SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
GABINETE DO REITOR

P O R T A R I A Nº 1900 / 2021

O REITOR DA UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG, no uso das atribuições que lhe conferem o Estatuto e o Regimento Geral da Universidade,

R E S O L V E:

Art. 1º - Instituir a Metodologia de Gestão de Riscos da Universidade Federal do Rio Grande – FURG, conforme anexo.

Art. 2º - Esta Portaria entra em vigor nesta data.

DÊ-SE CIÊNCIA E CUMPRA-SE
Reitoria da Universidade
Em 14 de setembro de 2021.

Prof. Dr. Danilo Giroldo
Reitor

METODOLOGIA DE GESTÃO DE RISCOS

Universidade Federal do Rio Grande - FURG

AGOSTO/2020

SUMÁRIO

1 INTRODUÇÃO

Este documento apresenta a estrutura e a Metodologia de Gestão de Riscos da Universidade Federal do rio Grande – FURG, com o objetivo de orientar a todas as Unidades formalmente estabelecidas no organograma da Universidade à implementá-la, dentro de sua área de competência, em conformidade com a Política de Gestão de Riscos (PGR/FURG), instituída através da Resolução 027/2019 – CONSUN.

A Fig. 1 a seguir apresenta os 13 eixos do Plano de Desenvolvimento Institucional (2019-2022) da FURG, que representam os 13 Macroprocessos da Universidade. Ao centro dessa figura estão representados os Macroprocessos Finalísticos relativos ao Ensino, Pesquisa e Extensão; e, em torno, estão dispostos os Macroprocessos de Apoio.

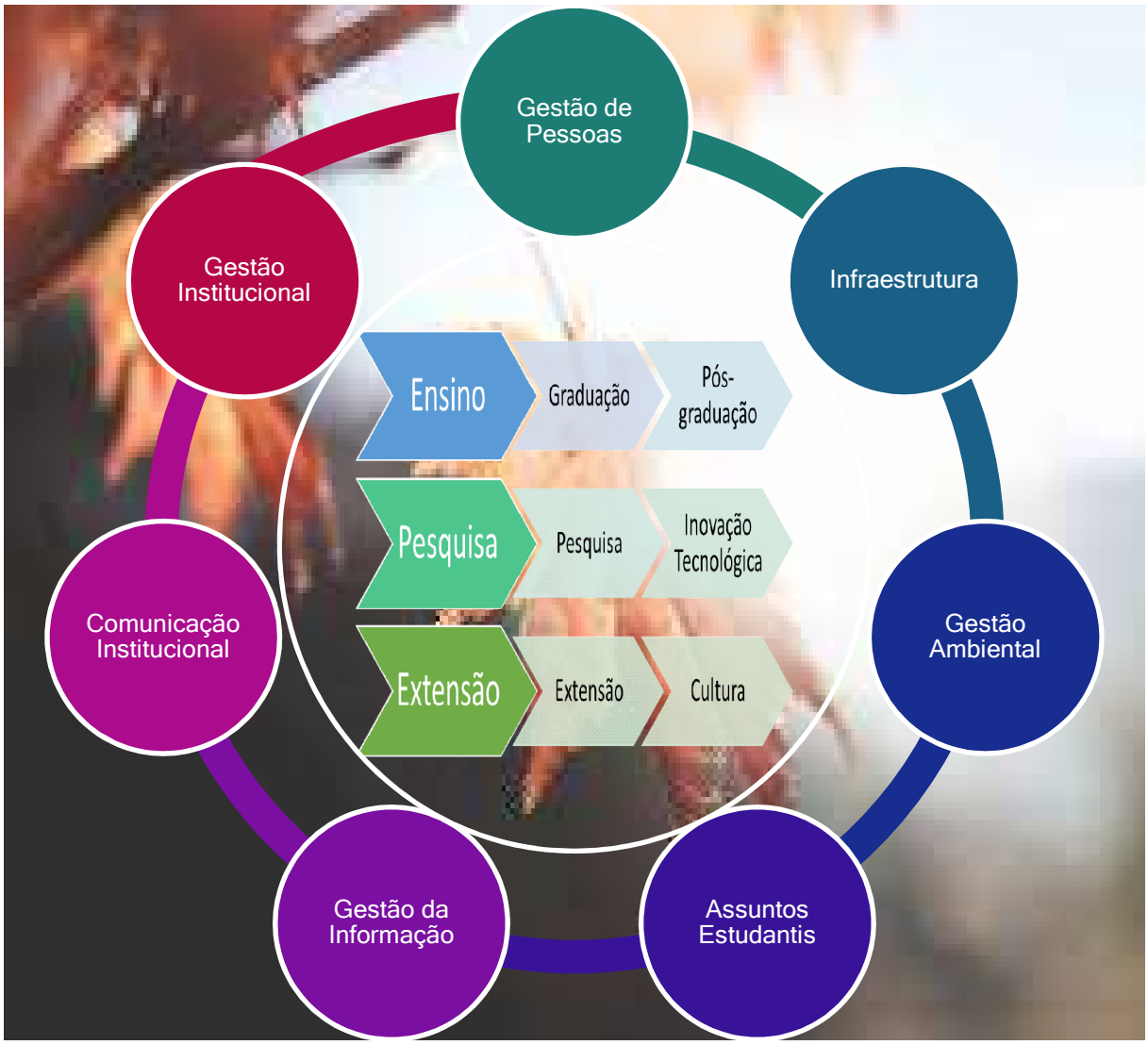

Figura 1: Macroprocessos Finalísticos e Apoio da FURG.
Fonte: Baseado no PDI (2019-2022) FURG.

A implementação da Política de Gestão de Riscos consta como estratégia no Eixo XIII – Gestão Institucional, do Plano de Desenvolvimento Institucional – PDI (2019-2022), para o alcance do objetivo "Aprimorar as práticas de gestão voltadas ao desenvolvimento institucional". Dentre os indicadores estabelecidos para mensurar o alcance deste objetivo no PDI está o "Número de processos organizacionais com mensuração de risco".

A Gestão de Riscos refere-se à arquitetura (princípios, objetivos, estrutura, competências e processo) para gerenciar riscos eficazmente. Assim, este documento aborda:

- Os Fundamentos da Gestão de Riscos da FURG, onde constam os conceitos básicos, a legislação, os princípios e objetivos que norteiam a gestão de riscos da FURG;
- A Estrutura de Gestão de Riscos da FURG com as competências, as instâncias e a forma de integração dos processos organizacionais. Também são apresentados os objetivos e princípios que norteiam a gestão de riscos da FURG.
- A Metodologia de Gestão de Riscos da FURG com a descrição das etapas do gerenciamento de riscos.

2 OBJETIVO DA GESTÃO DE RISCOS NA FURG (ART.1º DA PGR)

A Gestão de Riscos na FURG tem o objetivo de orientar os processos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos inerentes às atividades da Universidade, subsidiando a tomada de decisão em todos os níveis da Instituição e contribuindo para o alcance dos objetivos estabelecidos no Plano de Desenvolvimento Institucional - PDI e no Projeto Pedagógico Institucional – PPI.

3 FUNDAMENTOS DA GESTÃO DE RISCOS

O desenho e a implementação de estruturas e processos de gestão de riscos devem levar em consideração as necessidades específicas da organização em face dos objetivos que dão suporte à sua missão e dos riscos associados, envolvendo aspectos como natureza, complexidade, estratégia, contexto, estrutura, operações, processos, funções, projetos, produtos, serviços ou ativos e práticas empregadas (ABNT, 2009).

3.1 PARÂMETROS LEGAIS E FRAMEWORKS

No âmbito do Poder Executivo Federal, o marco regulatório que orienta os órgãos e as entidades públicas à estruturação de mecanismos de controles internos, gestão de riscos e governança é a Instrução Norma-

tiva MP/CGU nº 01, de 10 de maio de 2016, em que são apresentados conceitos, princípios, objetivos e responsabilidades relacionados aos temas.

Recentemente, foi publicado o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. Este decreto define atribuições à alta administração do Poder Executivo Federal sobre a gestão de riscos, conforme abaixo:

> Art. 17 A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar **Sistema de Gestão De Riscos** e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional, observados os seguintes princípios:
>
> I - Implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;
>
> II - Integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;
>
> III - estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e
>
> IV - Utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.

Neste aspecto é importante a utilização de modelos reconhecidos para a adoção de padrões e boas práticas, que estabeleçam uma abordagem sistemática, oportuna e estruturada para a gestão de riscos que, possam contribuir para a eficiência e a obtenção de resultados consistentes, evitando o uso de instrumentos e procedimentos burocráticos e desordenados (ABNT, 2009).

Existem quatro (4) modelos reconhecidos segundo o TCU (2017): i) COSO GRC 2004 – Gerenciamento de Riscos – Estrutura Integrada; ii) COSO GRC 2016 – Alinhando Risco com Estratégia e Desempenho; iii) ISO 31000 – Gestão de Riscos – Princípios e Diretrizes; iv) *The Orange Book* – Princípios e Conceitos.

A norma ISO 31000 tem o propósito de harmonizar os processos de gestão de riscos entre os diversos modelos e fornecer uma abordagem comum para aplicação em ampla gama de atividades, conforme a ABNT(2009). Assim, esta norma será utilizada para definir o processo de

gestão de riscos a ser utilizado pela FURG.

3.2 CONCEITOS

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

Risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

Risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

Gestão de Riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização dos seus objetivos;

Gestor do Risco: Agente responsável pelo gerenciamento de determinado risco com autoridade para orientar e acompanhar as ações de mapeamento, conforme a Política e a Metodologia de Gestão de Riscos da FURG;

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

4. ESTRUTURA DE GESTÃO DE RISCOS DA FURG

A **Estrutura da Gestão de Riscos** compreende o conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização (ABNT, 2009).

Os componentes dessa estrutura são: Mandato e Comprometimento, Concepção da Estrutura para Gerenciar Riscos, Implementação da Gestão de Riscos, Monitoramento e Análise Crítica da Estrutura e Melhoria Contínua da Estrutura, conforme Figura 2 a seguir.

