UNIVERSIDADE FEDERAL DO OESTE DA BAHIA
Gabinete da Reitoria

PORTARIA UFOB N° 678, DE 17 DE JUNHO DE 2026

Institui o Plano de Gestão de Riscos e Controles Internos.

O REITOR DA UNIVERSIDADE FEDERAL DO OESTE DA BAHIA, nomeado pelo Decreto de 11 de setembro de 2023, publicado no Diário Oficial da União em 12 de setembro de 2023, seção 2, pág. 1, tendo em vista o disposto no art. 8º da Lei nº 12.825, de 5 de junho de 2013, no uso das atribuições que lhe conferem o art. 51 do Regimento Geral da UFOB, resolve:

Art. 1º Instituir o Plano de Gestão de Riscos e Controles Internos, conforme anexo, o qual foi aprovado na reunião do Comitê de Governança, Riscos e Controles, realizada em 30 de março de 2026.

Art. 2º Esta Portaria entra em vigor a partir de sua data de publicação no Boletim de Serviços da UFOB.

ASSINADO DIGITALMENTE
JACQUES ANTONIO DE MIRANDA
A conformidade com a assinatura pode ser verificada em:
https://serpro.gov.br/assinador-digital
Serpro

JACQUES ANTONIO DE MIRANDA

Reitor

Rua Professor José Seabra de Lemos, n. 316 – Recantos dos Pássaros
Barreiras-Ba. Cep: 47808-021
Fone: (77) 3614-3590

UNIVERSIDADE FEDERAL
DO OESTE DA BAHIA

PLANO DE GESTÃO DE RISCOS E CONTROLES INTERNOS

2026 - 2028



Ministério da Educação

Universidade Federal do Oeste da Bahia

PLANO DE GESTÃO DE RISCOS E CONTROLES INTERNOS

VIGÊNCIA 2026 – 2028

Barreiras – BA

2026

COMITÊ DE GOVERNANÇA, RISCOS E CONTROLES

Reitor
Jacques Antonio de Miranda

Vice-Reitor
Antonio Oliveira de Sousa

Chefe de Gabinete
Marina Meirelles Paes

Diretor de Governança, Riscos e Conformidade
Angelo Marconi Maniero

Pró-Reitor de Ações Afirmativas e Assuntos Estudantis
Antonio Oliveira de Sousa

Pró-Reitora de Administração
Jaqueline Fritsch

Pró-Reitor de Extensão e Cultura
Anderson Breno Souza

Pró-Reitora de Graduação
Adma Katia Lacerda Chaves

Pró-Reitor de Gestão de Pessoas
Clayton da Silva Barcelos

Pró-Reitor de Planejamento e Desenvolvimento Institucional
Leriane Silva Cardozo

Pró-Reitora de Pós-Graduação e Pesquisa
Aurizangela Oliveira de Sousa

Pró-Reitor de Tecnologia da Informação e Comunicação
Uiliam Rangel Amorim Souza

Secretária Acadêmica
Leila Oliveira dos Anjos

Superintendente Administrativa do *campus* Reitor Edgard Santos
Marcus Vinicius Soares Figueiredo Castro Silva

Superintendente de Inovação e Tecnologia para o Desenvolvimento Regional
Erick Samuel Rojas Cajavilca

EQUIPE DE ELABORAÇÃO

Diretor de Governança, Riscos e Conformidade
Angelo Marconi Maniero

Coordenadora de Riscos e Conformidade
Vanessa Godoy Kinoshita

LISTA DE FIGURAS

Figura 1: Linha do tempo da regulamentação e ações da UFOB.....11
Figura 2: Mudanças na gestão de riscos do COSO-IC para o COSO-ERM 15
Figura 3: Modelo de três linhas de defesa adaptado para o ambiente da UFOB 19
Figura 4: Áreas de atuação da gestão de riscos na UFOB 21
Figura 5: Hierarquia de processos 22
Figura 6: Cadeia de Valor Integrada da UFOB 23
Figura 7: Etapas do processo de gestão de riscos 26
Figura 8: Etapas do processo de gerenciamento de riscos 30
Figura 9: Modelo de avaliação da maturidade em gestão de riscos 56
Figura 10: Planilha de mapeamento de riscos 68
Figura 11: Modelo de Plano de Tratamento 69
Figura 12: Modelo de Plano de Contingência 71
Figura 13: Modelo de Registro de Ocorrência 72

LISTA DE QUADROS

Quadro 1: Normas e regulamentações relacionadas à área de gestão de riscos 12
Quadro 2: Categorias de riscos 33
Quadro 3: Escala de probabilidade 35
Quadro 4: Escala de impacto 35
Quadro 5: Áreas de impacto 36
Quadro 6: Classificação de risco 37
Quadro 7: Matriz de riscos 38
Quadro 8: Fatores de avaliação dos controles 38
Quadro 9: Diretrizes de priorização dos riscos a serem tratados 40
Quadro 10: Opções de tratamento de risco 41
Quadro 11: Matriz de responsabilidades na gestão de riscos 46
Quadro 12: Plano de Comunicação 48
Quadro 13: Responsabilidades relativas ao monitoramento 53
Quadro 14: Pesos e exemplo de cálculo do índice de maturidade 58
Quadro 15: Níveis de maturidade da gestão de riscos 58
Quadro 16: Plano de Ações 59

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
Audin	Auditoria Interna
CGAG	Câmara de Gestão Administrativa e Governança
CGRC	Comitê de Governança, Riscos e Controles
CGU	Controladoria-Geral da União
Consuni	Conselho Universitário
COSO	*The Comitee of Sponsoring Organizations of the Treadway Commission*
COSO-ERM	COSO *Enterprise Risk Management* (Gerenciamento de Riscos Corporativos)
COSO-IC	COSO *Internal Control* (Controle Interno)
CVI	Cadeia de Valor Integrada
DGRC	Diretoria de Governança, Riscos e Conformidade
EAD	Educação à distância
FAC	Fator de avaliação dos controles
Forplad	Fórum Nacional de Pró-Reitores de Planejamento e de Administração das Instituições Federais de Ensino Superior
IIA	*The Institute of Internal Auditors*
IMD	Índice de maturidade das dimensões
INC	Instrução Normativa Conjunta
ISO	*International Organization for Standardization*
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
MP	Ministério do Planejamento
NBR	Normas Brasileiras
NC	Nível de confiança
PDI	Plano de Desenvolvimento Institucional
PGC	Sistema de Planejamento e Gerenciamento de Contratações
PGRCI	Política de Gestão de Riscos e Controles Internos
Proplan	Pró-Reitoria de Planejamento e Desenvolvimento Institucional
RNP	Rede Nacional de Ensino e Pesquisa

Sitai	Sistema de Integridade, Transparência e Acesso à Informação
TCU	Tribunal de Contas da União
UFOB	Universidade Federal do Oeste da Bahia

SUMÁRIO

1. INTRODUÇÃO 10
   1.1. Objetivo 11
   1.2. Normas e regulamentações relacionadas 12
   1.3. Referencial teórico 13
2. PAPÉIS E COMPETÊNCIAS NA GESTÃO DE RISCOS 16
   2.1. Comitê de Governança, Riscos e Controles (CGRC) 16
   2.2. Diretoria de Governança, Riscos e Conformidade (DGRC) 17
   2.3. Gestores de riscos 17
   2.4. Agentes Públicos 18
   2.5. Auditoria Interna (Audin) 18
   2.6. Modelo de três linhas de defesa 19
3. ÁREAS DE ATUAÇÃO DA GESTÃO DE RISCO 21
   3.1. Riscos no planejamento estratégico 21
   3.2. Riscos nos processos organizacionais 22
   3.3. Riscos de integridade 24
4. PROCESSO DE GESTÃO DE RISCOS 26
   4.1. Definição e fortalecimento do ambiente interno 27
   4.2. Processo de gerenciamento de riscos 28
   4.3. Supervisão da gestão de riscos 28
5. PROCESSO DE GERENCIAMENTO DE RISCOS 30
   5.1. Entendimento do contexto 30
   5.2. Identificação e Análise de riscos 31
   5.3. Avaliação de riscos 34
   5.4. Priorização de riscos 39
   5.5. Definição de respostas ao risco 40
   5.6. Comunicação e monitoramento 43
      5.6.1. Comunicação 44
      5.6.2. Monitoramento 52
6. SOLUÇÃO TECNOLÓGICA 54

7. CAPACITAÇÃO 55
8. MATURIDADE NA GESTÃO DE RISCOS 56
9. PLANO DE AÇÕES 59
10. CONSIDERAÇÕES FINAIS 61
11. REFERÊNCIAS 62
APÊNDICE A 66
APÊNDICE B 68
APÊNDICE C 69
APÊNDICE D 70
APÊNDICE E 71
APÊNDICE F 72
APÊNDICE G 73

1. INTRODUÇÃO

As atividades de uma organização, sejam elas públicas ou privadas, estão sujeitas a eventos não previstos. Diversos fatores, sejam de ordem interna ou externa, podem atrapalhar ou favorecer o atingimento dos resultados esperados. Convencionalmente, os eventos de impacto positivo, que influenciam favoravelmente na realização dos objetivos, são conhecidos como oportunidades. Os eventos negativos, que dificultam ou impedem a realização do que foi planejado, são generalizados como eventos de risco.

Um risco é medido pela combinação da probabilidade da ocorrência de uma ameaça (ou oportunidade) e a magnitude de seu impacto. Para aumentar a possibilidade de alcançar os resultados almejados, as organizações governamentais devem estruturar um processo de gestão de riscos, identificando, analisando, avaliando e respondendo a cada risco. E a UFOB já começou a trilhar esse caminho (sem volta), que começa com a conscientização sobre a importância do processo e avança com a consolidação de princípios e práticas de gestão de riscos, controles internos e governança. Assim, todos os agentes públicos adquirem conhecimentos para conduzirem seus trabalhos de modo a produzirem melhores resultados.

A Administração Pública vem incorporando as melhores práticas relacionadas ao tema a partir da Instrução Normativa Conjunta nº 01/2016, do então Ministério do Planejamento e do Ministério da Transparência e Controladoria-Geral da União, e do Decreto nº 9.203/2017. Os normativos determinam que todos os órgãos e entidades no âmbito do Poder Executivo Federal adotem medidas para a implementação e atualização do modelo de gestão de riscos.

A Administração da UFOB, reconhecendo a importância estratégica da área, instituiu o Comitê de Governança, Riscos e Controles (CGRC), por meio da Portaria UFOB nº 237, de 12 de abril de 2021. Posteriormente, o Conselho Universitário (Consuni) estabeleceu a Política de Gestão de Riscos e Controles Internos (PGRCI), com a publicação da Resolução CGAG/CONSUNI/UFOB nº 014, de 13 de dezembro 2022, compreendendo princípios, objetivos, diretrizes e responsabilidades no âmbito da Universidade. Por fim, a composição do CGRC foi atualizada por meio da Portaria UFOB nº 35, de 3 de março de 2023. A Figura 1 apresenta a linha do tempo da regulamentação e das ações da UFOB.

Figura 1: Linha do tempo da regulamentação e ações da UFOB



Fonte: Elaboração própria

Este documento visa dar cumprimento à legislação vigente e, além disso, tem o intuito de consolidar as políticas de governança, de gestão de riscos e controles internos na Universidade, assegurando o cumprimento de sua missão institucional e a melhoria do alcance dos objetivos estratégicos.

A gestão de riscos provê um conjunto de informações que permitem melhorar a tomada de decisões nos diversos níveis organizacionais, do estratégico ao operacional, além de estabelecer controles internos mais efetivos, contribuindo para o fortalecimento da governança. Dessa forma, este documento ratifica o compromisso da UFOB com a governança pública, promovendo a eficiência no cumprimento dos objetivos institucionais e a entrega de resultados mais efetivos para a sociedade.

1.1. Objetivo

Este plano visa detalhar os procedimentos e os instrumentos necessários ao processo de gestão de riscos e controles internos da UFOB em cumprimento às diretrizes da PGRCI estabelecida na Resolução CGAG/CONSUNI/UFOB nº 014.

Neste documento, a metodologia adotada para gerenciar riscos nas áreas acadêmicas e administrativas da Universidade será apresentada, detalhando as etapas previstas na PGRCI. Compreende também o planejamento de sua implementação dentro do período de vigência do plano, de 2026 a 2028, com o propósito de assegurar maior eficiência e eficácia no alcance dos objetivos institucionais e na prestação de serviços à sociedade.

1.2. Normas e regulamentações relacionadas

O processo de gestão de riscos da UFOB é estruturado em consonância com as leis, decretos e normas listados no Quadro 1.

Quadro 1: Normas e regulamentações relacionadas à área de gestão de riscos

DOCUMENTOS
Instrução Normativa Conjunta MP/CGU nº 01/2016, dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal
Decreto nº 9.203/2017, dispõe sobre a política de governança da Administração Pública Federal direta, autárquica e fundacional
Decreto nº 10.947/2022, regulamenta o inciso VII do *caput* do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da Administração Pública Federal direta, autárquica e fundacional.
Decreto nº 11.529/2023, institui o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal e a Política de Transparência e Acesso à Informação da Administração Pública Federal.
Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD)
Lei nº 14.129/2021, dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017.
Lei nº 14.133/2021, Lei de Licitações e Contratos Administrativos.

Fonte: Elaboração própria

Conforme mencionado anteriormente, a INC MP/CGU nº 1/2016 e, posteriormente, o Decreto nº 9.203/2017 foram marcos regulatórios que tornaram obrigatória a adoção da gestão de riscos no âmbito dos órgãos e entidades do Poder Executivo Federal.

Já a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), regulamenta o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Essa legislação determinou que os agentes responsáveis pelo tratamento de dados pessoais elaborem um Relatório de Impacto à Proteção de Dados, o qual deve descrever medidas, salvaguardas e mecanismos de mitigação de riscos.

O Capítulo VII da Lei nº 14.129/2021, por sua vez, estabelece que o sistema de gestão de riscos a ser implementado nas instituições deve incluir uma análise crítica de riscos da prestação digital de serviços públicos que impactem no cumprimento de suas missões. Entre os pontos citados na lei, estão: a gestão de riscos necessita estar integrada ao processo de planejamento estratégico e seus desdobramentos; o estabelecimento de controles internos deve ser proporcional aos riscos, considerando a relação custo-benefício; e os resultados serão empregados no apoio à melhoria contínua do desempenho dos processos de gestão de riscos, governança e controle.

A importância do sistema de gestão de riscos e seu impacto nas licitações e contratos da Administração Pública podem ser comprovados por meio de sua inclusão na Lei nº 14.133/2021. Esses processos devem ser avaliados, direcionados e monitorados com base no sistema de gestão de riscos, de modo que as aquisições e contratações estejam alinhadas ao planejamento estratégico e às leis orçamentárias e que sejam garantidas sua eficiência, eficácia e efetividade.

Ainda, tem-se o Decreto nº 10.947/2022, que trata do plano de contratações anual e institui o Sistema de Planejamento e Gerenciamento de Contratações (PGC), determinando que os setores de contratações devem elaborar, de acordo com as orientações da Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, relatórios de riscos referentes à provável não efetivação da contratação de itens constantes no plano de contratações anual até o término do exercício em questão.

Vale ressaltar que qualquer instituição está sujeita a riscos de integridade, como corrupção, fraudes, desvios éticos e outras irregularidades, que podem comprometer valores, metas e padrões institucionais, além de gerar riscos financeiros, operacionais e reputacionais. Com esse intuito, foi criado o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal (Sitai), instituído pelo Decreto nº 11.529/2023. Uma das competências do Sitai é orientar as atividades relativas à gestão de riscos para a integridade.

