UFRJ

Metodologia de Elaboração do Plano de Gestão de Riscos

EQUIPE DA REITORIA

ROBERTO DE ANDRADE MEDRONHO
Reitor

CÁSSIA CURAN TURCI
Vice-Reitora

HÉLIO DE MATTOS ALVES
Chefe de Gabinete da Reitoria

MARIA FERNANDA SANTOS QUINTELA DA COSTA NUNES
Pró-Reitora de Graduação – PR-1

JOÃO RAMOS TORRES DE MELLO NETO
Pró-Reitor de Pós-Graduação e Pesquisa – PR-2

HELIOS MALEBRANCHE OLBRISCH FREIRES FILHO
Pró-Reitor de Planejamento, Desenvolvimento e Finanças – PR-3

NEUZA LUZIA PINTO
Pró-Reitora de Pessoal – PR-4

IVANA BENTES OLIVEIRA
Pró-Reitora de Extensão – PR-5

CLÁUDIA FERREIRA DA CRUZ
Pró-Reitora de Gestão e Governança – PR-6

EDUARDO MACH QUEIROZ
Pró-Reitor de Políticas Estudantis – PR-7

MARCOS BENILSON GONÇALVES MALDONADO
Prefeito da UFRJ

ROBERTO MACHADO CORRÊA
Diretor do Escritório Técnico da Universidade – ETU

SUPERINTENDÊNCIA-GERAL DE GOVERNANÇA

(Absorvendo temporariamente o Núcleo de Gestão de Riscos – conforme Resolução Consuni/UFRJ nº 120, de 31 de outubro de 2022)

EQUIPE

ROSINEI CUSUMANO CHIAVO

Superintendente-Geral de Governança

TEREZA CRISTINA BRITO DE CARVALHO

Diretora de Governança

LEONARDO DE SOUZA FERNANDES DOURADO

Chefe da Seção de Informações Gerenciais

COLABORADORES

ANDREIA OLIVEIRA

CLÁUDIA FERREIRA DA CRUZ

GABRIELA DEL CARMEN SARASA URIBE

TATIANA LIMA

GRUPO DE TRABALHO DE GESTÃO DE RISCOS

Conforme Portaria nº 3058, de 5 de abril de 2023

LUCAS MARTINS DIAS MARAGNO
Representante da Unidade de Gestão de Integridade (UGI)

ELSON NALON LOPES
Representante do Gabinete da Reitoria

DANIELA DE SOUZA NEGREIROS
Representante da Pró-Reitoria de Graduação (PR-1)

PAULO DE OLIVEIRA REIS FILHO
Representante da Pró-Reitoria de Pós-Graduação e Pesquisa (PR-2)

OLAVO ALVES DIOGO
Representante da Pró-Reitoria de Planejamento, Desenvolvimento e Finanças (PR-3)

LARISSA BARUQUE PEREIRA
Representante da Pró-Reitoria de Pessoal (PR-4)

MARGARETH CRISTINA DE ALMEIDA GOMES
Representante da Pró-Reitoria de Extensão (PR-5)

MARCELO DA SILVA GONÇALVES
Representante da Pró-Reitoria de Gestão e Governança (PR-6)

ADILSON COUTO DE SOUZA FILHO
Representante da Pró-Reitoria de Políticas Estudantis (PR-7)

ANGELUCIA MUNIZ
Representante do Complexo Hospitalar e da Saúde (CHS)

GIL LOUZANO PEIXOTO DE ALENCAR
Representante do Escritório Técnico da Universidade (ETU)

ODENEL VASCONCELLOS DA SILVA
Representante da Prefeitura Universitária (PU)

LIDVALDO JOSÉ DOS SANTOS
Representante da Superintendência de Tecnologia da Informação e Comunicação da UFRJ (STIC)

SUMÁRIO

LISTA DE FIGURAS

LISTA DE QUADROS

1. APRESENTAÇÃO

A presente metodologia de gestão de riscos foi elaborada com base na Instrução Normativa (IN) Conjunta Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União (MP/CGU) nº 1, de 10 de maio de 2016, que trata da modernização de práticas administrativas nos órgãos públicos. A partir desse normativo, a Reitoria da UFRJ estabeleceu o Sistema de Governança da UFRJ[1] a fim de aprimorar os mecanismos adequados à boa governança institucional e instituir uma estrutura de governança no âmbito da Universidade, para implantação e acompanhamento da sua gestão estratégica. Em paralelo a essa iniciativa, foi formulada a Política de Gestão de Riscos (PGR) da UFRJ, instituída por meio da Resolução Consuni nº 120, publicada no Boletim UFRJ nº 43, 2ª parte, de 31 de outubro de 2022.

Essa resolução revogou a Portaria Reitoria nº 2.500, de 26 de março de 2019, publicada no Boletim UFRJ extraordinário nº 12, de mesma data, visando a readequá-la para um modelo exequível e compatível com o nível de maturidade institucional de nossa Universidade. A PGR anterior se consolidava pela sua integração ao Sistema de Governança da UFRJ, estabelecido por meio da Portaria UFRJ nº 2.499, também de 26 de março de 2019 e atualmente revogada.

A PGR/UFRJ vigente estabelece a Gestão de Riscos na instituição, visando a atender ao Decreto nº 9.203, de 22 de novembro de 2017, que tornou obrigatória a adoção da gestão de riscos no âmbito do Poder Executivo Federal. O gerenciamento de riscos é um processo que consiste, inicialmente, na identificação dos principais riscos que possam comprometer a efetividade das ações de um planejamento institucional ou que impeçam o alcance dos resultados desejados e na consequente avaliação dos riscos identificados, a partir da mensuração da probabilidade de ocorrência e do impacto de cada risco. Em seguida, há o tratamento dos riscos considerados inaceitáveis, por meio da definição de ações para reduzir a probabilidade de ocorrência dos eventos ou suas consequências, e, por fim, a definição das ações de contingência para o caso de os eventos correspondentes aos riscos se concretizarem.

Para viabilizar o gerenciamento dos riscos na UFRJ nos moldes preconizados pela legislação vigente, foi desenvolvida a presente Metodologia de Elaboração do Plano de Gestão de Riscos, que tem como objetivos estabelecer conceitos, diretrizes, atribuições e responsabilidades do processo de gestão de riscos, bem como orientar os servidores na identificação, análise, avaliação, tratamento, monitoramento e comunicação desses riscos, com vistas ao alcance dos objetivos institucionais.

1 De acordo com a Portaria nº 6.611, de 28 de setembro de 2020 (Publicada no BUFRJ nº 47/2020).

2. INTRODUÇÃO

A UFRJ é uma estrutura complexa, compatível com um município de médio porte. Suas dimensões são excepcionais, com 70 unidades acadêmicas que agregam 67 mil discentes, 9 mil servidores técnico-administrativos e 4,2 mil docentes[2]. Isso, somado à multiplicidade e à abrangência de suas áreas acadêmicas, com intensa atividade de ensino, pesquisa e extensão, traduz a diversidade e os desafios envolvidos na gestão dessa estrutura, com a devida transparência, e no monitoramento e avaliação de seu desempenho – tarefas necessárias para viabilizar seu desenvolvimento harmônico e equilibrado e em conformidade com padrões elevados de eficiência, efetividade e eficácia.

A gestão de riscos é um instrumento de apoio complementar à gestão institucional, uma vez que pode contribuir para o aperfeiçoamento dos controles internos e o monitoramento sistemático dos riscos relacionados às atividades gerencial, estratégica e operacional. Sabe-se que riscos e incertezas fazem parte do cotidiano de todas as instituições, públicas ou privadas. No caso das universidades públicas, porém, mudanças culturais, políticas, legais, regulatórias, financeiras, econômicas e ambientais, inerentes à variabilidade e alternância de políticas governamentais, criam um ambiente de instabilidade e volatilidade. Isso torna imperiosa a redução desses riscos a níveis aceitáveis e o monitoramento de incertezas que possam interferir nas decisões pelas quais se busca assegurar maior eficácia, eficiência e efetividade no alcance dos objetivos estratégicos da instituição.

2 Fonte: https://pdi.ufrj.br/wp-content/uploads/2024/02/pdi-2020.2024-revisao-fevereiro-2024-2.pdf.

2.1 Normas e regulamentações relacionadas

O modelo de Gestão de Riscos da UFRJ tem como premissa básica a priorização de riscos relacionados aos processos institucionais que impactam diretamente os objetivos estratégicos definidos em seu Plano de Desenvolvimento Institucional (PDI) e em seu Planejamento Estratégico, além daqueles definidos no Plano de Integridade da Universidade. Ele é estruturado, portanto, em consonância com as leis, decretos e normas listados a seguir:

- IN MP/CGU nº 1/2016;
- Decreto nº 9.203/2017 (arts. 2º, 5º, 17, 18 e 19);
- Lei nº 13.709/2018;
- Portaria CGU nº 1.089/2018;
- Portaria CGU nº 57/2019;
- Lei nº 14.129/2021 (Capítulo VII);
- Lei nº 14.133/2021 (arts. 11, 18, 22, 43, 46, 72, 98, 103, 117, 133, 147 e 169);
- Decreto nº 10.756/2021 (art. 5º);
- Decreto nº 10.947/2022.

A IN Conjunta MP/CGU nº 1/2016 e, posteriormente, o Decreto nº 9.203/2017 tornaram obrigatória a adoção da gestão de riscos no âmbito dos órgãos e entidades do Poder Executivo Federal.

A Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe sobre 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 estabeleceu que as pessoas – naturais ou jurídicas, de direito público ou privado – que realizam tratamentos de dados pessoais devem elaborar um Relatório de Impacto à Proteção de Dados, o qual deve descrever medidas, salvaguardas e mecanismos de mitigação de riscos.

Ainda, o Capítulo VII da Lei nº 14.129/2021 estabelece que o sistema de gestão de riscos (SGR) a ser implementado nas instituições deve incluir uma análise crítica de riscos da prestação digital de serviços públicos que impactem suas missões. Entre os pontos citados na lei, estão: a gestão de riscos necessita estar integrada ao processo de planejamento estratégico e seus desdobramentos; a implementação 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 não somente dos processos de gestão de riscos, como também de governança e controle. A auditoria interna, por sua vez, contribuirá para avaliar e melhorar a eficácia desses processos.

A importância do SGR 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 SGR, 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.

Uma instituição está igualmente suscetível à ocorrência de práticas de corrupção, fraudes, irregularidades ou desvios éticos de conduta – o que caracteriza risco à integridade. Tais riscos podem comprometer valores, padrões e até mesmo objetivos institucionais, inclusive gerando outros riscos, como os de natureza financeira, operacional ou reputacional. Dessa forma, no âmbito dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, foi instituído o Sistema de Integridade Pública do Poder Executivo Federal (Sipef), por meio do Decreto nº 10.756/2021. Uma das competências do Sipef é orientar as atividades relativas à gestão de riscos para a integridade. A este decreto vem se somar a Portaria CGU nº 1.089/2018, que traz orientações sobre como os órgãos e as entidades da administração pública federal devem estruturar, executar e monitorar seus programas de integridade, tendo sido posteriormente atualizada pela Portaria CGU nº 57/2019.

Por fim, tem-se o Decreto nº 10.947/2022, que dispõe sobre o plano de contratações anual e institui o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional. Ele estipula 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. Tais relatórios possuem uma frequência mínima bimestral e sua apresentação deverá ocorrer, no mínimo, nos meses de julho, setembro e novembro de cada ano.

2.2 Referencial teórico

O processo de gestão de riscos deve ser incorporado na cultura e nas práticas da UFRJ a partir da implantação de um conjunto de macroprocessos baseados em metodologias específicas, entre as quais o COSO I (ou COSO-IC)[3], o COSO II (ou COSO-ERM)[4], a ABNT NBR ISO 31000:2018 e a IN Conjunta MP/CGU nº 1/2016.

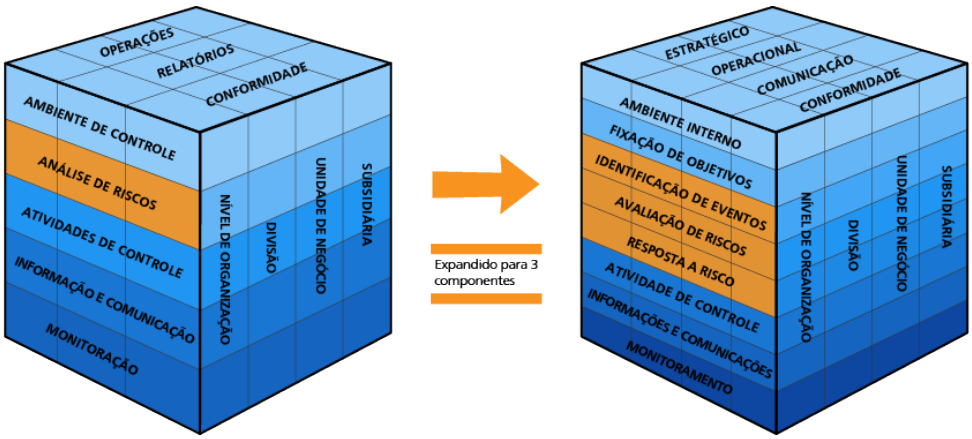
A metodologia COSO I foi estabelecida com o objetivo de orientar as organizações quanto aos princípios e melhores práticas de controles internos, em especial para assegurar a produção de relatórios financeiros confiáveis e prevenir fraudes. No modelo COSO I, o *controle interno* foi definido como um "processo projetado e implementado pelos gestores para mitigar riscos e alcançar objetivos". Por sua vez, *risco* é definido como "a possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos". A partir dessas definições, concebe-se o controle interno como um processo que busca mitigar riscos, com vistas ao alcance dos objetivos.

3 COSO – Committee of Sponsoring Organizations of the Treadway Commission; COSO I – Internal Control – Integrated Framework.

4 ERM – Enterprise Risk Management.

A inovação apresentada pela metodologia COSO II é a implementação do processo de gestão de riscos não só na realização de atividades administrativas, operacionais e de suporte, mas também naquelas de planejamento relacionadas à definição da estratégia institucional. Outro ponto é que a etapa de "análise de riscos" foi substituída e complementada pela etapa de identificação, avaliação e resposta (Figura 1). Ainda, é neste documento que conceitos como *apetite* e *tolerância a risco* são introduzidos: enquanto o primeiro se refere ao nível de risco que a entidade 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.

Figura 1: Mudanças na gestão de riscos do COSO-IC para o COSO-ERM



Fonte: Portal do TCU

Por sua vez, a ABNT NBR ISO 31000:2018 Gestão de Riscos – Princípios e Diretrizes está em consonância ao que é exposto no COSO II e em outras normas técnicas regionais que o antecederam. A última versão, que atualizou a norma publicada originalmente em 2009, não promoveu grandes mudanças, mas o processo de gestão de riscos desde então conta com as etapas de comunicação e consulta, estabelecimento do contexto, avaliação dos riscos (identificar, analisar e avaliá-los), monitoramento e, por último, registro e relato dos riscos.

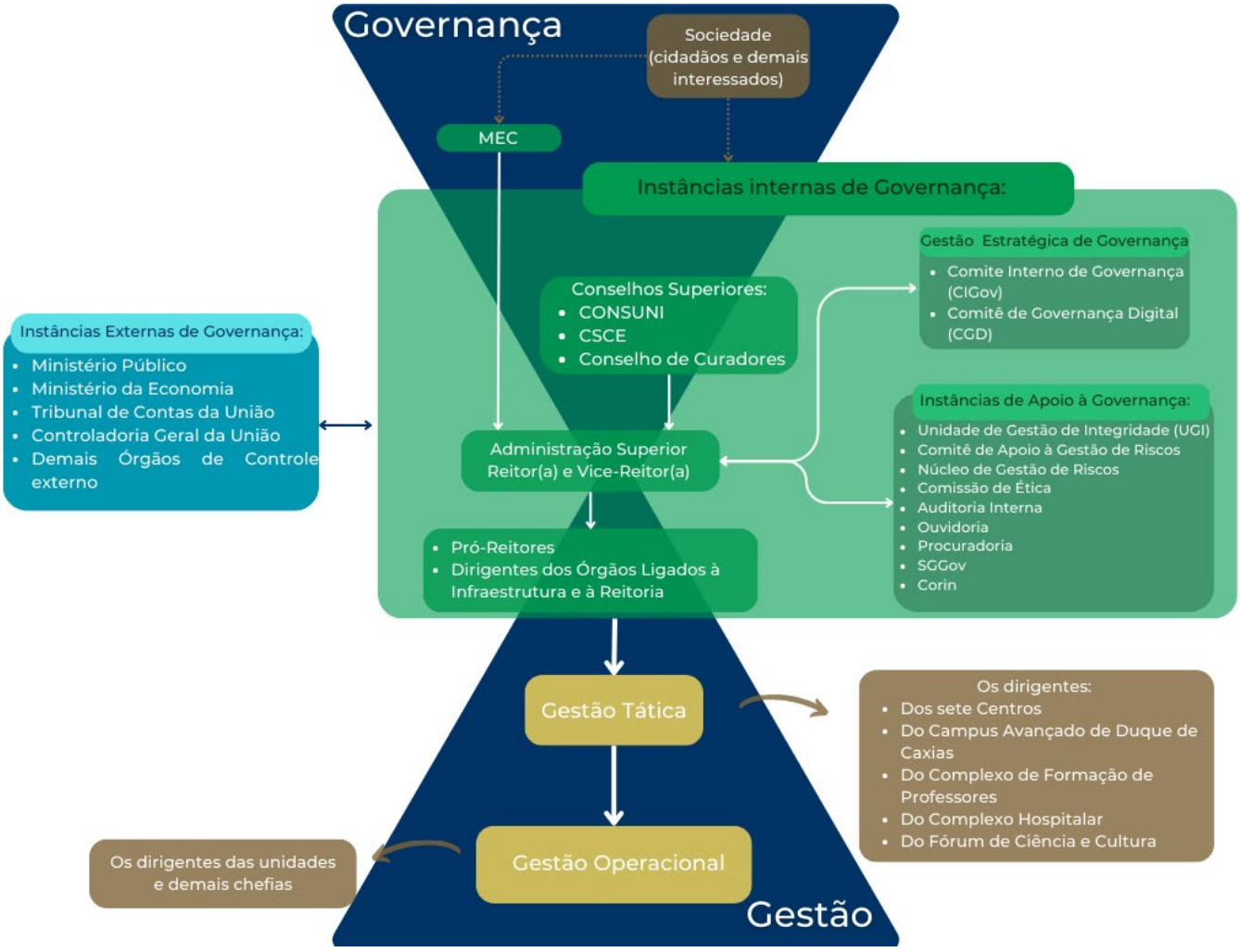
Já a IN Conjunta MP/CGU nº 1/2016, além de fornecer a estrutura do modelo de gestão de riscos, também elenca os princípios de uma boa governança e estabelece as linhas de defesa das organizações públicas para o alcance de seus objetivos. A primeira linha abrange os controles internos, que devem considerar os riscos que se deseja mitigar, enquanto a segunda linha se traduz pela supervisão e monitoramento dos controles internos por meio de comitês, diretorias ou assessorias específicas. Já a terceira linha é constituída pelas auditorias internas das instituições, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão.