Figura 2 – Relacionamento entre os Componentes da Estrutura de Gerenciamento de Riscos
Fonte: ABNT NBR ISO 31000 (2009)

Na Furg, os componentes Mandato e comprometimento estão definidos nas competências e responsabilidades que foram atribuídas na Política de Gestão de Riscos – PGR/FURG.

Os elementos da Estrutura para o gerenciamento de Riscos são tratados nos itens: (4.1) Competências, (4.2) Integração dos Processos Organizacionais, (4.3) Recursos e (4.4) Comunicação, no processo de gerenciamento de riscos.

Com o entendimento de que os resultados do Monitoramento e da Análise Crítica podem impactar na estrutura e na metodologia de Gestão de Riscos da FURG, deve ser realizada uma revisão anual desses componentes (Melhoria Contínua da Estrutura), sem prejuízo das alterações que possam ser feitas antecipadamente no processo para garantia da qualidade.

Nesta concepção a ISO 31000considera a Gestão de Riscos como sendo à arquitetura (princípios, objetivos, estrutura, competências e processo) para gerenciar riscos eficazmente, enquantoo Gerenciamento de Riscos trata da aplicação da arquitetura para riscos no estabelecimento de processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais específicos.Assim é importante que sejam estabelecidas medidas de controleno tratamento dos riscos, aumentando a

probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados.

Nesta Estrutura de Gestão de Riscos os"Processos"correspondem aoconjunto de ações e atividades inter-relacionadas, que são executadas para alcançar um produto, resultado ou serviço predefinido, de modo que a Governança trata da combinação destes processos e das estruturas implantadas pela alta administração, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade (ISO 31000, 2009).

4.1 COMPETÊNCIAS

A Gestão de riscos deve ser realizada de forma integrada. A Política de Gestão de Riscos da FURG estabelece um Sistema de Gestão de Riscos que consiste no conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos através de toda a organização.

De acordo com a Política de Gestão de Riscos da FURG, são responsáveis pelo **Sistema de Gestão de Riscos**: o Comitê de Governança Riscos e Controle Interno, o Comitê Operativo, os Grupos de Trabalho e os Gestores do Risco, conforme Figura 3, a seguir.

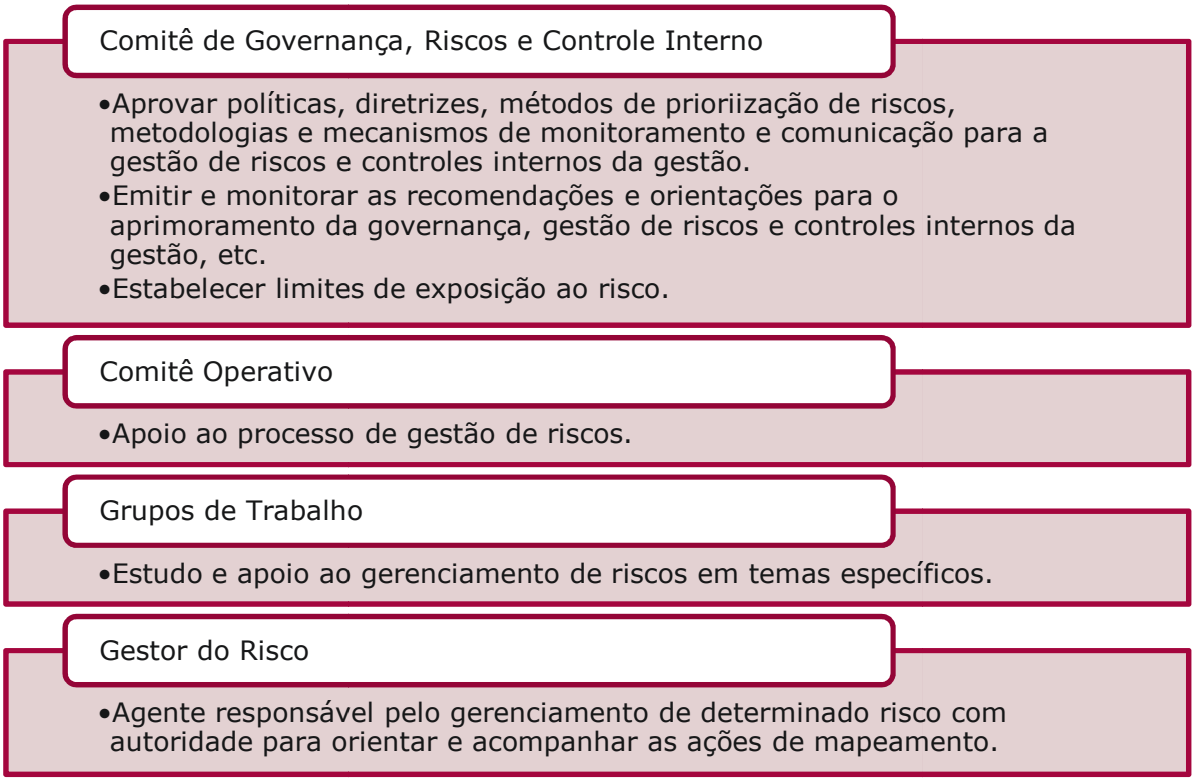

Figura 3: Principais competências dos responsáveis pelo Sistema de Gestão de Riscos – FURG
Fonte: o autor.

A IN Conjunta CGU/MP nº 01/2016 apresenta a estrutura de três linhas de defesa, conforme proposto pelo *The InstituteofInternalAuditors* (IIA) da seguinte forma:

1ª linha de defesa: Os controles internos da gestão se constituem na primeira linha (ou camada) de defesa das organizações públicas para propiciar o alcance de seus objetivos. Esses controles são operados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio dos órgãos e entidades do Poder Executivo federal. A definição e a operacionalização dos controles internos devem levar em conta os riscos que se pretende mitigar, tendo em vista os objetivos das organizações públicas.

2ª linha de defesa: supervisão e monitoramento dos controles internos executados por instâncias específicas, como comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e *compliance*;

3ª linha de defesa: constituída pelas auditorias internas no âmbito da Administração Pública, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa) e da supervisão dos controles internos (segunda linha ou camada de defesa).

Na FURG, a 1ª linha de defesa da Gestão de Riscos é composta pelos servidores e pelos responsáveis pelo gerenciamento de riscos dos processos organizacionais. Na 2ª linha, atuam o Comitê Operativo e o Comitê de Governança, Riscos e Controle Interno, cuja constituição é descrita conforme os Arts. 8º e 6º da PGR/FURG, conforme Figura 4 a seguir.

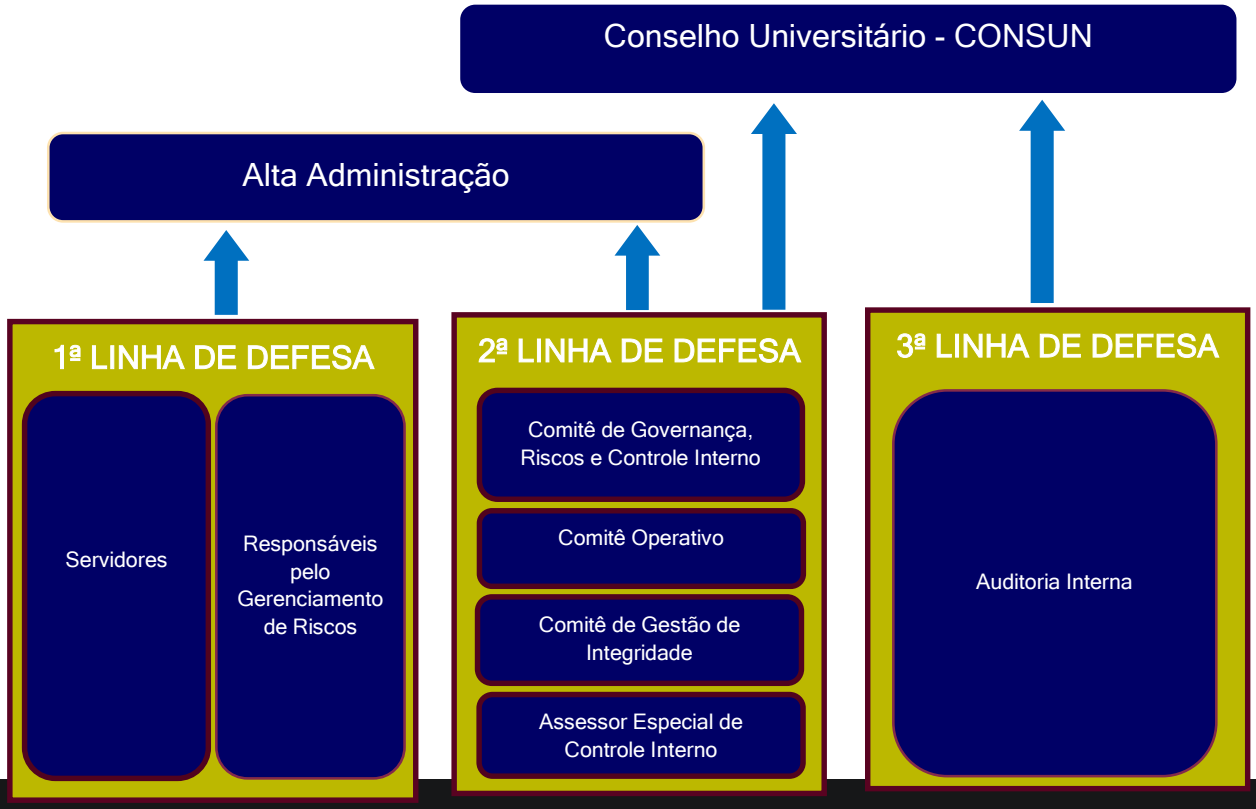

Figura 4: Linhas de Defesa na Gestão de Riscos da FURG
Fonte:Declaração de Posicionamento do IIA: as três linhas de defesa no gerenciamento eficaz de riscos e controles (IIA, 2013, adaptado)

4.1.1 COMITÊ DE GOVERNANÇA, RISCOS E CONTROLE INTERNO (ART.7º DA PGR)

Compete ao Comitê de Governança, Riscos e Controle Interno:

I. apoiar a inovação e a adoção de boas práticas de governança, gestão de riscos e controles internos da gestão;
II. promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, transparência e efetividade das informações;
III. promover a integração e o desenvolvimento contínuo dos agentes responsáveis pela governança, gestão de riscos e controles internos da gestão;
IV. institucionalizar estruturas adequadas de governança, gestão de riscos e controle internos da gestão;
V. aprovar políticas, diretrizes, metodologias e mecanismos de monitoramento e comunicação para a gestão de riscos e controles internos da gestão;
VI. aprovar as diretrizes de capacitação dos agentes públicos no exercício do cargo, função e emprego em gestão de riscos e controles internos da gestão;
VII. definir ações para disseminação da cultura de gestão riscos e controles internos da gestão;
VIII. aprovar método de priorização de processos para a gestão de riscos e controles internos da gestão;
IX. estabelecer limites de exposição a riscos e níveis de conformidade;
X. supervisionar os riscos que podem comprometer o alcance dos objetivos estratégicos e a prestação de serviços de interesse público;
XI. supervisionar o modelo de gestão de riscos e controles internos da gestão;
XII. tomar decisões considerando as informações sobre gestão de riscos e controles internos da gestão e assegurar que estejam disponíveis em todos os níveis;
XIII. emitir e monitorar as recomendações e orientações para o aprimoramento da governança, gestão de riscos e controles internos da gestão.