1.3. Referencial teórico

Atualmente, diversos modelos de gestão de riscos são adotados como referência em boas práticas. Essas estruturas conceituais oferecem diretrizes para a identificação, análise, avaliação, monitoramento e mitigação de riscos em uma organização, contribuindo para a implementação de processos sistemáticos e coerentes para gerenciar os riscos e auxiliar na tomada de decisões. A seguir, serão apresentados alguns desses modelos de melhores práticas.

Em 1992, o COSO (*The Comitee of Sponsoring Organizations of the Treadway Commission*), publicou o guia “Controle Interno – Estrutura Integrada” (COSO-IC ou COSO I), com

o objetivo de orientar as organizações quanto às melhores práticas de controle interno, especialmente no que se refere à produção de relatórios financeiros confiáveis e prevenir fraudes (COSO, 2013). Nesse modelo, o controle interno foi definido como um "processo projetado e implementado pelos gestores para mitigar riscos e alcançar objetivos". Por sua vez, risco é compreendido como "a possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos". A partir dessas definições, o controle interno é concebido como um processo voltado à mitigação de riscos, com vistas ao cumprimento dos objetivos institucionais.

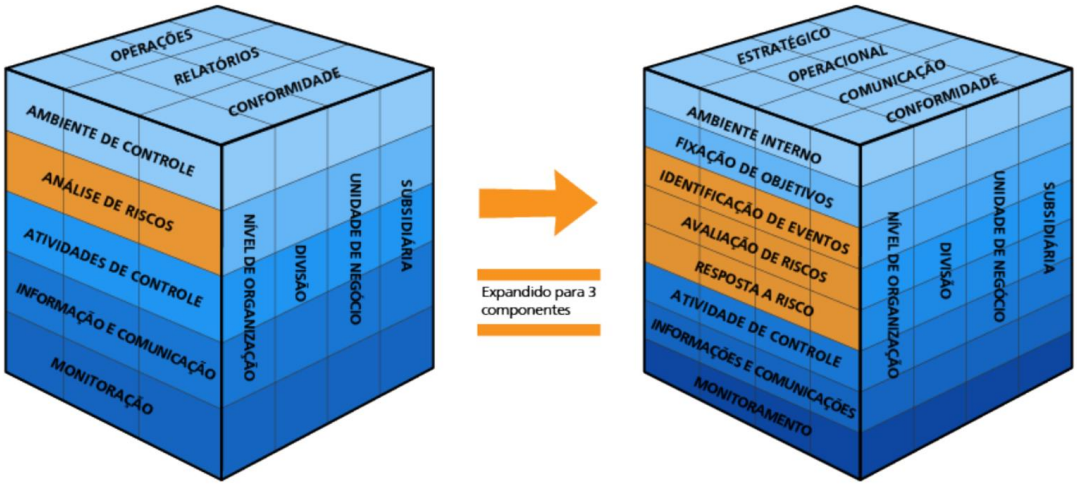
Em 2004, o COSO publicou o "Gerenciamento de Riscos Corporativos – Estrutura Integrada" (COSO-ERM ou COSO II), um documento mais voltado para o gerenciamento de riscos corporativos (COSO, 2007). A inovação apresentada pela metodologia COSO-ERM é a implementação do processo de gestão de riscos nas atividades de planejamento estratégico institucional, e não apenas nas administrativas, operacionais e de suporte. Outro ponto é que a etapa de "análise de riscos" foi substituída e complementada pela etapa de identificação, avaliação e resposta (Figura 2). Ainda, é neste documento que conceitos como apetite e tolerância ao risco são introduzidos: enquanto o primeiro se refere ao nível de risco que a organização estaria disposta a aceitar, o segundo representa o nível de variação admissível na conquista de um dado objetivo. Ressalta-se também que o COSO-ERM é uma evolução do COSO-IC, mantendo ainda o escopo do modelo anterior, ao passo que introduz as novas ferramentas já explicadas – ou seja, não pretende substituí-lo, mas sim incorporá-lo. Uma última atualização do COSO-ERM ocorreu em 2017, trazendo a importância de considerar os riscos estratégicos e os envolvidos na melhoria do desempenho organizacional.

Já a norma técnica ISO 31000 resultou de esforço da *International Organization for Standardization* (ISO) para criar um padrão internacional para a gestão de riscos corporativos, tendo sido publicada no Brasil sob o nome "ABNT NBR ISO 31000 Gestão de Riscos – Princípios e Diretrizes", em 2009 (ABNT, 2009).

O processo de gestão de riscos preconizado na ISO 31000:2009 não difere muito do que já era previsto em normas técnicas regionais que a antecederam e contempla as seguintes fases ou atividades: estabelecimento do contexto, identificação, análise, avaliação e tratamento de riscos, comunicação e consulta, monitoramento e análise crítica.

Em 2018, a ISO 31000:2009 foi revisada e seu conteúdo foi totalmente substituído pela nova versão, denominada "ABNT NBR ISO 31000 Gestão de Riscos – Diretrizes" (ABNT, 2018). Na essência, o processo de gestão de riscos continua o mesmo incluindo as etapas relativas às atividades de comunicação e consulta, ao estabelecimento do contexto, avaliação dos riscos (identificar, analisar e avaliar os riscos), uma etapa relativa ao monitoramento e, a seguir, registro e relato dos riscos.

Figura 2: Mudanças na gestão de riscos do COSO-IC para o COSO-ERM



Fonte: Portal do TCU (TCU, 2026)

Cabe também mencionar dois documentos publicados por órgãos de controle do Governo Federal que podem ser utilizados como referência. O documento “Metodologia de Gestão de Riscos - Manual”, publicado pela CGU em 2018, traz o processo de gerenciamento de riscos do órgão, contemplando as etapas de entendimento do contexto, identificação e análise dos riscos, avaliação, priorização dos riscos, definição de respostas, validação dos resultados, implementação do plano de tratamento e monitoramento (CGU, 2018a). Por fim, o documento “Gestão de Riscos – Avaliação da Maturidade”, publicado pelo Tribunal de Contas da União (TCU) em 2018, com o objetivo de apoiar a avaliação da maturidade da gestão de riscos de organizações públicas, a identificação de aspectos que necessitam ser aperfeiçoados, fornecer orientação e disponibilizar ferramentas para a realização de auditorias de maneira eficiente e eficaz (TCU, 2018).

2. PAPÉIS E COMPETÊNCIAS NA GESTÃO DE RISCOS

A gestão de riscos da UFOB é gerida de forma integrada, estando estruturada em conformidade com o modelo de três linhas de defesa apresentado pela INC MP/CGU nº 1/2016 e pelo *The Institute of Internal Auditors* – IIA (IIA, 2020).

Antes de descrever o modelo, serão apresentadas cada instância da estrutura e suas competências relacionadas à gestão de riscos.

2.1. Comitê de Governança, Riscos e Controles (CGRC)

Instituído em 12 de abril de 2021, por meio da Portaria UFOB nº 237, o Comitê de Governança, Riscos e Controles (CGRC) é uma instância colegiada e de natureza deliberativa, vinculada à Reitoria.

Ao CGRC, de acordo com o art. 5º da Portaria UFOB nº 237, compete:

a) institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos;
b) promover práticas e princípios de conduta e padrões de comportamentos;
c) promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de riscos e de controles internos;
d) garantir a aderência às regulamentações, às leis, aos códigos, às normas e aos padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;
e) promover a integração dos agentes responsáveis pela governança, pela gestão de riscos e pelos controles internos;
f) promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, na transparência e na efetividade das informações;
g) aprovar políticas, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;
h) supervisionar o mapeamento e a avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público;
i) liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão;

j) estabelecer limites de exposição a riscos globais do órgão, bem como os limites de alçada ao nível de unidade, política pública ou atividade;
k) aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;
l) emitir recomendação para o aprimoramento da governança, da gestão de riscos e dos controles internos;
m) monitorar as recomendações e orientações deliberadas pelo Comitê.

2.2. Diretoria de Governança, Riscos e Conformidade (DGRC)

A Diretoria de Governança, Riscos e Conformidade (DGRC) atua como órgão responsável pela gestão de riscos e desenvolverá as seguintes atividades, de acordo com o art. 11 da PGRCI:

a) propor o Plano de Gestão de Riscos e Controles Internos e suas revisões;
b) propor a definição dos níveis de apetite ao risco dos processos organizacionais da UFOB;
c) definir os requisitos funcionais necessários à solução tecnológica de suporte ao processo de gestão de riscos;
d) dar suporte à identificação, análise e avaliação de riscos dos processos organizacionais selecionados para a implementação da gestão de riscos;
e) consolidar e reportar os resultados das diversas áreas em relatórios gerenciais;
f) elaborar a estratégia de comunicação e transparência da gestão de riscos;
g) propor os indicadores de desempenho para a gestão de riscos, alinhados aos indicadores de desempenho da UFOB; e
h) monitorar o desempenho da gestão de riscos objetivando a sua melhoria contínua.

2.3. Gestores de riscos

Os gestores de riscos correspondem aos dirigentes das unidades acadêmicas e administrativas, responsáveis pelo gerenciamento de determinados riscos, com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação dos riscos.

Ao gestor de riscos, de acordo com o art. 12 da PGRCI, compete:

a) identificar, analisar e avaliar os riscos dos processos organizacionais sob sua responsabilidade, em conformidade ao que se define na PGRCI;

b) definir respostas aos riscos e implementar as medidas de controle nos processos organizacionais sob sua responsabilidade;
c) monitorar os níveis de riscos, os indicadores de desempenho e a efetividade das medidas de controles implementadas nos processos organizacionais sob sua responsabilidade;
d) informar à DGRC sobre o desempenho da gestão de riscos nos processos organizacionais sob sua responsabilidade;
e) atender às requisições da DGRC;
f) disponibilizar as informações adequadas quanto à gestão dos riscos dos processos sob sua responsabilidade aos órgãos de controle externos e demais partes interessadas;
g) primar pela inovação e a adoção de boas práticas à gestão de riscos.

2.4. Agentes Públicos

Agentes públicos são aqueles que, por força de lei, contrato ou qualquer ato jurídico, prestem serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, à UFOB.

Aos agentes públicos, de acordo com o art. 13 da PGRCI, compete o monitoramento dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais. Caso sejam identificadas mudanças ou fragilidades nos processos organizacionais, o agente público deverá reportar imediatamente o fato ao responsável pela gestão de riscos do processo em questão.

2.5. Auditoria Interna (Audin)

A Auditoria Interna é o órgão responsável pelo assessoramento ao (à) Reitor(a) e demais gestores da UFOB no cumprimento de metas, na comprovação da legalidade e na avaliação de resultados, quanto à economicidade, eficácia e eficiência da gestão.

Ao que se relaciona à gestão de riscos, compete à Audin, conforme o art. 34 da Resolução CNR/CONSUNI/UFOB nº 017:

a) analisar a regularidade da gestão contábil, orçamentária, financeira, patrimonial e operacional da UFOB;
b) avaliar a regularidade das contas, a eficiência e a eficácia na aplicação dos recursos disponíveis, observados os princípios da legalidade, legitimidade e economicidade;

c) assessorar o(a) Reitor(a) e os demais gestores da UFOB quanto à utilização adequada de recursos e bens disponíveis;

d) propor medidas visando à racionalização progressiva dos procedimentos administrativos, contábeis, orçamentários, financeiros e patrimoniais da UFOB;

e) avaliar a eficiência e a qualidade técnica dos controles contábeis, orçamentários, financeiros e patrimoniais da UFOB;

f) emitir orientações, de natureza administrativa, contábil e operacional quanto à aplicação das leis, normas, decisões do TCU e recomendações da CGU;

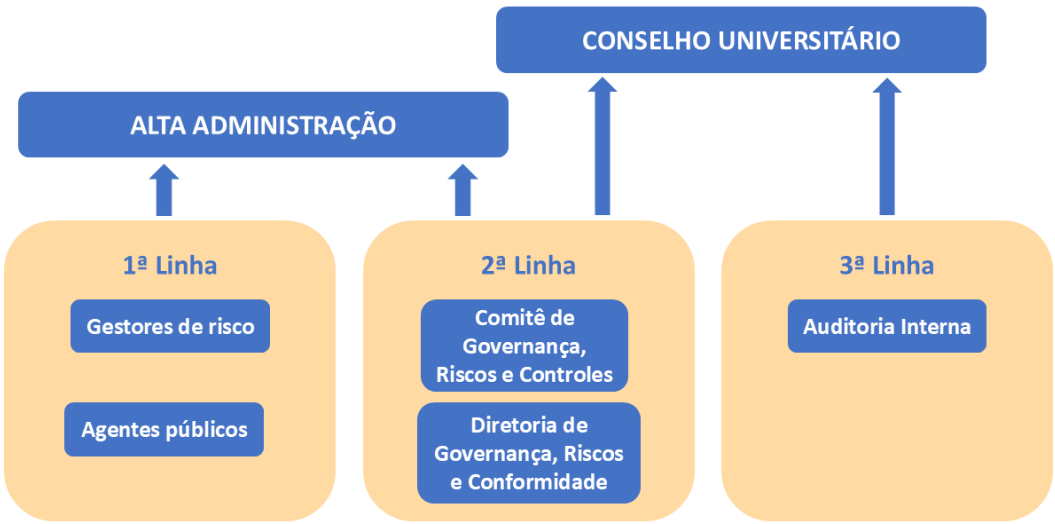
g) orientar os gestores com a finalidade de evitar o cometimento de equívocos, desperdícios, abusos, práticas antieconômicas e fraudes; e

h) acompanhar a implementação das recomendações exaradas pela CGU e das determinações do TCU.

2.6. Modelo de três linhas de defesa

As linhas de defesa são estruturadas conforme o modelo apresentado na Figura 3.

Figura 3: Modelo de três linhas de defesa adaptado para o ambiente da UFOB



Fonte: Elaboração própria

1ª linha – Operacionalização

Os gestores das unidades são os responsáveis pelo gerenciamento dos riscos em seu âmbito de trabalho, com o apoio técnico operacional dos demais agentes públicos. Para que esta

linha de defesa seja eficiente, é necessário seguir os procedimentos operacionais estabelecidos. Como primeira linha de defesa, esses gestores são os responsáveis por identificar, analisar, avaliar, tratar e monitorar os riscos sob sua competência de forma a garantir que eles sejam mantidos em níveis adequados. Compete-lhes, ainda, implementar ações corretivas destinadas a sanar deficiências em processos e controles. Além disso, devem acompanhar o desenvolvimento e a execução da PGRCI em suas unidades, promovendo a consolidação da cultura de gestão de riscos na Universidade.

2ª linha – Supervisão e monitoramento

A segunda linha de defesa é reconhecida através da atuação do Comitê de Governança, Riscos e Controles (CGRC), com o papel de supervisionar a primeira linha de defesa e também garantir o funcionamento adequado do processo de gestão de riscos. Esta supervisão ocorre por meio do monitoramento dos riscos e dos controles resultantes das análises, com o intuito de observar se estão sendo executados conforme planejado. Dessa forma, o Comitê pode intervir diretamente, sugerindo melhorias nos controles internos e na gestão dos riscos executada pelos gestores. As funções da segunda linha de defesa serão exercidas com a assessoria da Diretoria de Governança, Riscos e Conformidade (DGRC).

3ª linha – Avaliação

A terceira linha de defesa é exercida pela Auditoria Interna (Audin), que avalia de forma independente a eficácia do gerenciamento de riscos e controles internos adotado pela primeira linha e supervisão desempenhada pela segunda linha, reportando eventuais deficiências e propondo ações de melhorias.