Por último, para a elaboração deste plano foi igualmente utilizada como base teórico-conceitual a publicação *Metodologia de Gestão de Riscos*, do Ministério da Transparência e da Controladoria-Geral da União (2018).

2.3 Instâncias de supervisão e linhas de defesa aos riscos na UFRJ

Na UFRJ, a estrutura de governança é definida pelo Sistema de Governança, instituído pela Portaria UFRJ n° 6.611, de 28 de setembro de 2020, que provê meios para a organização, a participação e as diretrizes necessárias à interação de todos os atores relevantes para a gestão da Universidade. A condução da Política de Governança é de competência do(a) reitor(a), assessorado(a) por um comitê de alto nível, o Comitê Interno de Governança (CIGov). O modelo de governança da UFRJ se apresenta da seguinte forma:

Figura 2: Modelo de Governança da UFRJ



Fonte: Elaboração própria

A Governança é um conjunto de práticas de liderança, estratégia e controle que permite aos dirigentes de uma organização ou instituição o adequado conhecimento de sua situação e demandas, ao passo que também possibilita a execução dos objetivos estratégicos. No âmbito de uma instituição pública como a UFRJ, isto significa o alcance de políticas definidas pela Administração Superior e a prestação de serviços de interesse da sociedade.

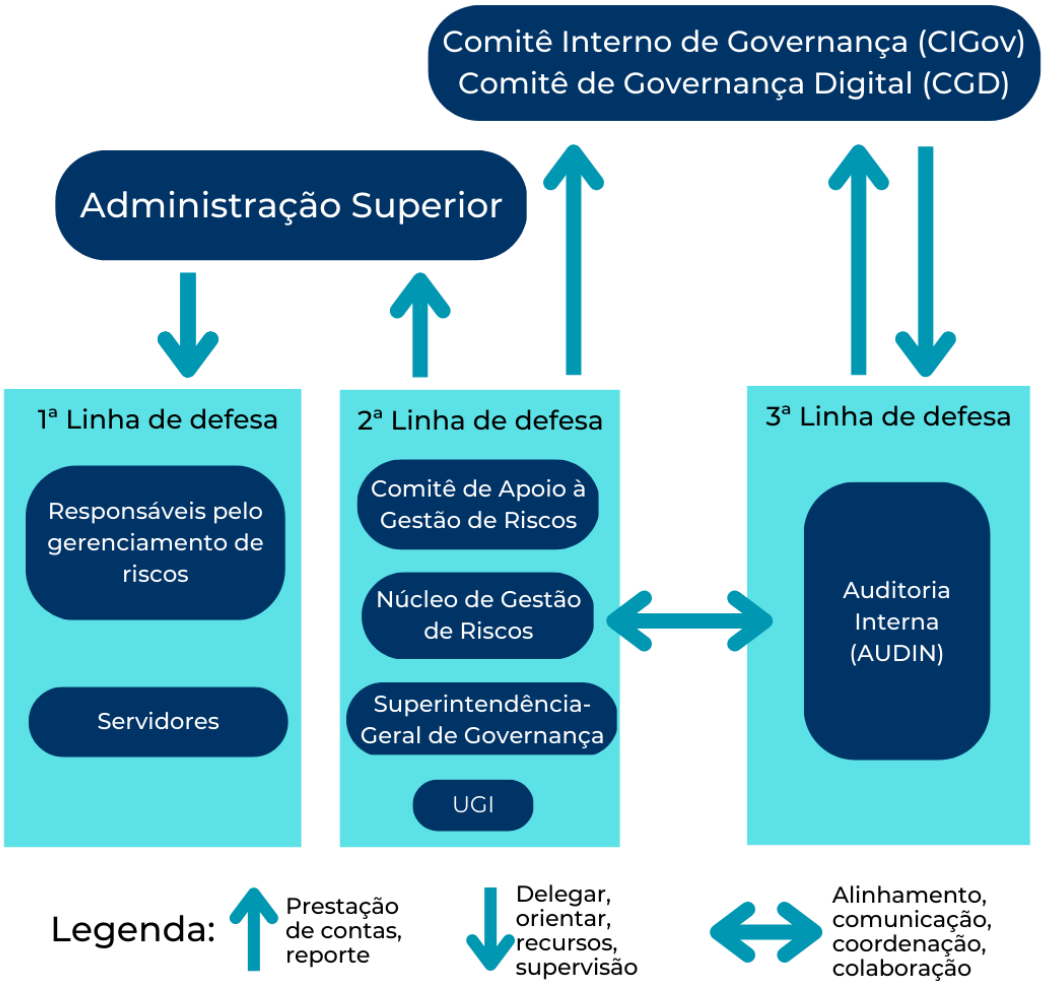
Na UFRJ as instâncias responsáveis pela gestão estratégica de Governança são o Comitê Interno de Governança (CIGov) e o Comitê de Governança Digital (CGD). Este último foi instituído pela Portaria nº 5.199, de 27 de julho de 2020, e tem as seguintes competências: coordenar e acompanhar as políticas de Tecnologia da Informação e de Segurança da Informação e o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC); garantir transparência nos processos de Tecnologias da Informação e Comunicação (TICs); promover a transparência e abertura de dados; e deliberar sobre os recursos às ações relacionadas às TICs. Em resumo, o CGD é o responsável pela gestão da Governança relacionada aos processos e projetos ligados às TICs, enquanto o CIGov trata dos demais assuntos de Governança da UFRJ.

A PGR/UFRJ define que compete aos servidores que sejam proprietários de riscos seu monitoramento e o consequente reporte aos responsáveis pelo gerenciamento desses riscos. Portanto, essa é a primeira linha de defesa.

A segunda linha é composta pela Unidade de Gestão da Integridade (UGI), pela Superintendência-Geral de Governança (SGGov), pelo Núcleo de Gestão de Riscos e pelo Comitê de Apoio à Gestão de Riscos. A UGI, instituída pela Portaria nº 8.236, de 25 de novembro de 2020, é a estrutura que coordena as ações que asseguram a conformidade dos servidores a princípios éticos, procedimentos administrativos e normas legais aplicáveis à instituição. A SGGov foi criada pela Resolução Consuni nº 4, de 28 de junho de 2018, e trata do desenvolvimento de instrumentos para o aprimoramento da gestão e governança institucional. Exerce, ainda, a Gerência Geral do Sistema de Governança, além de contribuir para o gerenciamento dos riscos inerentes ao exercício das atividades da UFRJ.

Por fim, na terceira linha encontra-se a Auditoria Interna da UFRJ (Audin), criada pela Portaria nº 810, de 3 de maio de 2001, com vinculação administrativa à alta administração da UFRJ e vinculação técnica à Controladoria-Geral da União (CGU), a partir de orientação normativa e supervisão técnica do Sistema de Controle Interno do Poder Executivo Federal. A figura a seguir ilustra a diagramação de como essas linhas se relacionam.

Figura 3: Modelo de Três Linhas do IIA 2020, adaptado para o ambiente da UFRJ



Fonte: Elaboração própria

2.4 Cadeia de Valor da UFRJ

A Cadeia de Valor é um conceito desenvolvido por Michael Porter (1996)[5], sendo útil para desagregar as atividades de uma organização ou instituição estrategicamente. Isto permite melhor compreensão de seus potenciais de diferenciação, tanto do ponto de vista econômico quanto tecnológico, além de contribuir para a execução de um modelo de serviços para geração de valor público. São as chamadas "atividades de valor". Na UFRJ, ela atualmente se divide em três grupos de processos: Macroprocessos Finalísticos, Governança e Gestão (Figura 4).

Esta informação é relevante, já que a IN Conjunta MP/CGU nº 1/2016 aponta que os riscos devem ser identificados e relacionados em diversos níveis da organização. Portanto, considerando a Cadeia de Valor da UFRJ e com base nos seus macroprocessos finalísticos, podem ser identificados:

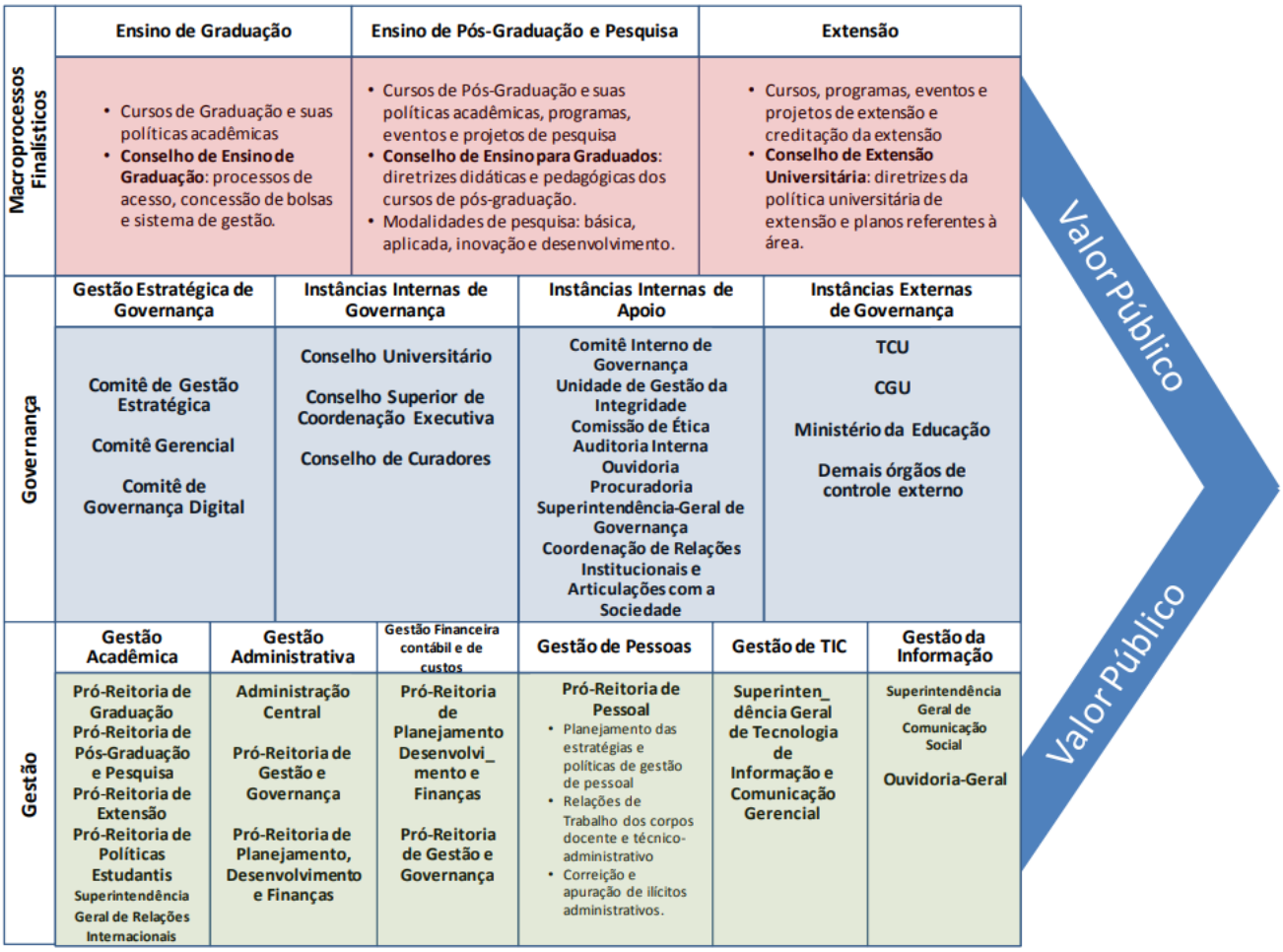
5 PORTER, Michael E. *Competição: estratégias competitivas essenciais.*, Rio de Janeiro: Campus, 2016.

- riscos no ensino de graduação;
- riscos no ensino de pós-graduação e pesquisa;
- riscos na extensão.

Já em relação aos macroprocessos de Gestão, temos os seguintes riscos:

- riscos na gestão acadêmica;
- riscos na gestão administrativa;
- riscos na gestão financeira, contábil e de custos;
- riscos na gestão de pessoas;
- riscos na gestão das Tecnologias da Informação e Comunicação (TICs);
- riscos na gestão da informação.

Figura 4: Cadeia de Valor da UFRJ



Fonte: Relatório de Gestão UFRJ 2022

3. MANUAL DE GESTÃO DE RISCOS E POLÍTICA DE GESTÃO DE RISCOS NA UFRJ

De acordo com a PGR/UFRJ, a gestão de riscos deverá estar integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura institucional. Além disso, seus objetivos são:

I. aumentar a probabilidade de alcance dos objetivos da Universidade, reduzindo os riscos a níveis aceitáveis;

II. fomentar uma gestão proativa;

III. atentar para a necessidade de se identificar e tratar riscos em toda a UFRJ;

IV. prezar pelas conformidades legal e normativa dos processos institucionais;

V. melhorar a governança;

VI. melhorar os controles internos da gestão;

VII. melhorar a eficácia e a eficiência operacional;

VIII. melhorar a aprendizagem institucional.

A citada resolução também estabeleceu que a PGR/UFRJ deverá ser operacionalizada considerando as seguintes etapas:

a) entendimento do contexto – identificação dos objetivos relacionados aos processos institucionais e análise dos ambientes externo e interno;

b) identificação de riscos – processo de encontrar, reconhecer e registrar os riscos para os objetivos da instituição;

c) análise de riscos – identificação das causas e consequências dos riscos levantados na etapa anterior;

d) avaliação de riscos – estimativa dos níveis de riscos identificados;

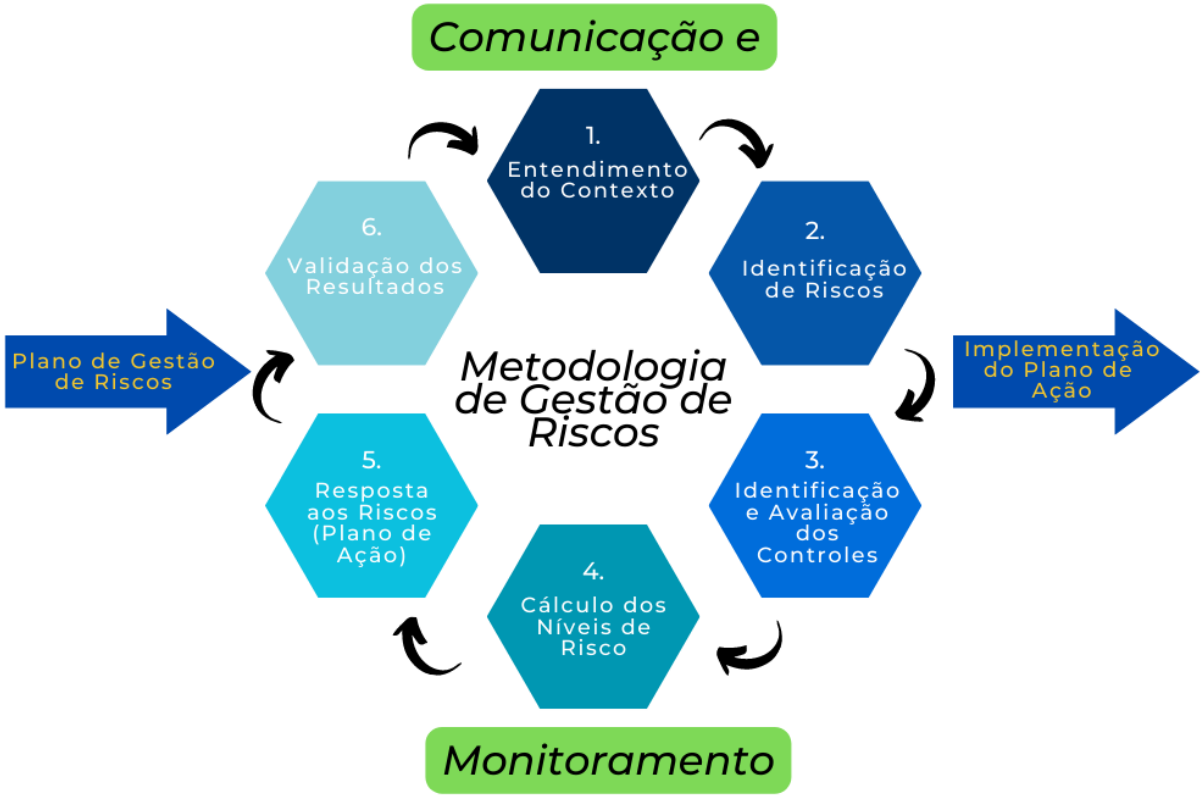
e) priorização de riscos – definição de quais riscos terão suas medidas de tratamento priorizadas;

f) definição de respostas aos riscos – definição da resposta ao risco conforme nível de apetite estabelecido para a UFRJ, além de estabelecimento das medidas de controle associadas a tais respostas;

g) comunicação e monitoramento – integra todas as etapas anteriores e é responsável pelo monitoramento constante visando à melhoria contínua.

A Figura 5 demonstra as etapas da PGR/UFRJ conforme a ISO 31000:2009 e como se dá o seu relacionamento com os princípios e a estrutura da Gestão de Riscos.

Figura 5: Etapas da Metodologia de Gestão de Riscos



Fonte: Elaboração própria

3.1 Competências da Gestão de Riscos na UFRJ

As estruturas intervenientes no processo de Gestão de Riscos na Universidade são o Comitê Interno de Governança (CIGov), o Comitê de Apoio à Gestão de Riscos e o Núcleo de Gestão de Riscos.

Ainda de acordo com a PGR/UFRJ, cada Objetivo Estratégico Institucional terá um Gestor Responsável, designado pelo CIGov. A esse gestor caberá a indicação dos gerentes dos riscos dos processos inerentes ao respectivo Objetivo.

Por fim, compete a todos os servidores da UFRJ que sejam proprietários de riscos o monitoramento da evolução dos níveis desses riscos e a efetividade das medidas de controle implementadas nos processos institucionais em que estiverem envolvidos ou de que tiverem conhecimento.