4.1.2 COMITÊ OPERATIVO (ART.8º DA PGR)

O **Comitê Operativo** irá apoiar a operacionalização da gestão de riscos e será constituído por um Assessor Especial para Gestão de Riscos e Controle Interno, representação da Auditoria Interna, das Pró-reitoras de Infraestrutura e de Planejamento e Administração, vinculado e definido pelo Comitê de Governança, Riscos e Controle Interno. O Comitê Operativo desempenha o papel de unidade central de coordenação e supervisão da gestão de riscos, sendo responsável por avaliar e propor mudanças no **Sistema de Gestão de Riscos – SGR/FURG**.

Neste sentido, cabe ao Comitê Operativo:

I. coordenar a implantação e a operação do SGR/FURG;
II. monitorar os riscos-chave e propor limites de exposição a riscos de abrangência institucional;
III. assessorar o Comitê de Governança, Riscos e Controle Interno em matérias relacionadas à gestão de riscos;
IV. propor a Metodologia de Gestão de Riscos e suas revisões;
V. definir os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
VI. monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;
VII. dar suporte à identificação, análise e avaliação dos riscos dos processos organizacionais selecionados para a implementação da Gestão de Riscos;
VIII. consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los ao Comitê de Governança Riscos e Controle Interno;
IX. oferecer capacitação continuada em Gestão de Riscos para os servidores da FURG;
X. elaborar Plano de Comunicação de Gestão de Riscos;
XI. medir o desempenho da Gestão de Riscos objetivando a sua melhoria contínua;
XII. construir e propor ao Comitê de Governança, Riscos e Controle Interno os indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho da FURG; e
XIII. requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais.

O Comitê Operativo poderá propor, conforme a Política de Gestão de Riscos, Parágrafo Único, Art. 8º, a constituição de Grupos de Trabalhos em temas específicos para a Implementação da Política de Gestão de Riscos.

4.1.3 GESTOR DO RISCO (ART.9º E 10º DA PGR)

O Gestor do Risco é o agente responsável pelo gerenciamento de determinado risco com autoridade para orientar e acompanhar as ações de mapeamento nos processos sob sua responsabilidade com competência para:

I. Identificar, analisar e avaliar os riscos dos processos sob sua responsabilidade, assegurando que o risco seja gerenciado de acordo com a política de gestão de riscos da organização;
II. monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos da FURG;
III. informar o Comitê Operativo sobre mudanças significativas nos processos organizacionais e garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da organização;
IV. Responder as requisições do Comitê Operativo.

4.1.4 UNIDADES ESTABELECIDAS NO ORGANOGRAMA DA FURG

Toda a Unidade formalmente estabelecida no organograma da Universidade deverá implementar, dentro de sua área de competência, procedimentos alinhados à Política de Gestão de Riscos da FURG, conforme o Art. 13 da PGR.

4.2 INTEGRAÇÃO NOS PROCESSOS ORGANIZACIONAIS

A Gestão de Riscos da FURG tem como objetivo subsidiar a tomada de decisão e como princípios a melhoria contínua dos processos organizacionais e o alinhamento aos objetivos estratégicos.

Para isso, cada unidade da FURG deve elaborar PLANO DE GESTÃO DE RISCOS (conforme seção 5.1), que será integrado ao seu PLANO DE AÇÃO ANUAL, com a identificação dos processos organizacionais sob sua responsabilidade que serão objeto da Gestão de Riscos.

O art. 17º da PGR/FURG, define que serão priorizados os processos organizacionais mais críticos, respeitando a maturidade organizacional sobre o tema (conforme seção 5.2).

4.3 RECURSOS

A unidade responsável pelo processo organizacional deve designar equipe para participar das etapas do processo de gerenciamento de riscos. Essa equipe deve ser composta por servidores que conheçam o processo,

seus objetivos, contextos, partes envolvidas, resultados e controles já existentes.

4.4 COMUNICAÇÃO

A comunicação sobre o processo de gerenciamento de riscos deve ser realizada de maneira formal, através da constituição de **Processo Administrativo pelo Responsável pela Unidade Administrativa/Acadêmica**, que deverá conter as Informações sobre o processo selecionado (Unidade, Responsável (Diretor ou equivalente), responsável pelo gerenciamento de riscos e equipe técnica), bem como todos documentos produzidos nas fases do gerenciamento de riscos, descritas a seguir: 1)Seleção do Processo 2)Estabelecimento do contexto; 3)Identificação dos Riscos; 4)Análise dos Riscos; 5)Avaliação dos Riscos; e 6)Tratamento dos riscos dos processos priorizados.

4.5 CAPACITAÇÃO

O Comitê Operativo, promoverá junto a Pró-Reitoria de Gestão de Pessoas – PROGEP capacitações anuais com o objetivo de formar multiplicadores de Gestão de Riscos na FURG. Também serão realizados treinamentos para capacitação de seus servidores por meio de:

I. Plano Anual de Capacitação, conforme disposto no Programa de Capacitação e Aperfeiçoamento dos Integrantes do Plano de Carreira dos Cargos Técnico-Administrativos em Educação da FURG;
II. Cursos promovidos pelos Órgãos de Controle Interno e Externo;
III. Palestras realizadas internamente pelos Comitês e Agentes envolvidos na operacionalização dos riscos.

Outros treinamentos sobre a aplicação da Metodologia de Gestão de Riscos podem ser solicitados pelas unidades.

5 METODOLOGIA DE GESTÃO DE RISCOS

A Metodologia de Gestão de Riscos da FURG tem o objetivo de estabelecer e estruturar as etapas necessárias para a operacionalização da Gestão de Riscos na FURG, por meio da definição de um processo de gerenciamento de riscos. Segundo o Art. 11º da PGR/FURG, são necessárias, no mínimo, as seguintes etapas:

I. **Estabelecimento do contexto:** envolve o entendimento da

organização, dos objetivos e do ambiente, inclusive do Controle Interno, no qual os objetivos são perseguidos, com o fim de obter uma visão abrangente dos fatores que podem influenciar a capacidade da organização para atingir seus objetivos, bem como fornecer parâmetros para a definição de como as atividades subsequentes do processo de gestão de riscos serão conduzidas.

II. **Identificação dos Riscos:** é o processo de busca, reconhecimento e descrição dos riscos, tendo por base o contexto estabelecido e apoiando-se na comunicação e consulta com as partes interessadas internas e externas.

III. **Análise dos Riscos**: é o processo de compreender a natureza e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento de riscos.

IV. **Avaliação dos Riscos**: A finalidade da avaliação de riscos é auxiliar na tomada de decisões, com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Envolve comparar o nível de risco com os critérios de risco estabelecidos quando o contexto foi considerado, para determinar se o risco e/ou sua magnitude são aceitáveis ou toleráveis ou se algum tratamento é exigido;

V. **Tratamento dos Riscos**: envolve a seleção de uma ou mais opções para modificar o nível de cada risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão em novos controles ou modificação dos existentes. Um dos benefícios da gestão de riscos é o rigor que proporciona ao processo de identificação e seleção de alternativas de respostas aos riscos.

A Figura 5 a seguir apresenta as etapas do processo de gerenciamento de riscos na FURG.