Apesar de não fazer parte de nenhuma das linhas de defesa acima citadas, os órgãos de controle externos desempenham um papel importante na estrutura geral de governança e controle, contribuindo para o fortalecimento institucional através de suas avaliações periódicas.

3. ÁREAS DE ATUAÇÃO DA GESTÃO DE RISCO

A gestão de riscos na UFOB será implementada de forma gradual nas áreas acadêmicas e administrativas. Esta 1ª edição do Plano de Gestão de Riscos e Controles Internos visa fortalecer a cultura da gestão de riscos por meio da priorização de ações relacionadas a três vertentes (Figura 4): planejamento estratégico, processos organizacionais e integridade.

Figura 4: Áreas de atuação da gestão de riscos na UFOB



Fonte: Elaboração própria

3.1. Riscos no planejamento estratégico

Um dos princípios da gestão de riscos na UFOB é subsidiar tanto a tomada de decisão, quanto a elaboração do planejamento estratégico, conforme art. 4º, inciso IV, da PGRCI. Dessa forma, o gerenciamento de riscos no planejamento estratégico consiste na identificação, na avaliação e no tratamento de riscos relacionados aos objetivos estratégicos definidos no Plano de Desenvolvimento Institucional (PDI) da UFOB.

A gestão de riscos vinculada ao planejamento estratégico concentra-se nos eventos de riscos que possam comprometer ou potencializar os projetos elaborados para atingir os objetivos estratégicos.

A seleção dos objetivos estratégicos que serão trabalhados na gestão de riscos deverá considerar sua relevância/criticidade na execução do PDI. Esse levantamento deverá ser observado na elaboração do planejamento estratégico. A partir dessa seleção, os gestores de riscos irão analisar os projetos vinculados a esses objetivos para aplicar o processo de gerenciamento de riscos.

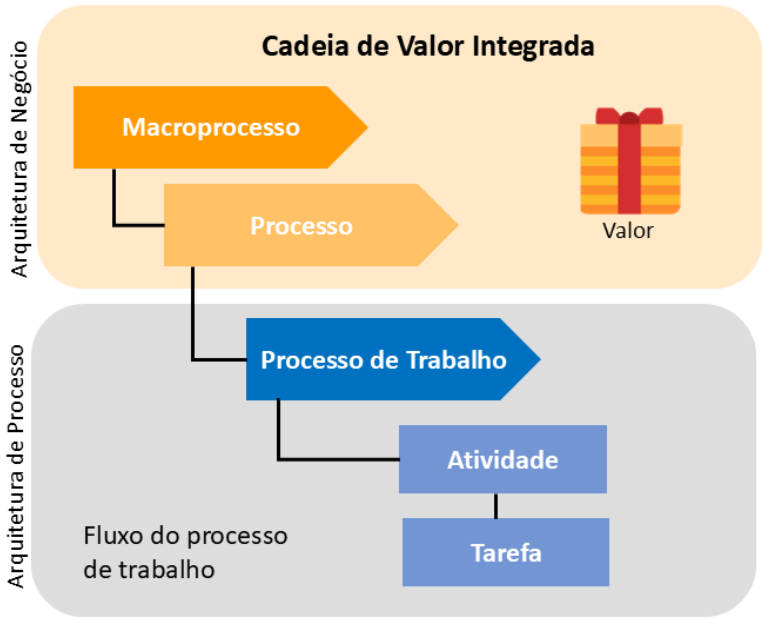
3.2. Riscos nos processos organizacionais

A gestão de riscos nos processos organizacionais visa apoiar a melhoria contínua dos fluxos de trabalho, prevenindo e tratando eventos que comprometam o desempenho dos serviços e ações da Universidade, de acordo com o art. 4º, inciso V, da PGRCI.

Os macroprocessos e processos da UFOB constam na Cadeia de Valor Integrada (CVI), instituída pela Resolução CGAG/CONSUNI/UFOB nº 022, de 3 de abril de 2025. A CVI é a representação de modelo que permite a visão lógica dos processos organizacionais (Figura 6).

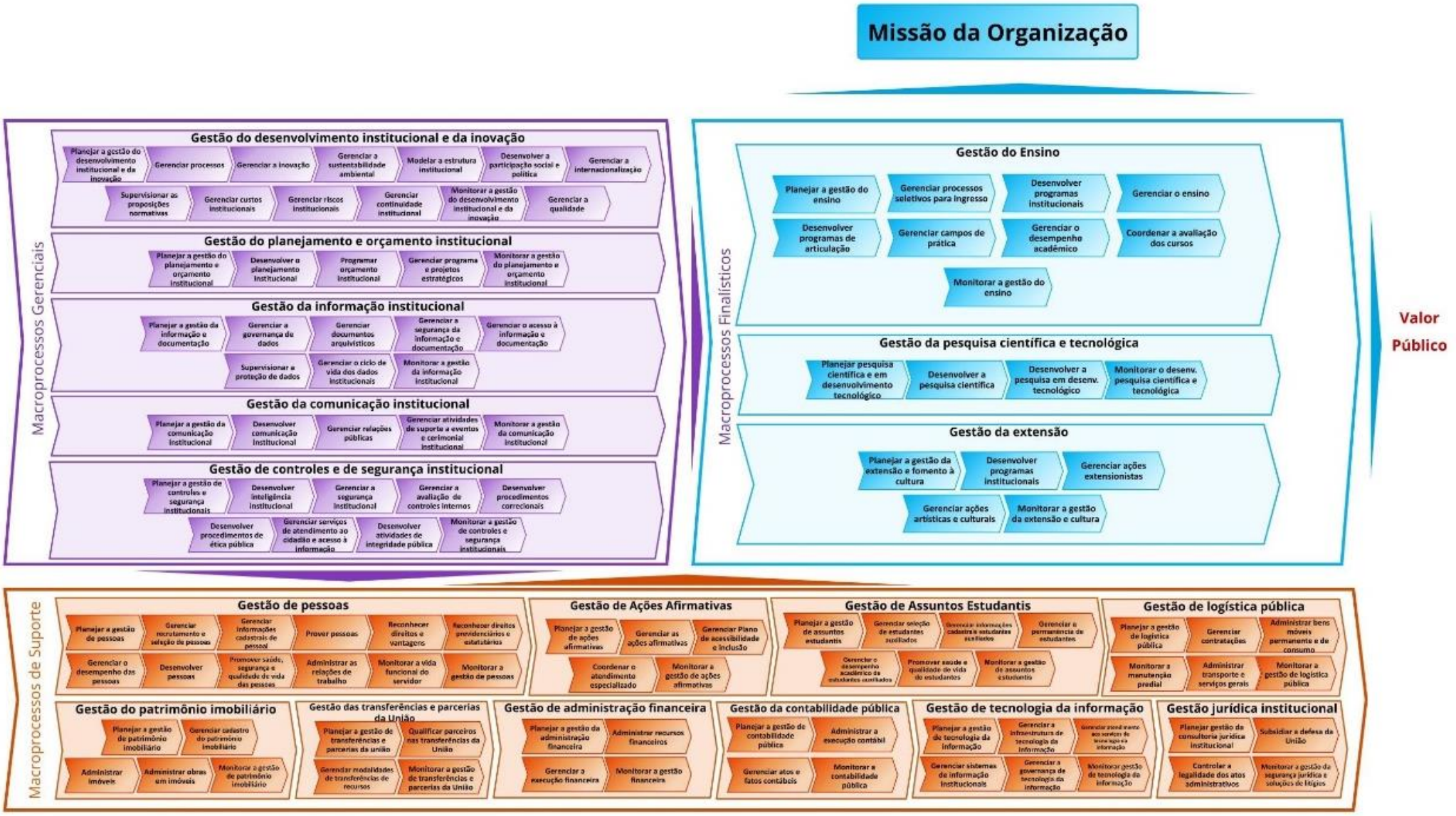
Cada processo da CVI pode gerar um ou mais processos de trabalho, que representam detalhadamente as atividades, o processamento, as entradas e saídas daquele processo (Figura 5).

Figura 5: Hierarquia de processos



Fonte: Elaboração própria

Figura 6: Cadeia de Valor Integrada da UFOB



Fonte: Resolução CGAG/CONSUNI/UFOB nº 022 (UFOB, 2025)

Normalmente, o processo de gerenciamento de riscos é aplicado após o mapeamento de processos, permitindo assim uma visualização e compreensão dos fluxos de trabalho, bem como uma melhor percepção de riscos e oportunidades associados. O mapeamento de processos possibilita também uma melhor implantação de controles e providências voltadas para o tratamento dos riscos, pois apresenta as relações entre atividades e tarefas componentes dos processos, assim como os gargalos existentes. Ainda, é possível uma análise para melhoria dos fluxos processuais e consequente prevenção de riscos.

A situação ideal seria que os processos da Cadeia de Valor Integrada (CVI) já estivessem mapeados. Considerando que a UFOB se encontra em estágio inicial do mapeamento de seus processos, a aplicação do gerenciamento de riscos será realizada concomitantemente com o processo de mapeamento, seguindo os critérios de priorização definidos pela Pró-Reitoria de Planejamento e Desenvolvimento Institucional (Proplan).

3.3. Riscos de integridade

A gestão de riscos de integridade consiste em importante área de atuação do Programa de Integridade, de acordo com a Portaria CGU nº 234, de 6 de novembro de 2025. Segundo a CGU (2018b), consiste em ferramenta que permite aos agentes públicos mapear os processos organizacionais da instituição, de modo a identificar fragilidades que possibilitem a ocorrência de fraudes e atos de corrupção.

À luz da Portaria CGU nº 57/2019, riscos de integridade são vulnerabilidades que podem favorecer ou facilitar a ocorrência de práticas de corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta. Essas vulnerabilidades decorrem de exposições externas, organizacionais ou individuais que possibilitam comportamentos caracterizados como quebra da integridade institucional.

Riscos de integridade podem afetar negativamente a instituição no alcance dos seus objetivos estratégicos, atribuições e/ou missão. Além disso, podem ser causa de outros eventos de risco, tais como financeiros, operacionais ou de imagem.

Os tipos de riscos para a integridade apontados pela CGU (2018b) como mais relevantes e comuns nas organizações públicas são, em uma listagem não exaustiva:

a) abuso de posição ou poder em favor de interesses privados;
b) nepotismo;
c) conflito de Interesses;
d) pressão interna ou externa ilegal ou antiética para influenciar agente público;
e) solicitação ou recebimento de vantagem indevida; e

f) utilização de recursos em favor de interesses privados.

A compreensão acerca dos riscos da integridade é bastante abrangente, porque não consiste apenas em desobediência a regulamentos ou não conformidade legal, mas entra na esfera pessoal. Eventos que possibilitem atitudes que impactem negativamente os princípios da administração pública podem ser entendidos como riscos de integridade, segundo a CGU (2018b).

Os riscos de integridade serão identificados por meio da aplicação do processo de gerenciamento de riscos nos processos organizacionais. Também será realizado um levantamento detalhado das ocorrências de quebras de integridade na instituição, de forma a subsidiar ações estratégicas. As principais fontes de informação para esse levantamento incluem:

a) denúncias registradas no Fala.BR;
b) informações provenientes da Ouvidoria, Corregedoria e da Comissão de Ética;
c) recomendações e determinações dos órgãos de controle;
d) processos judiciais ou encaminhamentos do Ministério Público Federal e Estadual;
e) processos instaurados para aplicação de penalidades a pessoas jurídicas;
f) oficinas com os gestores;
g) outras fontes pertinentes identificadas na UFOB.

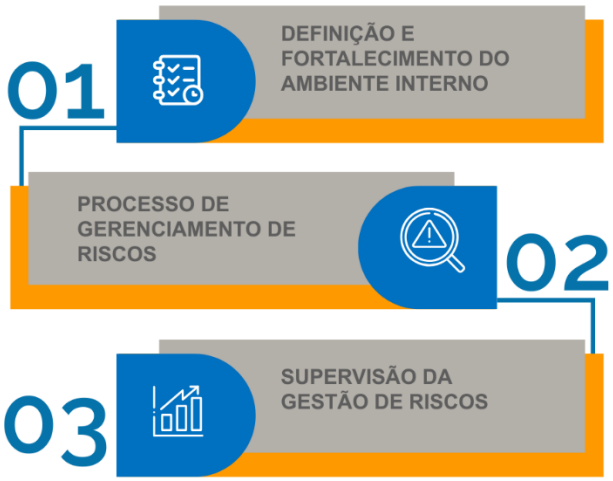
A cada exercício, esse levantamento será realizado para direcionar ações de gestão de riscos a serem realizadas no exercício subsequente.

4. PROCESSO DE GESTÃO DE RISCOS

De acordo com os princípios e diretrizes dispostos na PGRCI, a gestão de riscos deve ser realizada de forma sistemática, estruturada e oportuna, visando, sobretudo, a subsidiar a tomada de decisão e elaboração do planejamento estratégico, assim como promover a melhoria contínua dos processos organizacionais.

A partir dessas orientações e considerando as boas práticas da área, o processo de gestão de riscos na UFOB foi estruturado com as etapas apresentadas na Figura 7.

Figura 7: Etapas do processo de gestão de riscos



Fonte: Elaboração própria

As etapas de “Definição e fortalecimento do ambiente interno” e “Supervisão da gestão de riscos” servem de base para a gestão em nível estratégico e tático, atividades tipicamente desempenhadas pela 2ª linha (CGRC e DGRC). Essas atividades permeiam e impactam todas as etapas do processo de gestão de riscos, na medida que desenvolvem as competências e fornecem os parâmetros necessários para a sua condução.

Já o “Processo de gerenciamento de riscos” é a fase operacional da gestão de riscos, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar

a organização, destinado a fornecer segurança quanto à realização de seus objetivos. A execução dessa etapa cabe à 1ª linha (gestores de risco e agentes públicos).

A seguir são apresentadas as etapas com mais detalhes.

4.1. Definição e fortalecimento do ambiente interno

A definição e o fortalecimento do ambiente interno propício para a gestão de riscos requerem a implementação de um modelo pautado nas boas práticas de governança pública. Isso demanda significativas mudanças culturais, normativas e estruturais, com envolvimento efetivo de toda a comunidade acadêmica, implementação de uma política de capacitação na área de governança e disponibilização de recursos (humanos, tecnológicos, etc.) necessários para a consecução.

Em nível institucional, a responsabilidade por esta etapa concerne ao Consuni e ao CGRC, com o apoio da DGRC. Em nível setorial, os gestores das unidades são responsáveis por promover a cultura da gestão de risco em seus âmbitos de trabalho. O envolvimento efetivo de toda a comunidade demanda ações para a difusão de informações relativas à governança e gestão de riscos na UFOB, com o intuito de disseminar a real importância de gerenciar riscos em cada unidade.

As atividades que fazem parte dessa etapa são:

1. **Definição da Política de Gestão de Riscos e Controles Internos**: visa estabelecer os princípios, objetivos, diretrizes e responsabilidades;
2. **Estabelecimento do contexto externo**: visa entender as leis, normas, políticas, planos, procedimentos e boas práticas na área;
3. **Estabelecimento do ambiente interno**: visa definir claramente os papéis que formarão as linhas de defesa, prover recursos e condições para execução das atividades e capacitação dos responsáveis pela gestão de riscos, servidores e demais agentes públicos; e
4. **Elaboração do Plano de Gestão de Riscos e Controles Internos**: visa definir a metodologia e instrumentos de operacionalização da gestão de riscos e também a definição dos limites de exposição a riscos da Universidade.