3.1.1 Comitê Interno de Governança

Criado pela Portaria nº 6.611, de 28 de setembro de 2020, o CIGov/UFRJ é responsável por assessorar a Reitoria na condução da política de governança, a fim de garantir que as boas práticas sobre o tema se desenvolvam e sejam apropriadas pela instituição de forma contínua e progressiva. No tocante à Gestão de Riscos, é seu papel designar os gestores responsáveis por cada Objetivo Estratégico Institucional.

A composição do CIGov engloba o(a) reitor(a), que o preside; o(a) vice-reitor(a); o(a) chefe de Gabinete; os(as) pró-reitores(as), o(a) ouvidor(a)-geral; o(a) superintendente-geral de Governança; o(a) superintendente de Tecnologia da Informação e Comunicação; e o(a) coordenador(a) de Relações Institucionais e Articulações com a Sociedade (Corin).

As atividades do CIGov são desempenhadas a partir das seguintes competências:

I. elaborar e revisar a Política de Gestão de Riscos;
II. definir e atualizar as estratégias de implementação da Gestão de Riscos, considerando os contextos externo e interno;
III. apreciar e aprovar as propostas do Comitê de Apoio à Gestão de Riscos;
IV. aprovar a metodologia de gestão de riscos e suas revisões;
V. avaliar o desempenho da arquitetura de Gestão de Riscos e fortalecer a aderência dos processos à conformidade normativa;
VI. garantir o apoio institucional para promover a Gestão de Riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos atores envolvidos;
VII. garantir o alinhamento da gestão de riscos aos padrões do Plano de Conduta e Integridade da UFRJ;
VIII. supervisionar a atuação das demais instâncias da Gestão de Riscos.

3.1.2 Comitê de Apoio à Gestão de Riscos

Este comitê será composto por representantes e respectivos suplentes das unidades do Gabinete do(a) Reitor(a); da Superintendência-Geral de Governança; da Pró-Reitoria de Gestão e Governança; da Pró-Reitoria de Planejamento, Desenvolvimento e Finanças; da Pró-Reitoria de Pessoal; da Superintendência de Tecnologia da Informação e Comunicação; e da Superintendência-Geral de Comunicação Social. Ele será presidido pelo representante do Gabinete da Reitoria.

Ao Comitê de Apoio à Gestão de Riscos compete:

I. auxiliar o Comitê Interno de Governança (CIGov) na elaboração e revisão da Política de Gestão de Riscos e na definição e nas atualizações da estratégia de implementação da Gestão de Riscos, considerando os contextos externo e interno;
II. definir os níveis de apetite a risco dos processos inerentes aos objetivos institucionais;
III. definir a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos inerentes aos objetivos institucionais;
IV. aprovar as respostas e as respectivas medidas de controle a serem implementadas nos processos inerentes aos objetivos institucionais;
V. avaliar a proposta de metodologia de gestão de riscos e suas revisões;
VI. aprovar os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
VII. monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;
VIII. avaliar o desempenho e a conformidade legal e normativa da Gestão de Riscos;
IX. definir indicadores de desempenho para a Gestão de Riscos, alinhados aos indicadores de desempenho da UFRJ;
X. encaminhar suas decisões e propostas para apreciação e aprovação do Comitê Interno de Governança (CIGov).

A literatura especializada recomenda que comitês dessa natureza e com tais atribuições deverão ser compostos por servidores com profundo conhecimento dos processos para realizarem o adequado encaminhamento técnico dos temas, acrescido de um perfil com maior autonomia para decisões e que exerça alguma espécie de autoridade na estrutura hierárquica da UFRJ. Nesse sentido, sugere-se que sejam indicados os superintendentes de cada pró-reitoria para sua composição.

3.1.3 Núcleo de Gestão de Riscos

Quando da publicação da PGR/UFRJ, o Núcleo de Gestão de Riscos ainda não contava com uma estrutura própria. Dessa forma, a Superintendência-Geral de Governança absorveu, por um período de 12 meses, suas responsabilidades.

Dentre essas competências e habilidades, podem-se destacar:

I. elaborar, em conjunto com GT designado pelo CIGov, o Plano de Gestão de Riscos e a metodologia da gestão de riscos, parte integrante do plano, bem como as revisões da metodologia, sempre que se fizer necessário;
II. definir os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;

III. monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;

IV. dar suporte à identificação; análise e avaliação dos riscos dos processos inerentes aos Objetivos Institucionais selecionados para a implementação da Gestão de Riscos;

V. consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los ao Comitê de Apoio à Gestão de Riscos e ao Comitê Interno de Governança (CIGov);

VI. oferecer capacitação continuada em Gestão de Riscos para servidores da UFRJ;

VII. elaborar Plano de Comunicação de Gestão de Riscos;

VIII. construir e propor ao Comitê de Apoio à Gestão de Riscos e ao Comitê Interno de Governança (CIGov), para apreciação e aprovação, os indicadores de desempenho para a Gestão de Riscos;

IX. medir o desempenho da Gestão de Riscos de acordo com as decisões decorrentes da análise tratada no inciso VIII;

X. requisitar aos responsáveis pelo gerenciamento de riscos dos processos institucionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais;

XI. orientar e apoiar as unidades acadêmicas e administrativas na execução de seus planos internos de gestão de riscos e demais instruções relativas à gestão de riscos.

3.2. Entendimento do contexto

O contexto pode ser dividido em ambiente externo e interno. O primeiro abrange aspectos culturais, políticos, legais, econômicos e tecnológicos, além daqueles relacionados a *stakeholders* (partes interessadas) externos. Já o segundo considera a estrutura da instituição, sua governança, recursos humanos, financeiros e tecnológicos, fluxo de informações, matriz de competências e responsabilidades.

O processo organizacional e seus objetivos devem ser analisados à luz deste contexto e devem ser identificados por, pelo menos:

- descrição resumida do processo. A descrição é um breve relato sobre o processo que permite compreender o seu fluxo, a relação entre os atores envolvidos e os resultados esperados;
- fluxo (mapa) do processo organizacional. Caso o processo ainda não esteja mapeado, é interessante realizar essa ação observando a notação BPMN (Business Process Model and Notation);
- infraestrutura utilizada;

- objetivos geral e específicos do processo organizacional;
- relação de objetivos estratégicos alcançados pelo processo;
- unidade responsável pelo processo organizacional;
- leis e regulamentos relacionados ao processo organizacional;
- partes interessadas no processo (externas e internas);
- análise SWOT (pontos fortes e fracos; ameaças e oportunidades);
- principais problemas do passado;
- sistemas tecnológicos que apoiam o processo organizacional.

Já para os projetos estratégicos, a abordagem é um pouco distinta. O objetivo da gestão de riscos aqui é permitir que os gerentes de projeto tomem decisões informadas para reduzir ou eliminar os riscos e maximizar as chances de sucesso do projeto, já que se trata de um empreendimento temporário realizado para criar um produto, serviço ou resultado exclusivo[6]. Por ser algo com início e fim já preestabelecidos, seu escopo e recursos também são previamente definidos. Além disso, a equipe, na maioria das vezes, é formada por pessoas que não costumam trabalhar juntas. Dessa forma, a análise de contexto dos projetos pode ser auxiliada pelo Termo de Abertura de Projeto (TAP), que contém as seguintes informações:

- título do projeto;
- coordenação do projeto;
- gestão do projeto;
- unidades envolvidas;
- objetivos do projeto;
- resultados esperados;
- entregas relevantes (marcos do projeto);
- cronograma;
- orçamento estimado.

Outro aspecto que deve ser considerado é a existência, segundo o PMBOK (Project Management Body Of Knowledge), do total de 49 processos de gerenciamento de projetos – divididos em cinco grupos de processos e dez áreas de conhecimento. Os cinco grupos estão organizados em: iniciação; planejamento; execução; monitoramento e controle; e fechamento. Portanto, a gestão de riscos também deverá ser feita para cada um desses grupos ou etapas do projeto.

6 PMI, P. M. I. PMBOK Guide. (Project Management Institute, 2017).

3.3. Identificação dos riscos

Os eventos desencadeadores dos riscos devem ser localizados, reconhecidos e descritos. É importante ter em mente que tais eventos englobam aqueles que possam atrasar, prejudicar ou impedir o cumprimento dos objetivos estratégicos, dos processos organizacionais e de suas etapas críticas. Especial atenção deve ser dada aos problemas ocorridos em anos anteriores, que podem ser futuras fontes de risco.

De acordo com a Política de Gestão de Riscos da UFRJ aprovada pelo Consuni, foi definida a seguinte tipologia de riscos:

I. Riscos Operacionais – eventos que podem comprometer as atividades da UFRJ, normalmente associados a falhas, deficiência ou internos, pessoas, infraestrutura e sistemas;

II. Riscos Legais – eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da UFRJ;

III. Riscos Financeiros/Orçamentários – eventos que podem comprometer a capacidade da UFRJ de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;

IV. Riscos à Integridade – eventos relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela UFRJ e a realização de seus objetivos;

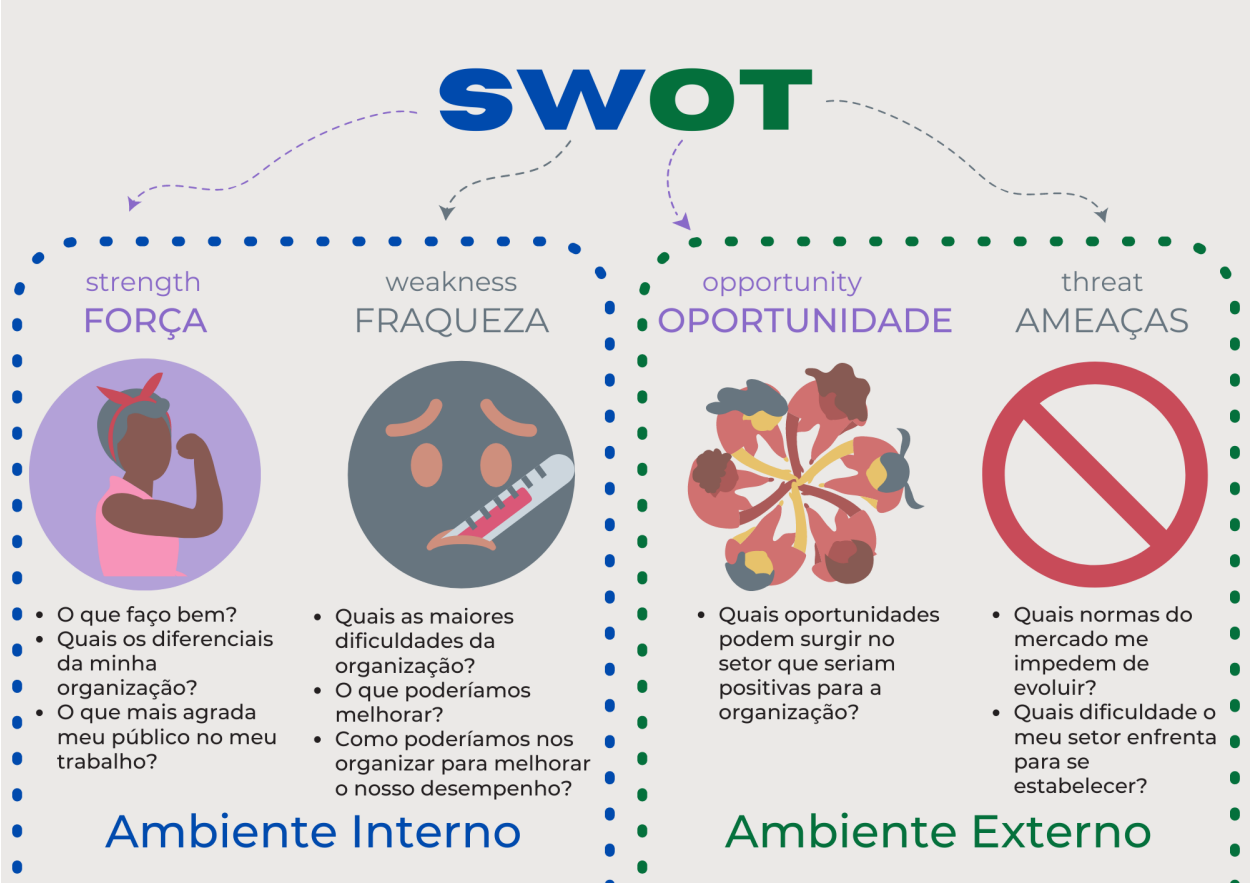
V. Riscos Estratégicos – eventos que afetam a estratégia ou os objetivos estratégicos da Universidade, estabelecidos no PDI;

VI. Riscos à Imagem e de Reputação – eventos que podem comprometer a confiança da sociedade em relação à capacidade da instituição em cumprir sua missão institucional.

Uma forma de auxiliar na identificação de riscos é por meio do uso de algumas técnicas (COSO, 2012; ISO 31010/2012) como:

- Reuniões – o gerente de riscos pode marcar encontros sobre identificação de riscos com as pessoas do setor envolvidas no processo, sendo necessário definir um limite de tempo para tornar a discussão mais objetiva;
- *Brainstorming* (tempestade de ideias) – explora a criatividade do grupo para expressar ideias acerca do processo em análise, sem julgamento imediato acerca da qualidade das ideias apresentadas;
- Análise SWOT (Figura 6) – consiste em uma ferramenta de identificação de forças e fraquezas (contexto interno), além de ameaças e oportunidades (contexto externo);

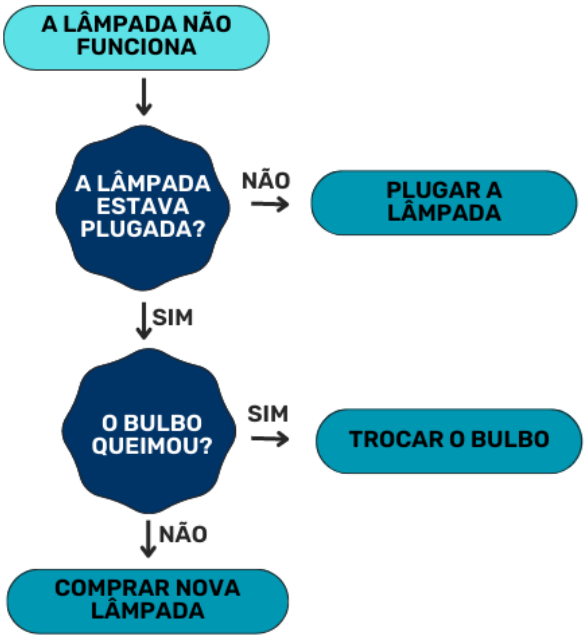
Figura 6: Análise SWOT



Fonte: Elaboração própria

- Entrevistas – conversas individuais com servidores, gestores e especialistas envolvidos com o processo;
- Análise de cenários – identificação de possíveis cenários futuros, de forma qualitativa ou quantitativa, considerando três tipos: otimista, realista e pessimista;
- *Benchmarking* – análise das melhores práticas de entidades que apresentem um desempenho superior nas práticas de gestão.
- Simultaneamente ao uso das técnicas indicadas, também podem ser empregadas as seguintes ferramentas:
- Fluxogramas (Figura 7) – o mapeamento do fluxo do processo por meio de uma representação gráfica pode auxiliar a identificar pontos de risco que podem ocorrer em cada etapa;

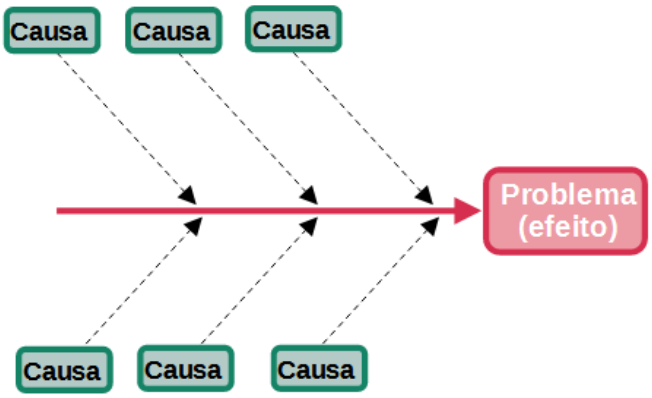
Figura 7: Exemplo de uso de fluxograma



Fonte: Elaboração própria, adaptado de Wikipedia

- Diagrama de Ishikawa (Figura 8) – identifica as causas-raiz e os efeitos do risco; as primeiras podem ser agrupadas em categorias distintas;

Figura 8: Diagrama de Ishikawa (de causa e efeito).



Fonte: Elaboração própria

- Técnica (ou método) Delphi – aplicada a grupos distantes geograficamente, consiste na utilização de um questionário solicitando a especialistas ideias de riscos. As respostas são compiladas e redistribuídas para novos comentários até haver consenso.

Adicionalmente, para o caso dos projetos é recomendado que seja feita uma análise e revisão de sua documentação (plano do projeto, escopo, requisitos, documentação técnica etc.) em busca de possíveis fontes de riscos. Outro ponto é o exame de lições aprendidas de projetos anteriores, já que os riscos neles identificados podem surgir novamente no projeto atual.

No Apêndice D há um caso prático que elucida como realizar esta etapa, por meio da utilização de um questionário de levantamento de riscos para um projeto de obras. Caso as respostas sejam negativas, isto implica a probabilidade de existência de um risco, e sua análise deve ser efetuada. A matriz causa-ciclo é preenchida com base na resposta a esse questionário (eventos prováveis devem ser preenchidos com 1 e improváveis com 0) e percebe-se uma identificação de riscos atravessando todo o ciclo de vida do projeto, segregando a análise tanto em um contexto externo (Políticos, Natureza e Outros) quanto interno (Técnicos, Organizacionais, Legais e Comercial). O detalhamento dessas categorias segue o preconizado pelo Project Management Institute (PMI) e já se encontra adaptado para o cotidiano da UFRJ.

Uma vez que os riscos tenham sido identificados (evento de risco) e classificados de acordo com as categorias predefinidas, é importante explicitar suas causas (fatores que aumentam a probabilidade de o risco ocorrer) e consequências (impactos gerados quando o risco ocorre efetivamente), além de identificar os gestores responsáveis. Todas estas informações podem ser consolidadas em um Mapa de Riscos, conforme indica o Quadro 1.

