unipampa

Universidade Federal do Pampa

Metodologia de Gestão de Riscos

versão 2.0

2026

ELABORAÇÃO E REVISÃO

Alexandre Borba de Oliveira - Contador

Ana Paula Almeida Lima - Administrador

Bruno Martinato de Barros - Administrador

Caren Hartwig Milech de Oliveira - Administrador

Caroline Costa Moraes - Professor do Magistério Superior

Caroline Lopes Fagundes - Assistente em Administração

Cesar Calçada Radtke - Técnico de Tecnologia da Informação

Domingos de Mello Aymone Filho - Administrador

Eder Pereira da Silva - Assistente em Administração

Ivan César Stachlewski Barão Dias - Assistente em Administração

Marcelo Souza de Mello - Engenheiro Mecânico

Pierre Correa Martin - Analista de Tecnologia da Informação

Allan Sampaio Pires - Analista de Tecnologia da Informação

Rita de Cássia Angeieski da Silveira - Técnico em Assuntos Educacionais

Tiago Gonçalves Salazart - Assistente em Administração

APOIO TÉCNICO

Gabriela Giacomini de Macedo - Auditor

SUMÁRIO

LISTA DE SIGLAS

BIA - *Business Impact Analysis* (Análise de Impacto no Negócio)
CCI - Coordenadoria de Conformidade Institucional
CE - Comitê Estratégico
CGR - Comitê de Gestão de Riscos
CGU - Controladoria-Geral da União
DGRC - Divisão de Gestão de Riscos e Controles - Unidade de Gestão de Riscos e Controles
MGR - Metodologia de Gestão de Riscos da Universidade Federal do Pampa
PGR/UNIPAMPA - Política de Gestão de Riscos da Universidade Federal do Pampa
RACI - *Responsible* (Responsável), *Arfccountable* (Aprovador/Autoridade), *Consulted* (Consultado), *Informed* (Informado)
SEI - Sistema Eletrônico de Informações
SWOT - *Strengths* (Forças), *Weaknesses* (Fraquezas), *Opportunities* (Oportunidades) e *Threats* (Ameaças)

CONCEITOS

Para fins deste documento, consideram-se os seguintes conceitos:

I - apetite a risco: nível de risco que uma organização está disposta a aceitar.

II - capacidade ao risco: nível máximo de risco que a organização pode suportar na perseguição aos seus objetivos.

III - controle interno da gestão: processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;

IV - gerenciamento de risco: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais;

V - gestão de riscos: arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente;

VI - governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade;

VII - medida de controle: ação, procedimento ou mecanismo aplicado pela organização para tratar riscos, com a finalidade de reduzir a probabilidade de sua ocorrência e/ou mitigar seu impacto, contribuindo para o alcance dos objetivos organizacionais;

VIII - meta: parâmetro mensurável e/ou marco temporal associado a um objetivo organizacional, que permite avaliar seu grau de alcance;

IX - objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização;

X - processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar um produto, resultado ou serviço predefinido;

XI - risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização;

XII - risco inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

XIII - risco positivo (oportunidade): evento incerto que, se ocorrer, terá um efeito positivo ou negativo nos objetivos de um projeto ou processo;

XIV - risco residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco;

XV - tolerância a risco: é o desvio do nível do apetite ao risco, o nível aceitável de variação referente à realização dos objetivos.

APLICAÇÃO

A MGR tem por objetivo estabelecer e estruturar as etapas necessárias para a operacionalização da Gestão de Riscos na Universidade. Sua aplicação ocorre em dois momentos distintos:

- o primeiro, denominado de "Identificação e análise dos riscos e definição do plano de tratamento", visa identificar os eventos de riscos e seus atributos principais;
- o segundo, denominado "Avaliação dos Controles", tem como objetivo analisar e avaliar a implementação das medidas de tratamento, que passam a integrar o conjunto de controles realizados pelas áreas responsáveis pelo gerenciamento dos riscos.

As modelagens dos processos de aplicação da metodologia, com seus respectivos atores e atividades podem ser acessadas através do link a seguir: https://sites.unipampa.edu.br/gestao-de-riscos/documentos/

Etapa 1: Identificação e análise dos riscos e definição do plano de tratamento

Esta etapa corresponde ao momento inicial de aplicação da metodologia, quando ainda não houve a identificação formal dos riscos pelo setor responsável.

A aplicação pode ocorrer em duas modalidades:

I. Processos Organizacionais: aplicação da metodologia a processos organizacionais constituindo-se na forma padrão de execução da metodologia.

II. Planos Institucionais: aplicação da metodologia aos planos institucionais da Universidade, hipótese em que se dispensa o mapeamento prévio dos processos envolvidos.

Na modalidade referente aos processos organizacionais, deverá ser observada integralmente a sequência metodológica das atividades apresentadas neste documento.