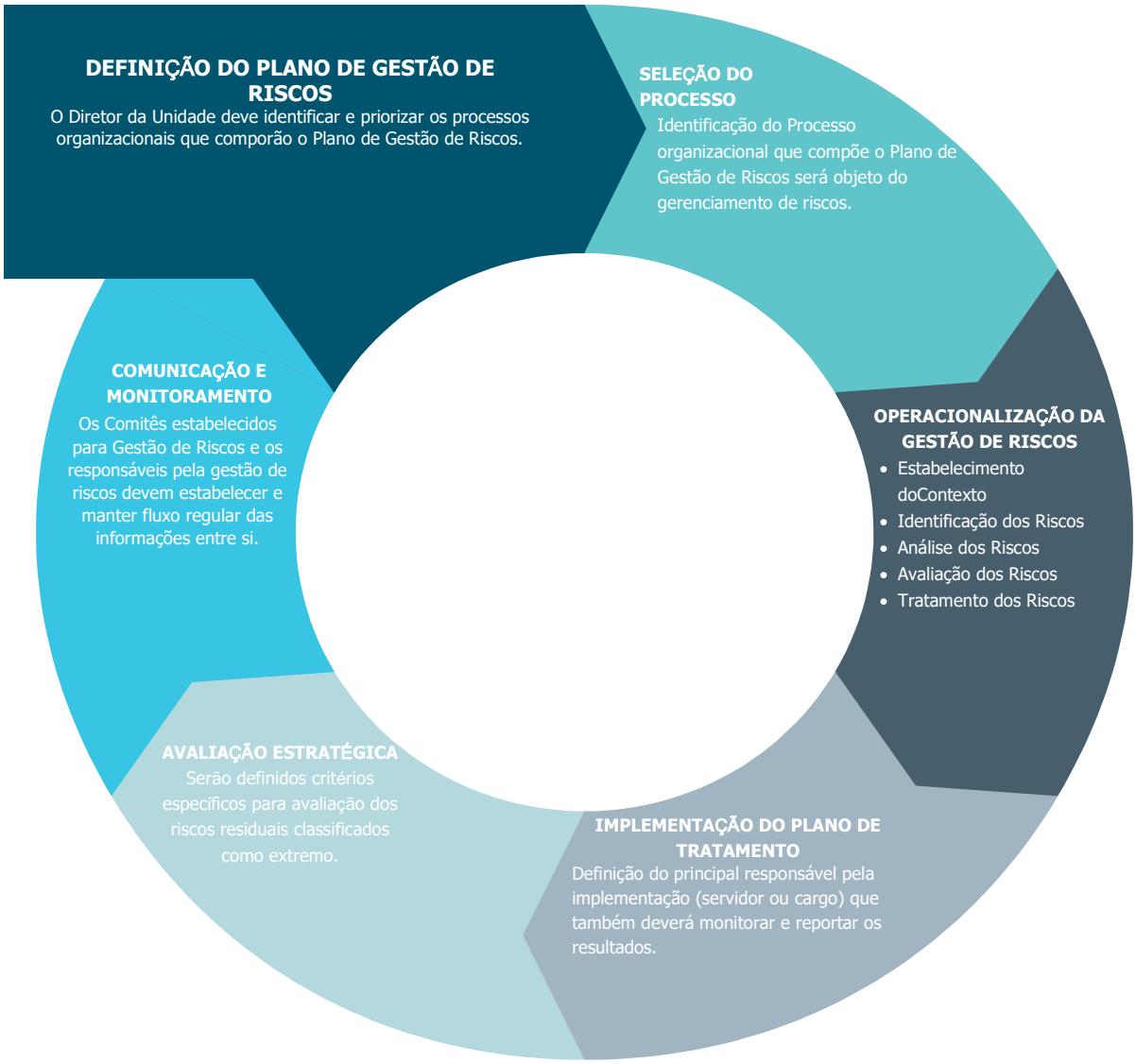

Figura 5: Etapas do Processo de Gerenciamento de Riscos
Fonte: Baseada na CGU (2018)

A Gestão de Riscos na FURG deve estar a alinhada a Metodologia de Gestão de Riscos descrita neste documento. As unidades organizacionais podem executar os processos de gerenciamento de riscos em processos sob sua responsabilidade, desde que obedecidas as diretrizes e orientações apresentadas nesta Metodologia. Os resultados desses processos devem ser informados ao **Comitê Operativo**, que os reportará ao **Comitê de Governança, Riscos e Controle Interno**. Caberá ao Comitê Operativo selecionar os riscos classificados como "Extremo" para a Avaliação Estratégica (seção 5.11 deste documento).

5.1 DEFINIÇÃO DO PLANO DE GESTÃO DE RISCOS

O Diretor da Unidade Acadêmica/Administrativa, conforme previsto na seção 4.2 deste documento, deve identificar e priorizar os processos

organizacionais que comporão o Plano de Gestão de Riscos da sua unidade, observando o critério estabelecido no art. 17º da PGR/FURG: "serão priorizados os processos organizacionais mais críticos, respeitando a maturidade organizacional sobre o tema".

Esse Plano de Gestão de Riscos também deve contemplar os Planos de Tratamento nos processos de gerenciamento de riscos, que após aprovados, devem ser integrados ao Plano de Ação Anual da Unidade.

5.2 SELEÇÃO DO PROCESSO ORGANIZACIONAL

Ainda que a gestão de riscos deva ser parte integrante de todos os processos organizacionais (princípio previsto pela ISO 31000), ela não deve ser aplicada a todos os seus processos com a mesma intensidade, visto que os recursos da organização são limitados. A priorização de processos organizacionais é importante para orientar a alocação de recursos para a gestão de riscos, bem como quando se planeja uma estratégia gradual de implantação dessa abordagem.

O Método de Seleção dos Processos contribui para estabelecer prioridades para o levantamento e o gerenciamento dos riscos, uma vez que é possível classificar os processos em função do seu grau de exposição.Assim, o ordenamento na priorização de processos deve ser feito com base em escalas, conforme a Figura 6 a seguir.

Figura 6: Escalas para Priorização de Processos

Fonte:o autor

A priorização de processos envolve uma visão sistêmica da organização e deve ser baseada nas melhores informações disponíveis. Neste sentido, os processos devem ser avaliados com base em um índice numérico, conforme Quadro 1 a seguir:

Fatores	Quadro 1 – Escala para Priorização de Processos			
	1	2	3	4
Relevância Estratégica do Processo	O processo tem pouca relevância para a realização dos objetivos-chave da	O processo tem média relevância para a realização	O processo tem alta relevância para a	O processo tem relevância muito alta para a

	organização(macroprodutos, macro-objetivos, ou resultados finalísticos).	dos objetivos-chave da organização.	realização dos objetivos-chave da organização.	realização dos objetivos-chave da organização.
Materialidade	Menos de 2% do orçamento anual.	De 2% a 10% do orçamento anual.	De 10% a 20% do orçamento anual.	Mais de 20% do orçamento anual.
Maturidade do Processo	A gestão do processo é feita com base em modelagem e com medição de desempenho plenamente incorporada. Métodos e tecnologias de gestão amplamente utilizados pelos servidores da área. Muito raro algum produto ou serviço não atender aos padrões de entrega.	A gestão do processo é feita com base em modelagem e indicadores avaliados periodicamente. Métodos e tecnologias de gestão concentradas no nível gerencial. Produtos e serviços atendem aos padrões de entrega na maioria das vezes.	O processo foi modelado e sua modelagem é de conhecimento dos servidores que executam o processo. Produtos e serviços costumam atender aos padrões de entrega, mas falhas significativas ainda ocorrem.	O processo não foi modelado ou sua modelagem não é utilizada para o seu gerenciamento. Os resultados acontecem graças a iniciativas individuais. Padrões de entrega de produtos e serviços não existem ou são ignorados. Prática de "apagar incêndios".

Quadro 1: Escala para Priorização de Processos.
Fonte: Referencial Básico para Gestão de Riscos - TCU (2018)

Nesta etapa devem ser identificados ainda:

- O responsável pelo gerenciamento de risco (conforme previsto no art. 9º da PGR). Esse servidor deve ter alçada suficiente para orientar e acompanhar as etapas de identificação, análise, avaliação e implementação das respostas aos riscos (art. 11º, da PGR);
- A equipe técnica que participará do processo de gerenciamento de riscos.

5.3 ESTABELECIMENTO DO CONTEXTO

Devem ser considerados no contexto dos objetivos da organização como um todo os objetivos do processo, do projeto ou da atividade que está sendo objeto do processo de gestão de riscos, de modo a assegurar a identificação dos riscos do objeto, que sejam significativos para os objetivos da organização.

De acordo com o TCU[1] (2017), nesta etapa, é necessário identificar

[1] Livro Roteiro de Auditoria de Gestão de Riscos – TCU. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/roteiro-de-auditoria-de-gestao-de-risco.htm

os fatores do ambiente, interno e externo, no qual a organização persegue seus objetivos, as partes interessadas, verificando suas necessidades, expectativas legítimas e preocupações, pois essas partes interessadas devem ser incluídas em cada etapa ou ciclo do processo de gestão de riscos, por meio do processo de comunicação e consulta.

Este processo é documentado através de:

a) um Relato conciso dos objetivos organizacionais e dos fatores críticos.
Exemplo: Análise *Swot,* conforme Figura7, a seguir.

Figura 7: Análise SWOT
Fonte: Ministério do Planejamento Desenvolvimento e Gestão (2017)

b) análise das Partes interessadas e seus interesses (Análise dos *Stakeholders*, Matriz de Responsabilidades, etc);
c) critérios mais importantes com base nos quais os níveis de risco serão analisados e avaliados: escalas de probabilidade; escalas de consequências ou impactos; como será determinado se o nível de risco é tolerável ou aceitável e se novas ações de tratamento são necessárias, isto é, diretrizes para priorização e tratamento de (ou resposta a) riscos.

Assim, devem ser identificados nesta etapa, 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;
- Objetivos do processo organizacional. É importante apontar quais objetivos são alcançados pelo processo organizacional. Sendo possível, devem ser indicados o objetivo geral e os objetivos específicos do processo, considerando perspectivas como estratégicas, temporais, relacionais, financeiras, orçamentárias, metas, entre outras.
- Relação de Objetivos Estratégicos da FURG alcançados pelo processo;
- A unidade deve propor qual o prazo necessário para a um novo gerenciamento de riscos do processo organizacional, considerando o Art. 16º da PGR/FURG.
- Unidade demandante do processo de gerenciamento de riscos no processo organizacional (a própria unidade ou o Comitê);
- Justificativa para o processo de gerenciamento de riscos no processo. Apresentar os motivos que levaram a implementar a gestão de riscos no processo organizacional.
- Unidade responsável pelo processo organizacional;
- Leis e regulamentos relacionados ao processo organizacional;
- Ciclo médio do processo organizacional (em dias);
- Sistemas tecnológicos que apoiam o processo organizacional;
- Partes interessadas no processo, podendo ser internas ou externas;
- Informações sobre o contexto externo do processo, considerando cenário atual ou futuro, oportunidades e ameaças relacionadas, percepções das partes interessadas externas e outros fatos relevantes;
- Informações sobre o contexto interno do processo, considerando políticas, objetivos, diretrizes e estratégias que o impactam, forças e fraquezas relacionadas, percepções das partes interessadas internas, principais ocorrências de problemas e outros fatos relevantes;
- Apetite a risco da unidade para o processo organizacional, caso seja diferente do definido neste documento (seção 5.6 deste documento).