Quadro 1: Mapa de Riscos

Identificação de Riscos				**Classificação dos Riscos**	
Objetivo (OBJ)	**Evento de Risco (ER)**	**Causas (CA)**	**Consequências (CO)**	**Classificação do Risco**	**Gestor de Risco**
OBJ1	ER 1	CA 1	CO 1	Ex.: Operacional	Nome (Cargo/Função)
		CA 2	CO 2		
	ER 2	CA 1	CO 1	Ex.: Legal	Nome (Cargo/Função)
		CA 2	CO 2		
OBJ2	ER 1	CA 1	CO 1	Ex.: Estratégico	Nome (Cargo/Função)
		CA 2	CO 2		
	ER 2	CA 1	CO 1	Ex.: Financeiro	Nome (Cargo/Função)
		CA 2	CO 2		

Fonte: Manual de Gestão de Riscos da UFSC, 2020

As causas são compostas pela associação da fonte (substantivo) com a respectiva vulnerabilidade (adjetivação). Exemplos de fontes podem ser pessoas, processos, sistemas informatizados, estrutura organizacional, infraestrutura física, sistemas de gestão, tecnologia, eventos externos etc. Podemos elencar alguns casos práticos para facilitar a compreensão:

I. Folha de pagamento: uma das causas de risco para um processo de elaboração de folha de pagamento dos servidores da UFRJ pode se relacionar à equipe de *pessoas* (FONTE) que atuam no processo, que, quando em número reduzido e *insuficiente*, indica uma VULNERABILIDADE.

II. Controle de acesso a sistemas: na ocorrência do desligamento de um(a) servidor(a) de uma determinada função ou setor, as suas credenciais de acesso podem se manter

ativas. Aqui a causa de risco é um processo **(FONTE)** mal desenhado **(VULNERABILIDADE)**, já que não há uma etapa de comunicação automática à STIC por parte das chefias de cada setor ou da PR-4.

III. Ausência de integração de sistemas informatizados: Uma fonte inequívoca de VULNERABILIDADE consiste na falta de integração **(FONTE)** dos diversos sistemas informatizados que a UFRJ mantém em funcionamento.

3.4. Identificação e avaliação dos controles

Antes de definir os tipos de tratamento ao risco, é necessário avaliar os controles que a instituição possui e que já foram implementados aos riscos inerentes, de modo a obter os riscos residuais (CGU, 2018). Esta etapa é denominada de identificação e avaliação dos controles internos e aqui é interessante verificar se os controles que já existem estão sendo eficazes e eficientes. Todo aquele controle que não se adequar a esses dois critérios deve ser eliminado, pois está gerando um custo desnecessário à Administração Pública.

A IN Conjunta MP/CGU nº 1/2016 define os controles internos da gestão como o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizado de forma integrada pela direção e pelo corpo de servidores das organizações e destinado a enfrentar os riscos e fornecer segurança razoável na consecução da missão da entidade.

Os controles internos podem ser classificados em distintas categorias que visam a ajudar no entendimento do tipo de risco associado ao controle, como ele trata o risco e a evidência que fornece. Segundo a CGU (2018), o tipo de controle é caracterizado com um atributo que lhe confere características de prevenção, detecção, atenuação ou recuperação.

O COSO faz distinção entre controles preventivos e controles de detecção. Tanto na literatura quanto na prática, há consenso de que uma combinação desses tipos de controles costuma ser mais eficaz do que utilizar apenas um deles. Tanto os controles preventivos, que evitam a concretização de determinadas transações, quanto os de detecção, que identificam oportunamente transações discrepantes ou ações inadequadas, podem ser (ou combinar) atividades de controles informatizados e manuais (COSO, 2007).

Por sua vez, a Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, embora não mencione diretamente o termo controles internos, faz uso do conceito – utilizando apenas uma nomenclatura distinta – em suas orientações sobre o relatório de gestão de riscos do Plano de Contratações Anual (PCA)[7]. A elaboração de seu Mapa de Riscos deve considerar ações preventivas e ações de contingência. Enquanto as primeiras visam a neutralizar ou minimizar a probabilidade de ocorrência do risco, as últimas devem ser tomadas caso o risco se efetive.

Ao projetar controles, é necessário considerar o que pode dar errado com a transação (ou seja, qual é o risco de distorção relevante ou de não atingimento do objetivo) que resultaria em um erro. Essa técnica é chamada de What Can Go Wrong (WCGW) [O que Pode Dar Errado]. É importante perceber que os controles preventivos eficazes devem evitar que os WCGW ocorram.

7 As orientações podem ser consultadas por meio deste link.

A CGU (2018) indica uma forma de avaliar o efeito mitigador dos controles internos em relação aos riscos identificados e analisados. A metodologia consiste em avaliar os controles internos existentes e quantificar em níveis de efetividade conforme critério de mensuração ilustrado adiante. A CGU (2018) sugere ainda algumas perguntas que podem direcionar esta fase, a saber:

a) Existem outros controles presentes neste processo/subprocesso? Caso existam, tais controles estão associados aos riscos identificados?

b) Na visão da equipe técnica e do gerente de riscos, os controles identificados são eficazes? Se a resposta for negativa, é possível corrigir tais controles a fim de torná-los eficazes?

c) O custo financeiro e/ou operacional de cada um dos controles identificados se justifica perante os riscos mitigados?

No âmbito da UFRJ, podemos considerar como responsáveis pelos controles internos os servidores incumbidos da atividade ou do processo, e avaliação de sua eficácia e efetividade deve ser feita em conjunto com a chefia direta.

3.5. Cálculo dos níveis de risco

Nesta etapa são calculados os níveis dos riscos identificados pela equipe técnica responsável pela gestão de risco – tanto a equipe dirigida pelo gestor responsável pelo objetivo estratégico em questão quanto a equipe coordenada pelo gerente do risco do processo inerente ao objetivo – a partir de critérios de probabilidade e impacto. Os critérios de peso devem ser utilizados conforme as definições apresentadas nos Quadros 2 e 3, os quais são baseados na *Metodologia de Gestão de Riscos* publicada pela CGU.

A análise da probabilidade considera o conhecimento técnico e experiências vivenciadas pelos servidores de cada área da UFRJ. Primeiro, deve-se realizar a avaliação quantitativa, por exemplo, com base nos dados históricos e estatísticos de eventos de riscos já materializados. Segundo o COSO (2007), dados de eventos passados observáveis fornecem uma base mais objetiva do que as estimativas inteiramente subjetivas.

Caso seja a primeira vez em que os eventos de riscos estejam sendo identificados e não existam bases históricas, podem ser utilizados dados de fontes externas ou, ainda, ser realizada uma avaliação qualitativa. Contudo, dados gerados internamente e embasados na experiência passada da própria organização podem refletir qualidades organizacionais menos subjetivas e propiciar melhores resultados do que os dados de fontes externas (COSO, 2007).

Quadro 2: Escala de Probabilidade segundo Metodologia de Gestão de Riscos

Probabilidade	Descrição da probabilidade, desconsiderando os controles	Frequência	Peso
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	<10%	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	>=10% <=30%	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	>30% <=50%	3
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	>50% <=90%	4
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, pois as circunstâncias indicam claramente essa possibilidade.	>90%	5

Fonte: Guia CGU, 2018

A frequência, descrita na tabela anterior, pode ser calculada por meio da razão entre o número de eventos de risco e a quantidade de processos, ambos ao longo do ano, conforme pode se verificar na equação a seguir.

F = ER/QP

em que:

F = frequência

ER = evento de risco

QP = quantidade de processos

O impacto, caso um evento de risco ocorra, é o efeito resultante de sua ocorrência e pode ser positivo ou negativo (BRASIL, 2017). Dessa forma, não se limita a consequências econômicas e deve ser avaliado conforme as consequências para âmbitos específicos, como desperdício de recursos ou mau desempenho do processo, desconformidade legal, danos ao erário e danos à imagem (MINISTÉRIO DA ECONOMIA, 2021).

Quadro 3: Escala de Impacto segundo Metodologia de Gestão de Riscos

Impacto	Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou desconformidade).	1
Baixo	Pequeno impacto nos objetivos (idem).	2
Médio	Moderado impacto nos objetivos (idem), porém irrecuperável.	3
Alto	Significativo impacto nos objetivos (idem), de difícil reversão.	4
Muito alto	Catastrófico impacto nos objetivos (idem), de forma irreversível.	5

Fonte: Guia CGU, 2018

De acordo com o Guia da CGU (2018), em primeiro lugar são analisados os riscos inerentes, que são aqueles identificados sem considerar qualquer ação de mitigação ou, ainda, sem que nenhum tipo de controle tenha sido aplicado. O nível de risco inerente é então calculado a partir da multiplicação dos valores de probabilidade e o impacto entre si.

RI = NP x NI

em que:

RI = nível do risco inerente

NP = nível de probabilidade do risco

NI = nível do impacto do risco

A partir do resultado do cálculo, é feita a classificação do risco inerente dentro de uma das faixas descritas no Quadro 4.

Quadro 4: Classificação do Risco segundo Metodologia de Gestão de Riscos

Classificação	Faixa
Risco baixo – RB	0 – 4,99
Risco médio – RM	5 – 11,99
Risco alto – RA	12 – 19,99
Risco extremo – RE	20 – 25

Fonte: Guia CGU, 2018

De forma geral, nos ciclos seguintes da metodologia de gerenciamento de riscos do processo organizacional, a unidade deve considerar o nível de risco inerente calculado no primeiro ciclo e reavaliar os controles existentes para o cálculo do risco residual. A comparação entre os níveis de riscos residuais de diferentes ciclos objetiva identificar se os controles definidos nos Planos de Tratamento estão sendo eficazes para tratar o risco.

Em função da classificação e das possíveis combinações das escalas de probabilidade e impacto, é montada a Matriz de Riscos, ou mapa de calor, conforme indica o Quadro 5.

Quadro 5: Matriz de Riscos segundo Metodologia de Gestão de Riscos

IMPACTO					
Muito alto 5	5 RM	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 RM
	Muito baixa 1	Baixa 2	Média 3	Alta 4	Muito alta 5

PROBABILIDADE

Fonte: Guia CGU, 2018

O risco inerente, cujo nível foi calculado previamente na etapa de *Avaliação de Riscos,* deve ser multiplicado pelo valor do nível de avaliação dos controles internos a fim de estabelecer o nível do risco residual.

Quadro 6: Avaliação e mensuração dos controles internos

Nível		Descrição
Qualitativo	Quantitativo	
Inexistente	1,0	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.
Fraco	0,8	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.
Mediano	0,6	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.
Satisfatório	0,4	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.
Forte	0,2	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.

Fonte: Guia CGU, 2018

A IN Conjunta MP/CGU nº 1/2016 define risco residual como aquele a que uma organização está exposta após a implementação de ações gerenciais para o tratamento e mitigação do risco.

RR = RI x FAC

em que:

RR = risco residual

RI = risco inerente

FAC = fator de avaliação dos controles

Assim, percebe-se que, quanto mais forte o controle interno, menor será o resultado do risco residual. Em seguida, um novo mapa de calor deve ser construído para servir de suporte à avaliação dos riscos e à adoção de novas medidas de mitigação.

Na lógica da gestão da identificação e avaliação de riscos, a análise sobre controles e medidas mitigadoras é de fundamental importância para um direcionamento dos esforços e recursos organizacionais para a gestão dos seus riscos.

No caso da gestão de riscos em projetos estratégicos, a Matriz de Riscos já adaptada à presente metodologia se encontra disponível no Apêndice D. Enquanto a análise de probabilidade segue o exposto anteriormente, a estimativa do impacto é feita com base em quatro critérios: custo, tempo, escopo e qualidade – aquele que apresentar a maior pontuação representará o impacto total do evento de risco analisado. O nível de risco de cada evento é obtido então por meio da multiplicação desses dois fatores e, ao final, é calculado o somatório de todos os níveis de risco para que se obtenha o risco total do projeto. Este critério, associado ao impacto quantitativo (financeiro), auxiliará na tomada de decisão pelo gerente de projetos.

3.6 Resposta aos riscos

Os riscos nesta etapa são priorizados conforme o apetite a risco definido pelo Comitê de Apoio à Gestão de Riscos e aprovado pelo Comitê Interno de Governança (CIGov). Considerando a condição da UFRJ de instituição pública (autarquia federal), sem fins lucrativos, com autonomia legalmente definida, cujas atividades são custeadas com recursos do Tesouro Nacional, inicialmente se admite um **nível moderado** de apetite a risco. Dessa forma, as atividades, projetos e processos avaliados no âmbito da Universidade podem suportar riscos de níveis baixo a médio.

Apetite a risco, conforme já citado neste documento, significa o nível de risco que a instituição está disposta a aceitar. Em resumo, todos os riscos cujos níveis estejam dentro do apetite definido pela organização podem ser admitidos e, se houver priorização de tratamento de algum deles, isso deverá ser devidamente justificado. Em contrapartida, para aqueles riscos cujos níveis estejam acima do apetite aceitável, tratamentos deverão obrigatoriamente ser realizados e, quando não forem, também deverá haver justificativa.

As ações que devem ser adotadas em relação aos tipos de riscos e suas exceções estão detalhadas no Quadro 7, conforme orientações relativas à Gestão de Riscos elaboradas pela CGU. Ressalta-se, entretanto, que, para os casos de riscos alto e extremo envolvendo os objetivos institucionais, o Comitê de Apoio à Gestão de Riscos deverá aprovar as respostas e as respectivas medidas de controle a serem implementadas – uma vez que essa instância já tenha sido criada.

Quadro 7: Atitude perante o risco de acordo com a classificação

Classificação	Ação necessária	Exceção
Risco Baixo	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, entretanto cabe uma avaliação do custo-benefício sobre os controles internos existentes, a fim de verificar se precisam ser mantidos ou não.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Médio	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pelo gerente de risco e aprovada pelo dirigente da unidade organizacional/ gestor responsável, quando for o caso.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao dirigente da unidade organizacional/ gestor responsável e ter uma ação tomada em curto intervalo de tempo. Postergação de medidas só com autorização do dirigente da unidade organizacional/ gestor responsável.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo dirigente da unidade organizacional/ gestor responsável e aprovada pelo Comitê Interno de Governança.
Risco Extremo	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao Comitê de Governança Interna e ao dirigente da unidade organizacional/ gestor responsável. Postergação de medidas só com autorização do Comitê de Governança Interna.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo dirigente da unidade organizacional/ gestor responsável e aprovada pelo Comitê Interno de Governança.

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

As equipes técnicas, em colaboração com os respectivos gerentes de riscos, assim como os gestores dos projetos estratégicos, definirão o tipo de tratamento (descritos no Quadro 8) com base no nível de risco e no apetite ao risco definido pela UFRJ. Os tipos de tratamento envolvem:

Quadro 8: Os quatro tipos de ações para tratamento de riscos

Tipo de Tratamento ao Risco	Descrição do Tratamento
Aceitar	A exposição ao risco pode ser tolerada pela instituição e não há necessidade de implementar quaisquer ações adicionais para mitigá-lo (aceitação passiva). A aceitação do risco também pode ser do tipo ativa, na qual um plano de contingência pode ser elaborado caso o risco ocorra, a fim de reduzir seu impacto.
Evitar	O processo organizacional deve ser descontinuado.
Mitigar	Ações para tratar causas e consequências dos riscos são implementadas, ou seja, sua probabilidade de ocorrência e/ou impacto é reduzida.
Compartilhar/ Transferir	Indicados para riscos altos e extremos, quando as medidas de tratamento não possuem um bom custo-benefício. Neste caso, a chefia da unidade e o Núcleo de Gestão de Riscos deverão ser comunicados.

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

Para os casos em que há uma quantidade excessiva de eventos de riscos a serem mitigados ou compartilhados/transferidos, um critério para orientar e otimizar a tomada de decisão dos gestores e gerentes de risco em relação a quais eventos priorizar é a utilização da matriz GUT. Essa é uma técnica que permite evitar o desperdício de tempo e de recursos financeiros e humanos, ao elencar as prioridades por meio dos critérios de gravidade, urgência e tendência, cujas iniciais formam a sigla GUT e definições estão descritas a seguir.

- **Gravidade** – significa o impacto que dado evento pode causar na instituição e na continuidade de seus negócios;
- **Urgência** – atrelada ao prazo que a equipe possui para resolução do problema. Quanto mais curto for esse prazo, mais urgente é o problema;
- **Tendência** – contempla a avaliação da probabilidade do problema de piorar ou não com o tempo. Quanto maior a tendência, maior a chance de que a piora se concretize.

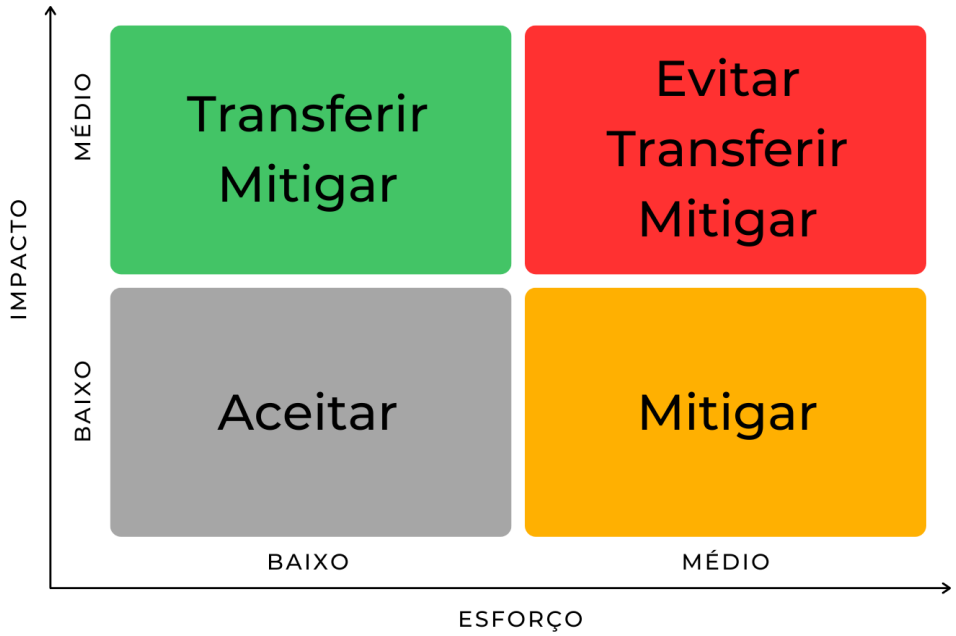
A escala para cada um desses critérios varia de 1 a 5, conforme detalhado no Quadro 9.