Na modalidade aplicada aos planos institucionais, a execução das atividades terá início a partir da atividade III.

Em ambas as modalidades, a aplicação da metodologia deverá contar, obrigatoriamente, com o suporte e o acompanhamento da Divisão de Gestão de Riscos e Controles (DGRC).

I - Definição do processo organizacional

A seleção dos processos a serem contemplados pela gestão de riscos compete aos gestores das unidades organizacionais, que deverão priorizá-los considerando os seguintes critérios:

- legislação vigente;
- recomendações dos órgãos de controle externos e da auditoria interna;
- alinhamento aos objetivos estratégicos da Instituição;
- impacto nas atividades finalísticas;
- relação com o atendimento a pessoas com deficiência ou que integram outros grupos vulnerabilizados;
- necessidades institucionais; e
- quantidade de retrabalho gerado pelo processo.

Essa priorização poderá ser realizada pela própria unidade ou mediante consulta institucional conduzida pela área demandante ou pela DGRC.

Na ausência de definição prévia dos processos prioritários, a unidade poderá utilizar a metodologia Business Impact Analysis - BIA (Análise de Impacto no Negócio), constante no Anexo I desta Metodologia Institucional, a qual possibilita a avaliação dos processos mediante dois critérios:

- Critério 1: impacto;
- Critério 2: tempo de retomada das operações.

A aplicação desta metodologia resulta na classificação dos processos por nível de criticidade, subsidiando o processo de priorização.

II - Mapeamento e modelagem do processo

Caso o processo não esteja mapeado e modelado, devem ser realizadas, sob a coordenação da Coordenadoria de Conformidade Institucional (CCI), as etapas necessárias para aplicação da metodologia de mapeamento e modelagem. Essa atividade visa assegurar a documentação adequada e a padronização das informações do processo que será submetido ao gerenciamento de riscos.

III - Organização da documentação

A DGRC deverá elaborar os instrumentos necessários à aplicação da metodologia, utilizando os modelos previamente estabelecidos conforme a modalidade adotada.

Para a aplicação da metodologia em processos organizacionais, os documentos a serem utilizados são:

- Análise de Contexto (Anexo II);
- Matriz SWOT (Anexo III);
- Planilha de Identificação e Análise de Riscos e Oportunidades (Anexo IV) e;
- Planilha do Plano de Tratamento de Riscos (Anexo V).

Para a aplicação da metodologia em Planos Institucionais, os documentos a serem utilizados são:

- Planilha de Identificação e Análise de Riscos e Oportunidades (Anexo IV) e;
- Planilha do Plano de Tratamento de Riscos (Anexo V).

A adoção de instrumentos padronizados assegura a uniformidade e a consistência das informações ao longo do processo de gerenciamento de riscos institucionais.

IV - Apresentação dos conceitos e metodologia de trabalho

Após a indicação, pela área, dos servidores que participarão do processo

de aplicação da MGR, a DGRC realizará reunião de alinhamento, para apresentar os principais conceitos e fundamentos da gestão de riscos aos servidores da unidade responsável pelo processo organizacional ou pelos objetivos estratégicos objeto de análise.

Essa etapa tem por finalidade assegurar o entendimento comum acerca dos conceitos de gestão de riscos e garantir o alinhamento necessário à execução das atividades subsequentes.

Concluída a apresentação inicial, os participantes darão início aos trabalhos de identificação e análise de riscos, conforme previsto nesta metodologia institucional.

V - Identificação, categorização e análise de riscos

Etapa na qual, mediante reuniões estruturadas de *brainstorming*, são identificados os potenciais eventos de risco. Nesta fase, deverão ser preenchidos os seguintes atributos da Planilha de Identificação e Análise de Riscos e Oportunidades (Anexo IV): eventos de risco, categorias, fontes, causas e consequências. Além disso, tratando-se de processo organizacional, a área responsável deverá preencher o Anexo II - Análise de Contexto e o Anexo III - Matriz SWOT.

Para realizar a identificação dos riscos, pode ser realizado o seguinte questionamento:

● Quais eventos podem comprometer (evitar, atrasar, prejudicar ou impedir) o atingimento de um ou mais objetivos do processo organizacional?

Os eventos identificados inicialmente poderão ser analisados, revisados, reorganizados, reformulados ou eliminados nesta etapa. Para tanto, poderá ser utilizada a seguinte questão norteadora:

● O evento constitui um risco capaz de comprometer o alcance de objetivo estratégico ou de objetivo relacionado ao processo organizacional analisado?

Para os eventos identificados e analisados como riscos, deverá ser indicada a **categoria** do risco, dentre as estabelecidas para a Unipampa:

- **Operacionais**: eventos que podem comprometer as atividades da Instituição ou de alguma unidade organizacional. Relacionam-se a processos

externos e internos, pessoas, infraestrutura e sistemas, podendo resultar em perdas decorrentes de falhas ou inadequações nesses elementos.