5.4 IDENTIFICAÇÃO E ANÁLISE DOS RISCOS

Deve-se elaborar uma lista de riscos e trabalhar com um processo

de forma sistematizada ou estruturada (mapa de processos, fluxogramas). Em situações não claramente estruturadas, como a identificação de riscos estratégicos, utilizam-se processos de identificação mais genéricos ou análise de cenários. A utilização da abordagem "*top-down*" para a identificação de riscos, considera o aspecto mais geral para o mais específico. Nesta abordagem, identificam-se riscos em um nível geral ou superior, como ponto de partida para estabelecer prioridades para, em um segundo momento, identificarem-se e analisarem-se riscos em nível específico e ou mais detalhado (TCU, 2017).

A identificação de riscos pode se basear em dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, necessidades das partes interessadas. É importante que as pessoas com conhecimento adequado sejam envolvidas na identificação de riscos e que a organização utilize ferramentas e técnicas de identificação de riscos que sejam adequadas aos seus objetivos, às suas capacidades e aos riscos enfrentados (ABNT, 2009). Este processo é documentado através de:

a) o escopo do processo, projeto ou atividade coberto pela identificação;
b) os participantes do processo de identificação;
c) a abordagem ou o método utilizado para identificação dos riscos e as fontes de informação consultadas;
d) o registro dos riscos identificados em sistema, planilha ou matriz de avaliação de riscos, descrevendo os componentes de cada risco separadamente com, pelo menos, suas causas, o evento (risco) e as consequências.

Desta forma, nesta etapa, deve ser elaborada uma lista abrangente de eventos que podem evitar, atrasar, prejudicar ou impedir o cumprimento dos objetivos do processo organizacional ou das suas etapas críticas.

Os riscos podem ser identificados a partir de perguntas, como:

- Quais eventos podem EVITAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional?
- Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?

Por meio da identificação de eventos de riscos, pode-se planejar a forma de tratamento adequado e qual o tipo de resposta a ser dada a esse risco, destacando que os eventos de riscos devem ser entendidos como parte de um contexto, e não de forma isolada.

A Figura 8, a seguir, destaca os componentes do evento de Risco.

Figura 8: Componentes do Evento de Risco
Fonte: Ministério do Planejamento Desenvolvimento e Gestão (2017)

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

- O evento é um risco que pode comprometer claramente um objetivo do processo?
- O evento é um risco ou uma falha no desenho do processo organizacional?
- À luz dos objetivos do processo organizacional, o evento identificado é um risco ou uma causa para um risco?
- O evento é um risco ou uma fragilidade em um controle para tratar um risco do processo?

Para eventos identificados e analisados como riscos do processo, deve-se indicar:

- Objetivo do processo organizacional/etapa impactado pelo risco;
- Categorias dos riscos, definidas no Art. 15 da PGR/FURG, dispostas na Figura 9, a seguir:

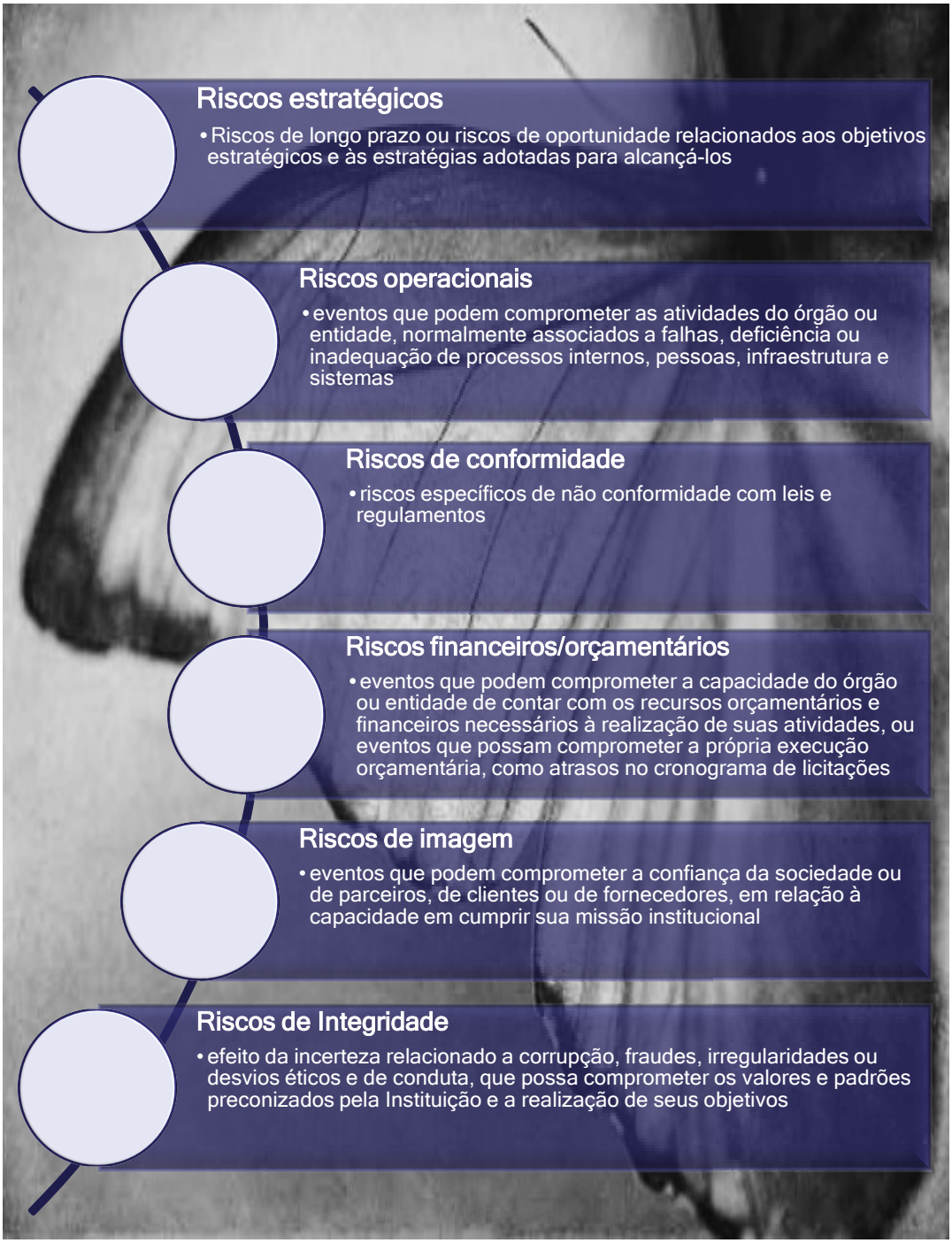

Figura 9: Categorias de Riscos definidas no Art. 15 da PGR/FURG.
Fonte: o autor.

- Causas: motivos que podem promover a ocorrência do risco;
- Consequências: resultados do risco que afetam os objetivos;
- Controles preventivos: controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência. Exemplos de controles preventivos: requisitos /

checklist definidos para o processo e capacitação dos servidores envolvidos no processo;

- Controles de atenuação e recuperação: controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências. Exemplos de controles de atenuação e recuperação: plano de contingência; tomada de contas especiais; procedimento apuratório.

A análise *Bow Tie*será utilizada para auxiliar na análise do Risco. Esta ferramentaidentifica e descreve os caminhos de um evento de risco, desde suas causas até as consequências, por meio de uma representação pictográfica semelhante a uma gravata borboleta (*bow tie*). O método tem como foco as barreiras entre as causas e o evento de risco e as barreiras entre o evento de risco e suas consequências, conforme Figura 10, a seguir.

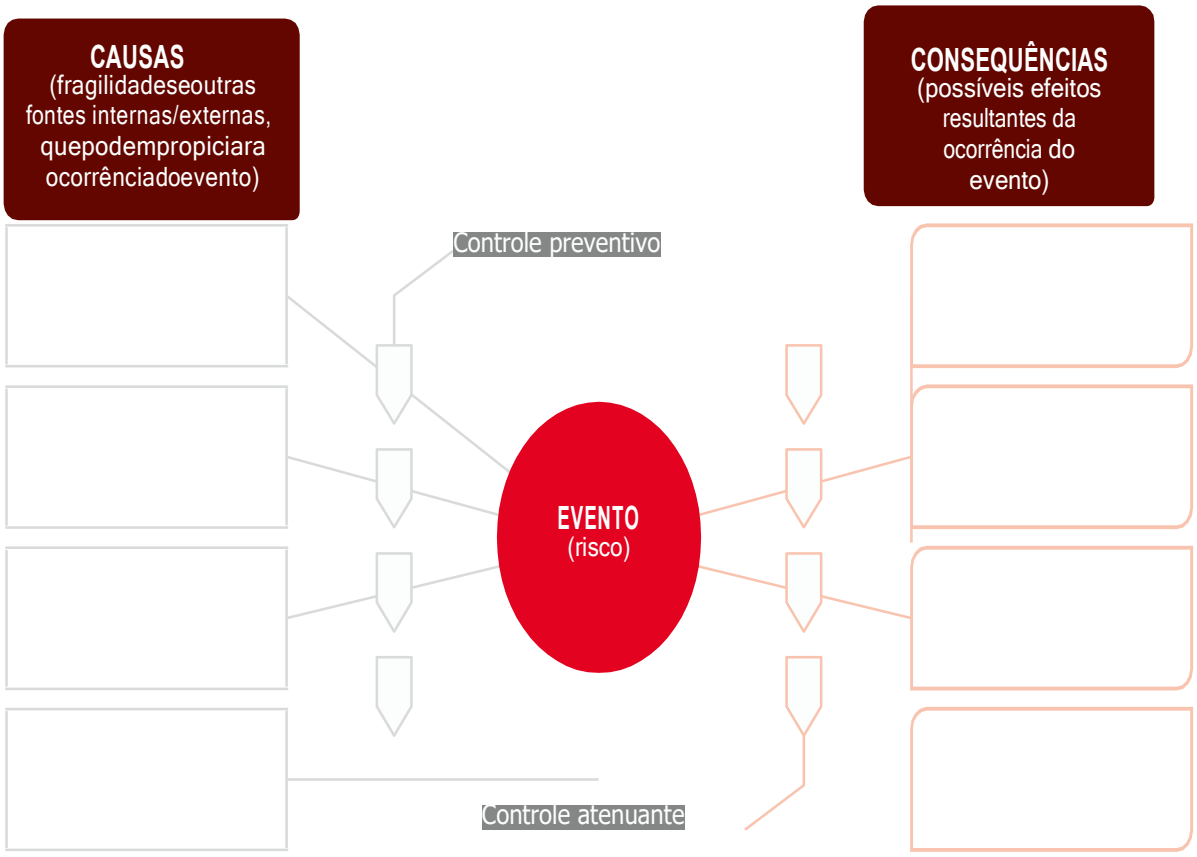

Figura 10: Análise *Bow Tie*
Fonte: Referencial Básico para Gestão de Riscos - TCU (2018)