Quadro 9: Escalas da matriz GUT de acordo com os critérios de gravidade, urgência e tendência

Nota	Gravidade	Urgência	Tendência
1	Nada grave	Não é urgente	Estável
2	Pouco grave	Pouco urgente	Pode piorar a longo prazo
3	Grave	Urgente	Pode piorar a médio prazo
4	Muito grave	Muito urgente	Pode piorar a curto prazo
5	Extremamente grave	Extremamente urgente	Pode piorar no momento atual

Um resumo das ações de tratamento de acordo com as escalas de probabilidade e impacto do risco é indicado na Figura 9. Riscos dentro do nível de apetite da instituição podem ser aceitos ou tolerados sem quaisquer ações adicionais. Assim, se o gestor julgar oportuno elaborar um plano de resposta considerando o risco em questão, é necessário apresentar uma justificativa oportuna ou evidenciar que isso não irá gerar custos desnecessários ao processo. Em contrapartida, quando o risco está acima do que a UFRJ pode suportar, deve-se notar que são necessárias ações mais elaboradas, que vão desde a mitigação (ou redução); passando pela sua transferência, por meio da contratação de uma seguradora, ou o compartilhamento com instâncias ou órgãos superiores; e culminando inclusive em evitar o risco, o que implica a descontinuidade do processo ou projeto.

Figura 9: Resumo das ações de tratamento possíveis de acordo com o nível de risco



Fonte: Elaboração própria

Ao final desta etapa, o Mapa de Riscos terá evoluído para sua versão completa, apresentada no Quadro 10 e composta pelos eventos de riscos identificados no início do processo de Gestão de Riscos e por suas respectivas causas e consequências, assim como a tipologia dos riscos e o gestor responsável (Quadro 1). Os valores de probabilidade e impacto foram considerados conforme as escalas dos Quadros 2 e 3, respectivamente, e multiplicados entre si para se obter o nível de risco – classificado de acordo com o Quadro 4. Posteriormente, a eficácia dos controles também foi analisada segundo o exposto no Quadro 6, transformando o risco inerente em residual e permitindo avaliar qual a opção de tratamento será a mais indicada (Quadro 8).

Quadro 10: Mapa de Risco após a definição das respostas

Identificação			
Objetivo	Evento de Risco	Causa	Consequência
Obj1	ER1	CA1 CA2	CO1 CO2
Análise			
Classificação		Gestor	
Legal		Nome (setor A)	
Avaliação Risco Inerente			
Probabilidade	Impacto	Nível do Risco Inerente	Avaliação do Risco Inerente
2	2	4	Risco Baixo
Avaliação Controle			
Descrição do Controle	Nível do Controle		Avaliação
1.1 ... 1.2...	Satisfatório		0,4
Avaliação Risco Residual			
Nível do Risco Residual	Avaliação do Risco Residual	Resposta ao Risco	Plano de Ação
1,6	Risco Baixo	Aceitar	Não

Fonte: Adaptado do Manual de Gestão de Riscos da UFSC

3.6.1 Plano de Ação (ou Plano de Tratamento)

Uma vez que uma das quatro ações de tratamento do risco descritas anteriormente tenha sido definida para cada risco identificado, é chegado o momento de elaborar o Plano de Tratamento ou Plano de Ação. Trata-se de um documento que detalha as medidas de tratamento dos riscos dos processos organizacionais avaliados, permitindo sua implementação. Orientamos que para sua confecção seja utilizada a ferramenta 5W2H, que abrange as seguintes perguntas:

- **W**HAT: **o que** será feito?
- **W**HY: **por que** será feito?
- **W**HERE: **onde** será feito?
- **W**HEN: **quando** será feito?
- **W**HO: **por quem** será feito?
- **H**OW: **como** será feito?
- **H**OW MUCH: **quanto** custará?

Dessa forma, o Plano de Ação deverá conter, no mínimo:

- iniciativa, com a proposta de projeto ou ação que implementará um conjunto de medidas de tratamento;
- medida(s) de tratamento contemplada(s) na iniciativa e o risco relacionado que desejam tratar;
- objetivos/benefícios esperados por medida de tratamento;
- unidade organizacional responsável pela implementação da iniciativa;
- unidades organizacionais corresponsáveis pela implementação da iniciativa, ou seja, unidades envolvidas na implementação da medida de tratamento;
- servidor ou cargo responsável pela implementação;
- breve descrição sobre a implementação;
- custo estimado para a implementação;
- datas previstas para início e término da implementação;
- status atualizado da iniciativa.

Um modelo do Plano de Ação pode ser visualizado no Quadro 11, apresentado a seguir.

Quadro 11: Modelo de Plano de Ação ou Plano de Tratamento

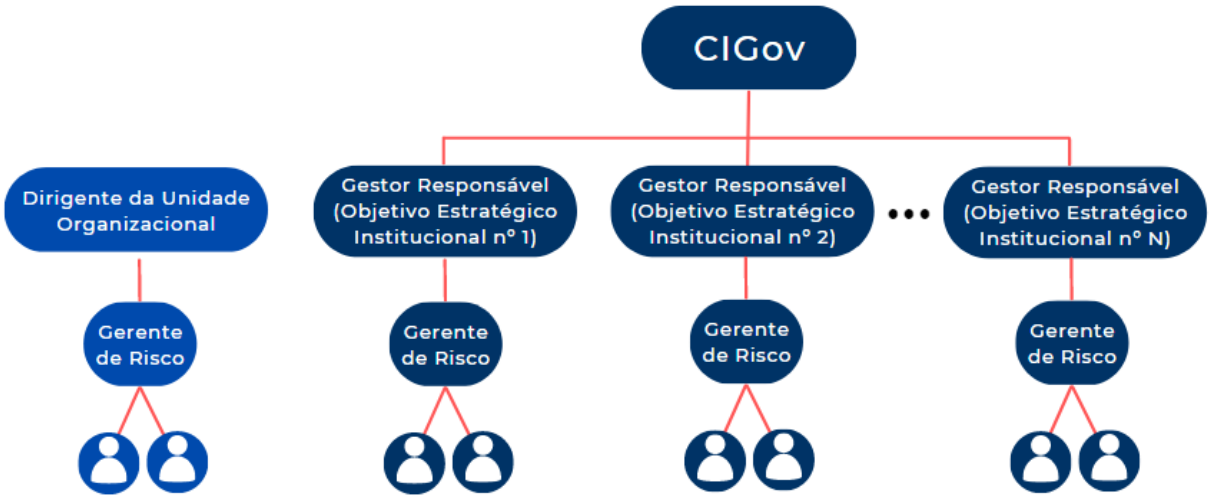
Iniciativa	Evento de Risco	Medida de Tratamento	Unidade Responsável	Unidades Corresponsáveis	Responsável pela Implementação	Como será implementado	Custo Previsto	Data Prevista para Início da Implementação	Data Prevista para o Término da Implementação	Status

Fonte: Metodologia de Gestão de Riscos da CGU, 2018

3.7 Validação dos resultados

Conforme disposto na PGR/UFRJ, cabe ao CIGov designar um Gestor Responsável por cada Objetivo Estratégico Institucional e a este, por sua vez, compete indicar os gerentes dos riscos dos processos inerentes ao respectivo Objetivo. Além disso, os dirigentes de cada Unidade organizacional devem indicar os gerentes dos riscos de cada processo que não esteja relacionado com o Objetivo Estratégico Institucional, a fim de evitar redundâncias (Figura 10).

Figura 10: Fluxo de designação dos responsáveis pelos riscos dos Objetivos Estratégicos Institucionais e dos processos no âmbito da UFRJ



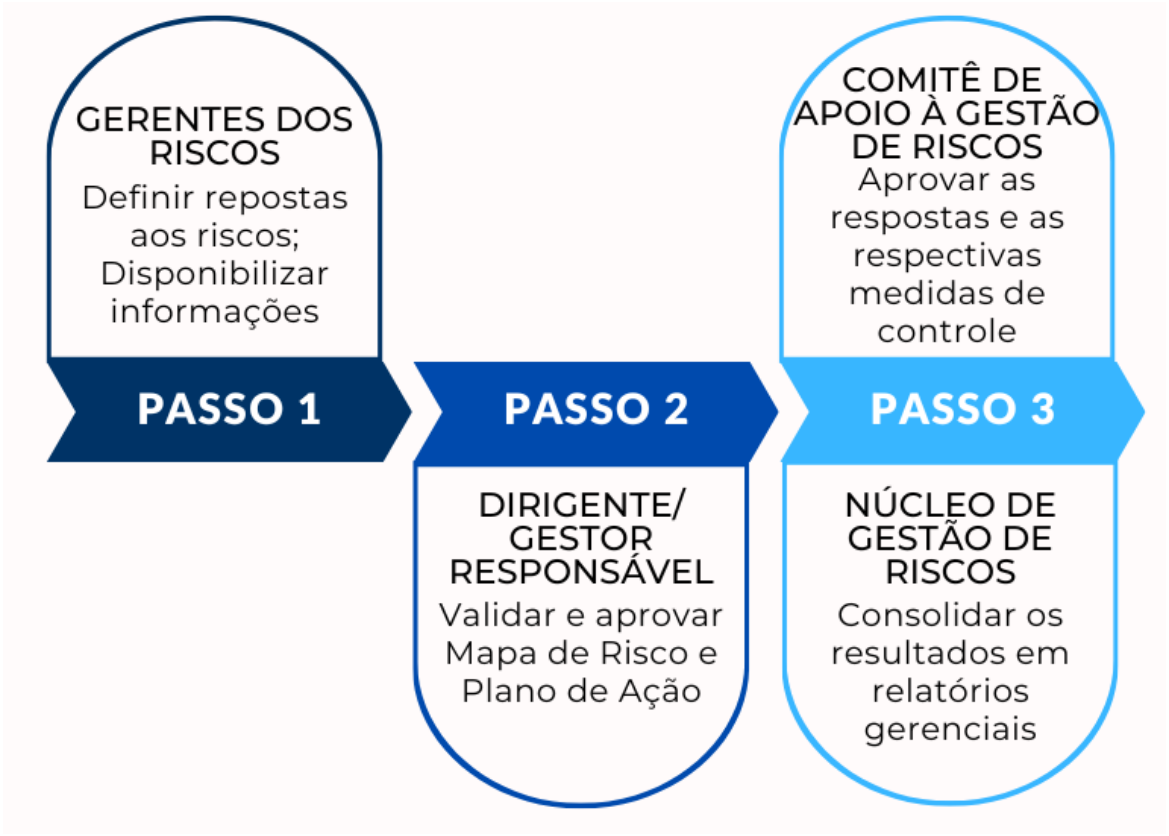
Fonte: Elaboração própria

Cabe ao gerente dos riscos e à equipe técnica por ele designada realizar a definição de respostas aos riscos, enquanto ao dirigente ou gestor das instâncias com riscos mapeados cabe a validação e aprovação dos resultados das etapas anteriores da gestão de riscos (Entendimento do contexto; Identificação de Riscos; Identificação e Avaliação dos Controles; Cálculo dos Níveis de Risco) assim como do Plano de Ação.

Em seguida, tais informações deverão ser encaminhadas ao Comitê de Apoio à Gestão de Riscos e ao Núcleo de Gestão de Riscos. Isto porque ao primeiro compete aprovar as respostas e as respectivas medidas de controle a serem implementadas nos processos inerentes aos objetivos institucionais; e ao segundo compete consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los ao Comitê de Apoio à Gestão de Riscos e ao Comitê Interno de Governança. Além disso, ambas as instâncias são responsáveis por monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas.

Em caso de envolvimento de outras unidades (Unidades Corresponsáveis) para a implementação do plano de ação, essa negociação deve ser feita antes da aprovação do Plano de Ação. Cabe ao responsável pelo processo a validação das ações com as demais áreas. Um resumo desse fluxo de validação de resultados e transmissão de informações foi indicado na Figura 11.

Figura 11: Fluxo de transmissão de informações e validação de Mapa de Riscos e Plano de Ação da UFRJ



Fonte: Elaboração própria

Os gerentes dos riscos também deverão responder às requisições do Núcleo de Gestão de Riscos, assim como disponibilizar informações adequadas e tempestivas quanto à gestão dos riscos dos processos sob sua responsabilidade às instâncias decisórias e/ou aos colegiados da UFRJ para as análises e decisões cabíveis.

4. COMUNICAÇÃO E MONITORAMENTO

A comunicação do risco deverá permear todo o processo de gestão de riscos, sendo uma ação multidirecional. As informações que alimentarão esta etapa podem ser as mais variadas, referindo-se à natureza, tratamento, custo, probabilidade e impacto do risco, e podem ser obtidas por meio de fontes externas e internas, de modo qualitativo ou quantitativo. Os dados obtidos devem ser confiáveis, íntegros e tempestivos, já que oferecem suporte à tomada de decisões e alcance dos objetivos estratégicos da instituição. A comunicação em direção à comunidade acadêmica e à sociedade também deverá ser objeto de monitoramento, a fim de reduzir riscos de respostas inadequadas aos interesses desses agentes.

O período de monitoramento dos riscos deverá ser definido por cada unidade, que ficará responsável por reavaliá-lo e aprová-lo periodicamente. Quaisquer modificações repentinas nos níveis de risco considerados estratégicos aos objetivos ou processos da UFRJ ou, ainda, a verificação de valores elevados deverão ser comunicadas imediatamente ao gestor responsável e ao Núcleo de Gestão de Riscos por vias formais.

Nos níveis operacionais e táticos, tanto os servidores técnico-administrativos quanto os proprietários dos riscos deverão assegurar que:

- controles internos se mostrem eficientes;
- tratamentos aos riscos identificados sejam realizados;
- ocorrências de novos riscos sejam analisadas.

Segundo a PGR/UFRJ, compete a todos os servidores da UFRJ que sejam proprietários de riscos o monitoramento da evolução dos níveis de riscos e a efetividade das medidas de controle implementadas nos processos institucionais em que estiverem envolvidos ou de que tiverem conhecimento. Durante o monitoramento, caso sejam identificadas mudanças ou fragilidades nos processos institucionais, o servidor deverá reportar imediatamente o fato ao responsável pelo gerenciamento de riscos do processo em questão.

Já em nível estratégico, o Núcleo de Gestão de Riscos será responsável por:

- monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;
- medir o desempenho da Gestão de Riscos de acordo com os indicadores elaborados;
- requisitar aos responsáveis pelo gerenciamento de riscos dos processos institucionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais;
- orientar e apoiar as unidades acadêmicas e administrativas na execução de seus planos internos de gestão de riscos e demais instruções relativas à gestão de riscos.

Orienta-se que o Mapa de Risco seja a principal ferramenta, porém não a única, para o monitoramento da gestão de riscos de cada unidade. Associados ao Mapa, os relatórios gerenciais serão úteis para o acompanhamento da evolução de cada unidade e deverão sempre se embasar em informações que obedeçam aos seguintes requisitos, conforme orientações do Ministério da Economia (2021):

- relevância: a informação deve ser útil para o objetivo do trabalho;
- integralidade: as informações importantes e suficientes para a compreensão devem estar presentes;
- adequação: o volume de informação deve ser adequado e suficiente;
- concisão: a informação deve ser apresentada de forma compacta;
- consistência: as informações apresentadas devem ser compatíveis;
- clareza: a informação deve ser facilmente compreensível;
- padronização: a informação deve ser apresentada no padrão aceitável.

Ao final do presente documento (Apêndice E), encontra-se disponível um Plano de Comunicação em Riscos que contempla diretrizes, estratégias e ações de comunicação sobre a Gestão de Riscos no âmbito da UFRJ.

5. CONSIDERAÇÕES FINAIS

Este Plano de Gestão de Riscos, embora também esteja voltado para os processos de cada unidade da Universidade, possui especial ênfase nos objetivos estratégicos da UFRJ, dispostos no Plano de Desenvolvimento Institucional (PDI).

A periodicidade de sua revisão será definida de acordo com a análise conjunta do Núcleo de Gestão de Riscos e do CIGov.

Estamos cientes de que o presente documento inaugura um passo importante na disseminação e implementação da PGR/UFRJ, assim como permite evitar descontinuidades nos serviços fornecidos ao público – baseados no tripé pesquisa, ensino e extensão. Além disso, outro ganho a longo prazo que esperamos é o fomento a uma cultura interna voltada à Gestão de Riscos, com capacitação de todos os servidores no tema e uma evolução da maturidade organizacional para que sua missão institucional seja cada vez mais executada com maior qualidade.

6. REFERÊNCIAS

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Gestão de riscos – Técnicas para o processo de avaliação de riscos. Norma Brasileira ABNT NBR ISO/IEC 31010. 1. ed., São Paulo, 2012.

ABNT, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Gestão de riscos – Diretrizes. Norma Brasileira ABNT NBR ISO 31000. 2. ed., São Paulo, 2018.

BRASIL. CONTROLADORIA-GERAL DA UNIÃO. Guia Prático de Gestão de Riscos para a Integridade: Orientações para a administração pública federal direta, autárquica e fundacional. 2018. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manual-gestao-de-riscos.pdf.

BRASIL. CONTROLADORIA-GERAL DA UNIÃO. Metodologia de Gestão de Riscos da CGU. 2021. Disponível em: https://repositorio.cgu.gov.br/handle/1/65535. Acesso em: 3 nov.2022.

BRASIL. CONTROLADORIA-GERAL DA UNIÃO. GABINETE DO MINISTRO (GM). NÚCLEO DE GESTÃO DE RISCOS E INTEGRIDADE (NGRI). Metodologia de Gestão de Riscos da CGU [versão 2.0]. Disponível em: https://repositorio.cgu.gov.br/handle/1/65535. Acesso em: 14 abr. 2023.

BRASIL. MINISTÉRIO DA ECONOMIA. Guia de Gestão de Riscos do Ministério da Economia [versão 2.0]. 2021. Disponível em: https://www.gov.br/economia/pt-br/acesso-a-informacao/acoes-e-programas/integra/governanca/comites-tematicos-de-apoio-a-governanca/arquivos/documentos-crtci/arquivos-de-reuniao/guia-gestao-de-riscos-v-final-31-05.pdf/view. Acesso em: 19 abr. 2023.

BRASIL. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO. Gabinete do Ministro. Portaria n. 1.089, de 25 de abril de 2018. 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. Disponível em: https://repositorio.cgu.gov.br/handle/1/33467. Acesso em: 25 nov. 2022.

BRASIL. MINISTÉRIO DA TRANSPARÊNCIA E CONTROLADORIA-GERAL DA UNIÃO. Metodologia de Gestão de Riscos da CGU: GR-Riscos. Disponível em: https://repositorio.cgu.gov.br/handle/1/41816. Acesso em: 17 abr. 2023.