- **Conformidade**: eventos associados ao descumprimento da legislação brasileira, bem como das normas e resoluções internas da Instituição.
- **Estratégicos**: eventos relacionados ao insucesso na implementação das estratégias institucionais voltadas ao alcance dos objetivos estratégicos, da missão e das metas da Instituição.
- **Orçamentários/Financeiros**: eventos associados à insuficiência de recursos orçamentários e financeiros, que possam comprometer e/ou prejudicar a execução das atividades institucionais.
- **Imagem/Reputação**: eventos que possam afetar a imagem e a reputação da Instituição perante a sociedade, impactando sua credibilidade e comprometendo sua capacidade de alcançar seus objetivos.
- **Integridade**: eventos relacionados à corrupção, fraude, irregularidades, ilícitos, violações ou desrespeito a direitos, ou outros desvios éticos e de conduta que possam comprometer valores e padrões preconizados pelo órgão ou entidade ou impactar no atendimento das necessidades e do interesse público legítimos e no cumprimento dos objetivos institucionais.
- **Tecnologia da Informação**: eventos relacionados aos recursos de Tecnologia da Informação e Comunicação que possam comprometer o funcionamento institucional, a disponibilidade dos serviços ou a segurança das informações.

Os demais atributos podem ser identificados seguindo os seguintes conceitos:

- **Fonte**: refere-se ao elemento, substância, atividade ou condição que possui o potencial intrínseco de causar o dano ou dar origem ao risco. Representa a origem do risco, isto é, o ponto a partir do qual o risco emerge.
- **Causa**: consiste no motivo ou fator que pode promover a ocorrência do evento de risco. Corresponde aos fatores ou as condições subjacentes que, quando presentes, aumentam a probabilidade de o evento de risco se manifestar.
- **Consequência**: representa o resultado do evento de risco que afeta os objetivos institucionais ou do processo organizacional. Corresponde ao impacto negativo ou dano que a Instituição pode sofrer caso o risco se concretize, prejudicando ou impedindo o alcance dos objetivos estabelecidos.

VI - Avaliação de riscos

Etapa na qual são estimados os níveis dos riscos identificados, de modo que, mediante a análise da probabilidade e do impacto, seja possível determinar o risco inerente.

Nesta fase, deverão ser preenchidos, na Planilha de Identificação e Análise de Riscos e Oportunidades (Anexo IV), os seguintes atributos:

- probabilidade de ocorrência e,
- impacto em caso de ocorrência.

O risco inerente será calculado automaticamente pela multiplicação da probabilidade pelo impacto, resultando na classificação do nível de exposição ao risco.

Os quadros 1 e 2 trazem as escalas de probabilidade e impacto, respectivamente:

Quadro 1: Escala de probabilidade para eventos de risco

Probabilidade	Descrição da probabilidade, desconsiderando os controles	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, pois as circunstâncias indicam claramente essa possibilidade.	10

Fonte: Elaborado pelo CGR, com base em CGU (2018).

Quadro 2: Escala de impacto para eventos de risco

Impacto	Escala de impacto Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	**Mínimo** impacto nos objetivos estratégicos ou do processo.	1
Baixo	**Pequeno** impacto nos objetivos estratégicos ou do processo.	2

Médio	**Moderado** impacto nos objetivos do processo, porém recuperável.	5
Alto	**Significativo** impacto nos objetivos do processo, de difícil reversão.	8
Muito alto	**Catastrófico** impacto nos objetivos do processo, de forma irreversível.	10

Fonte: Elaborado pelo CGR, com base em CGU (2018).

A multiplicação entre os valores de probabilidade e impacto determina o nível do risco inerente, isto é, o nível do risco desconsiderando quaisquer controles existentes que possam reduzir a probabilidade de sua ocorrência ou a magnitude de seu impacto.

RI = NP x NI

em que:

RI = nível do risco inerente

NP = nível de probabilidade do risco

NI = nível de impacto do risco

Com base no resultado obtido, o risco poderá ser classificado conforme as faixas estabelecidas no Quadro 3.

Quadro 3: Classificação do Risco

Classificação	Faixa
Risco Baixo - RB	0 - 9,99
Risco Médio - RM	10 - 39,99
Risco Alto - RA	40 - 79,99
Risco Extremo - RE	80 - 100

Fonte: Elaborado pelo CGR, com base em CGU (2018).

A seguinte matriz representa os possíveis resultados da combinação das escalas de probabilidade e impacto.

Figura 1: Matriz de Riscos (Inerente)

Fonte: Elaborado pelo CGR, com base em CGU (2018).