4.2. Processo de gerenciamento de riscos

O processo de gerenciamento de riscos consiste em um conjunto ordenado de atividades que permitem avaliar o contexto organizacional e identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos de cada objetivo estratégico ou processo organizacional selecionado.

Nesse contexto, considerando as orientações constantes no art. 7º da PGRCI, o processo de gerenciamento de riscos contemplará as seguintes etapas:

1. **Entendimento do contexto**: etapa em que são identificados os objetivos relacionados ao projeto ou processo organizacional e definidos os contextos interno e externo a serem levados em consideração ao gerenciar riscos;
2. **Identificação de riscos**: etapa em que são identificados possíveis riscos para objetivos associados aos projetos ou processos organizacionais;
3. **Análise de riscos**: etapa em que são identificadas as possíveis causas e consequências do risco;
4. **Avaliação de riscos**: etapa em que são estimados os níveis dos riscos identificados;
5. **Priorização de riscos**: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;
6. **Definição de respostas aos riscos**: etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os projetos e processos organizacionais além de escolha das medidas de controle associadas a essas respostas; e
7. **Comunicação e monitoramento**: etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo do próprio processo de gestão de riscos, com vistas à sua melhoria.

O processo será apresentado de forma mais detalhada no capítulo subsequente.

4.3. Supervisão da gestão de riscos

A supervisão da gestão de riscos tem como finalidade acompanhar o desenvolvimento e o desempenho das ações planejadas para os diversos níveis de atuação. Busca-se, por meio da supervisão, avaliar a efetividade da PGRCI da UFOB. A supervisão é realizada pelo Consuni e CGRC, com apoio da DGRC.

As atividades que fazem parte dessa etapa são:

1. **Acompanhar a Política de Gestão de Riscos e Controles Internos**: visa analisar, avaliar e propor revisões para a política;
2. **Avaliar o desempenho da gestão de riscos e controles internos**: visa avaliar, por meio de relatórios gerenciais, indicadores e avaliação da maturidade, o desempenho da implementação da gestão de riscos e a qualidade dos controles internos na Universidade, promovendo a sua melhoria contínua; e
3. **Supervisionar a atuação das instâncias da gestão de riscos**: visa acompanhar se as instâncias envolvidas no processo estão cumprindo as suas responsabilidades definidas na PGRCI.

5. PROCESSO DE GERENCIAMENTO DE RISCOS

Conforme mencionado anteriormente, o processo de gerenciamento de riscos possui 7 (sete) etapas (Figura 8). Cada etapa será detalhada a seguir.

Figura 8: Etapas do processo de gerenciamento de riscos



Fonte: Elaboração própria

5.1. Entendimento do contexto

A gestão de riscos visa levantar e tratar eventos que possam comprometer o alcance dos objetivos definidos pela organização. Dessa forma, a Etapa 1 do processo de gerenciamento de riscos consiste em examinar minuciosamente o objeto de análise (projeto do planejamento estratégico ou processo organizacional) à luz de seus ambientes interno e externo, identificando e detalhando os seus objetivos específicos.

Para os projetos do planejamento estratégico é necessário vislumbrar os objetivos específicos, as iniciativas e os indicadores relacionados, e também outras informações que permitam uma visão ampla e consubstanciada do contexto interno e externo.

No caso dos processos organizacionais é necessário fixar os objetivos alcançados pelo processo. Se for possível, devem ser indicados o objetivo geral e os objetivos específicos do processo, considerando as perspectivas estratégica, temporal, legal, financeira/orçamentária, entre outras, alinhados ao PDI e CVI.

Questionamento orientativo para esta etapa:

O que deve ser atingido na perspectiva _____para se concluir que o projeto/processo ocorreu com sucesso?

Uma vez fixados os objetivos (gerais e específicos), pode-se iniciar a identificação e análise de riscos.

5.2. Identificação e Análise de riscos

Nessa etapa, o gestor de risco, com o apoio dos agentes públicos envolvidos no projeto/processo, deve construir uma lista abrangente de eventos de risco que possam comprometer o alcance dos objetivos gerais e específicos estabelecidos na Etapa 1.

Os riscos em potencial podem ser obtidos a partir do seguinte questionamento:

Que eventos podem EVITAR, ATRASAR, PREJUDICAR ou IMPEDIR o atingimento dos objetivos?

Os eventos identificados inicialmente podem ser analisados e revisados, reorganizados, reformulados e até eliminados nesta etapa, e, para tanto, podem ser utilizadas as seguintes questões:

a) O evento é um risco que pode comprometer claramente um dos objetivos?
b) O evento identificado é um risco ou uma causa para um risco?
c) O evento é um risco ou uma falha no desenho do processo? (processo organizacional)
d) O evento é um risco ou uma falha no planejamento das ações estratégicas? (projeto estratégico)

e) O evento é um risco ou uma fragilidade em um controle para tratar um risco do processo?

Os resultados dessa análise devem ser documentados na Planilha de Mapeamento de Riscos (APÊNDICE B), preenchendo os seguintes campos:

a) **Evento de risco**: evento que pode evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos identificados na Etapa 1;
b) **Tipo do risco**: indica se o evento de risco é uma oportunidade ou uma ameaça; e
c) **Categoria do risco**: diz respeito à origem dos fatores que influenciam o evento de risco, conforme Quadro 2;

Por fim, deve-se realizar a análise de cada evento e preencher os seguintes campos:

a) **Causas do risco**: fatores que desencadeiam a ocorrência do evento de risco; e
b) **Consequências do risco**: possíveis efeitos da ocorrência do evento de risco.

Existem diversas ferramentas para identificação e análise de riscos, notadamente especificadas no documento "ABNT NBR ISO 31010:2012 Gestão de riscos – Técnicas para o processo de avaliação de riscos", que traz dezenas de ferramentas que apoiam e dão estrutura para a gestão de riscos (ABNT, 2012). Na UFOB, considerando que a maturidade do processo gestão de riscos se encontra em estágio inicial, sugere-se utilizar ferramentas mais simples com as pessoas envolvidas nos projetos/processos, tais como:

a) levantamento de dados históricos – pesquisa em dados cadastrados nos diversos sistemas da Universidade, informações de processos, de órgãos de controle, entre outros;
b) reuniões e realização de entrevistas – identificação de eventos com base na experiência e no conhecimento acumulado da gestão, do pessoal, ou de outras partes interessadas por meio de discussões estruturadas; e
c) análise do fluxo de processo – essa técnica reúne as entradas, as tarefas, as responsabilidades e as saídas que se combinam para formar um processo, sendo assim, é possível identificar eventos que possam afetar o cumprimento dos objetivos deste.

Via de regra, os eventos não ocorrem de forma isolada, um evento poderá desencadear outro, ou ocorrerem concomitantemente. A avaliação dos relacionamentos entre dois ou mais eventos de riscos permite determinar em que pontos os esforços da gestão de riscos devem ser direcionados.

Quadro 2: Categorias de riscos



Fonte: Elaboração própria

5.3. Avaliação de riscos

O objetivo dessa etapa é compreender a natureza do risco e suas características, avaliando-se o nível do risco em termos da gravidade dos impactos, as incertezas, a tendência e a eficácia dos controles.

A etapa de avaliar os riscos identificados considera a probabilidade de ocorrência e o impacto dos riscos para então priorizá-los, de modo a permitir que se direcione o foco para os riscos de alta prioridade, essas informações vão subsidiar as decisões para o tratamento dos riscos.

Para cada evento identificado, o gestor de risco, com o apoio dos agentes públicos envolvidos no projeto/processo, deve calcular o nível de risco, a partir dos critérios de probabilidade e de impacto. É importante frisar que a metodologia adotada na Universidade será quali-quantitativa, em que as percepções dos envolvidos no processo serão convertidas em valores ordinais tanto para a probabilidade quanto para o impacto. A partir disso, serão realizadas operações algébricas simples como forma de avaliar o nível de risco do evento e o risco residual gerado após a implementação de controles.

Para o contexto da UFOB foi definida uma escala de 5 (cinco) pontos para avaliação da probabilidade, cada uma possui uma chance de ocorrência e uma descrição diferenciada (Quadro 3).

Com relação ao impacto definiu-se também uma escala de 5 (cinco) pontos, cuja base da avaliação é o atendimento dos objetivos da organização, detalhada no Quadro 4.

A análise das consequências (impacto) requer a parametrização de questões de apoio, como por exemplo: “Qual o impacto na atividade, objetivo do processo, ou objetivo estratégico presente no PDI, caso o risco identificado se materialize?”. Como na análise de probabilidades, a resposta à esta questão de apoio deve ser classificada a partir da análise do impacto das consequências. O Quadro 5 permite que o gestor de risco possa avaliar o impacto baseado nas consequências em algumas áreas que podem ser afetadas.

Quadro 3: Escala de probabilidade

PROBABILIDADE	DESCRIÇÃO, DESCONSIDERANDO OS CONTROLES	PESO
Muito baixa	**Improvável**. Em situações excepcionais, o evento pode até ocorrer, mas nada nas circunstâncias indica essa possibilidade. Este evento pode ter acontecido anteriormente na instituição. Entretanto, na ausência de outras informações ou circunstâncias excepcionais, não seria esperado que ocorresse na instituição no futuro próximo.	**1**
Baixa	**Rara**. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade. O evento não ocorre de maneira frequente na instituição. Os controles atuais e as circunstâncias sugerem que a ocorrência seria considerada altamente não usual.	**2**
Média	**Possível**. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade. O evento pode ter ocorrido ocasionalmente na instituição. Os controles atuais ou as circunstâncias sugerem que há uma possibilidade plausível de ocorrência.	**3**
Alta	**Provável**. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade. Este evento pode ocorrer regularmente na instituição. Com os controles atuais ou circunstâncias, pode-se esperar que ocorra ao longo de um ano.	**4**
Muito alta	**Praticamente certa**. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade. Este evento ocorre frequentemente na instituição. Com os controles atuais ou circunstâncias, espera-se sua ocorrência.	**5**

Fonte: Adaptado de Metodologia de Gestão de Riscos (CGU, 2018)

Quadro 4: Escala de impacto

IMPACTO	DESCRIÇÃO DO IMPACTO NOS OBJETIVOS, CASO O EVENTO OCORRA	PESO
Muito baixo	**Mínimo** impacto nos objetivos (estratégicos, operacionais, de informação / comunicação / divulgação ou de conformidade).	**1**
Baixo	**Pequeno** impacto nos objetivos (idem).	**2**
Médio	**Moderado** impacto nos objetivos (idem), porém recuperável.	**3**
Alto	**Significativo** impacto nos objetivos (idem), de difícil reversão.	**4**
Muito alto	**Catastrófico** impacto nos objetivos (idem), de forma irreversível.	**5**

Fonte: Adaptado de Metodologia de Gestão de Riscos (CGU, 2018)

Quadro 5: Áreas de impacto

ÁREAS DE IMPACTO					
NÍVEL	**ABRANGÊNCIA**	**DESEMPENHO OPERACIONAL**	**LEGAL/ CONFORMIDADE**	**IMAGEM/ REPUTAÇÃO**	**FINANCEIRO/ ORÇAMENTÁRIO**
	Impacta na instituição inteira ou somente algumas unidades?	Interrompe as operações ou a entrega de produtos/serviços? Afeta projetos, programas ou ações?	Viola leis, normas ou procedimentos? Pode resultar em litígios ou multas?	Afeta a imagem da Universidade? Traz exposição na mídia? Quem representa a Universidade frente a mídia?	Afeta o orçamento institucional? Compromete a sustentabilidade financeira?
Muito baixo	Impacto mínimo. Apenas um setor é afetado.	Impacto mínimo nas operações ou resultados dos processos. Não compromete o alcance dos objetivos propostos. Regularização rápida pela equipe interna através da revisão de processos de trabalho.	Não afeta a conformidade com a legislação, regulação vigente ou procedimentos internos.	Apenas o setor envolvido toma conhecimento. Gera pouca preocupação interna. Sem cobertura ou exposição na mídia.	Impacto mínimo no orçamento institucional, recuperável no exercício financeiro atual.
Baixo	Vários setores de uma mesma unidade são afetados.	Pode ocorrer alguma interrupção nas operações ou resultados dos processos. Regularização rápida pela equipe interna.	Resulta em questões legais menos complexas. Afeta pouco as questões de legislação/regulação, mas que podem, eventualmente, ser tratadas pela Procuradoria Jurídica.	Apenas os envolvidos tomam conhecimento. Pode ocorrer algum impacto de imagem na comunidade interna. Eventual atenção e exposição negativa na mídia local.	Impacto pequeno, mas perceptível, no orçamento institucional, recuperável no exercício financeiro atual.
Médio	Uma unidade inteira é afetada.	Ocorre interrupção nas operações ou resultados dos processos, com impacto no fluxo do trabalho. Requer priorização na unidade para regularizar a situação.	Afeta a conformidade de legislação/regulação, resulta em incidente sério, com possível investigação e avaliação sobre responsabilidade legal.	Atenção e exposição negativa na mídia, podendo levar a perda de confiança na instituição. Gera preocupação na alta administração.	Impacto alto no orçamento institucional, recuperável no exercício financeiro atual, mas requer priorização.
Alto	Várias unidades são afetadas.	Ocorre interrupção severa nas operações ou resultados dos processos, com impacto negativo na imagem da Universidade. Requer priorização da alta gestão para regularizar a situação.	Resulta em violações graves de legislação e regulação vigente. Pode envolver litígios que requeiram envolvimento da Procuradoria Jurídica.	Atenção e exposição negativa e prolongada na mídia, podendo levar a perda de confiança na instituição. Requer foco total da alta administração para regularizar a situação.	Impacto muito alto no orçamento institucional, não recuperável no exercício financeiro atual, nem no próximo.
Muito alto	Toda a Universidade é afetada.	Ocorre interrupção completa nas operações ou resultados dos processos por tempo indeterminado, exigindo intervenção da alta administração para regularizar a situação.	Resulta em violações graves de legislação e regulação vigente. Resulta em litígios e multas significativas.	Atenção e exposição extremamente negativa e prolongada na mídia. Perda de confiança na instituição. Requer foco total da alta administração para regularizar a situação.	Impacto crítico de longo prazo no orçamento institucional, não recuperável no exercício financeiro atual, nem no próximo.

Fonte: Plano Institucional de Gestão de Riscos e Controles Internos da UFSB (UFSB, 2020)

A multiplicação entre os valores de probabilidade e de impacto define o **nível do risco inerente** (RI), ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade de sua ocorrência ou de seu impacto.

Risco Inerente = Probabilidade X Impacto

A partir do resultado do cálculo, o risco pode ser classificado dentro das seguintes faixas (Quadro 6):

Quadro 6: Classificação de risco

CLASSIFICAÇÃO	FAIXA
Risco Baixo – RB	**1 - 5**
Risco Médio - RM	**6 - 11**
Risco Alto - RA	**12 -19**
Risco Extremo - RE	**20 - 25**

Fonte: Adaptado de Metodologia de Gestão de Riscos (CGU, 2018)

O Quadro 7 representa a matriz de possíveis resultados da combinação das escalas de probabilidade e impacto, considerando a classificação de risco definida.

Em seguida, o gestor de risco, com o apoio dos agentes públicos envolvidos no projeto/processo, deve avaliar a eficácia dos controles internos existentes em relação aos objetivos estabelecidos, ou seja, é necessário verificar se os controles instituídos têm auxiliado no tratamento adequado desse risco. Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações e medidas que a gestão adota com o objetivo de modificar o nível de risco (ABNT, 2009). O nível de confiança (NC) será correspondente a um fator de avaliação dos controles (FAC) existentes, conforme apresentado no Quadro 8.