BRASIL. MINISTÉRIO DO PLANEJAMENTO. Controladoria-Geral da União. Instrução Normativa Conjunta n° 1, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/governanca/Gestao-de-Riscos/biblioteca/.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. Controladoria-Geral da União. Decreto n. 9.203, de 22 de novembro de 2017. Dispões sobre a política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: https://repositorio.cgu.gov.br/handle/1/41841. Acesso em: 25 nov. 2022.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. Gestão de Riscos: Avaliação da Maturidade. 2018. Disponível em: https://portal.tcu.gov.br/gestao-de-riscos-avaliacao-da-maturidade.htm. Acesso em: 3 nov. 2022.

BRASIL. UNIVERSIDADE FEDERAL DE SANTA CATARINA. Manual para Elaboração do Plano de Gestão de Riscos. 2020. Disponível em: https://gestaoderiscos.ufsc.br/manual/. Acesso em: 3 nov. 2022.

COSO. COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. Gerenciamento de Riscos Corporativos – Estrutura Integrada. 2007. Disponível em: https://auditoria.mpu.mp.br/pgmq/COSOIIERMExecutiveSummaryPortuguese.pdf.

COSO. COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. 2012. Risk assessment in practice. Disponível em: https://www.coso.org/Documents/COSO-ERM%20Risk%20Assessment%20in%20Practice%20Thought%20Paper%20October%202012.pdf.

GOVERNO DO DISTRITO FEDERAL. Projeto Gestão de Riscos – Proposta de plano de comunicação. 2022. Disponível em: http://www.gestaoderiscos.cg.df.gov.br/wp-content/uploads/2022/01/Modelo-de-artefato-Plano-de-Comunica%C3%A7%C3%A3o-para-Gest%C3%A3o-de-Riscos.pdf.

IIA. THE INSTITUTE OF INTERNAL AUDITORS. Modelo das Três Linhas do IIA 2020 – Uma atualização das Três Linhas de Defesa. 2020 Disponível em: https://iiabrasil.org.br/korbilload/upl/editorHTML/uploadDireto/20200758glob-th-editorHTML-00000013-20082020141130.pdf.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Campanha de Divulgação Programa de Integridade – Plano de Comunicação. 2022. Disponível em: https://www.tjdft.jus.br/institucional/governanca/integridade-e-etica/comunicacao/plano-de-comunicacao_v1.pdf.

UNIVERSIDADE FEDERAL DO CARIRI. Plano Anual de Comunicação da Auditoria Interna. 2022. Disponível em: https://documentos.ufca.edu.br/wp-folder/wp-content/uploads/2022/05/AUDIN.UFCA-Plano-de-Comunica%C3%A7%C3%A3o-UAIG.UFCA-2022-17.05.22.pdf.

APÊNDICE A – GLOSSÁRIO

Aceitar o risco: uma das quatro ações para tratamento de eventos de riscos. Neste caso, a exposição ao risco pode ser tolerada pela instituição e não há necessidade de implementar quaisquer ações adicionais para mitigá-lo (aceitação passiva). A aceitação do risco também pode ser do tipo ativa, na qual um plano de contingência pode ser elaborado caso o risco ocorra, a fim de reduzir seu impacto.

Apetite a risco: nível de risco que uma instituição está disposta a aceitar, dentro de padrões considerados institucionalmente aceitáveis.

Compartilhar/transferir o risco: uma das quatro ações para tratamento de eventos de riscos. Neste caso, os riscos estão em níveis altos e extremos, acima do apetite a risco da UFRJ. Instâncias superiores serão envolvidas para compartilhar o risco ou seguradoras poderão ser contratadas para transferir o risco. A chefia da unidade e o Núcleo de Gestão de Riscos deverão ser comunicados.

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 e destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos institucionais serão alcançados.

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

Evitar o risco: uma das quatro ações para tratamento de eventos de riscos. Neste caso, qualquer probabilidade de ocorrência do evento deve ser eliminada a fim de que o evento de risco não ocorra. Isto pode significar a alteração ou descontinuidade do processo/atividade.

Gerentes de Risco: responsáveis por executar as atividades do gerenciamento de riscos e coordenar esforços para identificá-los e estimá-los, bem como propor melhorias necessárias para mitigar riscos, além de comunicar os resultados de análises a todos os interessados.

Gerenciamento de riscos: processo contínuo que consiste em identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos institucionais.

Gestão de riscos: processo de natureza permanente, direcionado e monitorado pela Alta Administração, pautado em arquitetura necessária para se gerenciarem riscos eficazmente – princípios, objetivos, estrutura, competências e processo.

Gestor: pessoa que ocupa função de gestão em qualquer nível hierárquico da organização.

Gestão: estruturas responsáveis pelo planejamento, execução, controle, ação, enfim, pelo manejo dos recursos e poderes colocados à disposição de órgãos e entidades para a consecução de seus objetivos, com vistas ao atendimento das necessidades e expectativas dos cidadãos e demais partes interessadas.

Impacto: resultado ou efeito de um evento, podendo ser positivo ou negativo em relação aos objetivos de uma instituição.

Incerteza: diz respeito à incapacidade de conhecer antecipadamente a probabilidade exata ou o impacto de eventos futuros.

Meta: alvo ou propósito com que se define um objetivo a ser alcançado.

Medidas de controle: medidas aplicadas pela instituição para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas institucionais estabelecidos sejam alcançados.

Mitigar o risco: uma das quatro ações para tratamento de eventos de riscos. Neste caso, ações para tratar as causas e consequências dos riscos são implementadas, ou seja, sua probabilidade de ocorrência e/ou impacto é reduzida.

Nível de risco: o nível de criticidade do risco, o quanto um risco pode afetar os objetivos, processos de trabalho e projetos da organização, a partir da escala predefinida de criticidades possíveis.

Objetivos institucionais: situação que se deseja alcançar de forma a evidenciar-se êxito no cumprimento da missão e no atingimento da visão de futuro da instituição.

Política de Gestão de Riscos: declaração das intenções e diretrizes gerais de uma instituição relacionadas à Gestão de Riscos.

Probabilidade: a chance de o risco acontecer, estabelecida a partir de uma escala predefinida de probabilidades possíveis.

Processos Institucionais: conjunto de ações e atividades inter-relacionadas, executadas para alcançar produto, resultado ou serviço predefinido.

Proprietário do risco: pessoa responsável pelo monitoramento de um risco e pela execução de ações de resposta (mitigação ou contingência) ao risco, quando necessário. (Conceito adaptado da ABNT NBR ISO 31.000/2009).

Responsáveis por Unidades (ou responsáveis técnicos): responsáveis, nas Unidades Organizacionais, pela coleta de informações necessárias à identificação e à estimação de riscos e realização de melhorias quando as análises indicarem esta necessidade.

Resposta ao risco: medidas de tratamento e/ou controle para os riscos identificados e priorizados.

Risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da instituição.

Riscos à Imagem e de Reputação: eventos que podem comprometer a confiança da sociedade em relação à capacidade da instituição de cumprir sua missão institucional.

Riscos de Integridade: eventos relacionados à corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela UFRJ e a realização de seus objetivos.

Riscos Estratégicos: eventos que afetam a estratégia ou os objetivos estratégicos da Universidade, estabelecidos no PDI.

Riscos Financeiros/Orçamentários: eventos que possam comprometer a capacidade da UFRJ de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

Risco Inerente: riscos identificados sem considerar qualquer ação de mitigação, ou ainda sem que nenhum tipo de controle tenha sido aplicado.

Riscos Legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da UFRJ.

Riscos Operacionais: eventos que podem comprometer as atividades da UFRJ, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.

Risco Residual: riscos aos quais uma organização está exposta após a implementação de ações gerenciais para o tratamento e mitigação do risco.

Unidade Organizacional: para fins deste documento, definem-se como unidades organizacionais as pró-reitorias e todas as demais unidades acadêmicas e administrativas que compõem a estrutura da UFRJ.

APÊNDICE B – EXEMPLO DE UM MAPA DE RISCO PREENCHIDO

Identificação				Análise		Avaliação Risco Inerente				Avaliação controles			Avaliação Risco Residual			
Objetivo	Evento de Risco	Causa	Consequência	Classificação	Gestor	Probabilidade	Impacto	Nível do Risco Inerente	Avaliação do Risco Inerente	Descrição do controle	Nível do Controle	Avaliação	Nível do Risco Residual	Avaliação do Risco Residual	Resposta ao Risco	Plano de Ação
Ampliar a segurança nos processos e controle da tecnologia da informação	Licitação deserta para compra de equipamentos de informática segundo as especificações técnicas exigidas	CA1: divulgação insuficiente do edital CA2: especificações técnicas excedentes dos equipamentos em relação às possibilidades ofertadas	CO1: indisponibilidade para compras de equipamentos de informática aos servidores da UFRJ CO2: morosidade na compra de equipamentos de informática aos servidores da UFRJ	Operacional e Estratégico	Coordenação Geral de Licitação (SGG/PR6)	1	3	3	Risco Baixo	CI1: listagem de fornecedores frequentes para órgãos do governo federal CI2: pesquisa específica para construção do edital de licitação	Satisfatório	0,4	1,2	Risco Baixo	Aceitar	Não

Diminuir as taxas de evasão e de retenção nos cursos de graduação	Falhas nos processos de compras	CA1: planejamento insuficiente pelos setores demandantes dos materiais CA2: falta de estrutura de pessoal adequada no Departamento de Compras para fazer frente a todos os procedimentos e orientações relacionadas	CO1: falta dos materiais necessários ao desenvolvimentos das atividades CO2: utilização de procedimentos inadequados para as compras CO3: utilização inadequada dos recursos públicos	Legal e Estratégico	Coordenação Geral de Licitação (SGG/PR6)	2	4	8	Risco Médio	CI1: solicitações de compras excepcionais (por dispensa de licitação, adesão, licitação fora dos prazos estabelecidos no Calendário de Compras da UFRJ) CI2: dividir igualitariamente as demandas recebidas entre os servidores lotados	Fraco	0,8	6,4	Risco Médio	Aceitar	Não

Ampliar o acesso às políticas de assistência estudantil a fim de contribuir para a permanência e o desempenho acadêmico (programas, serviços e auxílios financeiros)	Contingenciamento do Orçamento Federal do MEC às Universidades	CA1: crise econômico-financeira no país CA2: decisão discricionária do MEC	CO1: precisar escolher entre as prioridades para pagamento CO2: redução nos contratos CO3: redução nas assistências estudantis CO4: atraso no pagamento de fornecedores CO5: limitação e/ou descontinuidade de atividades	Financeiro/Orçamentário e Estratégico	Superintendência-Geral de Finanças/PR-3	3	5	15	Risco Alto	CI1: fonte de recursos extraordinários	Fraco	0,8	12	Risco Alto	Transferir/Compartilhar	Sim

Promover o aperfeiçoamento e a avaliação da maturidade da governança institucional, por meio de monitoramento de ações pautadas nos pilares da governança pública	Contratações diretas de forma antieconômica	CA1: pressão interna ou externa ilegal ou antiética para influenciar agente público	CO1: alocação inadequada de recursos financeiros em aquisições que poderiam ser licitadas	Integridade e Estratégica	Coordenação Geral de Licitação (SGG/PR-6)	4	5	20	Risco Elevado	CI1: capacitar e treinar servidores para formação de equipe adequada ao bom desempenho das atividades de compras e contratações. CI2: evitar que servidores em período probatório sejam responsáveis por contratações diretas	Mediano	0,6	12	Risco Alto	Aceitar	Não

	Aumento no número de denúncias de servidores relacionadas a comportamentos contrários à integridade	CA1: falta de capacitação sobre integridade no serviço público CA2: falta de aplicação de medidas corretivas e/ou punitivas quando constatada má conduta de servidores públicos	CO1: sensação de impunidade nos servidores CO2: comprometimento da cultura de integridade na instituição	Imagem /Reputação e Estratégia	Ouvidoria e SGGov/PR-6	3	5	15	Risco Alto	CI1: capacitação dos servidores da UFRJ em integridade	Fraco	0,8	12	Risco Alto	Mitigar	Sim

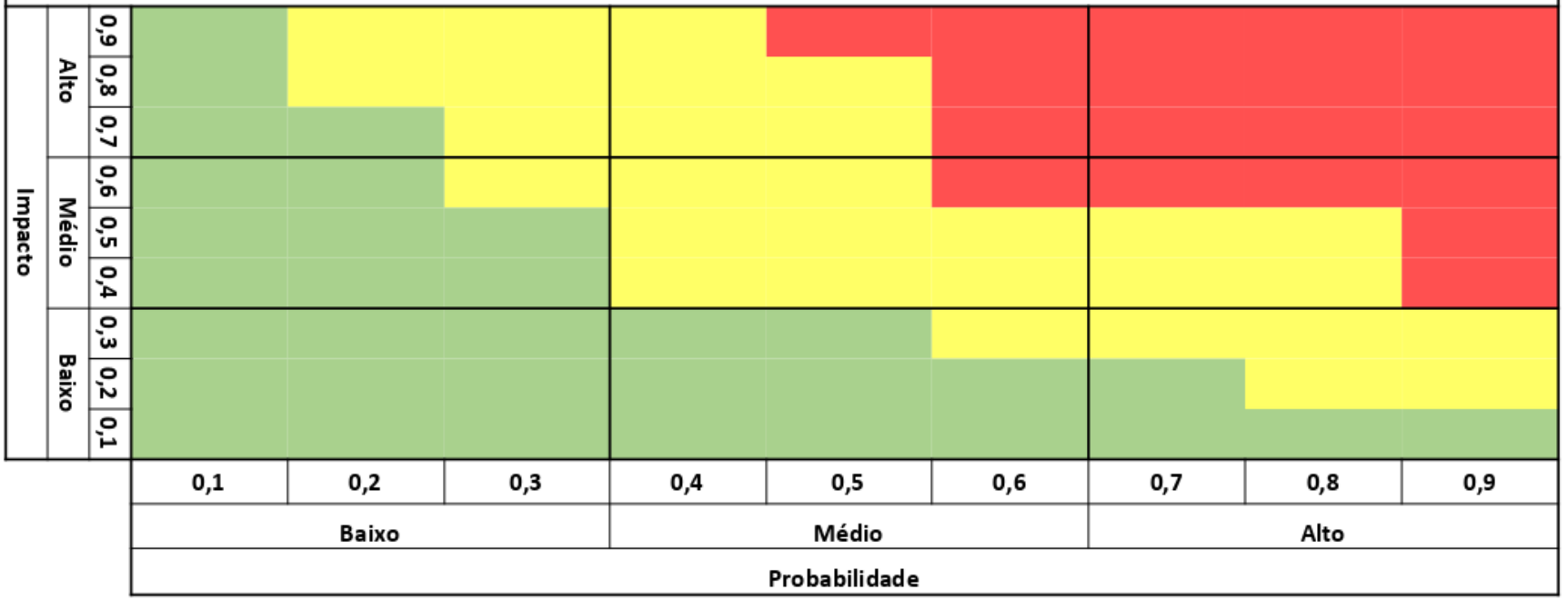
APÊNDICE C – EXEMPLO DE GESTÃO DE RISCOS PARA UM PROJETO DE OBRA

MATRIZ PROBABILIDADE X IMPACTO			
Código Projeto:	1	Nome Projeto:	Projeto Obras

Probabilidade	Impacto								
	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
0,9	0,09	0,18	0,27	0,36	0,45	0,54	0,63	0,72	0,81
0,8	0,08	0,16	0,24	0,32	0,4	0,48	0,56	0,64	0,72
0,7	0,07	0,14	0,21	0,28	0,35	0,42	0,49	0,56	0,63
0,6	0,06	0,12	0,18	0,24	0,3	0,36	0,42	0,48	0,54
0,5	0,05	0,10	0,15	0,2	0,25	0,3	0,35	0,4	0,45
0,4	0,04	0,08	0,12	0,16	0,2	0,24	0,28	0,32	0,36
0,3	0,03	0,06	0,09	0,12	0,15	0,18	0,21	0,24	0,27
0,2	0,02	0,04	0,06	0,08	0,10	0,12	0,14	0,16	0,18
0,1	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09

Limites de Tolerânica		
Baixo	<=	0,15
Médio	<=	0,35
Alto	<=	0,81

MATRIZ PROBABILIDADE X IMPACTO			
Código Projeto:	1	Nome Projeto:	Projeto Obras



MATRIZ CAUSA - CICLO			
Código Projeto:	1	Nome Projeto:	Projeto Obras

Ciclo de Vida	Externos														INTERNOS																	
	Políticos			Natureza			Outros								Técnicos						Organizacionais						Legais				Comercial				
	Alterações legislação	Opinião pública	Economia	Terremoto	Incêndio	Chuvas e alagamentos	Fornecedores	Regulamentação	Mercado	Cliente	Mão de obra externa	Novos entrantes	Força maior	Grupos de pressão	Mudança Tecnologica	Mudança ambiente	Complexidade	Mudança	Performance	Teste e aceitação	Financiamento	Estouro de custo	Corte orçamento	Mudança de pessoal	Mudança organizacional	Priorização projetos	Contratos	Ações de terceiros	Recall	Defeito do produto	Estabilidade parceiros	Condições pagamento	Garantias	Suspensão / Recisão	Estabilidade cliente
Iniciação	0	1	1	0	0	1	0	1	0	0	1	0	1	0	0	0	1	1	0	1	0	1	0	1	1	1	0	0	0	0	0	0	1	0	1
Planejamento	1	1	1	0	1	1	1	0	0	1	0	1	1	0	0	1	1	1	1	1	0	0	1	1	1	1	0	1	1	0	1	0	1	1	1
Execução	1	0	0	0	1	1	0	1	0	1	1	1	0	1	0	1	1	1	1	1	0	0	1	1	1	0	1	0	0	0	0	0	0	1	1
Monit. E Controle	0	1	1	0	1	1	1	0	1	1	1	1	1	0	1	0	0	0	1	0	1	1	1	0	0	0	0	0	0	1	1	0	1	0	1
Encerramento	1	0	1	0	1	1	1	0	0	0	1	0	1	0	1	1	1	0	1	0	1	1	1	1	1	1	0	1	0	1	1	0	0	1	0

Preenchimento	
0	Para ausência de risco
1	Para presença de risco

QUESTÕES PARA LEVANTAMENTO DOS RISCOS			
Código Projeto:	**1**	**Nome Projeto:**	**Projeto Obras**

Se respondermos "NÃO", devemos gerar um risco e suas respectivas análises		
Nº	**Questão**	**Risco ?**
1	Que tipo de estrutura organizacional estamos? Se for funcional ou matricial fraca certamente temos um alto risco do projeto se perder na sua gestão.	
2	A autoridade do gerente do projeto está definida e clara para toda a organização?	
3	Temos um patrocinador do projeto com influência na organização?	
4	Temos a equipe do projeto claramente definida?	
5	Foi feito o plano de comunicação para esta equipe e todos os membros compreendem a finalidade do projeto?	
6	Todos os stakeholders foram identificados? Sabemos seus graus de influência e importância para o projeto?	
7	Temos uma matriz de responsabilidade claramente definida para todos os participantes do projeto?	
8	Na definição do escopo do produto ou serviço a ser entregue, está claro para nós e para o cliente o que deverá ser entregue?	
9	Os critérios de aceitação do produto ou serviço são mensuráveis?	
10	Os objetivos dos projetos foram claramente definidos?	
11	Temos uma justificativa para o projeto?	
12	Temos claramente definido o propósito do projeto e seus benefícios?	
13	O projeto está formalmente aprovado pela organização e faz parte do scorecard de priorização de projetos para o ano?	
14	Temos o orçamento do projeto aprovado?	
15	O prazo para cumprirmos a execução do projeto é factível?	
16	O prazo para cumprirmos a execução do projeto é muito apertado?	
17	Temos fatores culturais que podem influenciar o andamento do projeto?	
18	Temos leis que podem influencia o andamento do projeto?	
19	Estamos obedecendo todas as regras e procedimentos da nossa empresa no nosso projeto?	
20	Estamos obedecendo todas as regras e procedimentos da empresa que nos contratou o projeto?	