Sobre o apetite a risco do processo organizacional

O nível de apetite a risco, definido como o nível de risco que a Instituição está disposta a aceitar, deverá ser estabelecido pelo CE. Uma vez definido, a unidade organizacional deverá observar que:

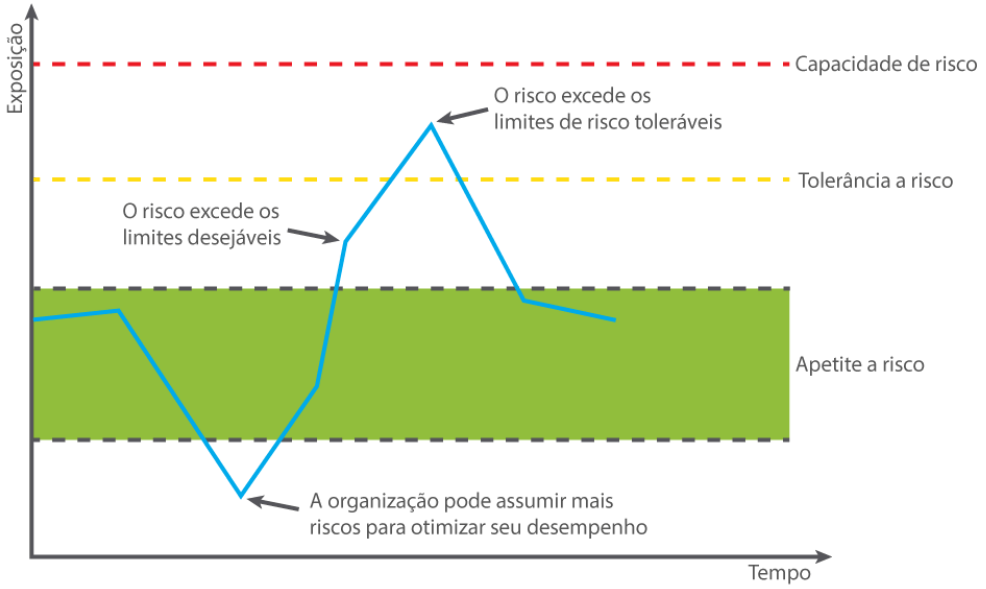
I. os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco poderão ser aceitos, sendo que eventual priorização para tratamento deverá ser devidamente justificada;

II. os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco deverão ser tratados e monitorados, sendo que eventual ausência de tratamento deverá ser devidamente justificada.

Relacionados ao conceito de apetite a risco, também se encontram os conceitos de tolerância e capacidade ao risco. O apetite representa o nível de risco que a organização deseja aceitar, enquanto a tolerância consiste no nível aceitável de variação em relação à realização dos objetivos.

Por sua vez, a capacidade de assumir riscos corresponde ao nível máximo de risco que a organização pode suportar na busca por seus objetivos (BRASILIANO, 2018), conforme apresentado na Figura 2.

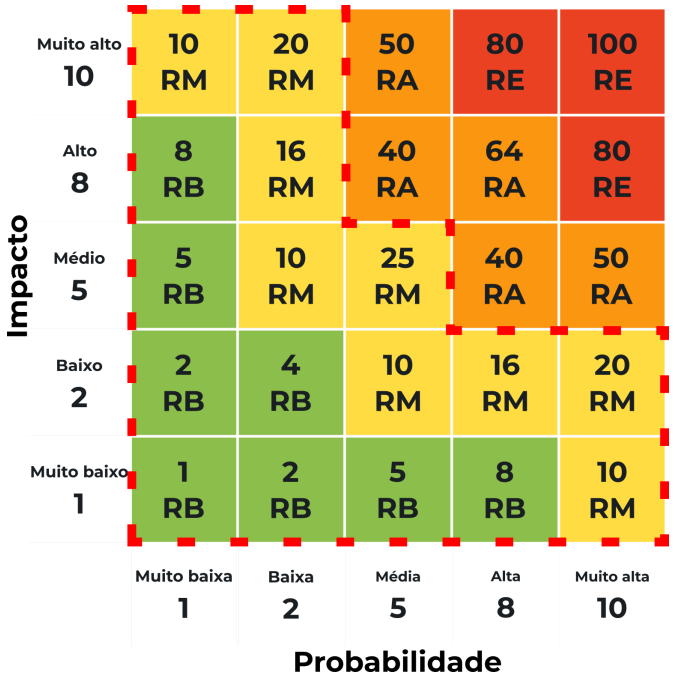
Figura 2: Apetite, Tolerância e Capacidade de Risco



Fonte: Adaptado de Instituto de Auditores Internos de España, 2015, p. 27.

Na figura 3, pode ser observado o apetite a risco que foi definido no âmbito da Unipampa.

Figura 3: Apetite a risco



Fonte: Elaborado pelo CGR, com base em CGU (2018).