Quadro 7: Matriz de riscos

IMPACTO						
	Muito alto 5	5 RB	10 RM	15 RA	20 RE	25 RE
	Alto 4	4 RB	8 RM	12 RA	16 RA	20 RE
	Médio 3	3 RB	6 RM	9 RM	12 RA	15 RA
	Baixo 2	2 RB	4 RB	6 RM	8 RM	10 RM
	Muito Baixo 1	1 RB	2 RB	3 RB	4 RB	5 RB
		Muito baixa 1	Baixa 2	Média 3	Alta 4	Muito Alta 5
	PROBABILIDADE					

Fonte: Adaptado de Metodologia de Gestão de Riscos (CGU, 2018)

Quadro 8: Fatores de avaliação dos controles

NÍVEL DE CONFIANÇA	DESCRIÇÃO	FATOR DE AVALIAÇÃO DOS CONTROLES
Inexistente	Controles existentes, mal desenhados ou mal implantados, isto é, não funcionais.	**1**
Fraco	Controles têm abordagens *ad hoc*, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas, em geral realizados de maneira manual.	**0,8**
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	**0,6**
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	**0,4**
Forte	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco. São periodicamente testados, revisados e aperfeiçoados.	**0,2**

Fonte: Adaptado de Metodologia de Gestão de Riscos (CGU, 2018)

O valor final da multiplicação entre o valor do risco inerente e o fator de avaliação dos controles corresponde ao **nível de risco residual** (RR).

Risco Residual = Risco Inerente X Fator de Avaliação dos Controles

Pela fórmula é possível deduzir que quanto maior for o RR, menor será o NC e vice-versa, porém este nunca será “zero”, uma vez que o nível de confiança jamais será 100%.

O valor de risco residual pode fazer com que o risco se enquadre em uma faixa de classificação diferente da faixa definida para o risco inerente.

Saliente-se que o nível do risco determinado a partir da avaliação servirá de base para a classificação e priorização dos riscos e posterior planejamento das ações. Assim, a partir do resultado dessa avaliação, os riscos que deverão ser constantemente monitorados serão definidos, assim como as estratégias para tratamento de cada um deles.

As informações destas etapas devem ser registradas na Planilha de Mapeamento de Riscos (APÊNDICE B).

5.4. Priorização de riscos

Nessa etapa, devem ser considerados os valores dos níveis de riscos residuais calculados na etapa anterior para identificar quais riscos serão priorizados para tratamento e o tipo de resposta aplicável a cada caso.

A priorização dos riscos residuais para tratamento deve ser determinada a partir do apetite ao risco. Apetite ao risco é o nível de risco que uma organização está predisposta a assumir para implementar sua estratégia, atingir seus objetivos e agregar valor para as partes interessadas, no cumprimento de sua missão. Assim, por definição, apetite ao risco é o limite que a "organização está predisposta a assumir", sem a obrigatoriedade de realização de uma ação adicional de tratamento do risco.

A UFOB, por meio deste plano, define como “apetite ao risco” aqueles riscos residuais considerados BAIXO e MÉDIO, conforme valores estabelecidos no Quadro 6.

Dessa forma, todos os riscos cujos níveis estejam dentro dos níveis aceitáveis (BAIXO e MÉDIO) podem ser assumidos, e um possível tratamento pode ser realizado caso o gestor de risco entenda ser necessário.

Todos os riscos cujos níveis estejam fora dos níveis aceitáveis (ALTO e EXTREMO) deverão ser tratados e monitorados, e uma possível inexistência de tratamento deve ser justificada. O Quadro 9 mostra, por classificação, quais ações devem ser adotadas em relação ao risco.

Quadro 9: Diretrizes de priorização dos riscos a serem tratados

NÍVEL DE RISCO	AVALIAÇÃO DE RISCO	ORIENTAÇÃO
RISCO BAIXO (1 a 5)	Aceitável	Nível 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-benefício, como diminuir o nível de controles. O risco deve ser registrado, mas não é necessário seu tratamento.
RISCO MÉDIO (6 – 11)	Gerenciável	Nível dentro do apetite a risco. O risco deve ser registrado, mas seu tratamento é opcional, cabendo ao gestor julgar se é oportuno ou conveniente elaborar plano de tratamento. Requer atividades de monitoramento e atenção da unidade com os controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.
RISCO ALTO (12 – 19)	Indesejável	Nível além do apetite a risco. Riscos altos devem ser reduzidos ou tratados e é necessário ter planos de tratamento elaborados. Demandam atividades específicas de monitoramento e controle por parte do gestor de risco para que se mantenham nesse nível ou sejam reduzidos.
RISCO EXTREMO (20 – 25)	Inaceitável	Nível além do apetite a risco. É necessário elaborar plano de tratamento com possibilidade de execução imediata para sua mitigação. O gestor de risco deverá comunicar o risco ao Comitê para ser discutido em âmbito estratégico.

Fonte: Adaptado de Metodologia de Gestão de Riscos (CGU, 2018)

As informações desta etapa devem ser registradas na Planilha de Mapeamento de Riscos (APÊNDICE B).

5.5. Definição de respostas ao risco

A definição de respostas ao risco envolve a seleção de uma opção de tratamento para modificar o nível do risco e a elaboração de planos que, uma vez implementados, implicarão em novos controles ou alteração dos existentes.

Para cada risco priorizado deve ser selecionada uma opção de tratamento. Essa escolha depende do nível do risco e dos custos associados à implementação dos controles, conforme Quadro 10. Portanto, essa decisão deve contar com a participação de todos os envolvidos no tratamento, assim como das instâncias responsáveis por prover os recursos necessários.

Quadro 10: Opções de tratamento de risco

OPÇÃO DE TRATAMENTO	DESCRIÇÃO
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.
MITIGAR	Um risco normalmente é mitigado quando é classificado como **"Alto"** ou **"Extremo"**. A implementação de controles, neste caso, apresenta um custo/benefício adequado. Mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas nas etapas de Identificação e Avaliação de Riscos.
COMPARTILHAR	Um risco normalmente é compartilhado quando é classificado como **"Alto"** ou **"Extremo"**, mas a implementação de controles não apresenta um custo/benefício adequado. Pode-se identificar outra unidade que tenha mais robustez para tratá-lo ou 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 **"Extremo"**, mas a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades (internas ou externas) dispostas a compartilhar o risco com a UFOB. Caso essa opção incorra na interrupção do projeto ou processo organizacional, a decisão deve ser aprovada pelo Comitê de Governança, Riscos e Controles.

Fonte: Adaptado de Metodologia de Gestão de Riscos (CGU, 2018)

As informações sobre a opção de tratamento devem ser registradas na Planilha de Mapeamento de Riscos (APÊNDICE B).

Após determinar a resposta ao risco, deve-se estabelecer controles, levando em consideração as causas e as consequências, sendo que para as causas orienta-se estabelecer um plano de tratamento, visando mitigar ou evitar a probabilidade de sua ocorrência. Já para as consequências orienta-se estabelecer plano de contingência, visando reduzir seus impactos caso os riscos se concretizem.

O Plano de Tratamento é um planejamento de ações para a implementação das medidas preventivas. Ele deve conter:

a) **Responsável pela implementação das medidas de tratamento:** esse deve ser um agente público que será designado pelo gestor de risco e será automaticamente associado ao Plano de Tratamento;

b) **Ações preventivas**: medidas que visam diminuir a probabilidade de ocorrência do evento;

c) **Monitoramento**: periodicidade e/ou mecanismos adotados para verificar a implementação das ações;

d) **Recursos**: descrição dos recursos necessários, incluindo pessoal e financeiro;

e) **Data prevista para o início da implementação**;

f) **Data prevista para o término da implementação**.

A implementação do Plano de Tratamento visa à redução do nível do risco residual (RR), ou seja, do risco ainda existente mesmo após a implementação dos controles. Caso o novo risco residual ainda não esteja dentro do apetite a risco da Universidade após a implementação do plano de tratamento elaborado, outro plano deve ser planejado e executado, até que o risco residual possa ser aceito.

O própria C deste documento traz um modelo de Plano de Tratamento. Cabe ao gestor de risco o gerenciamento das atividades e o registro das ações adotadas, com vistas à construção de um histórico de melhores práticas e à elaboração de relatórios de monitoramento.

É importante que, em uma primeira abordagem da elaboração do Plano de Tratamento, se avalie a necessidade de melhorar ou extinguir controles já existentes. Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, observados sempre critérios de eficiência e eficácia de sua implementação. O APÊNDICE D apresenta sugestões de controles que podem ser implementados.

A responsabilidade primária pelo tratamento de cada risco é atribuída ao gestor responsável pelo processo. Entretanto, se as iniciativas definidas no Plano de Tratamento envolverem mais de uma unidade, o responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta de plano para que essas unidades validem as iniciativas de que participarem. Independente da situação, o principal responsável pela implementação da iniciativa deverá monitorar e reportar a evolução das iniciativas.

Ainda na etapa de definição de respostas ao risco, está prevista a elaboração do Plano de Contingência, que se trata de uma definição prévia das ações que serão tomadas caso um risco venha a se concretizar. Ele deve conter:

a) **Gatilho**: situação que determina o início das ações de contingência.

b) **Responsável pela implementação das medidas de contingência**, esse deve ser um agente público que será designado pelo gestor de risco e será automaticamente associado ao Plano de Contingência. O responsável deve ser imediatamente comunicado

em caso de ocorrência do risco para que possa demandar a execução das ações de contingência;

c) **Ações de contingência**: ações imediatas que devem ser executadas em caso de ocorrência do evento, com o objetivo de atenuar seu impacto (consequências).

O APÊNDICE E deste documento traz um modelo de Plano de Contingência.

Como continuidade desta etapa, em caso de ocorrência do evento de risco, a unidade dele realizar seu registro. Registrar as ocorrências possibilitam mapear a instituição e demonstrar as unidades com maiores tendências de incidentes, gerando um histórico, possibilitando a implementação de medidas mais assertivas na prevenção dos fatores de risco e mitigação dos impactos gerados pelas consequências do risco.

Importante salientar que o gestor do risco, bem como os responsáveis pelo plano de tratamento e contingência, deve informar à DGRC quando houver a ocorrência do evento de risco.

No Registro da Ocorrência deve conter:

d) **Evento de Risco**: evento que pode evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos identificados na Etapa 1;
e) **Data da ocorrência**: data em que ocorreu o evento;
f) **Descrição da ocorrência**: descrição da ocorrência de forma detalhada e sua relação com o evento de risco;
g) **Responsável pela solução**: responsável pela implementação das medidas de tratamento e/ou contingência;
h) **Solução**: descrição detalhada das soluções adotadas para resolução do evento de risco;
i) **Resultados**: descrever de forma sucinta os resultados alcançados com a solução do evento de risco.

O APÊNDICE F deste documento traz um modelo de Registro de Ocorrência.

5.6. Comunicação e monitoramento

Na PGRCI está previsto que a comunicação e monitoramento é a etapa que ocorre durante todo o processo de gerenciamento de riscos, sendo responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo do próprio processo de gestão de riscos, com vistas à sua melhoria.

5.6.1. Comunicação

A comunicação objetiva garantir um fluxo constante de informações com as pessoas envolvidas, internas e externas, durante todas as etapas do processo de gestão de riscos, de modo a compartilhar e obter informações relevantes. Algumas orientações devem ser estabelecidas e de amplo conhecimento de todos:

a) Conhecimento deste plano e das responsabilidades em seus diversos níveis de gestão;
b) Mecanismos utilizados para o registro das informações;
c) Disponibilidade de informações necessárias para a gestão de riscos em todas as etapas.

Conhecimento deste plano e das responsabilidades em seus diversos níveis de gestão

A implementação deste plano requer ampla divulgação em todas as unidades acadêmicas e administrativas da UFOB. Essa divulgação deve ser iniciada no âmbito do CGRC, que conta com a participação de gestores. No âmbito de cada unidade, cabe a cada gestor divulgar o documento aos agentes públicos. É indispensável que todas as partes envolvidas estejam, durante todo o processo, cientes de suas responsabilidades e de posse de informações que assegurem a tomada de decisões precisas no âmbito das unidades e em nível institucional.

Nesse sentido, o Quadro 11 apresenta a matriz de responsabilidades do processo de gestão de riscos, considerando todas as etapas do processo, as responsabilidades das unidades e agentes públicos envolvidos. Essa matriz define as responsabilidades de acordo com as atividades que cada um deve desempenhar no processo de gestão de riscos:

a) **Autoridade**: quem aprova a tarefa ou produto (pode delegar a função, mas mantém a responsabilidade);
b) **Responsável**: quem executa a atividade;
c) **Consultado**: quem presta informações essenciais ou que pode agregar valor para a implementação do processo;
d) **Informado**: quem deve ser informado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

Mecanismos utilizados para o registro das informações

O processo de gestão de riscos exige que informações sejam salvas e também transmitidas entre as pessoas por diversos mecanismos, com o propósito de orientar todos os envolvidos e garantir o acesso aos dados necessários para a execução das atividades.

O Quadro 12 apresenta o Plano de Comunicação, que tem como objetivo orientar para cada etapa, as atividades de comunicação que são necessárias, quais ferramentas devem ser utilizadas, quem são as partes envolvidas, o objetivo da comunicação, as informações transmitidas e a periodicidade.

Disponibilidade de informações necessárias para a gestão de riscos em todas as etapas

O acesso às informações tempestivas, precisas, íntegras, confiáveis e disponíveis é primordial para que a gestão de riscos seja adequada e eficaz no alcance de seus objetivos.

A comunicação interna e externa sobre a gestão de riscos e seus resultados deve observar os requisitos para acesso à informação. De forma geral, as informações produzidas durante as etapas do processo de gerenciamento de riscos têm caráter restrito, uma vez que a sua ampla divulgação pode expor a Universidade a vulnerabilidades. Já as informações gerenciais acerca do monitoramento da gestão de riscos constituem informação pública nos termos da Lei de Acesso à Informação - LAI (Lei nº 12.527/2011). Casos específicos deverão ser avaliados pelo CGRC.

Nesse sentido, a transparência ativa das informações relativas à gestão de riscos na UFOB será promovida por intermédio do CGRC e DGRC, por meio de relatórios gerenciais, painéis de dados e materiais publicados no portal da UFOB, entre outros.

De forma complementar, e sempre que necessário, a DGRC poderá solicitar às unidades acadêmicas e administrativas:

a) informações relativas à gestão de riscos dos projetos e processos sob sua responsabilidade;
b) demais informações necessárias ao atendimento de demandas internas ou externas relativas a este plano.

Ainda no âmbito da comunicação, cabe à DGRC alertar ao CGRC sobre questões emergentes ou alterações no cenário regulatório da gestão de riscos, que possam eventualmente impactar o processo de gestão de riscos da UFOB.

