</i>	Anual
Apoiar as unidades administrativas na identificação e priorização dos riscos	<i>PLAD/PROPLAN</i>	2026 / 2027
Disponibilizar modelo de Plano de Ação para tratamento de riscos no site da PROPLAN.	<i>PLAD / PROPLAN</i>	2027
Estruturar a gestão de riscos relacionados à proteção de dados pessoais (LGPD)	<i>Comissão CGDP / PROPLAN</i>	2027
Integrar a gestão de riscos ao Relatório de Impacto à Proteção de Dados (RIPD)	<i>Comissão CGDP / PROPLAN</i>	2027
Elaborar Plano de Ação para os riscos relacionados à LGPD.	<i>Comissão CGDP / PROPLAN</i>	2027
Promover ações de capacitação em gestão de riscos	<i>EGGP / PROPLAN</i>	Contínua
Apoiar as unidades no monitoramento dos riscos	<i>Pró-Reitorias e Superintendências</i>	<i>Anual</i>
Elaborar relatório anual de gestão de riscos	<i>PLAD/PROPLAN</i>	<i>Anual</i>