VII - Identificação de oportunidades

Momento em que são identificadas as principais oportunidades relacionadas ao processo organizacional ou aos objetivos estratégicos, capazes de ampliar a capacidade institucional para o alcance de suas metas, bem como as respectivas ações para seu aproveitamento.

O registro das informações deverá ser realizado na Planilha de Identificação e Análise de Riscos e Oportunidades (Anexo IV), contemplando a descrição das oportunidades identificadas, categorias, fontes, origem da fonte (interna ou externa), probabilidade, impacto e as ações para aproveitá-las.

Os quadros a seguir trazem as escalas de probabilidade e impacto respectivamente, considerando as oportunidades:

Quadro 4: Escala de probabilidade para oportunidades

Probabilidade	Descrição da probabilidade	Peso
Muito baixa	**Improvável**. Em situações excepcionais, a oportunidade poderia se concretizar, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	**Rara**. De forma inesperada ou casual, a oportunidade poderá se concretizar, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	**Possível**. De alguma forma, a oportunidade poderá se concretizar, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	**Provável**. De forma até esperada, a oportunidade deverá se concretizar, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito alta	**Praticamente certa**. De forma inequívoca, a oportunidade se concretizará, pois as circunstâncias indicam claramente essa possibilidade.	10

Fonte: CGR, 2026.

Quadro 5: Escala de impacto para oportunidades

Impacto	Escala de impacto Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	**Benefício mínimo.** Pequena contribuição aos objetivos estratégicos ou do processo, com ganhos marginais.	1
Baixo	**Benefício baixo.** Contribuição limitada aos objetivos estratégicos ou do processo, com ganhos perceptíveis, porém restritos.	2
Médio	**Benefício moderado.** Contribuição relevante aos objetivos do processo,	5

	com ganhos claros e sustentáveis.	
Alto	**Benefício significativo.** Forte contribuição aos objetivos do processo, gerando vantagem competitiva ou melhoria expressiva de desempenho.	8
Muito alto	**Benefício transformador (ou máximo).** Contribuição decisiva aos objetivos estratégicos, com ganhos substanciais e duradouros para a organização.	10

Fonte: CGR, 2026.

VIII - Identificação e avaliação de controles e reavaliação dos riscos

Nesta etapa, para os riscos classificados como baixo e médio, adota-se o risco inerente apurado no momento da análise, dispensando-se a avaliação de controles.

Para os riscos classificados como alto e extremo, ou seja, aqueles situados acima do apetite a risco definido pela instituição, procede-se à identificação e análise dos controles preventivos e de atenuação já existentes, permitindo a determinação do risco residual.

Essa ação visa assegurar que recursos e esforços não sejam destinados à implementação de novos controles desnecessários, considerando a suficiência dos controles já aplicados. Para tanto, devem ser preenchidos os campos referentes aos controles preventivos, aos controles de atenuação e à avaliação dos controles, conforme descrito a seguir:

- **Controles preventivos:** são aplicados antes da ocorrência do evento de risco, com o objetivo de reduzir sua probabilidade de ocorrência e/ou minimizar seu impacto.
- **Controles de atenuação/recuperação:** são aplicados após a ocorrência do evento de risco, visando, principalmente, reduzir os impactos decorrentes do evento.

A dispensa da avaliação detalhada de controles aplica-se exclusivamente ao ciclo inicial de aplicação da metodologia, sendo obrigatória a sua verificação nas etapas subsequentes de revisão.

Após a identificação dos controles existentes, procede-se à avaliação do nível de efetividade de cada um deles. O quadro a seguir apresenta os níveis possíveis de avaliação:

Quadro 6: Níveis de avaliação dos controles internos existentes

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

Fonte: Elaborado pelo CGR, com base em CGU (2018).

O risco residual é calculado automaticamente pelo produto entre o valor do risco inerente e o fator de avaliação dos controles, representando o nível de exposição remanescente após a aplicação dos controles existentes.

RR = RI x FC

em que:

RR = nível do risco residual

RI = nível do risco inerente

FC = fator de avaliação dos controles existentes

O valor de risco residual pode fazer com que o risco se enquadre em uma faixa de classificação diferente da faixa definida inicialmente para o risco inerente, conforme figura a seguir:

Figura 4: Matriz de risco (residual)

Fonte: CGR, 2026.

Para fins de registro no sistema ForRisco, considerando que o mesmo não possui a funcionalidade de registro do risco residual, será considerada a seguinte conversão:

Quadro 7: Conversão probabilidade e impacto para risco residual

Risco residual	Risco inerente para cadastro no sistema ForRisco	
	Probabilidade	Impacto
0,2 até 8,0	Baixa	Baixo
9,6 até 25,0	Média	Médio
25,6 até 64,0	Alta	Alto

80,0 até 100,0	Muito alta	Muito alto

Fontes: CGR, 2026

A conversão dos valores de risco residual para as categorias de probabilidade e impacto adotadas no sistema ForRisco possui finalidade exclusivamente operacional, com o objetivo de adequar a representação dos riscos à estrutura técnica da ferramenta.