Quadro 11: Matriz de responsabilidades na gestão de riscos

ETAPAS	RESPONSÁVEIS					
	CONSUNI	Comitê de Governança, Riscos e Controles	Diretoria de Governança Riscos e Conformidade	Gestor do Risco	Agentes públicos envolvidos no processo	Responsável pelo Plano de Tratamento
DEFINIÇÃO E ESTABELECIMENTO DO AMBIENTE INTERNO						
Definição da Política de Gestão de Riscos e Controles Internos	Autoridade	Responsável				
Estabelecimento do contexto externo		Autoridade	Responsável			
Estabelecimento do ambiente interno		Autoridade	Responsável			
Elaboração do Plano de Gestão de Riscos e Controles Internos		Autoridade	Responsável			
ETAPAS DO PROCESSO DE GERENCIAMENTO DE RISCOS						
Entendimento do contexto (Etapa 1)			Informado	Autoridade	Responsável	
Identificação e análise de riscos (Etapas 2 e 3)			Informado	Autoridade	Responsável	
Avaliação de riscos (Etapa 4)			Informado	Autoridade	Responsável	
Priorização de riscos (Etapa 5)			Informado	Autoridade	Responsável	
Plano de Tratamento (Etapa 6)			Informado	Autoridade		Responsável
Plano de Contingência (Etapa 6)			Informado	Autoridade		Responsável
Plano de Comunicação (Etapa 7)		Autoridade	Responsável	Responsável	Responsável	Responsável
Monitoramento (operacional) (Etapa 7)			Informado	Responsável	Responsável	Responsável
Monitoramento (gerencial) (Etapa 7)		Autoridade	Responsável	Consultado		

ETAPAS	RESPONSÁVEIS					
	CONSUNI	Comitê de Governança, Riscos e Controles	Diretoria de Governança Riscos e Conformidade	Gestor do Risco	Agentes públicos envolvidos no processo	Responsável pelo Plano de Tratamento
SUPERVISÃO DA GESTÃO DE RISCOS						
Acompanhar a Política de Gestão de Riscos e Controles Internos	Autoridade	Responsável				
Avaliar o desempenho da gestão de riscos e controles internos		Autoridade	Responsável			
Supervisionar a atuação das instâncias da gestão de riscos		Autoridade	Responsável			

Fonte: Elaboração própria

Quadro 12: Plano de Comunicação

PRODUTOS O que precisa ser comunicado?	OBJETIVO Qual é o propósito da comunicação?	COMUNICADOR Quem é o responsável pela emissão da comunicação?	DESTINATÁRIOS Quem é o receptor da comunicação?	MEIO DE COMUNICAÇÃO Qual instrumento deve ser utilizado?	SISTEMA Onde a comunicação será divulgada?	FREQUÊNCIA Quando a comunicação deve ser emitida?
DEFINIÇÃO E FORTALECIMENTO DO AMBIENTE INTERNO						
Política de Gestão de Riscos e Controles Internos	Estabelecer princípios, objetivos, diretrizes e responsabilidades.	Consuni	Comunidade interna e externa à UFOB	Resolução	Portal da UFOB	Imediatamente após a aprovação do documento.
Plano de Gestão de Riscos e Controles Internos	Orientar a operacionalização da gestão de riscos na UFOB em cumprimento às diretrizes da PGRCI.	CGRC	Comunidade interna e externa à UFOB	Plano	Portal da UFOB	Imediatamente após a aprovação ou atualização do documento.
Capacitação em gestão de riscos	Propiciar o desenvolvimento das pessoas envolvidas com o processo de gestão de riscos	DGRC	Agentes públicos	Material de divulgação	Sistema de e-mail e Portal da UFOB	Conforme a necessidade
Informações sobre o processo de gestão de riscos	Orientar a execução técnica e operacional do processo gerenciamento de riscos.	DGRC	Agentes públicos	Manuais, guias, tutoriais, cartilhas, etc.	Sistema de e-mail e Portal da UFOB	Conforme a necessidade
ETAPAS DO PROCESSO DE GERENCIAMENTO DE RISCOS						
Entendimento do contexto (Etapa 1)	Examinar o objeto de análise à luz de seus ambientes interno e externo, identificando e detalhando os objetivos específicos e os fatores que podem influenciar a sua consecução.	Gestores de riscos, com o apoio dos agentes públicos envolvidos no projeto/processo	DGRC	Planilha de maneira inicial e inserção das informações no sistema	A planilha utilizará o sistema de e-mail e as informações serão inseridas no sistema	Após o término da aplicação do processo de gerenciamento de riscos.

PRODUTOS O que precisa ser comunicado?	OBJETIVO Qual é o propósito da comunicação?	COMUNICADOR Quem é o responsável pela emissão da comunicação?	DESTINATÁRIOS Quem é o receptor da comunicação?	MEIO DE COMUNICAÇÃO Qual instrumento deve ser utilizado?	SISTEMA Onde a comunicação será divulgada?	FREQUÊNCIA Quando a comunicação deve ser emitida?
ETAPAS DO PROCESSO DE GERENCIAMENTO DE RISCOS						
Identificação e análise de riscos (Etapas 2 e 3)	Construir uma lista de eventos de risco que possam comprometer o alcance dos objetivos estabelecidos na Etapa 1	Gestores de riscos, com o apoio dos agentes públicos envolvidos no projeto/processo	DGRC	Planilha de maneira inicial e inserção das informações no sistema	A planilha utilizará o sistema de e-mail e as informações serão inseridas no sistema	Após o término da aplicação do processo de gerenciamento de riscos.
Avaliação de riscos (Etapa 4)	Avaliar os riscos para cada um dos eventos identificados na etapa anterior, considerando os critérios de probabilidade e de impacto.	Gestores de riscos, com o apoio dos agentes públicos envolvidos no projeto/processo	DGRC	Planilha de maneira inicial e inserção das informações no sistema	A planilha utilizará o sistema de e-mail e as informações serão inseridas no sistema	Após o término da aplicação do processo de gerenciamento de riscos.
Priorização dos riscos (Etapa 5)	Identificar quais riscos serão priorizados para tratamento e o tipo de resposta aplicável a cada caso.	Gestores de riscos, com o apoio dos agentes públicos envolvidos no projeto/processo	DGRC	Planilha de maneira inicial e inserção das informações no sistema	A planilha utilizará o sistema de e-mail e as informações serão inseridas no sistema	Após o término da aplicação do processo de gerenciamento de riscos.
Plano de Tratamento (Etapa 6)	Planejar ações para a implementação das medidas preventivas.	Responsável pelo Plano de Tratamento	Gestor do risco e DGRC	Planilha de maneira inicial e inserção das informações no sistema	A planilha utilizará o sistema de e-mail e as informações serão inseridas no sistema	Após o término da aplicação do processo de gerenciamento de riscos.
Plano de Contingência (Etapa 6)	Planejar ações para a implementação das medidas de contingência.	Responsável pelo Plano de Contingência	Gestor do risco e DGRC	Planilha de maneira inicial e inserção das informações no sistema	A planilha utilizará o sistema de e-mail e as informações serão inseridas no sistema	Após o término da aplicação do processo de gerenciamento de riscos.
Plano de Comunicação (Etapa 7)	Orientar os gestores quanto aos procedimentos que deverão ser observados no gerenciamento dos riscos de suas unidades.	DGRC	Comunidade interna e externa à UFOB	Inserção no Plano de Gestão de Riscos e Controles Internos	Portal da UFOB	Imediatamente após a aprovação ou atualização do documento.

PRODUTOS O que precisa ser comunicado?	OBJETIVO Qual é o propósito da comunicação?	COMUNICADOR Quem é o responsável pela emissão da comunicação?	DESTINATÁRIOS Quem é o receptor da comunicação?	MEIO DE COMUNICAÇÃO Qual instrumento deve ser utilizado?	SISTEMA Onde a comunicação será divulgada?	FREQUÊNCIA Quando a comunicação deve ser emitida?
ETAPAS DO PROCESSO DE GERENCIAMENTO DE RISCOS						
Registro de ocorrência (Etapa 7)	Informar sobre a ocorrência de risco (gatilho acionado) para início das ações de contingência.	Gestor do risco e/ou responsáveis pelo Plano de Tratamento e Plano de Contingência	DGRC e CGRC	Planilha de maneira inicial e inserção da informação no sistema posteriormente	A planilha utilizará o sistema de e-mail e as informações serão inseridas no sistema	Imediatamente após o gatilho ser acionado.
Alteração no contexto de um ou mais riscos (Etapa 7)	Reportar mudanças que possam requerer revisão dos controles e/ou do Plano de Tratamento e Plano de Contingência	Gestor do risco	DGRC e CGRC	Planilha de maneira inicial e inserção da informação no sistema posteriormente	A planilha utilizará o sistema de e-mail e as informações serão inseridas no sistema	Imediatamente após a detecção de mudança de cenário.
Monitoramento do processo de gerenciamento de riscos das unidades (Etapa 7)	Consolidar o andamento das ações de tratamento concluídas ou em andamento em toda a Universidade, assim como mudanças identificadas durante o monitoramento.	DGRC	CGRC	Relatório	Portal da UFOB	Imediatamente após a aprovação do documento.
SUPERVISÃO DA GESTÃO DE RISCOS						
Revisão da Política de Gestão de Riscos e Controles Internos	Propor ajustes e melhorias ao documento.	Consuni	Comunidade interna e externa à UFOB	Resolução	Portal da UFOB	Imediatamente após a atualização do documento.
Relatório de Gestão de Riscos e Controles Internos	Disponibilizar informações gerenciais sobre a gestão de riscos.	CGRC	Comunidade interna e externa à UFOB	Relatório	Portal da UFOB	Imediatamente após a aprovação do documento, anualmente.

PRODUTOS O que precisa ser comunicado?	OBJETIVO Qual é o propósito da comunicação?	COMUNICADOR Quem é o responsável pela emissão da comunicação?	DESTINATÁRIOS Quem é o receptor da comunicação?	MEIO DE COMUNICAÇÃO Qual instrumento deve ser utilizado?	SISTEMA Onde a comunicação será divulgada?	FREQUÊNCIA Quando a comunicação deve ser emitida?
SUPERVISÃO DA GESTÃO DE RISCOS						
Indicadores	Disponibilizar informações gerenciais sobre a gestão de riscos	DGRC	Comunidade interna e externa à UFOB	Painel de dados	Portal da UFOB	Semestralmente.
Questões emergentes ou alterações no cenário regulatório	Disponibilizar informações que impactem a gestão de riscos	CGRC e DGRC	Agentes públicos	Material de divulgação	Sistema de e-mail e Portal da UFOB	Conforme a necessidade.

Fonte: Elaboração própria

5.6.2. Monitoramento

O monitoramento compreende o acompanhamento, a revisão e análise periódica da gestão de riscos, objetivando o aprimoramento contínuo da instituição. Na etapa de monitoramento deve-se acompanhar o desempenho dos indicadores de riscos, supervisionar a implementação do plano de ações e verificar o alcance das metas estabelecidas.

O monitoramento é feito continuamente por todos os agentes públicos envolvidos no projeto/processo. Detalhadamente, em nível operacional e tático o monitoramento é feito pelos gestores dos riscos e sua equipe cujos objetivos básicos são:

a) manter os controles internos eficientes;
b) cumprir as medidas planejadas nos planos de tratamento aos riscos identificados na unidade;
c) detectar mudanças que possam requerer revisão dos controles, do Plano de Tratamento ou do Plano de Contingência;
d) analisar eventuais ocorrências de novos riscos.

Em nível gerencial, o monitoramento é feito pela DGRC e CGRC. Os objetivos do monitoramento nesse nível são:

a) acompanhar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas;
b) acompanhar o desempenho dos indicadores do processo de gestão de riscos;
c) supervisionar a plano de ações;
d) avaliar continuamente os mecanismos de monitoramento instituídos;
e) consolidar as informações em relatórios gerenciais.

Conforme disposto na PGRCI, os indicadores são instrumentos importantes para acompanhar e monitorar o processo de gestão de riscos. Os indicadores de desempenho propostos são apresentados no APÊNDICE G.

O Quadro 13 apresenta de forma detalhada as responsabilidades das instâncias envolvidas na etapa de monitoramento.

Quadro 13: Responsabilidades relativas ao monitoramento

Aspectos a serem monitorados	Comitê de Governança, Riscos e Controles	Diretoria de Governança, Riscos e Conformidade	Gestor do Risco	Agentes públicos envolvidos
Riscos identificados		- Acompanhar a evolução dos níveis de riscos, considerando o monitoramento realizado pelas unidades.	- Monitorar, ao longo do tempo, os riscos mapeados, de modo a garantir que as respostas adotadas resultem na manutenção dos riscos em níveis aceitáveis. - Reportar registros de ocorrências. - Reportar novos riscos identificados.	- Reportar imediatamente ao gestor do risco qualquer mudança que possa requerer revisão dos controles, Plano de Tratamento ou Plano de Contingência.
Ações implementadas para tratar os riscos		- Acompanhar a efetividade das medidas de controle implementadas para tratamento de riscos, considerando o monitoramento realizado pelas unidades.	- Monitorar a evolução da efetividade das medidas de controles implementadas nos projetos/processos sob sua responsabilidade, para tratamento de riscos.	- Reportar imediatamente ao gestor do risco qualquer mudança que possa requerer revisão dos controles, Plano de Tratamento ou Plano de Contingência.
Execução do Plano de Gestão de Riscos e Controles Internos	- Acompanhar a execução do Plano por meio de relatórios gerenciais e dos indicadores. - Acompanhar a efetividade dos controles internos definidos nas unidades.	- Requisitar aos gestores as informações necessárias para a consolidação dos dados e a elaboração de relatórios gerenciais; - Consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-las ao Comitê. - Acompanhar a execução do Plano de Ações. - Consolidar os dados para os cálculos dos indicadores.	- Validar e monitorar, no seu âmbito de atuação, a execução das atividades previstas no Plano de Ações e dos projetos decorrentes de sua implementação;	

Fonte: Elaboração própria

6. SOLUÇÃO TECNOLÓGICA

Nos tempos atuais torna-se imprescindível uma ferramenta tecnológica para auxiliar a implementação do processo de gestão de riscos. Nesse sentido, para acompanhar a gestão de riscos a nível institucional, teremos o apoio do *software* ForRisco, desenvolvido pelo Fórum Nacional de Pró-Reitores de Planejamento e de Administração das Instituições Federais de Ensino Superior (Forplad) e mantido pela Rede Nacional de Ensino e Pesquisa (RNP).

Dentre as principais funcionalidades do *software* destacam-se a possibilidade de estabelecer o plano de gestão de riscos, suporte para o registro dos riscos, identificação das causas e consequências, definição de ações corretivas, indicação de periodicidade de análise do risco, apoio ao monitoramento de riscos e a geração de relatórios dinâmicos, entre outras.

O *software* ForRisco poderá ser utilizado por todos os agentes públicos da Universidade nas etapas do ciclo de gerenciamento de riscos, em conjunto com os demais documentos mencionados ao longo deste plano.

7. CAPACITAÇÃO

A consolidação da gestão de riscos e de controles internos demanda não apenas a definição de metodologias e instrumentos, mas também o desenvolvimento das pessoas envolvidas no processo. Nesse contexto, consta na PGRCI que a capacitação dos agentes públicos deve ser realizada de forma continuada em todos os níveis. Assim, são previstas ações sistemáticas de capacitação e suporte, descritas a seguir, com o objetivo de promover a compreensão, a adoção e a efetiva aplicação das práticas de gestão de riscos no âmbito institucional. Essas ações ocorrerão de 3 (três) formas:

a) Capacitação por meio de cursos ofertados nas escolas de governo, dando conhecimentos básicos para o entendimento da gestão de riscos e controles internos;
b) Treinamentos presenciais e remotos ofertados pela DGRC; e
c) Disponibilização de manuais para a execução do processo de gestão de riscos.