O processo de elaboração do esquema *bow tie* ocorre da seguinte forma:

a) Representa-se o evento de risco como sendo o nó de uma gravata borboleta.

b) As possíveis causas ou fontes do evento de risco são listadas no lado esquerdo do desenho e cada uma delas é conectada por uma linha ao nó da gravata.

c) Barreiras que impedem ou diminuem a possibilidade da causa ou fonte de produzir o evento de risco são representadas como barras verticais cruzando essas linhas horizontais do lado esquerdo.

d) De forma análoga, no lado direito do desenho, identificam-se possíveis consequências e cada uma delas é ligada ao nó central por uma linha.

e) Barreiras que impedem ou diminuem o efeito das consequências são representadas como barras verticais cruzando essas linhas horizontais do lado direito. As barreiras do lado esquerdo do esquema representam controles preventivos, no caso de risco negativo ou controles de intensificação ou promoção, no caso de risco positivo/oportunidades. As barreiras do lado direito representam controles reativos visando à atenuação dos efeitos, caso o evento de risco negativo se materialize.

O produto resultante dessa análise é o próprio diagrama esquemático gerado, bem como as informações a ele associadas que foram identificadas: evento de risco, fontes, causas, controles preventivos ou intensificadores e controles reativos de atenuação.

O Anexo I deste documento traz o modelo de planilha para o registro de informações produzidas nas etapas de Identificação e Análise de Riscos (colunas 1 a 8).

5.5 AVALIAÇÃO DOS RISCOS

Nesta etapa, são calculados os níveis dos riscos identificados pela equipe técnica designada, a partir de critérios de probabilidade e impacto. O Quadro 2 a seguir apresenta a escala de probabilidades.

Quadro 2 - Escala de Probabilidades		
Probabilidade	Descrição	Peso
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

Quadro 2: Escala de Probabilidades
Fonte: Gestão de Riscos - Avaliação da Maturidade (TCU, 2018)

O Quadro 3 a seguir apresenta a escala de impactos.

Quadro 3 - Escala de Impactos		
Impacto	Descrição	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/ comunicação/divulgação ou de conformidade).	1
Baixo	Pequeno impacto nos objetivos (idem).	2
Médio	Moderado impacto nos objetivos (idem), porém recuperável.	5
Alto	Significativo impacto nos objetivos (idem), de difícil reversão.	8
Muito alto	Catastrófico impacto nos objetivos (idem), de forma irreversível.	10

Quadro 3: Escala de Impactos
Fonte: Gestão de Riscos - Avaliação da Maturidade (TCU, 2018)

A multiplicação entre os valores de probabilidade e impacto define o nível do risco inerente, ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade da sua

ocorrência ou do seu impacto.

Risco Inerente = Probabilidade X Impacto

Quadro 4 - Escala para Classificação de Níveis de Risco			
RB (Risco Baixo)	**RM** (Risco Médio)	**RA** (Risco Alto)	**RE** (Risco Extremo)
0 - 9,99	10 – 39,99	40 – 79,99	80 – 100

Quadro 4: Escala para Classificação dos Níveis de Risco
Fonte: Gestão de Riscos - Avaliação da Maturidade (TCU, 2018)

Os resultados das combinações de probabilidade e impacto, classificados de acordo com a escala de níveis de risco, podem ser expressos em uma matriz, como a seguir.

Quadro 5 - Matriz de Risco

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

Quadro 5: Matriz de Riscos
Fonte: Gestão de Riscos - Avaliação da Maturidade (TCU, 2018)

Segue-se exemplo de um registro de riscos (parcial) com a determinação dos Níveis dos Riscos Inerentes (NRI), de acordo com o método apresentado.

Quadro 6-Determinação dos Riscos (Exemplo)			
Riscos Identificados	**Probabilidade**	**Impacto**	**Nível De Risco Inerente (Nri)**
Risco 1 – Descrição do risco 1	Alta 8	Muito Alto 10	80 RE (Extremo)
Risco 2 – Descrição do risco 2	Média 5	Alto 8	40 RA (Alto)
Risco 3 – Descrição do risco 3	Baixa 2	Médio 5	10 RM (Médio)
Risco n – Descrição do risco n	Muito Baixa 1	Médio 5	5 RB (Baixo)

Quadro 6: Exemplo de Determinação dos Riscos
Fonte: Gestão de Riscos - Avaliação da Maturidade (TCU, 2018)

Em seguida, a equipe técnica designada deve avaliar a eficácia dos controles internos existentes em relação aos objetivos do processo organizacional. Ou seja, é necessário verificar se os controles apontados durante a etapa de Identificação e Análise do risco têm auxiliado no tratamento adequado desse risco. O quadro 7 mostra os níveis de avaliação da eficácia dos controles existentes:

A avaliação das respostas a riscos e atividades de controle correspondentes – ou simplesmente controles – é parte integrante da análise de riscos. Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações e medidas que a gestão adota com o objetivo de modificar o nível de risco (ABNT, 2009).

As atividades de controle são as ações estabelecidas por meio de políticas e procedimentos, desempenhadas em todos os níveis da organização, em vários estágios dentro do processo organizacional e no ambiente tecnológico, que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos (COSO, 2013). As atividades de controle também são geralmente referidas como controles internos.

Uma forma de avaliar o efeito dos controles na mitigação de riscos consiste em determinar um nível de confiança (NC), mediante análise dos atributos do desenho e da implementação dos controles, utilizando uma escala como a exemplificada a seguir.

Quadro 7-Avaliação dos Controles Internos Existentes		
Nível de Confiança (NC)	Descrição	Risco de Controle (RC)
Inexistente NC = 0% (0,0)	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	Muito Alto 1,0
Fraco NC = 20% (0,2)	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.	Alto 0,8
Mediano NC = 40% (0,4)	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.	Médio 0,6
Satisfatório NC = 60% (0,6)	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Baixo 0,4
Forte NC = 80% (0,8)	Controles implementados podem ser considerados a "melhor prática", mitigando todos os aspectos relevantes do risco.	Muito Baixo 0,2

Quadro 7: Avaliação dos Controle Internos Existentes
Fonte: Gestão de Riscos - Avaliação da Maturidade (TCU, 2018)

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

$$RC = 1 - NC$$

Pela fórmula é possível deduzir que quanto mais eficaz for o desenho e a implementação dos controles, ou seja, quanto maior for o RC, menor será o NC e vice-versa, porém este nunca será "zero", uma vez que o nível de confiança jamais será 100%.

Uma vez estabelecido o RC, é possível estimar o nível de risco residual (NRR), ou seja, o risco que permanece após o efeito das respostas adotadas pela gestão, incluindo controles internos e outras ações, para reduzir a probabilidade e ou o impacto do evento. Para isso, deduz-se do nível de risco inerente (NRI) o percentual de confiança (NC) atribuído ao controle, o que equivale a multiplicar o NRI pelo NC, utilizando a seguinte fórmula:

NRR = NRI X RC

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

O Anexo I deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Avaliação de Riscos (colunas 9 a 13).

Segue-se um exemplo de um registro de riscos (parcial) com a determinação dos níveis dos riscos residuais (NRR) de alguns riscos identificados, de acordo com o método apresentado.

Quadro 8 - Determinação dos Níveis de Riscos Residuais

Riscos Identificados	P	I	Nível De Risco Inerente (Nri)	Nível De Confiança Do Controle	Risco De Controle (Rc)	Nível De Risco Residual (Nrr)
Risco 1	Alta - 8	M. Alto - 10	RE - 80	Inexistente	1,0	RE - 80
Risco 2	Média - 5	Alto - 8	RM - 40	Mediano	0,6	RM-24
Risco 3	Baixa - 2	Alto - 5	RM - 10	Fraco	0,8	RB - 8

Quadro 8: Determinação dos Níveis de Riscos Residuais
Fonte: Gestão de Riscos - Avaliação da Maturidade (TCU, 2018)

A documentação da etapa de análise de riscos é normalmente feita no registro de riscos e geralmente inclui:

a) a abordagem ou o método de análise utilizado, as fontes de informação consultadas e os participantes do processo de análise;
b) as especificações utilizadas para as classificações de probabilidade e impacto dos riscos;
c) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e sua descrição, bem como considerações quanto à análise desses elementos e o resultado de sua combinação, o risco inerente;
d) a descrição dos controles existentes e as considerações quanto à sua eficácia, e o risco de controle;
e) o nível de risco residual, resultante da combinação dos dois riscos anteriores (inerente e de controle).

A extensão da documentação dos riscos de níveis mais baixos pode

ser menos detalhada, porém deve ser mantido registro do fundamento lógico para justificar a determinação inicial dos níveis de risco nesse patamar.

5.6 PRIORIZAÇÃO DOS RISCOS

Nesta etapa, devem ser considerados os valores dos níveis de riscos residuais calculados na etapa anterior para identificar quais riscos serão priorizados para tratamento.

A faixa de classificação do risco residual deve ser considerada para a definição da atitude da unidade em relação à priorização para tratamento. O Quadro 9 mostra, por classificação, quais ações devem ser adotadas em relação ao risco e suas exceções.