Tal conversão não altera o julgamento técnico originalmente atribuído ao risco residual, tampouco substitui a análise qualitativa realizada pelas unidades responsáveis, servindo apenas para fins de padronização, registro e acompanhamento sistêmico.

IX - Classificação, priorização e análise de riscos

Momento em que os eventos de risco são classificados conforme a matriz de riscos (risco baixo, médio, alto ou extremo) e é estabelecida a respectiva ordem de priorização. Riscos com o mesmo nível receberão priorização idêntica.

Nesta etapa, os eventos que não passaram pela identificação dos controles, terão como referência os valores do risco inerente, já para os demais, a referência será o risco residual.

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

Quadro 8: Priorização dos riscos

Classificação	Ação necessária	Exceção
Risco Baixo	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada 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	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve

	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.	ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco neste nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Extremo	Nível de risco muito além do apetite a risco. Qualquer risco neste nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo e pelo Comitê Estratégico.

Fonte: Elaborado pelo CGR, com base em CGU (2018).

Concluída a etapa de classificação e priorização dos riscos, a DGRC e a unidade responsável deverão realizar uma análise para identificar se, na avaliação das áreas envolvidas, existem eventos de risco que devam ser submetidos a reavaliação. Adicionalmente, todos os eventos de risco classificados como extremos deverão passar por revisão, a fim de assegurar que seus atributos foram corretamente definidos.

X - Definição de respostas aos riscos

Etapa na qual são estabelecidas as respostas aos riscos, de forma a adequar seus níveis ao apetite a risco estabelecido pela Instituição.

O tipo de tratamento deverá ser definido, em conformidade com o apetite ao risco institucional, dentre uma das seguintes opções: aceitar, compartilhar, evitar ou mitigar.

As medidas de tratamento deverão ser indicadas para os eventos de risco cujos tipos de tratamento sejam compartilhar, evitar ou mitigar.

Cada risco priorizado deverá ser associado a uma opção de tratamento. A escolha da opção dependerá do nível do risco, do contexto institucional ou do custo do controle, conforme apresentado no quadro a seguir:

Quadro 9: Opções de tratamento do risco

Opção de Tratamento	Descrição
Mitigar	Tratamento a ser realizado quando o risco é classificado como Alto ou Extremo. A implementação de controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos é a ação mais indicada para este caso.
Compartilhar	Os riscos podem ser compartilhados por meio de terceirização ou apólice de seguro, por exemplo. Normalmente ocorre com riscos classificados como Alto ou Extremo.
Evitar	Para riscos classificados como Alto ou Extremo, evitar é utilizado quando a implementação de controles não apresenta um bom custo/benefício, inviabilizando a mitigação. Para evitar um risco, pode-se encerrar um processo organizacional, porém, para que isso ocorra, é necessária a aprovação do CE.
Aceitar	A aceitação do risco se dá geralmente quando está nas faixas do apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.

Fonte: Elaborado pelo CGR, com base em CGU (2018).

Quando a opção de tratamento do risco for compartilhar ou mitigar, devem ser definidas medidas específicas de tratamento capazes de reduzir os níveis de probabilidade e/ou de impacto do risco, buscando enquadrá-lo nas faixas de apetite a risco da instituição (níveis "Baixo" ou "Médio"). Tais medidas devem ser formalmente registradas no campo de medidas de tratamento e no Plano de Tratamento de Riscos.

Para os eventos de risco cuja opção de tratamento for evitar, a área responsável deverá definir, no campo medidas de tratamento e no Plano de Tratamento de Riscos, as ações que, quando implementadas, sejam capazes de eliminar a possibilidade de ocorrência do evento.

XI - Plano de Tratamento de Riscos

Nesta etapa, define-se a forma pela qual será realizado o tratamento dos eventos de risco que possuem medidas de tratamento definidas. Essa ação se concretiza mediante o preenchimento da planilha "Plano de Tratamento de Riscos",

constante no Anexo V desta metodologia.

Devem ser preenchidos os seguintes atributos para cada medida de tratamento: unidade responsável, unidades corresponsáveis, responsável pela implementação, como será implementado, custo previsto, data prevista para início da implementação e data prevista para conclusão da implementação.

Além disso, nesta etapa deve-se definir a periodicidade da revisão do projeto, podendo ser estabelecida em 3 (três) meses, 6 (seis) meses ou 12 (doze) meses.

A implementação do Plano de Tratamento de Riscos envolve a participação da unidade responsável pelo processo organizacional e das unidades relacionadas como corresponsáveis em cada iniciativa, quando previstas.