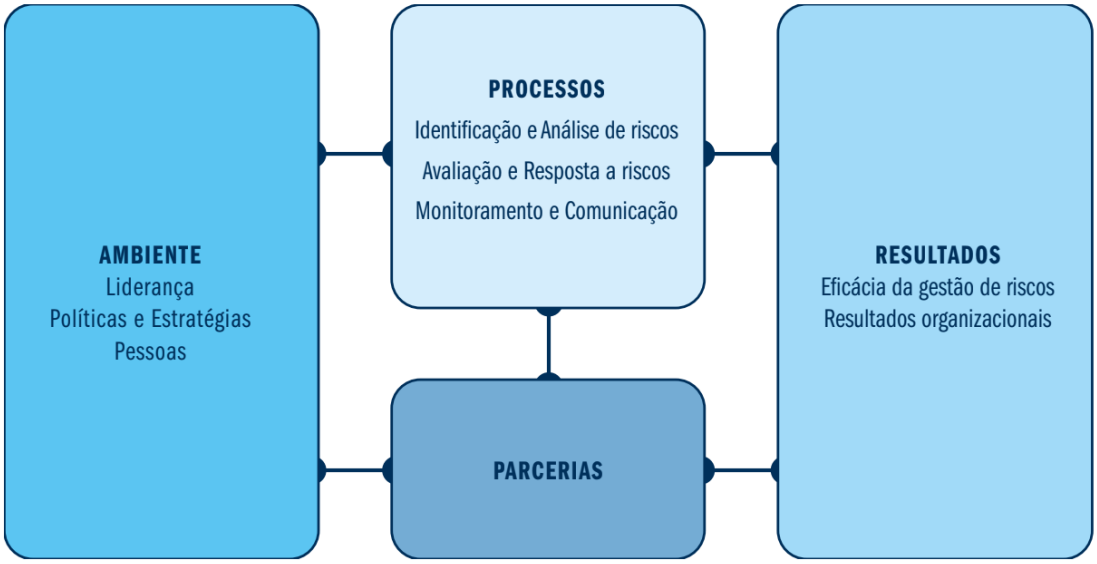
Além dessas ações de capacitação institucional, a qualquer momento, a unidade que desejar mais algum suporte poderá entrar em contato com a DGRC que estará à disposição para auxiliar no processo.

8. MATURIDADE NA GESTÃO DE RISCOS

Avaliar o nível de maturidade significa compreender o estágio atual da Universidade quanto ao seu processo de gestão de riscos, visando o autoconhecimento da organização.

A avaliação da maturidade será conduzida pelo CGRC, com o apoio da DGRC e utilizará o modelo desenvolvido pelo TCU (TCU, 2018). O modelo é composto por quatro dimensões, conforme Figura 9:

Figura 9: Modelo de avaliação da maturidade em gestão de riscos



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

O modelo tem como premissas que a maturidade da gestão de riscos de uma organização é determinada pelas capacidades existentes em termos de liderança, políticas e estratégias, e de preparo das pessoas para gestão de riscos, bem como pelo emprego dessas capacidades aos processos e parcerias e pelos resultados obtidos na melhoria do desempenho da organização no cumprimento de sua missão institucional de gerar valor para as partes interessadas com eficiência e eficácia, transparência e *accountability*, e conformidade com leis e regulamentos.

A dimensão “Ambiente” está relacionada à cultura, à governança de riscos e à consideração dos riscos no momento da elaboração da estratégia e dos objetivos. Busca verificar se há na organização um ambiente propício para a gestão de riscos avaliando três aspectos:

a) liderança: que busca verificar qual o nível de assunção de responsabilidades da área de governança e da alta administração com a gestão de riscos, buscando alcançar o comprometimento de todos os níveis da organização;
b) políticas e estratégias: avalia em que grau a organização possui políticas e estratégias de gestão de riscos definidas, divulgada e postas em prática, além de analisar se os riscos são considerados na definição de estratégias, planos e objetivos; e
c) pessoas: busca avaliar em que nível as pessoas da organização estão informadas e capacitadas para exercerem seus papéis no gerenciamento de riscos.

A dimensão “Processos” trata dos processos de gestão de riscos, buscando identificar em que medida a organização possui processo formal, com métodos e critérios bem definidos para:

a) identificação e análise de riscos, de modo que sejam priorizados os riscos mais significativos para posterior tratamento;
b) avaliação e resposta a riscos, a fim de analisar se essas atividades são aplicadas de forma consistente para garantir um tratamento adequado aos riscos identificados; e
c) monitoramento e avaliação, que busca avaliar em que medida essas atividades estão definidas e são aplicadas de forma consistente para assegurar que a gestão de riscos e controles seja eficiente e eficaz.

A dimensão “Parcerias” está relacionada aos arranjos colaborativos estabelecidos entre o órgão avaliado e outras entidades públicas ou privadas. Aborda como os riscos são geridos nessas relações, buscando avaliar se a definição dos riscos e da responsabilidade por cada um deles é feita de forma clara e se há um canal de comunicação estabelecido para tratar o tema entre as partes.

Por fim, na dimensão “Resultados”, é avaliado como as práticas da gestão de riscos trazem resultados eficazes para a melhoria dos processos de governança, dos produtos e serviços entregues à sociedade, da transparência e prestação de contas, além do cumprimento de leis e regulamentos.

Nesse modelo, é possível avaliar o índice de maturidade de cada dimensão ou o índice global, que considera todas as dimensões. O índice de maturidade global é composto pela média ponderada do índice de maturidade das dimensões (IMD), o Quadro 14 apresenta os pesos de cada dimensão e um exemplo de cálculo de índice de maturidade:

Quadro 14: Pesos e exemplo de cálculo do índice de maturidade

DIMENSÃO	PESO	EXEMPLO		
		IMD	PESO	PONDERADO
Ambiente	40	52,6	0,4	21,0
Processos	30	45,9	0,3	13,8
Parcerias	10	80,1	0,1	8,0
Resultados	20	49,5	0,2	9,9
ÍNDICE DE MATURIDADE GLOBAL				**52,7**

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

O resultado obtido no índice de maturidade global pode ser enquadrado em 5 (cinco) níveis de maturidade:

Quadro 15: Níveis de maturidade da gestão de riscos

ÍNDICE DE MATURIDADE APURADO	NÍVEL DE MATURIDADE
De 0% a 20%	1 - Inicial
De 20,1 a 40%	2 - Básico
De 40,1% a 60%	3 - Intermediário
De 60,1% a 80%	4 - Aprimorado
De 80,1% a 100%	5 - Avançado

Fonte: Adaptado de Gestão de Riscos – Avaliação da Maturidade (TCU, 2018)

9. PLANO DE AÇÕES

O Plano de Ações constitui um instrumento estratégico, concebido para orientar, de forma estruturada e progressiva, a implementação e o fortalecimento das práticas de gestão de riscos e controles internos na instituição. O Plano de Ações, apresentado no Quadro 16, considera as três áreas de atuação da gestão de riscos: riscos associados aos objetivos estratégicos, aos processos organizacionais e à integridade.

Quadro 16: Plano de Ações

ATIVIDADE	ENVOLVIDOS	PRAZO	OBSERVAÇÕES
Capacitação em gestão de riscos	Agentes públicos e equipe da DGRC	De acordo com a necessidade	
Elaboração de informações sobre o processo de gestão de riscos (manuais, guias, tutoriais, cartilhas, etc.)	DGRC	De acordo com a necessidade	
Levantamento dos riscos nos projetos relacionados aos objetivos estratégicos do PDI e aplicação do processo de gerenciamento de riscos	Gestores e demais agentes públicos das unidades e DGRC	Permanente	
Aplicação do processo de gerenciamento de riscos nos processos mapeados	Gestores e demais agentes públicos das unidades e DGRC	Permanente	Estima-se a aplicação em 10 processos por ano
Levantamento dos riscos de integridade provenientes de diversas fontes e aplicação do processo de gerenciamento de riscos	Gestores e demais agentes públicos das unidades e DGRC	Anualmente	
Manutenção das informações sobre a gestão de riscos no sistema (riscos identificados, planos, ocorrências, etc.)	Gestores e demais agentes públicos das unidades e DGRC	Permanente	
Elaboração e manutenção do painel de indicadores	DGRC	Semestralmente	

ATIVIDADE	ENVOLVIDOS	PRAZO	OBSERVAÇÕES
Realização do monitoramento dos riscos críticos e controles internos	Gestores e demais agentes públicos das unidades e DGRC	De acordo com os prazos dos planos de tratamento	
Avaliação da maturidade	CGRC e DGRC	Anualmente	O resultado será inserido no Relatório de Gestão de Riscos e Controles Internos
Publicação do Relatório de Gestão de Riscos e Controles Internos	CGRC e DGRC	Anualmente	O Relatório com os resultados do acompanhamento das ações do Plano de Gestão de Riscos e Controles Internos será submetido ao CGRC para avaliação e deliberações.
Revisão do Plano de Gestão de Riscos e Controles Internos	CGRC e DGRC	De acordo com a necessidade	
Revisão da Política de Gestão de Riscos e Controles Internos	Consuni e CGRC	De acordo com a necessidade	
Levantamento de questões emergentes ou alterações no cenário regulatório	CGRC e DGRC	Permanente	

Fonte: Elaboração própria

10. CONSIDERAÇÕES FINAIS

Este documento apresentou o Plano de Gestão de Riscos e Controles Internos da UFOB previsto para o período de 2026 a 2028, bem como, explicitou os fundamentos legais e teóricos que norteiam as ações de gestão de riscos na Universidade.

Como objetivo primordial buscou atender a INC MP/CGU n° 01/2016, o Decreto nº 9.203/2017 e a Resolução CGAG/CONSUNI/UFOB nº 014, que estabelece princípios, objetivos, diretrizes e responsabilidades da PGRCI na UFOB.

Apresentou também, o processo de gestão de riscos da Universidade e suas respectivas etapas. A pretensão foi de orientar os agentes públicos envolvidos no processo de implementar as ações de mapeamento dos riscos em suas unidades em conformidade com a metodologia e instrumentos definidos na PGRCI.

Demonstrou no plano de ações as três áreas de atuação e implementação da gestão de riscos na UFOB: identificação dos riscos nos objetivos estratégicos da Universidade (PDI); identificação dos riscos nos processos organizacionais e registro de riscos identificados como riscos para a integridade. Buscando-se cumprir da melhor forma possível os papéis e competências das instâncias envolvidas na gestão de riscos, previstas na PGRCI.

Finalmente, ressalta-se que em qualquer iniciativa de implementação de metodologias é essencial considerar o caráter dinâmico da gestão e da legislação, e assim, buscar a realização de acertos e ajustes para se adequar ao contexto e às necessidades da UFOB.

O Plano de Gestão de Riscos e Controles Internos deve ser visto, essencialmente, como um processo de construção e de reforço da política interna de governança na área de gestão de integridade, riscos e controles internos da Universidade.

11. REFERÊNCIAS

ABNT. **ABNT NBR ISO 31000:2009 Gestão de riscos – Princípios e diretrizes.** Rio de Janeiro: ABNT, 2009. Disponível em: https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso em: 29 dez. 2025.

ABNT. **ABNT NBR ISO 31010:2012 Gestão de riscos – Técnicas para o processo de avaliação de riscos**. Rio de Janeiro: ABNT, 2012. Disponível em: https://wp.ufpel.edu.br/labserg/files/2022/04/abnt_nbr_iso_31010_2012_-_gestao_de_riscos_-_tecnicas_para_o_processo_de_avaliacao_de_riscos.pdf. Acesso em: 29 dez. 2025.

ABNT. **ABNT NBR ISO 31000:2018 Gestão de riscos – Diretrizes**. Rio de Janeiro: ABNT, 2018. Disponível em: https://dintegcgcin.saude.gov.br/attachments/download/23/2018%20-%20Diretrizes%20%20Gest%C3%A3o%20de%20Riscos_ABNT%20NBR%20ISO%2031000.pdf. Acesso em: 31 dez. 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 02 jan. 2026.

BRASIL. **Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Brasília, DF, 2016. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/33947/8/Instrucao%20Normativa%20Conjunta%20MP-CGU%2001-2016.pdf. Acesso em: 27 dez. 2025.

BRASIL. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Brasília, DF, 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm. Acesso em: 27 dez. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 27 dez. 2025.

BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei

nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília, DF, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 27 dez. 2025.

BRASIL. **Lei nº 14.133, de 1º de abril de 2021**. Lei de Licitações e Contratos Administrativos. Brasília, DF, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 27 dez. 2025.

BRASIL. **Decreto nº 10.947, de 25 de janeiro de 2022**. Regulamenta o inciso VII do **caput** do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional. Brasília, DF, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/D10947.htm. Acesso em: 27 dez. 2025.

BRASIL. **Decreto nº 11.529, de 16 de maio de 2023**. Institui o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal e a Política de Transparência e Acesso à Informação da Administração Pública Federal. Brasília, DF, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11529.htm. Acesso em: 27 dez. 2025.

CGU. **Metodologia de Gestão de Riscos – Manual**. Brasília: CGU, 2018a. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/74036/1/Manual_Operacional.pdf. Acesso em: 29 dez. 2025.

CGU. **Guia Prático de Gestão de Riscos para a Integridade**. Brasília: CGU, 2018b. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manual-gestao-de-riscos.pdf. Acesso em: 29 dez. 2025.

CGU. **Portaria CGU nº 57, de 4 de janeiro de 2019**. Altera a Portaria CGU nº 1.089, de 25 de abril de 2018, que estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências. Brasília, DF, 2019. Disponível em: . Acesso em: 29 dez. 2025.

CGU. **Portaria Normativa CGU nº 234, de 06 de novembro de 2025**. Aprova o Referencial Técnico da Atividade de Gestão da Integridade do Poder Executivo Federal. Brasília, DF, 2025. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/95890/1/Portaria_Normativa_234_2025.pdf. Acesso em: 29 dez. 2025.

COSO. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. Jersey City, EUA: COSO, 2007. Disponível em: https://auditoria.mpu.mp.br/pgmq/COSOIIERMExecutiveSummaryPortuguese.pdf. Acesso em: 29 dez. 2025.

COSO. **Controle Interno – Estrutura Integrada**. Durham, EUA: COSO, 2013. Disponível em: https://auditoria.mpu.mp.br/pgmq/COSOIICIF_2013_Sumario_Executivo.pdf. Acesso em: 29 dez. 2025.

IIA. **Modelo das três linhas do IIA 2020**. Lake Mary, EUA: IIA, 2020. Disponível em: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-portuguese.pdf. Acesso em: 29 dez. 2025.

TCU. **Gestão de Riscos – Avaliação da Maturidade**. Brasília: TCU, 2018. Disponível em: https://portal.tcu.gov.br/publicacoes-institucionais/cartilha-manual-ou-tutorial/gestao-de-riscos-avaliacao-da-maturidade. Acesso em: 29 dez. 2025.

TCU. **Portal do TCU**. Brasília: TCU, 2026. Disponível em: https://portal.tcu.gov.br. Acesso em: 07 jan. 2026.

UFOB. **Plano de Desenvolvimento Institucional – PDI, vigência 2019 – 2023.** Barreiras: UFOB, 2019. Disponível em: https://ufob.edu.br/a-ufob/planos-e-projetos/plano-de-desenvolvimento-institucional/pdi-2019-2013-2023. Acesso em: 31 dez. 2025.

UFOB. **Portaria UFOB nº 237, de 12 de abril de 2021**. Institui o Comitê de Governança, Riscos e Controles da Universidade Federal do Oeste da Bahia (CGRC/UFOB). Barreiras, BA, 2021. Disponível em: https://caju.ufob.edu.br/boletim, Edição nº 51 de 2021. Acesso em: 27 dez. 2025.