Quadro 9 - Determinação dos Níveis de Riscos Residuais

Classificação	Ação Necessária	Exceção
RISCO EXTREMO	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser objeto de Avaliação Estratégica (seção 5.11). Assim, deverá ser comunicado peloGestor do Risco ao Diretor da Unidade (ou equivalente), que comunicará ao Comitê Operativo, que por sua vez comunicará ao Comitê de Governança, Riscos e Controle Interno. Postergação de medidas só com autorização do Comitê de Governança, Riscos e Controle Interno.	Caso o risco não seja priorizado para implementação de medidas de tratamento, este deverá ser justificado pela unidade e aprovado pelo seu Diretor (ou equivalente) e pelo Comitê de Governança, Riscos e Controle Interno.
RISCO ALTO	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao Diretor da unidade que comunicará ao Comitê Operativo,para o estudo da ação a ser tomada em período determinado. Postergação de medidas só com autorização do Comitê Operativo.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo Comitê Operativo.
RISCO MÉDIO	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu Diretor.
RISCO BAIXO	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu Diretor.

Quadro 9: Determinação dos Níveis de Riscos Residuais
Fonte: Gestão de Riscos - Avaliação da Maturidade (TCU, 2018, adaptado)

5.7 DEFINIÇÃO DE RESPOSTAS AOS RISCOS

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar o nível de cada risco e a elaboração de planos de tratamento que, uma vez implementados, implicarão em novos controles ou modificação dos existentes. Um dos benefícios da gestão de riscos é o rigor que proporciona ao processo de identificação e seleção de alternativas de respostas aos riscos (ABNT, 2009; COSO, 2006).

Esta etapa objetiva definir as opções e as medidas de tratamento (controles) para os riscos priorizados na etapa anterior, conforme Quadro 10 a seguir.

Quadro 10 - Opções de tratamento do risco

Opções de Tratamento	Descrição
Mitigar	Consiste em adotar medidas para reduzir a probabilidade ou a consequência dos riscos ou até mesmo ambos. Os procedimentos que uma organização estabelece para tratar riscos são denominados de atividades de controle interno. Um risco normalmente é mitigado quando é classificado como "Alto" ou "Extremo". A implementação de controles, neste caso, apresenta um custo/benefício adequado. Na FURG, mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
Compartilhar	Compartilhar ou transferir o risco é o caso especial de se mitigar a consequência ou probabilidade de ocorrência do risco por meio da transferência ou compartilhamento de uma parte do risco, mediante contratação de seguros ou terceirização de atividades nas quais a organização não tem suficiente domínio. Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas a implementação de controles não apresenta um custo/benefício adequado. Na FURG, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar	Evitar o risco é a decisão de não iniciar ou de descontinuar a atividade, ou ainda desfazer-se do objeto sujeito ao risco. Um risco normalmente é evitado quando é classificado como "Alto" ou "Extremo", e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não existe a possibilidade de compartilhá-lo. Na FURG, evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Governança Riscos e Controle Interno.
Aceitar	Aceitar ou tolerar o risco é não tomar, deliberadamente, nenhuma medida para alterar a probabilidade ou a consequência do risco. Ocorre quando o risco está dentro do nível de tolerância da organização.Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Quadro 10: Opções de Tratamento do Risco
Fonte: Baseado na CGU (2018)

Cada risco priorizado deve ser relacionado a uma opção de tratamento. A escolha da opção depende do nível do risco.Devem ser definidas medidas de tratamento para o risco se a opção de tratamento do risco for MITIGAR. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível mais próximo possível das faixas de apetite a risco (risco "Baixo" ou "Médio").

O Plano de Tratamento gerado pelo processo de gerenciamento de riscos do processo organizacional é um plano de ação para a implementação das medidas de tratamento dos riscos desse processo organizacional. Por isso, deve conter, pelo menos:

a) Iniciativa, com a proposta de projeto ou ação que implementará um conjunto de medidas de tratamento;
b) Medida(s) de tratamento contemplada(s) na iniciativa e o risco relacionado que deseja tratar;
c) Objetivos/benefícios esperados por medida de tratamento;
d) Unidade organizacional responsável pela implementação da iniciativa;
e) Unidades organizacionais corresponsáveis pela implementação da iniciativa, ou seja, unidades envolvidas na implementação da medida de tratamento;
f) Servidor ou cargo responsável pela implementação;
g) Breve descrição sobre a implementação;
h) Custo estimado para a implementação;
i) Data prevista para início da implementação;
j) Data prevista para o término da implementação;
k) Situação da iniciativa.

O Plano de Tratamento deve avaliar a necessidade de melhorar ou extinguir controles internos já existentes. Após essa avaliação podem ser propostos novos controles, observados sempre critérios de eficiência e eficácia da sua implementação.

Caso as ações definidas no Plano de Tratamento envolvam mais de uma unidade, o responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta de Plano para que essas unidades validem as iniciativas de que participarem.

O Anexo II deste documento traz um modelo de Plano de Tratamento.

5.8 VALIDAÇÃO DOS RESULTADOS DAS ETAPAS DO PROCESSO DE GERENCIAMENTO DE RISCOS

Os resultados das etapas anteriores do processo de gerenciamento de riscos (estabelecimento do contexto, identificação e análise dos riscos, avaliação dos riscos, priorização dos riscos e definição de respostas aos riscos) devem ser avaliados e aprovados pelo Diretor da unidade Administrativa/Acadêmica.

Após a aprovação desses resultados, o Diretor da unidade deve:

- Encaminhar esses resultados ao Comitê Operativo;
- Incluir as iniciativas previstas no Plano de Tratamento no Plano de Gestão de Riscos da sua unidade;
- Encaminhar o Plano de Tratamento aprovado às unidades corresponsáveis pelas iniciativas para que essas também incluam as ações em seu Plano Operacional corrente.

5.9 IMPLEMENTAÇÃO DO PLANO DE TRATAMENTO

A implementação do Plano de Tratamento envolve a participação da Unidade Administrativa/Acadêmica responsável pelo processo organizacional e das unidades relacionadas como corresponsáveis em cada iniciativa, se previstas.

A responsabilidade primária pelo Plano de Tratamento permanece com a unidade organizacional responsável pelo processo organizacional. No Plano de Tratamento, deve ser definido o principal responsável pela implementação da iniciativa (servidor ou cargo), que também deverá monitorar e reportar a evolução das iniciativas.

5.10 COMUNICAÇÃO E MONITORAMENTO

De acordo com o TCU (2018), durante todas as etapas ou atividades do processo de gestão de riscos deve haver uma efetiva comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas, para:

a) auxiliar a estabelecer o contexto apropriadamente e assegurar que as visões e percepções das partes interessadas, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração;

b) auxiliar a assegurar que os riscos sejam identificados e analisados adequadamente, reunindo áreas diferentes de especialização;

c) garantir que todos os envolvidos estejam cientes de seus papéis e responsabilidades, e avalizem e apoiem o tratamento dos riscos.

O monitoramento e análise crítica é etapa essencial da gestão de riscos e tem por finalidade: (a) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar riscos emergentes; (b) obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos; (c) analisar eventos (incluindo os "quase incidentes"), mudanças, tendências, sucessos e fracassos e aprender com eles; e (d) assegurar que os controles sejam eficazes e eficientes no projeto e na operação (ABNT, 2009).

Dentro do escopo de um processo de gerenciamento de riscos, deve ser observada a Matriz de Responsabilidade RACI. Essa Matriz tem o objetivo de definir: Responsável, Autoridade, Consultado e Informado para o processo de gerenciamento de riscos na FURG, conforme Figura 11 a seguir.

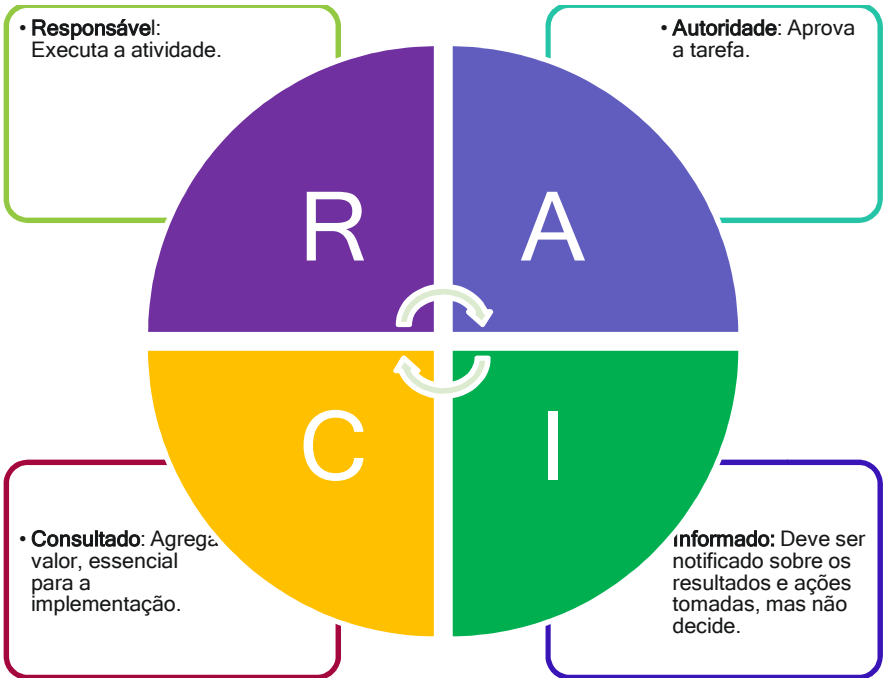

Figura 11: Matriz de RACI
Fonte: Baseado em SOUZA e BRASIL (2017)

Durante as etapas do processo de gerenciamento de riscos da FURG, é importante que a comunicação observe os agentes ou unidades apontadas como consultados ou informados na Matriz RACI do quadro 11.