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

XII - Análise dos riscos e medidas de tratamento

O gestor da unidade avalia se as medidas de tratamento propostas estão adequadas às necessidades e à viabilidade institucional, devendo sugerir as alterações que considerar necessárias.

XIII - Comunicação de eventos de risco

Riscos categorizados como "estratégicos" ou classificados como "extremos" devem ser comunicados à Reitoria. Já os riscos classificados como de “integridade” devem ser informados ao setor responsável pela Integridade na Instituição.

XIV - Cadastro de eventos de risco no sistema gerencial

Cadastrar os eventos de risco e seus respectivos atributos no sistema de apoio ao gerenciamento de riscos (ForRisco). Após o cadastro, comunicar a área responsável e encaminhar o manual do usuário desenvolvido pela DGRC.

XV - Formalização da finalização das atividades

Ao término dos trabalhos, a DGRC deverá formalizar, por meio do Sistema Eletrônico de Informações (SEI), a execução das atividades previstas na MGR.

XVI - Execução do plano de tratamento de riscos

Concluída a aplicação inicial da metodologia, a unidade responsável pelo processo ou pelos objetivos estratégicos deverá realizar a gestão de riscos, implementando as medidas de tratamento, realizando o monitoramento contínuo dos eventos de risco e registrando, no sistema de gestão (ForRisco), todas as ocorrências relacionadas aos riscos identificados. Em caso de dúvidas, a área responsável deverá consultar a DGRC para orientação.

XVII - Comunicação e monitoramento contínuos

Etapa transversal que perpassa todo o processo de gerenciamento de riscos, responsável pela integração de todas as instâncias envolvidas e pelo monitoramento permanente da própria Gestão de Riscos, visando ao seu aprimoramento contínuo.

A Matriz de Responsabilidade RACI foi adaptada e define Responsável, Autoridade, Consultado, Informado e Suporte para o processo de gerenciamento de riscos na Unipampa. Dentro do escopo de um projeto de gerenciamento de riscos, deve ser observada a Matriz de Responsabilidade RACI apresentada a seguir:

- Responsável (R): quem executa a atividade;
- Autoridade (A): quem aprova a atividade ou entrega. Pode delegar a função, mas mantém a responsabilidade final;
- Consultado (C): quem pode agregar valor ou é essencial para a implementação;
- Informado (I): quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.
- Suporte (S): quem pode prestar consultoria ou apoio no desenvolvimento da atividade.

Quadro 10: Matriz RACI

CE: Comitê Estratégico
DGRC: Divisão de Gestão de Riscos e Controles
DRU: Dirigente Responsável pela Unidade
RGR / ETD: Responsável pelo Gerenciamento de Riscos / Equipe Técnica Designada
SU: Servidores da Unipampa

	CE	DGRC	DRU	RGR/ETD	SU
Definição da modalidade (processo ou plano)	-	I	R	C, I	-
Definição do Processo Organizacional	-	S	A,R	C,I	-
Mapeamento e Modelagem do Processo	-	S	A,R	R	-
Organização da Documentação	-	R	I	I	-
Apresentação dos Conceitos e Metodologia de Trabalho	-	R	I	I	-
Identificação e Análise de Riscos	-	S	C, I, R	R	-
Identificação de Oportunidades	-	S	C, I, R	R	-
Avaliação de Riscos	-	S	C, I, R	R	-
Classificação, Priorização e Análise de Riscos	-	S	C, I, R	R	-
Reavaliação de Riscos	-	R	C, I, R	R	-
Definição de Respostas aos Riscos	-	S	C, I, R	R	-
Plano de Tratamento de Riscos	-	S	C, I, R	R	-
Análise dos Riscos e Medidas de Tratamento	-	S	R	C, I	-
Comunicação de Eventos de Risco	I	R	I	I	-
Cadastramento de Eventos de Risco no Sistema Gerencial	-	R	I	I	-
Formalização da Finalização das Atividades	I	R	I	I	-
Execução do Plano de Tratamento de Riscos	-	C, I	R	R	-
Comunicação e Monitoramento Contínuos	-	C, I	R	R	R

Fonte: Elaborado pelo CGR, com base em CGU (2018).

O monitoramento, no âmbito do gerenciamento de riscos, deverá ser conduzido pela unidade gestora do respectivo processo organizacional ou, quando se tratar de planos institucionais, pela área responsável pelo objetivo estratégico correspondente, com vistas 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 de Riscos;
- Identificar os riscos emergentes.

A PGR/Unipampa delega também, em seu art. 10, a todos os servidores da Instituição, a responsabilidade de monitorar os níveis de riscos e suas medidas de tratamento.

Mudanças identificadas durante o monitoramento devem ser encaminhadas à DGRC, a quem compete supervisionar os resultados de todos os projetos de gerenciamento de riscos já aplicados nos processos organizacionais ou planos institucionais.