UFOB. **Resolução CGAG/CONSUNI/UFOB nº 014, de 13 de dezembro 2022**. Estabelece a Política de Gestão de Riscos e Controles Internos da Universidade Federal do Oeste da Bahia. Barreiras, BA, 2022. Disponível em: https://ufob.edu.br/a-ufob/instrumentos-normativos/resolucoes/2022/cgag/resolucao-cgag-014-2022-estabelece-a-politica-de-gestao-de-riscos-e-controles-internos-da-ufob.pdf. Acesso em: 27 dez. 2025.

UFOB. **Portaria UFOB nº 35, de 3 de março de 2023**. Cria o Comitê de Governança, Riscos e Controles – CGRC/UFOB. Barreiras, BA, 2023. Disponível em: https://caju.ufob.edu.br/boletim, Edição nº 29 de 2023. Acesso em: 27 dez. 2025.

UFOB. **Resolução CNR/CONSUNI/UFOB nº 017, de 31 de outubro de 2024**. Dispõe sobre o Regimento Interno da Reitoria da Universidade Federal do Oeste da Bahia – UFOB. Barreiras, BA, 2024. Disponível em: https://ufob.edu.br/a-ufob/instrumentos-normativos/resolucoes/2024/cnr/copy_of_RESOLUOCNR0172024DispesobreoRegimentoInternodaReitoriadaUFOB.pdf. Acesso em: 27 dez. 2025.

UFOB. **Resolução CGAG/CONSUNI/UFOB nº 022, de 3 de abril de 2025**. Institui a Cadeia de Valor Integrada - CVI da Universidade Federal do Oeste da Bahia - UFOB representada pelos macroprocessos e seus respectivos processos finalísticos, gerenciais e de suporte. Barreiras, BA, 2025. Disponível em: https://ufob.edu.br/a-ufob/instrumentos-normativos/resolucoes/2025/cgag/RESOLUOCGAG0222025InstituiaCadeiadeValorIntegradarepresentadapelosmacroprocessoseprocessosfinalsticosgerenciaisedesuportedaUFOB.pdf. Acesso em: 27 dez. 2025.

UFOB. **Portal da UFOB**. Barreiras: UFOB, 2026. Disponível em: https://ufob.edu.br/. Acesso em: 07 jan. 2026.

UFSB. **Plano Institucional de Gestão de Riscos e Controles Internos.** Itabuna: UFSB, 2020. Disponível em: https://ufsb.edu.br/propa/images/UFSB_Plano_de_Gest%C3%A3o_de_Riscos8_2.pdf. Acesso em: 31 dez. 2025.

APÊNDICE A
GLOSSÁRIO

Agente público: é aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, à UFOB.

Apetite ao risco: nível de risco que a UFOB está disposta a aceitar.

Categoria do risco: diz respeito à origem dos fatores que influenciam o evento de risco, podendo ser estratégico, financeiro/orçamentário, operacional, legal/conformidade, imagem/reputação, integridade ou ambiental.

Causa do risco: fator que desencadeia a ocorrência do evento de risco.

Consequência do risco: possível efeito da ocorrência do evento de risco.

Controles internos: processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados.

Evento: ocorrência gerada com base em fontes internas ou externas que pode causar impacto negativo, positivo ou ambos.

Gerenciamento de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança no alcance dos objetivos organizacionais.

Gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela Administração Central, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança quanto à realização de seus objetivos.

Governança: conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas institucionais e à prestação de serviços de interesse da sociedade.

Nível de risco: magnitude de um risco, expressa em termos da combinação de suas consequências e probabilidades de ocorrência.

Objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da Universidade.

Plano de Contingência: planejamento de ações que serão tomadas caso um risco venha a se concretizar.

Plano de Tratamento: planejamento de ações para a implementação das medidas preventivas.

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

Registro de ocorrência: documentação da ocorrência de um evento de risco.

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos.

Risco de integridade: vulnerabilidade que pode favorecer ou facilitar a ocorrência de práticas de corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta.

Risco inerente: nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade de sua ocorrência ou de seu impacto.

Risco residual: nível do risco que permanece após a implementação dos controles internos.

APÊNDICE B
PLANILHA DE MAPEAMENTO DE RISCOS

Figura 10: Planilha de mapeamento de riscos

PLANILHA DE MAPEAMENTO DE RISCOS	
Data:	
Unidade:	
Nome do gestor do risco:	
Nº processo ou projeto:	
Nome do processo ou projeto:	
Descrição:	
Objetivo geral:	
Objetivos específicos:	

Identificação e Análise						Avaliação do Risco Inerente				Avaliação dos controles			Avaliação do Risco Residual		Priorização	Definição de resposta	
Nº evento	Evento de risco	Tipo	Categoria	Causa(s)	Consequência(s)	Probabilidade	Impacto	Risco Inerente	Classificação	Descrição dos controles	Nível Confiança	FA controles	Risco Residual	Classificação	Priorização	Opção de tratamento	Justificativa

Fonte: Elaboração própria

APÊNDICE C
PLANO DE TRATAMENTO

Figura 11: Modelo de Plano de Tratamento

PLANO DE TRATAMENTO	
Data:	
Unidade:	
Nome do gestor do risco:	
Nº processo ou projeto:	
Nome do processo ou projeto:	
Descrição:	

Planejamento das ações preventivas										Monitoramento
Nº evento	Evento de risco	Unidade Responsável	Unidades Corresponsáveis	Responsável pela implementação	Ações preventivas	Recursos	Data início	Data término	Monitoramento	Situação

Fonte: Elaboração própria

APÊNDICE D
CONTROLES INTERNOS

Os controles adotados pela gestão precisam ser eficazes para prevenir, detectar e permitir corrigir, em tempo hábil, a ocorrência de eventos que possam afetar adversamente a realização de objetivos. É importante que, na elaboração do Plano de Tratamento, avalie- se a necessidade de melhorar ou extinguir controles já existentes. Somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, observados sempre critérios de eficiência e eficácia da sua implementação.

Sugestões de controles que podem ser implementados:

a) controles automatizados em substituição aos manuais, quando possível;
b) combinação de controles manuais e informatizados (automatizados);
c) indicadores de desempenho, com estabelecimento de indicadores, como por exemplo, índice de rotação de pessoal, cumprimento de prazos legais, entre outros;
d) segregação de funções, com atribuição de obrigações entre pessoas com finalidade de reduzir riscos, erro ou fraude;
e) limites para transações;
f) políticas e procedimentos;
g) procedimentos de autorização e aprovação;
h) controles de acesso a recursos e registros;
i) verificações;
j) conciliações;
k) avaliação das operações, dos processos e das atividades (permanente ou por amostragem);
l) supervisão (orientação e garantia de conformidade);
m) capacitação; e
n) monitoramento tempestivo ou contínuo.

APÊNDICE E
PLANO DE CONTINGÊNCIA

Figura 12: Modelo de Plano de Contingência

PLANO DE CONTINGÊNCIA			
Data:			
Unidade:			
Nome do gestor do risco:			
Nº processo ou projeto:			
Nome do processo ou projeto:			
Descrição:			

Planejamento das ações de contingência				
Nº evento	Evento de risco	Gatilho	Responsável pela implementação	Ações de contingência

Fonte: Elaboração própria

APÊNDICE F
REGISTRO DE OCORRÊNCIA

Figura 13: Modelo de Registro de Ocorrência

REGISTRO DA OCORRÊNCIA	
Unidade:	
Nome do gestor do risco:	
Nº processo ou projeto:	
Nome do processo ou projeto:	
Descrição:	

Ocorrência						
Nº evento	Evento de risco	Data da ocorrência	Descrição da ocorrência	Responsável pela solução	Solução	Resultados

Fonte: Elaboração própria

APÊNDICE G
INDICADORES

Os indicadores são instrumentos fundamentais para medir o desempenho do Plano de Gestão de Riscos e Controles Internos, permitindo o monitoramento e análise dos resultados, assim como a tomada de ações corretivas e/ou preventivas visando otimizar as ações. Os indicadores devem apontar para informações pertinentes, oportunas e precisas.

A seguir, é apresentada uma lista não exaustiva de indicadores que serão utilizados para acompanhar a execução deste plano:

1. IDENTIFICAÇÃO			
Código do indicador:	IGR1		
Nome do indicador:	Nível de conformidade em gestão de riscos		
2. DESCRIÇÃO TÉCNICA			
Descrição:	Mede o grau de conformidade da UFOB em relação às práticas e requisitos estabelecidos pelo TCU.		
Finalidade:	Avaliar o nível de aderência da instituição aos padrões de gestão de riscos e identificar áreas críticas de aperfeiçoamento.		
3. ESTRUTURA E CÁLCULO DO INDICADOR			
Fórmula:	$\text{IGR1} = \frac{\text{Pontuação obtida na avaliação do TCU}}{\text{Pontuação máxima possível}} x\ 100$		
Unidade de medida:	Percentual (%)		
Tipo de indicador:	Indicador de resultado		
Natureza:	Quantitativa		
Sentido de melhoria:	Quanto mais próximo de 100%, melhor o desempenho		
4. FONTE DE DADOS E PERIODICIDADE			
Periodicidade:	Anual		
Fonte de dados:	Dados da DGRC		
Responsável pela apuração:	DGRC		
5. METAS			
2025*	2026	2027	2028
8%	30%	50%	60%
*linha de base			
6. CRITÉRIOS E OBSERVAÇÕES			
Critérios de inclusão:	Avaliação oficial do TCU (iESGo), questões específicas da área de gestão de riscos		
Critérios de exclusão:	Avaliações não homologadas		

1. IDENTIFICAÇÃO			
Código do indicador:	IGR2		
Nome do indicador:	Índice de maturidade em gestão de riscos		
2. DESCRIÇÃO TÉCNICA			
Descrição:	Avalia o nível de maturidade da Universidade na gestão de riscos institucionais com base em metodologia reconhecida.		
Finalidade:	Monitorar o avanço da instituição na implementação de práticas de gestão de riscos, identificando áreas que necessitam de fortalecimento.		
3. ESTRUTURA E CÁLCULO DO INDICADOR			
Fórmula:	Média ponderada do índice de maturidade das dimensões (IMD), conforme detalhado no documento "Gestão de Riscos - Avaliação da Maturidade" (TCU, 2018)		
Unidade de medida:	Índice (1 a 5)		
Tipo de indicador:	Indicador de Resultado		
Natureza:	Quantitativa		
Sentido de melhoria:	Quanto mais próximo de 5, melhor o desempenho		
4. FONTE DE DADOS E PERIODICIDADE			
Periodicidade:	Anual		
Fonte de dados:	Dados DGRC		
Responsável pela apuração:	DGRC		
5. METAS			
2025*	2026	2027	2028
N/A	2	2	3
* linha base N/A = Não se aplica. Este indicador começará a ser mensurado a partir de 2026			
6. CRITÉRIOS E OBSERVAÇÕES			
Critérios de inclusão:	Inclui questões da avaliação definida pelo TCU no documento "Gestão de Riscos - Avaliação da Maturidade", 2018		
Critérios de exclusão:	Questões não homologadas.		

1. IDENTIFICAÇÃO			
Código do indicador:	IGR3		
Nome do indicador:	Percentual de processos de trabalho com gerenciamento de riscos implementado		
2. DESCRIÇÃO TÉCNICA			
Descrição:	Mede a proporção de processos de trabalho da Universidade que possuem práticas formais de gerenciamento de riscos implementadas.		
Finalidade:	Avaliar a disseminação da cultura de gestão de riscos nos processos institucionais, fortalecendo a governança e a prevenção de falhas.		
3. ESTRUTURA E CÁLCULO DO INDICADOR			
Fórmula:	$\text{IGR3} = \frac{\text{Processos com gerenc. de riscos implementado}}{\text{Processos de trabalho mapeados}} x\ 100$		
Unidade de medida:	Percentual (%)		
Tipo de indicador:	Indicador de Desempenho		
Natureza:	Quantitativa		
Sentido de melhoria:	Quanto mais próximo de 100%, melhor o desempenho		
4. FONTE DE DADOS E PERIODICIDADE			
Periodicidade:	Anual		
Fonte de dados:	Dados DGRC		
Responsável pela apuração:	DGRC		
5. METAS			
2025*	2026	2027	2028
N/A	70%	75%	80%
* linha base N/A = Não se aplica. Este indicador começará a ser mensurado a partir de 2026			
6. CRITÉRIOS E OBSERVAÇÕES			
Critérios de inclusão:	Processos de trabalho da CVI que já foram mapeados		
Critérios de exclusão:	Processos de trabalho não mapeados		

1. IDENTIFICAÇÃO				
Código do indicador:	IGR4			
Nome do indicador:	Percentual de riscos críticos com planos de tratamento implementados			
2. DESCRIÇÃO TÉCNICA				
Descrição:	Mede a proporção de riscos classificados como críticos (altos e extremos) que possuem planos de tratamento devidamente implementados.			
Finalidade:	Garantir que os principais riscos identificados pela instituição estejam sendo tratados, reduzindo impactos potenciais e aumentando a resiliência organizacional.			
3. ESTRUTURA E CÁLCULO DO INDICADOR				
Fórmula:	$\text{IGR4} = \frac{\text{Nº de riscos críticos com planos de trat. implementados}}{\text{Total de riscos críticos identificados}} x\ 100$			
Unidade de medida:	Percentual (%)			
Tipo de indicador:	Indicador de Desempenho			
Natureza:	Quantitativa			
Sentido de melhoria:	Quanto mais próximo de 100%, melhor o desempenho			
4. FONTE DE DADOS E PERIODICIDADE				
Periodicidade:	Anual			
Fonte de dados:	Dados DGRC			
Responsável pela apuração:	DGRC			
5. METAS				
2025*	2026	2027	2028	
N/A	60%	70%	75%	
* linha base N/A = Não se aplica. Este indicador começará a ser mensurado a partir de 2026				
6. CRITÉRIOS E OBSERVAÇÕES				
Critérios de inclusão:	Riscos classificados como alto e extremo, identificados em processos e projetos institucionais.			
Critérios de exclusão:	Demais riscos com outras classificações.			

1. IDENTIFICAÇÃO	
Código do indicador:	IGR5
Nome do indicador:	Percentual de eficácia dos controles internos
2. DESCRIÇÃO TÉCNICA	
Descrição:	Mede o percentual de riscos que, após a avaliação dos controles, passaram para o nível aceitável.
Finalidade:	Verificar a qualidade dos controles internos implementados.
3. ESTRUTURA E CÁLCULO DO INDICADOR	
Fórmula:	

$$\text{IGR5} = \frac{\text{Total de RR baixos e médios} - \text{total de RI baixos e médios}}{\text{Total de RI altos e extremos}} x\ 100$$

Onde:
RR = riscos residuais
RI = riscos inerentes

Unidade de medida:	Percentual (%)
Tipo de indicador:	Indicador de Desempenho
Natureza:	Quantitativa
Sentido de melhoria:	Quanto mais próximo de 100%, melhor o desempenho
4. FONTE DE DADOS E PERIODICIDADE	
Periodicidade:	Anual
Fonte de dados:	Dados DGRC
Responsável pela apuração:	DGRC

5. METAS			
2025*	2026	2027	2028
N/A	30%	40%	50%

* linha base
N/A = Não se aplica. Este indicador começará a ser mensurado a partir de 2026

6. CRITÉRIOS E OBSERVAÇÕES	
Critérios de inclusão:	Riscos críticos identificados em processos e projetos institucionais.
Critérios de exclusão:	Demais riscos com outras classificações.