Quadro 11 – Matriz RACI para o Processo de Gerenciamento de Riscos na FURG

Ações	Comitê de Governança, Riscos e Controles Internos	Comitê Operativo	Diretor da Unidade	Gestor do Risco	Grupo de Trabalho Designado	Responsável pela Implementação	Servidores da FURG
Definir Plano de Gestão de Riscos da Unidade	I	A	R	C	I	I	I
Selecionar Processo Organizacional	I	A	R	C	I		
Realizar o Entendimento do Contexto	I	I	A	R	R		
Realizar a Identificação e Análise dos Riscos	I	I	A	R	R		
Realizar a Avaliação dos Riscos	I	I	A	R	R		
Realizar a Priorização dos Riscos	I	I	A	R	R		
Realizar a Definição de Respostas aos Riscos	I	I	C	A	R		
Validar os Riscos Levantados	I	I	C	R	C		
Implementar o Plano de Tratamento	I	I	C	A	I	R	
Monitorar	I/R	R	C	A	R	C	R
Realizar Avaliação Estratégica	A	C	R	C	C		

Quadro 11: Matriz RACI Gerenciamento de Riscos - FURG
Fonte: Baseado na CGU (2018)

O monitoramento, no âmbito do processo de gerenciamento de riscos, deve ser realizado principalmente pela unidade responsável pelo processo organizacional, de forma a:

- Garantir que os controles sejam eficazes e eficientes;
- Analisar as ocorrências dos riscos;
- Detectar mudanças que possam requerer revisão dos controles e/ou do Plano de Tratamento;
- Identificar os riscos emergentes.

Mudanças identificadas durante o monitoramento devem ser encaminhadas ao Comitê Operativo, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos já realizados nos processos organizacionais da FURG.

Semestralmente, o Comitê Operativo produzirá um boletim com o resultado do acompanhamento das ações relacionadas ao Plano de Gestão de Riscos de cada unidade, que será enviado ao Comitê de Governança Riscos e Controle Interno.

Além disso, o Comitê Operativo deverá elaborar o Relatório de Monitoramento da Gestão de Riscos da FURG com a consolidação desses resultados, que deve ser encaminhado, no mínimo, uma vez por ano ao Comitê de Governança, Riscos e Controle Interno.

5.11 AVALIAÇÃO ESTRATÉGICA

Riscos residuais classificados como "Extremo" na etapa de Avaliação de Riscos (seção 5.6 deste documento) serão avaliados novamente pelo Comitê Operativo e pela equipe técnica designada por meio de critérios de mensuração específicos para as dimensões de probabilidade e impacto. O Anexo III apresenta o processo de elaboração e o formato desses critérios, denominados critérios de Avaliação Estratégica.

Essa comparabilidade auxilia a decisão, pelo Comitê de Governança, Riscos e Controle Interno, para a priorização para tratamento de riscos de diferentes processos.

Durante a Avaliação Estratégica, a equipe técnica designada pela Unidade responsável pelo processo organizacional e o Comité Operativo devem discutir e determinar os níveis dos riscos selecionados dentro de cada critério que compõe a probabilidade e o impacto. O resultado será, então, a média ponderada dos valores desses níveis, considerando os pesos desses critérios. Esse resultado será apresentado ao Comitê de

Governança, Riscos e Controle Interno.Os critérios de probabilidade e impacto da Avaliação Estratégica e seus respectivos pesos comporão documento específico.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT.**GestãodeRiscos–Princípioediretrizes.**NBRISO31000.AssociaçãoBrasileiradeNormas Técnicas.2009.

BRASIL.**Instrução Normativa Conjunta MP/CGUNº01**, de 10 de maio de 2016, que estabelece a adoção de uma série de medidas para a sistematização de práticas relacionadas a gestão de riscos, controles internos e governança. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197. Acesso em 17 de agosto de 2020.

BRASIL. Ministério da Transparência e Controladoria Geral da União – CGU. **Metodologia de Gestão de Riscos**. Brasília. 34 p., 2018. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/41833/5/Metodologia_gestao_riscos_2018.pdf. Acesso em 17 de agosto de 2020.

BRASIL.Ministério do Planejamento, Desenvolvimento e Gestão. Assessoria Especial de Controles Internos. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.** Brasília. Brasília. V1.1.2 –2017. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/41827/8/Manual_de_GIRC_Versao_2.pdf. Acesso em 17 de agosto de 2020.

BRASIL. Tribunal de Contas da União. **Referencial Básico deGestão de Riscos**. Brasília. 154 p., 2018. Disponível em:https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm. Acesso em 17 de agosto de 2020.

BRASIL.TribunaldeContasdaUnião.**GestãodeRiscos–AvaliaçãodaMaturidade**.Brasília.164 p.,2018. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/gestao-de-riscos-avaliacao-da-maturidade.htm. Acesso em 17 de agosto de 2020.

COSO. *CommitteeofSponsoringOrganizationsoftheTreadwayCommission*. **Gerenciamento de Riscos Corporativos–EstruturaIntegrada**.2007.Tradução:InstitutodosAuditoresInternosdoBrasil (Au-

dibra)e*PricewaterhouseCoopersGovernance,RiskandCompliance*,Estado sUnidosdaAmérica,2007. Disponível em: https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf.Acesso em 17 de agosto de 2020.

COSO. *CommitteeofSponsoringOrganizationsoftheTreadway Commission*. **Risk Assessment in Practice**. Disponível em: https://www.coso.org/Documents/COSO-ERM%20Risk%20Assessment%20in%20Practice%20Thought%20Paper%20October%202012.pdf. Acesso em 17 de agostode 2020.

IIA. *The InstituteofInternalAuditors*. **As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles, 2013.** Disponível em: https://global.theiia.org/translations/PublicDocuments/3LOD-IIA-Exposure-Document-Portuguese.pdf. Acesso em 17 de agosto de 2020.

SOUZA, Kleberson; BRASIL, Franklin. **Como gerenciar riscos na administração pública – Estudo prático em licitações**. Editora Negócios Públicos. Curitiba. 149 p. 2017.

ANEXO I – MODELO DE PLANILHAS DE APOIO PROCESSO DE GERENCIAMENTO DE RISCOS

Identificação e Análise do Risco								**Avaliação dos Riscos**					**Priorizaçãodos Riscos**			**Respostas aos Riscos**	
						Controles											
Processo /Etapa (1)	Objetivo (2)	Evento de Risco (3)	Categoria (4)	Causa (5)	Consequências (6)	Preventivo (7)	Atenuação e recuperação (8)	Probabilidade (9)	Impacto (10)	Risco Inerente (11)	Avaliação dos Controles Internos (12)	Risco Residual (13)	Classificação (14)	Priorização (15)	Justificativa (16)	Tipo de tratamento (17)	Medidas de Tratamento (18)

Fonte: CGU (2018)

ANEXO II – MODELO DE PLANO DE TRATAMENTO

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

Fonte: CGU (2018)

ANEXO III – FORMATO E PROCESSO DE ELABORAÇÃO DOS CRITÉRIOS DE AVALIAÇÃO ESTRATÉGICA

A etapa de Avaliação Estratégica utiliza critérios de avaliação específicos para as dimensões de probabilidade e impacto para os riscos residuais classificados como "Extremo" ou indicados pelos dirigentes máximos das unidades da FURG. Esses critérios devem ser estáveis o suficiente para que seja possível a comparabilidade entre riscos de diferentes processos organizacionais da FURG que utilizaram a metodologia proposta neste documento.

O quadro 12 apresenta o modelo utilizado para os critérios de Avaliação Estratégica da FURG. Cada critério possui alternativas, com valores entre 0% e 100%, estabelecendo um peso para cada critério.

Quadro 12 –Critérios de Avaliação Estratégica					
Probabilidade			Impacto		
Critério 1 (Peso P.A)	Critério 2 (PesoP.B)	Critério 3 (Peso P.C)	Critério 4 (Peso I.A)	Critério 5 (Peso I.B)	Critério 6 (Peso I.C)
Alternativa 1.1	Alternativa 2.1	Alternativa 3.1	Alternativa 4.1	Alternativa 5.1	Alternativa 6.1
Alternativa 1.2	Alternativa 2.2	Alternativa 3.2	Alternativa 4.2	Alternativa 5.2	Alternativa 6.2
Alternativa 1.3	Alternativa 2.3	Alternativa 3.3	Alternativa 4.3	Alternativa 5.3	Alternativa 6.3
Alternativa 1.4	Alternativa 2.4	Alternativa 3.4	Alternativa 4.4	Alternativa 5.4	Alternativa 6.4
Alternativa 1.5	Alternativa 2.5	Alternativa 3.5	Alternativa 4.5	Alternativa 5.5	Alternativa 6.5
Alternativa 1.6	Alternativa 2.6	Alternativa 3.6	Alternativa 4.6	Alternativa 5.6	Alternativa 6.6

Quadro 12: Critérios de Avaliação Estratégica
Fonte:CGU (2018)

ANEXO IV – INDICADORES DE DESEMPENHO DO PROCESSO DE GERENCIAMENTO DE RISCOS

Sugerimos uma lista exemplificativa e não exaustiva de indicadores que podem ser acompanhados e reportados, tais como:

Quadro 12 – Indicadores de Desempenho do Processo de Gerenciamento de Riscos

Indicador	Fórmula
% processos mapeados por unidade	processos mapeados/total de processos
% processos essenciais mapeados por unidade	processos essenciais mapeados/processos essenciais
% processos relevantes mapeados por unidade	processos relevantes mapeados/processos essenciais
% processos moderados mapeados por unidade	processos moderados mapeados/processos essenciais
% processos essenciais com riscos mapeados por unidade	processos essenciais com riscos mapeados/processos essenciais
% processos relevantes com riscos mapeados por unidade	processos relevantes comriscos mapeados/processosrelevantes
% processos moderados com riscos mapeados por unidade	processos moderados comriscos mapeados/processosmoderados
% controles implementados por processo	controles concluídos/total de controles do processo
% controles em andamento por processo	controles em andamento/total de controles do processo
% controles atrasados por processo	controles atrasados/total de controles do processo
% controles não iniciados por processo	controles não iniciados/total de controles do processo

Quadro 12: Indicadores de Desempenho da Gestão de Riscos
Fonte: Ministerio do Planejamento, Desenvolvimento e Gestão (2017)