Anualmente a DGRC elaborará o Relatório de Monitoramento da Gestão de Riscos da Unipampa com a consolidação desses resultados, que deve ser encaminhado, no mínimo, uma vez por ano ao CE.

A aplicação da metodologia para processos organizacionais deverá contemplar, ainda, o preenchimento da Matriz SWOT do processo e do Documento de Entendimento de Contexto.

Etapa 2: Revisão

Esta etapa será realizada periodicamente, após o decurso do período estabelecido na primeira etapa, o qual poderá ser de 3 (três) meses, 6 (seis) meses ou 12 (doze) meses. Durante o processo de revisão, serão desenvolvidas as seguintes atividades:

I - Análise do monitoramento e execução do plano de tratamento

A primeira atividade a ser desenvolvida na revisão periódica é a de identificar as dificuldades, os desafios e as oportunidades na aplicação da gestão de riscos ao longo do período. Caso a área não tenha realizado as medidas de tratamento previstas para o período, as mesmas devem ser justificadas e avaliadas quanto a necessidade de manutenção e urgência na execução.

II - Identificação e avaliação de novos eventos de riscos

Caso sejam identificados novos eventos de risco que surgiram ao longo do período, estes deverão passar por todas as atividades correspondentes listadas na etapa 1 da metodologia.

III - Avaliação das ocorrências

Havendo registro de ocorrências, estas deverão ser analisadas a fim de verificar se algum evento de risco demanda reavaliação. Tais registros podem estar relacionados à materialização de eventos já identificados ou à necessidade de implementação de novas medidas de controle ainda não previstas.

IV - Avaliação de riscos

A área gestora deverá realizar uma revisão sistemática dos eventos de risco identificados, visando verificar a necessidade de atualização das fontes, causas e consequências, bem como reavaliar os níveis de probabilidade e impacto anteriormente atribuídos.

V - Avaliação dos controles

Considerando que a dispensa da avaliação de controles para riscos baixo e médio aplica-se apenas ao ciclo inicial (Etapa 1 desta metodologia), nesta atividade todos os eventos de risco, independentemente do nível de risco inerente e residual, passarão pela identificação ou revisão dos controles preventivos e de atenuação existentes, bem como pela avaliação de sua efetividade, conforme previsto na atividade "Identificação e avaliação de controles e reavaliação dos riscos" da Etapa 1

desta metodologia.

A avaliação dos controles deverá observar a seguinte ordem de execução:

1. Identificação e avaliação de controles: para eventos de risco cujos controles ainda não tenham sido identificados, procede-se à identificação dos controles preventivos e de atenuação existentes e à respectiva avaliação de efetividade.
2. Revisão e reavaliação de controles: para eventos de risco cujos controles já tenham sido previamente identificados, procede-se à revisão e reavaliação. Nesta etapa, as medidas de tratamento definidas pela área gestora em ciclos anteriores e já implementadas deverão ser incorporadas ao rol de controles existentes e consideradas na avaliação.

Após a conclusão desta atividade, os registros deverão ser atualizados no sistema ForRisco, mantendo-se o histórico de cada etapa em planilhas eletrônicas para fins de rastreabilidade e auditoria.

VI - Revisão de oportunidades

Proceder à revisão das oportunidades elencadas, a fim de identificar sua ocorrência e respectivo aproveitamento, realizando os devidos registros. Novas oportunidades poderão ser identificadas neste momento.

VII - Formalização da finalização das atividades

Ao término dos trabalhos, a DGRC deverá formalizar, por meio do SEI, a execução das atividades previstas na Etapa 2 da MGR.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Controladoria-Geral da União. **Metodologia de Gestão de Riscos**. Brasília, DF: CGU, 2018. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf. Acesso em: 2 out. 2020.

BRASILIANO, Antonio Celso Ribeiro. **Inteligência em riscos**: gestão integrada em

riscos corporativos. 2. ed. rev. e ampl. São Paulo: Sicurezza, 2018.

INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA. **Caso práctico sobre apetito de riesgo**. Madri: La Fábrica de Pensamento, 2015. Disponível em: https://auditoresinternos.es/uploads/media_items/150629-caso-pr%C3%A1ctico-sobre-apetito-de-riesgo.original.pdf. Acesso em: 10 mar. 2021.

UNIVERSIDADE FEDERAL DO PAMPA. Conselho Universitário. **Resolução CONSUNI/UNIPAMPA nº 345, de 19 de julho de 2022**: institui a Política de Gestão de Riscos da Universidade Federal do Pampa. Bagé, RS: UNIPAMPA, 2022. Disponível em: https://sites.unipampa.edu.br/consuni/files/2022/07/res-_345_2022-politica-de-gestao-de-riscos.pdf. Acesso em: 23, nov. 2025.

Anexos

https://sites.unipampa.edu.br/gestao-de-riscos/metodologia-de-gestao-de-risco/