QUESTÕES PARA LEVANTAMENTO DOS RISCOS			
Código Projeto:	**1**	**Nome Projeto:**	**Projeto Obras**

Se respondermos "NÃO", devemos gerar um risco e suas respectivas análises		
Nº	**Questão**	**Risco ?**
21	Se estamos fazendo aquisições temos um único fornecedor para determinado produto ou serviço?	
22	Estamos fazendo transporte de equipamentos e/ou materiais para o projeto?	
23	Estamos fazendo importação de bens ou serviços?	
24	Temos alguma data crítica para conclusão do projeto, principalmente por motivação comercial?	
25	Temos multas ou penalidades previstas no contrato caso não consigamos cumprir prazos ou o produto gerado não estiver conforme?	
26	Todas as métricas de qualidade do produto ou serviço estão definidas através de critérios claros e mensuráveis?	
27	Temos a declaração de escopo do projeto elaborada e aprovada por todos?	
28	Temos um cronograma e orçamento elaborados e aprovados por todos?	
29	Temos um plano de qualidade elaborado e aprovado por todos?	
30	Temos um plano de risco elaborado e aprovado por todos?	
31	Os limites de alcance do projeto estão claramente definidos? Temos os itens que não fazem parte do escopo claramente explicitados na nossa documentação?	
32	A responsabilidade do cliente no projeto está claramente definida?	
33	Temos uma EAP e seu dicionário de dados elaborada e aprovada?	
34	Na EAP elaborada temos sub-produtos com seus respectivos critérios de aceitação descritos de forma que possam ser mensurados de uma forma explícita?	
35	Temos calculado o impacto caso o projeto fracasse?	
36	Temos todo o conhecimento técnico requerido disponível na equipe?	
37	Temos alguma limitação técnica no projeto?	
38	Estamos usando alguma tecnologia nova ou pouco difundida?	
39	Estamos usando equipamentos de difícil manuseio?	
40	Temos todas as informações necessárias para o projeto disponíveis?	

QUESTÕES PARA LEVANTAMENTO DOS RISCOS			
Código Projeto:	**1**	**Nome Projeto:**	**Projeto Obras**

Se respondermos "NÃO", devemos gerar um risco e suas respectivas análises		
Nº	**Questão**	**Risco ?**
41	O escopo está claro ou ainda temos dúvidas sobre o mesmo?	
42	Todas as etapas elementares foram claramente identificadas?	
43	As dependências das etapas elementares foram estabelecidas e definidas?	
44	A duração das etapas está claramente definida e aprovadas por todos incluindo o cliente?	
45	Os responsáveis por trabalhar nas etapas estão identificados e devidamente alocados?	
46	Temos algum recurso crítico para o projeto?	
47	Temos o SOW devidamente elaborado com os tipos de contratos definidos para as aquisições que iremos fazer?	
48	Todos os recursos estão disponíveis de fato? Estamos tratando a alocação de recursos de forma realista?	
49	Temos o compartilhamento de recursos com outros projetos?	
50	As prioridades de carga de trabalho estão claramente definidas?	
51	Os gerentes funcionais concordaram em ceder os recursos para o nosso projeto?	
52	Os gerentes funcionais estão devidamente informados e envolvidos com o nosso projeto?	
53	Todos os recursos alocados aceitaram trabalhar no nosso projeto e estão comprometidos com o mesmo?	
54	O plano do projeto está suficientemente detalhado de forma que consigamos entender claramente o que devemos produzir em cada pacote de trabalho?	
55	Os principais interessados assinados os documentos do projeto, incluindo o plano de projeto gerado?	
56	Os procedimentos que devemos seguir no projeto foram estabelecidos e compreendidos?	
57	Temos uma ferramenta eficaz de comunicação definida e divulgada para todos?	
58	Todos conhecem e sabem lidar com as ferramentas de comunicação definidas para o projeto?	
59	A informação de tarefas, execução, problemas e soluções estão disponíveis para os membros da equipe?	
60	Temos um cronograma de marcos para fazermos os relatórios gerenciais?	
61	Temos um software para elaborar cronograma e orçamento?	
62	Temos templates para gerar a documentação do projeto?	
63	As medidas de desempenhos, os critérios adotados para medir o desempenho estão devidamente definidos e aprovados por todos?	
64	Temos uma ferramenta (framework) para gestão de todo o projeto?	
65	Temos um repositório de dados para armazenarmos as informações do projeto?	
66	Temos templates para gerarmos as atas de reuniões?	
67	Temos definido como faremos para tomarmos ações corretivas no projeto em caso de problemas com custos, escopo, qualidade ou tempo?	
68	Se os recursos do terceiro não trabalharem adequadamente temos definido a regra de reposição deste recurso?	
69	Está definido como cobriremos férias e afastamento médico caso tenhamos recursos tercerizados no nosso projeto?	

Análise de Risco

Nº	Tipo Risco	Descrição do Risco	Impacto Qualitativo					Probabilidade	Exposição	Prioridade	Impacto Quantitativo	
			Custo	Tempo	Escopo	Qualidade	Geral				R$	V.E.
1	Negativo	Ocorrência de chuvas	0,5	0,7	0,3	0,1	0,7	0,3	0,21		R$ 5.000,00	R$ 1.050,00
2	Negativo	Falta de materia prima	0,3	0,5	0,1	0,7	0,7	0,7	0,49		R$ 9.000,00	R$ 4.410,00
3	Negativo	Paralização da obra	0,6	0,3	0,1	0,4	0,6	0,4	0,24		R$ 3.250,00	R$ 780,00
4	Negativo	Incêndio	0,9	0,7	0,5	0,8	0,9	0,1	0,09		R$ 100.000,00	R$ 9.000,00
5	Positivo	Término da obra antes do prazo	0,4	0,8	0,2	0,5	0,8	0,6	0,48		R$ 70.000,00	R$ 33.600,00
6									0		R$ -	R$ -
7									0		R$ -	R$ -
8									0		R$ -	R$ -
9									0		R$ -	R$ -
10									0		R$ -	R$ -
11									0		R$ -	R$ -
12									0		R$ -	R$ -
13									0		R$ -	R$ -
14									0		R$ -	R$ -
15									0		R$ -	R$ -

Número total de riscos identificados	5
Valor máximo assumido pelo risco	0,81

Soma Exposição	1,51
Risco Geral do Projeto	37,28%

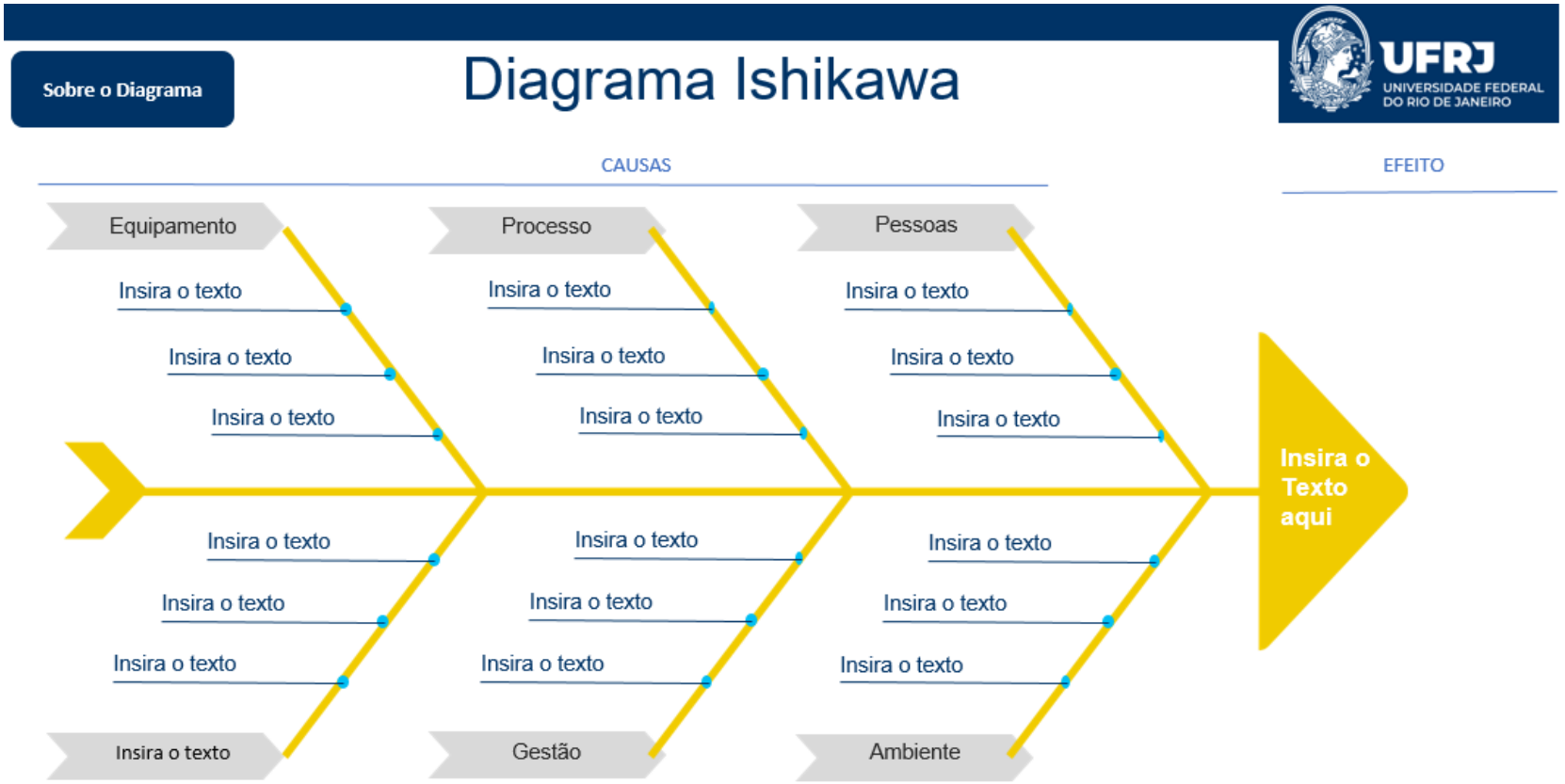
Riscos +	R$ 15.240,00
Riscos -	R$ 33.600,00

Resposta ao Risco

ESTRATÉGIA DE RESPOSTA AOS RISCOS			
Código Projeto:	1	Nome Projeto:	Projeto Obras

Nº	Tipo Risco		Descrição do Risco	Estratégia de Resposta	Ação Recomendada	Responsável pela Ação	Data Conclusão	
							Prevista	Real
1		Negativo	Ocorrência de chuvas	Aceitação passiva				
2		Negativo	Falta de matéria prima	Eliminação				
3		Negativo	Paralização da obra	Mitigação				
4		Negativo	Incêndio	Transferência				
5		Positivo	Término da obra antes do prazo	Aceitação ativa				
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								

APÊNDICE D – FERRAMENTAS DE SUPORTE À GESTÃO DE RISCOS



UFRJ
UNIVERSIDADE FEDERAL
DO RIO DE JANEIRO

Análise SWOT

Ambiente Interno		
	Forças	**Fraquezas**
	Quais são os melhores desempenhos e benefícios do processo?	Quais são as ineficiências e os problemas do processo?

Ambiente externo		
	Oportunidades	**Ameaças**
	Como melhorar o processo?	Quais obstáculos os processos possuem?
		Quais obstáculos e incertezas eu preciso controlar?

APÊNDICE E – PLANO DE COMUNICAÇÃO EM RISCOS

APRESENTAÇÃO

O presente documento destina-se a propor diretrizes, estratégias e ações de comunicação sobre a Gestão de Riscos no âmbito da UFRJ a serem desempenhadas pelo Núcleo de Gestão de Riscos e todos os servidores e demais colaboradores da UFRJ, além de cada estrutura interveniente na Gestão de Riscos da Universidade e as indicadas no Modelo de Três Linhas do IIA 2020. A revisão do instrumento poderá ocorrer, a critério do Núcleo de Gestão de Riscos, anualmente.

Além disso, o documento busca esclarecer e divulgar amplamente as atribuições e competências de cada estrutura interveniente na Gestão de Riscos da Universidade, bem como descrever o passo a passo do fluxo de informações e comunicação entre a equipe, os gerentes de riscos, os gestores responsáveis, o Núcleo de Gestão de Riscos, o Comitê de Apoio à Gestão de Riscos e o Comitê Interno de Governança.

INTRODUÇÃO

O que é Gestão de Riscos?

A gestão de riscos é um processo que consiste na identificação, análise e propostas de soluções para possíveis riscos e fornece suporte à gestão institucional, já que pode contribuir para o aperfeiçoamento dos controles internos e monitoramento contínuo dos riscos relacionados às atividades gerencial, estratégica e operacional.

Sabe-se que riscos e incertezas fazem parte do cotidiano de todas as instituições, públicas ou privadas. No caso das universidades públicas, porém, mudanças culturais, políticas, legais, regulatórias, financeiras, econômicas e ambientais, inerentes à variabilidade e alternância de políticas governamentais, criam um ambiente de instabilidade e volatilidade, tornando imperiosa a redução a níveis aceitáveis e o monitoramento de incertezas que possam interferir nas decisões pelas quais se busca assegurar maior eficácia, eficiência e efetividade no alcance dos objetivos estratégicos da instituição.

O que é a Comunicação de Riscos e o Plano de Comunicação em Riscos?

Sob a perspectiva da gestão de riscos corporativos, a Estrutura Integrada para Gerenciamento de Riscos Corporativos proposta pelo COSO (The Comitee of Sponsoring Organizations) e o Modelo de Três Linhas do IIA (The Institute of Internal Auditors) de 2020 recomendam que as informações relevantes sejam identificadas, colhidas e comunicadas de forma e no prazo que permitam o cumprimento de suas responsabilidades. A comunicação eficaz também deve ocorrer em um sentido mais amplo, fluindo em todos os níveis da organização.

Nessa Estrutura Integrada, a comunicação é uma das categorias de objetivos que a organização se empenha em alcançar e também um dos componentes do gerenciamento de riscos corporativos, que representam aquilo que é necessário para o seu alcance.

A Estrutura Integrada (também conhecida por COSO II) orienta que os colaboradores (no caso da UFRJ, servidores e terceirizados) recebam uma mensagem clara da alta administração (Reitoria e pró-reitorias), alertando que as responsabilidades do gerenciamento de riscos sejam levadas a sério. O ideal é que cada pessoa compreenda a sua própria função no gerenciamento de riscos dentro da organização, assim como as atividades individuais que se relacionam com o trabalho dos demais. A organização deve estruturar o seu processo de comunicação de maneira que as pessoas tenham uma forma de comunicar informações significativas dos escalões inferiores aos superiores. Adicionalmente, não se pode prescindir de uma comunicação eficaz com partes relevantes dos processos organizacionais. No caso da UFRJ, destacam-se: fornecedores, usuários de serviços, estruturas governamentais (superiores, parceiras, provedoras de recursos), órgãos de controle (como CGU e TCU) etc.

QUEM É O PÚBLICO-ALVO?

Público interno:

- servidores TAE;
- servidores docentes;
- colaboradores (terceirizados, estagiários, extraquadro, entre outros);
- discentes.

Público externo:

- sociedade em geral;
- órgãos de controle externo.

OBJETIVOS

Geral

Promover a conscientização e o entendimento do risco para todas as partes interessadas, visando a uma tomada de decisões embasada em informações com maior qualidade.

Específicos:

- fomentar a disseminação de conhecimentos de gestão de riscos e controles internos, criando uma cultura voltada ao tema;
- subsidiar os servidores, gerentes de riscos e gestores responsáveis com informações relevantes sobre o Plano e a Metodologia de Gestão de Riscos adotados pela UFRJ;
- estabelecer ações de comunicação e divulgação, como envio de e-mails e newsletters, produção de cartazes para ambientes de trabalho, além de vídeos, folders e demais conteúdos para as redes sociais, voltadas tanto para o público interno quanto para o externo;
- reduzir ruídos na comunicação, disponibilizando as informações de modo exato, tempestivo e completo.

INSTÂNCIAS DE GOVERNANÇA E ESTRUTURAS INTERVENIENTES NA GESTÃO DE RISCOS DA UFRJ

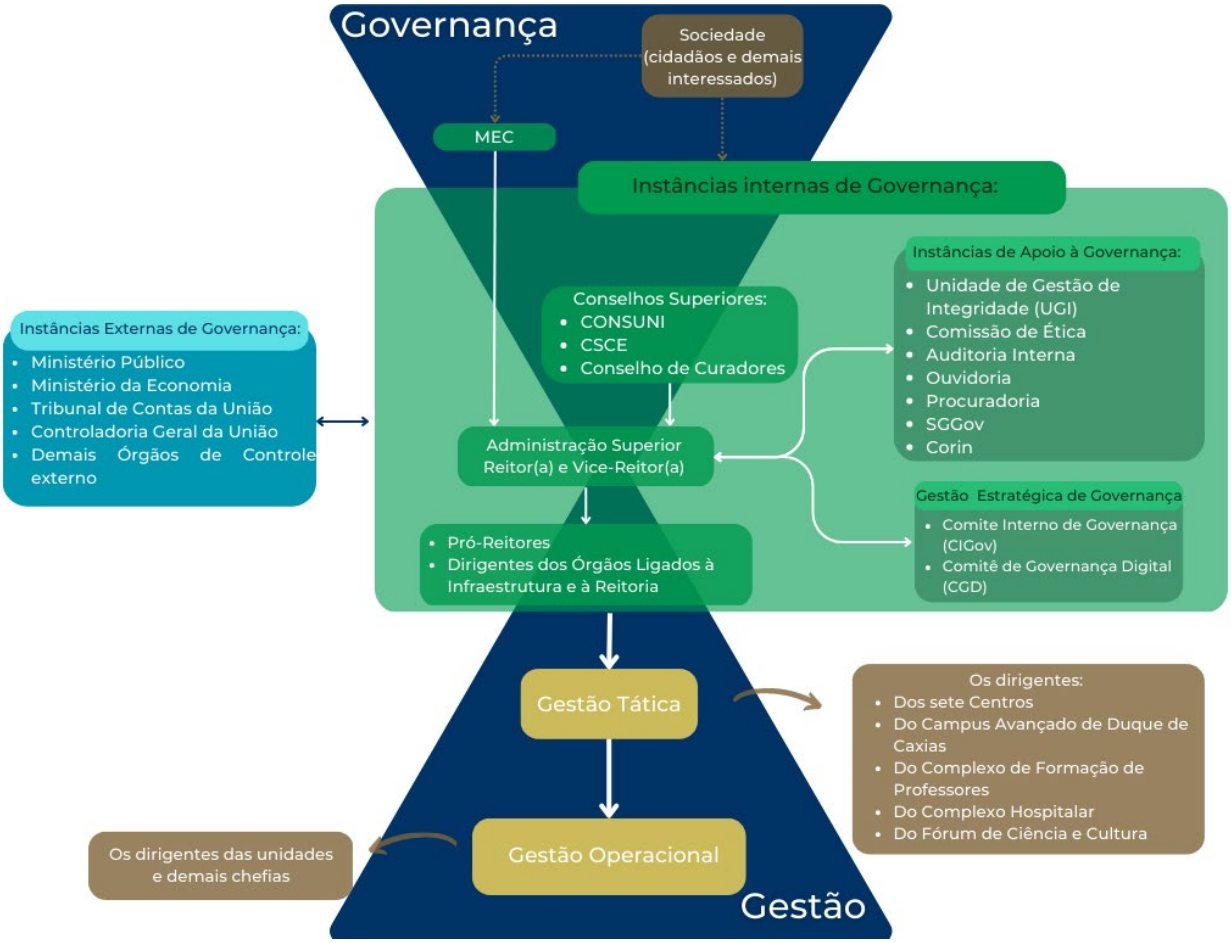
Na UFRJ, a estrutura de governança é definida pelo Sistema de Governança, instituído pela Portaria UFRJ nº 6.611, de 28 de setembro de 2020, que provê meios para a organização e a participação, bem como as diretrizes necessárias à interação de todos os atores relevantes para a gestão da UFRJ. A condução da Política de Governança é da competência do(a) reitor(a), assessorado(a) por um comitê de alto nível, o Comitê Interno de Governança (CIGov). O modelo de governança atual da UFRJ se encontra detalhado na Figura 1.

A Governança consiste em um conjunto de práticas de liderança, estratégia e controle que permite aos dirigentes de uma instituição o adequado conhecimento de sua situação, ao passo que também permite a execução dos objetivos estratégicos. No âmbito de uma instituição pública como a UFRJ, isto significa o alcance de políticas definidas pela Reitoria e conselhos superiores e prestação de serviços de interesse da sociedade. Na UFRJ, o Sistema de Governança foi instituído por meio da Portaria nº 6.611, de 28 de setembro de 2020 (BUFRJ nº 47, 2020).

Na UFRJ as instâncias responsáveis pela gestão estratégica de Governança são o Comitê Interno de Governança (CIGov) e o Comitê de Governança Digital (CGD). O primeiro foi instituído a fim de assessorar a Reitoria na condução da política de governança, visando a

garantir que as boas práticas de governança se desenvolvam e sejam apropriadas pela instituição de forma contínua e progressiva, nos termos recomendados pelo Comitê Interministerial de Governança da Presidência da República (CIG). Ele também é uma das estruturas intervenientes na Gestão de Riscos da Universidade, conforme indica a Figura 2, junto com o Comitê de Apoio à Gestão de Riscos (instância ainda não criada) e o Núcleo de Gestão de Riscos. Dentre as suas competências, está garantir o apoio institucional para promover a Gestão de Riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos atores envolvidos, e supervisionar a atuação das demais instâncias da Gestão de Riscos.

Figura 1: Modelo de Governança da UFRJ



Fonte: Elaboração própria

Já o CGD foi instituído pela Portaria nº 5.199, de 27 de julho de 2020, e tem como competências coordenar e acompanhar as políticas de Tecnologia da Informação e de Segurança da Informação e o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), garantir transparência nos processos de Tecnologias da Informação e Comunicação (TICs), promover a transparência e abertura de dados e deliberar sobre os recursos às ações relacionadas às TICs. Ou seja, o CGD é o responsável pela gestão da Governança relacionada aos processos e projetos ligados às TICs enquanto o CIGov trata dos demais assuntos de Governança da UFRJ.

Figura 2: As três estruturas que intervêm na Gestão de Riscos da Universidade

Fonte: Elaboração própria

As outras duas estruturas intervenientes na Gestão de Riscos são o Comitê de Apoio à Gestão de Riscos – instância ainda não criada até o momento da publicação do presente documento, a qual será presidida por um representante do Gabinete da Reitoria – e o Núcleo de Gestão de Riscos, absorvido por um período de 12 meses pela Superintendência-Geral de Governança (SGGov/PR-6), até que conte com estrutura própria. Este último tem como uma de suas competências elaborar o Plano de Comunicação de Gestão de Riscos, além de requisitar aos responsáveis pelo gerenciamento de riscos dos processos institucionais as informações necessárias à consolidação dos dados e a elaboração dos relatórios gerenciais.

É importante ressaltar que, segundo a PGR/UFRJ, estas três instâncias e os responsáveis pelo gerenciamento de riscos dos processos institucionais deverão manter fluxo regular e constante de informações entre si.

O CIGov terá o auxílio do Comitê de Apoio à Gestão de Riscos para a revisão da Política de Gestão de Riscos, bem como para a definição e atualizações da implementação da Gestão de Riscos, considerando os contextos externo e interno. Além disso, esta última instância tem a responsabilidade de definir a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos inerentes aos objetivos institucionais, bem como aprovar as respostas e respectivas medidas de controle a serem implementadas, avaliando sua efetividade e monitorando a evolução dos níveis de riscos, atividade a ser realizada em conjunto com o Núcleo de Gestão de Riscos.

Ao Comitê de Apoio à Gestão de Riscos também caberá a avaliação da proposta de metodologia de gestão de riscos e suas revisões, devendo encaminhar todas as suas decisões e propostas para apreciação e aprovação do CIGov.

Já o Núcleo de Gestão de Riscos contempla, como algumas de suas competências, o suporte à identificação, a análise e a avaliação dos riscos dos processos inerentes aos objetivos institucionais, a consolidação dos resultados das diversas áreas em relatórios gerenciais e seu encaminhamento para apreciação do CIGov e do Comitê de Apoio à Gestão de Riscos e a orientação e o apoio das unidades acadêmicas e administrativas na execução de seus planos internos de gestão de riscos e demais instruções relativas ao tema.

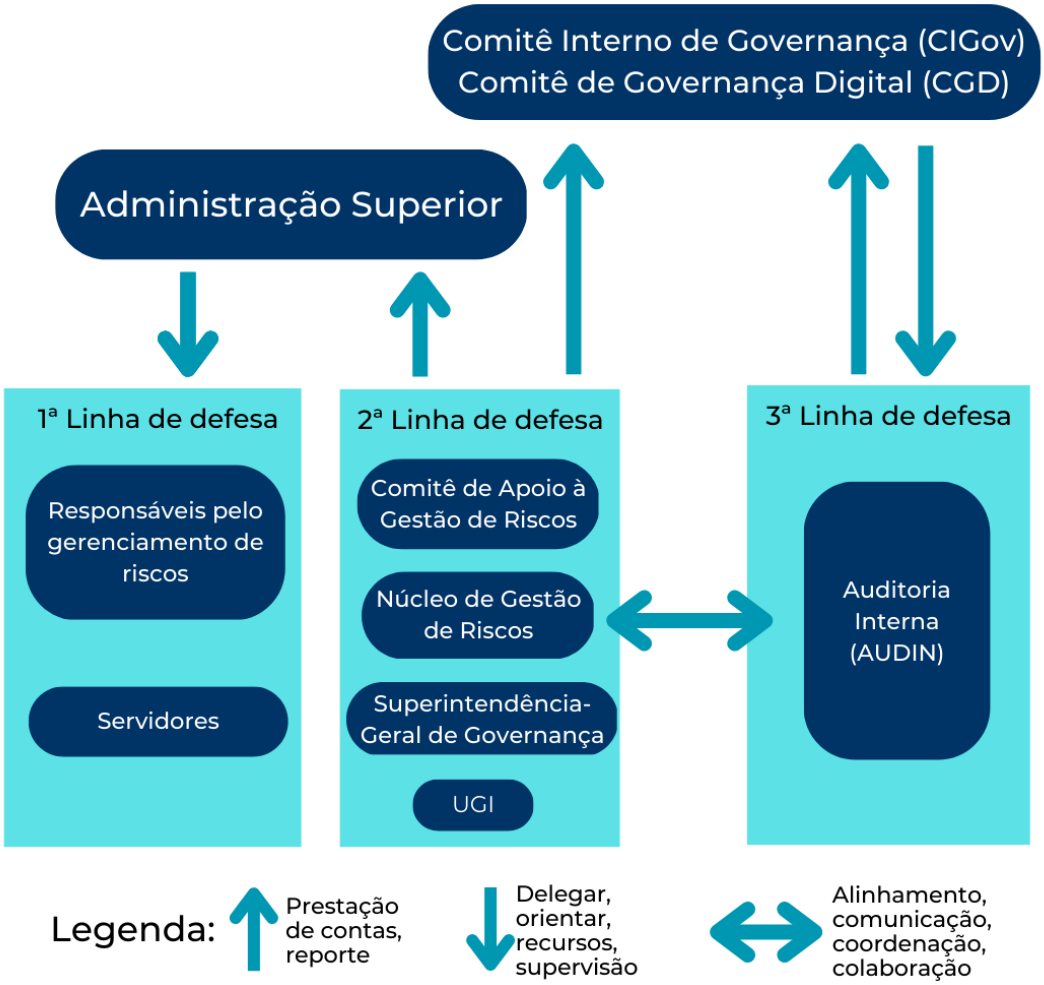
Cada objetivo estratégico institucional terá um gestor responsável, designado pelo CIGov. Ao gestor cabe a indicação dos gerentes dos riscos dos processos inerentes ao respectivo objetivo, os quais, por sua vez, devem disponibilizar as informações adequadas quanto à gestão dos riscos dos processos sob sua responsabilidade a todos os níveis da UFRJ e demais partes interessadas. No caso das unidades organizacionais, cabe ao dirigente designar os gerentes dos riscos de cada processo. É essencial que todos os dados destes servidores, como e-mail e telefone institucional, sejam mantidos atualizados em uma lista disponível para as três instâncias – CIGov, Comitê de Apoio à Gestão de Riscos e Núcleo de Gestão de Riscos –, devendo ser imediatamente reportadas quaisquer alterações dos servidores designados.

Por último, a PGR/UFRJ estabelece que compete aos servidores da UFRJ que sejam proprietários de riscos o monitoramento da evolução dos níveis de riscos e a efetividade das medidas de controle implementadas nos processos institucionais em que estiverem envolvidos ou de que tiverem conhecimento. Caso sejam identificadas mudanças ou fragilidades nos processos institucionais, o servidor deverá reportar imediatamente o fato ao responsável pelo gerenciamento de riscos do processo em questão. Esta ação, portanto, estabelece a primeira linha de defesa, segundo o Modelo de três linhas do IIA 2020 (Figura 3), em conjunto com os responsáveis pelo gerenciamento de riscos.

Já a segunda linha é composta pelo Núcleo de Gestão de Riscos e pelo Comitê de Apoio à Gestão de Riscos, detalhados anteriormente, e pela Unidade de Gestão da Integridade (UGI) e a Superintendência-Geral de Governança (SGGov). A UGI, instituída pela Portaria nº 8.236, de 25 de novembro de 2020, é a estrutura que coordena as ações que asseguram a conformidade dos servidores aos princípios éticos, aos procedimentos administrativos e às normas legais aplicáveis à Instituição. A SGGov foi criada pela Resolução Consuni nº 04, de 28 de junho de 2018, e trata do desenvolvimento de instrumentos para o aprimoramento da gestão e governança institucional, exerce a Gerência Geral do Sistema de Governança, além de contribuir para o gerenciamento dos riscos inerentes ao exercício das atividades da UFRJ.

Por fim, na terceira linha encontra-se a Auditoria Interna da UFRJ (Audin), criada pela Portaria nº 810, de 3 de maio de 2001, com vinculação administrativa à alta administração da UFRJ e vinculação técnica à Controladoria Geral da União (CGU), a partir de orientação normativa e supervisão técnica do Sistema de Controle Interno do Poder Executivo Federal.

Figura 3: Modelo de Três Linhas do IIA 2020, adaptado para o ambiente da UFRJ



Fonte: Elaboração própria

ESTRATÉGIAS E AÇÕES DE COMUNICAÇÃO

Como a UFRJ ainda está em um estágio inicial de sua implementação de Gestão de Riscos, é importante que ações de conscientização sejam realizadas a fim de fomentar este tipo de cultura na instituição. Tais ações focarão nos seguintes temas:

- o que é a Gestão de Riscos e qual a sua importância para a UFRJ;
- como é a estrutura do atual Sistema de Governança;
- funcionamento do Modelo de Três Linhas (desenvolvido por The Institute of Internal Auditors e institucionalizado pelo Poder Executivo Federal, por meio da Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016) e as competências do Núcleo de Gestão de Riscos;
- o que é apetite a risco e qual o apetite definido pela UFRJ.

Além dos temas apontados, está prevista uma pesquisa sobre a percepção dos riscos no ambiente de trabalho e as ações de treinamento de 200 servidores em Gestão de Riscos, considerando casos práticos e envolvendo tanto os riscos em processos quanto projetos estratégicos.

Por último, será implementado um sítio eletrônico da Governança da UFRJ para apresentar, de forma integrada, as informações relacionadas à Gestão de Riscos.

FERRAMENTAS (CANAIS E FORMATOS)

As ações a seguir serão conduzidas pelo Núcleo de Gestão de Riscos, cujas funções estão sendo temporariamente absorvidas pela Superintendência-Geral de Governança até outubro de 2023.

Ferramenta	Proposta	Público Atingido
E-mail	Envio de e-mails com as campanhas de conscientização	Todos os servidores
	Envio de e-mail com pesquisa sobre percepção dos riscos no ambiente de trabalho	
	Envio de e-mail com divulgação do novo sítio eletrônico de Governança da UFRJ	
	Divulgação do treinamento em Gestão de Riscos	200 servidores
	E-mail próprio para recebimento de opiniões, críticas e sugestões sobre a Gestão de Riscos na Unidade	Todos os servidores
Câmara Técnica de Gestão de Riscos e Núcleo de Gestão de Riscos	Canal de comunicação na Ouvidoria para recebimento de dúvidas e sugestões dos servidores sobre a Gestão de Riscos na Unidade	Todos os servidores
Redes sociais	Divulgação de campanhas de conscientização	Todos os servidores
	Divulgação do treinamento em Gestão de Riscos	200 servidores
	Divulgação do novo sítio eletrônico de Governança da UFRJ	Todos os servidores
	Divulgação da pesquisa sobre percepção dos riscos no ambiente de trabalho	Todos os servidores
Realização de reuniões do Núcleo de Gestão de Riscos	Estabelecimento de reuniões bimestrais com os Gestores Responsáveis pelos Objetivos Institucionais, os Gerentes de Riscos nomeados por eles e o Núcleo de Gestão de Riscos com troca de experiências a fim de aumentar senso de comprometimento e pertencimento	Gestores Responsáveis e Gerentes de Riscos

QUALIDADE DA INFORMAÇÃO

A informação é um elemento primordial no processo de gestão das organizações. Com o avanço cada vez maior dos sistemas informatizados, o processamento de dados tem sido um suporte de crescente relevância para o processo de tomada de decisões. Nesse contexto, as organizações precisam adotar medidas que garantam a confiabilidade das informações geradas, uma vez que dados imprecisos podem gerar riscos não identificados ou avaliações deficientes e decisões gerenciais inadequadas (COSO II, 2007).

Com o objetivo de assegurar e aperfeiçoar a qualidade das informações geradas no processo de gerenciamento de riscos na UFRJ, devem ser considerados os seguintes princípios:

- **ESPECIFICAÇÃO:** a informação deve ser gerada em um nível de detalhamento adequado para sua análise;
- **OPORTUNIDADE:** a informação deve estar disponível no momento necessário para sua análise e seu uso deve atuar como subsídio para tomada de decisão;
- **ATUALIDADE:** as informações disponíveis devem ser as mais recentes sobre o processo ou projeto em análise;
- **PRECISÃO:** as informações devem ser corretas e apresentadas no melhor nível de exatidão possível;
- **ACESSIBILIDADE:** as informações devem ser facilmente obtidas pelos gestores e gerentes de riscos, responsáveis pelas instâncias da estrutura da Universidade e por outras partes que delas necessitem para uso no contexto da gestão de riscos.

Para viabilizar o fluxo de coleta de dados e geração de informações para gestão de riscos no âmbito organizacional, foram definidos requisitos para adoção de uma solução tecnológica. Optou-se, neste primeiro momento, pela adoção do uso por um período de testes do sistema ForRisco, já que este sistema fornece suporte para o registro, processamento, manutenção e distribuição de informações relevantes nas diferentes etapas da gestão de riscos.

A despeito das suas funcionalidades, o sistema possui limitações que, aliadas à falta de integração dos processos organizacionais e com os demais sistemas da Universidade, afetam a geração de informações úteis para o processo de gestão. Diante desses desafios, a UFRJ, a partir de iniciativas do Comitê Interno de Governança (CIGov), reforçará a definição de responsabilidades pela integridade dos dados e executará avaliações periódicas da qualidade dos dados.

Dessa forma, o gerenciamento de riscos na UFRJ deve ser conduzido por pessoas (gestores, gerentes de riscos e gestores da estrutura administrativa) a partir de informações adequadamente especificadas, oportunas, atualizadas, precisas e acessíveis.