unipampa Universidade Federal do Pampa

Metodologia de Gestão de Riscos

2023

PROPOSTA - METODOLOGIA DE GESTÃO DE RISCOS - COMITÊ DE GESTÃO DE RISCOS - 04/03/2021

METODOLOGIA DE GESTÃO DE RISCOS

CONCEITOS

Para fins deste documento, consideram-se os seguintes conceitos (extraídos do art. 2º da Política de Gestão de Riscos da UNIPAMPA):

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: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados;

VIII - meta: alvo ou propósito com que se define um objetivo a ser alcançado;

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

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

METODOLOGIA DE GESTÃO DE RISCOS

A Metodologia de Gestão de Riscos da Unipampa objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da Gestão de Riscos na Universidade, por meio da definição de um processo de gerenciamento de riscos, seguindo as seguintes etapas:

I - definição do processo organizacional a ser contemplado pela gestão de riscos. A escolha dos processos prioritários ficará a cargo dos responsáveis pelos setores organizacionais, de acordo com critérios previstos nessa metodologia ou pelo gestor, desde que, devidamente justificado.

II - realização do mapeamento e da modelagem do processo: realizar, sob gerência do Escritório de Processos, as etapas necessárias para formalização das atividades e características dos processos que passarão pelo gerenciamento de riscos.

III - elaboração do plano de gestão de riscos: consiste na confecção ou revisão do plano por parte do gestor, com o objetivo de desenvolvê-lo ou adequá-lo às necessidades do processo previamente definido.

IV – entendimento do contexto: etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos;

V – identificação e análise de riscos: etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais e analisados de acordo com possíveis causas e consequências.

VI - análise da identificação dos riscos: momento em que o gestor da área revisa as atividades anteriores, desenvolvidas pela equipe técnica, com o objetivo de validar as informações e, se necessário for, propor alterações.

VII – avaliação de riscos e controles: etapa em que são estimados os níveis dos riscos identificados;

VIII – priorização de riscos: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;

IX – definição de respostas aos riscos: etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas;

X - análise dos riscos e medidas de tratamento: o gestor da unidade avalia se as medidas de tratamento estão de acordo com a necessidade e a viabilidade institucional.

XI - realização de reavaliação do risco: para riscos específicos ou classificados como baixo ou extremo, uma reavaliação deve ser feita para confirmar a classificação e os impactos desse risco (mantida a classificação como extremo). A reavaliação se dá por parte da Unidade de Gestão de Riscos, que acompanhará o processo de implementação do plano de tratamento.

XII - a implementação do plano de tratamento é realizada pela equipe técnica e representa a efetiva aplicação de alternativas para tratar o risco de acordo com as respostas definidas anteriormente.

XIII – comunicação e monitoramento: etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria Gestão de Riscos, com vistas a sua melhoria.

A modelagem do processo de gerenciamento de riscos da UNIPAMPA, com seus respectivos atores e atividades pode ser acessada através do link: https://processos.unipampa.edu.br/proplan/gestao_de_riscos

A Metodologia de Gestão de Riscos da Unipampa é orientada ao processo organizacional e obedece a um modelo de aplicação descentralizado. Ou seja, as unidades organizacionais podem executar os processos de gerenciamento de riscos em processos sob sua responsabilidade, desde que obedecidas as diretrizes e orientações apresentadas neste documento. Os resultados desses processos devem ser informados à Unidade de Gestão de Riscos, que os reportará ao Comitê Estratégico. Além disso, a Unidade de Gestão de Riscos deve realizar a reavaliação dos riscos classificados como baixo e extremo.

DEFINIÇÃO DO PROCESSO ORGANIZACIONAL

Definir o processo organizacional que passará pelas atividades de gestão de riscos, priorizando-o de acordo com a necessidade da unidade, alinhado aos objetivos estratégico, às recomendações de auditoria, necessidade de retrabalho ou impacto na atividade fim. Caso o processo não esteja publicado no repositório de processos, deverá passar pelas etapas de mapeamento e modelagem, com acompanhamento do Escritório de Processos.

Caso a área não tenha certeza na definição dos seus processos prioritários, poderá utilizar a metodologia Business Impact Analysis - BIA, ou Análise do Impacto no Negócio, a qual possibilita a avaliação dos processos através de dois critérios: impacto e tempo de retorno da operação. Ao aplicar a metodologia, tem-se como resultado a escala de criticidade dos processos, facilitando a priorização.

Quadro 1: Análise do Impacto dos Processos

Avaliação do impacto	Peso
Imagem/reputação	4
Orçamentário	4
Conformidade	4
Operacional	4
Imagem/Reputação	**Pontuação**
Repercussão prolongada ou não na mídia internacional: Possível boicote aos serviços, manifestações de massa. Preocupação pública, da mídia, da política nacional e internacional. Restrição ou revogação de uma ou múltiplas licenças de funcionamento. Também tende a mobilizar grupos de ação. Atenção para reações de sindicatos de trabalhadores e de redes sociais e possíveis greves de funcionários. Viabilidade financeira ameaçada. Repercussão internacional no ambiente organizacional.	5
Repercussão nacional: Preocupação pública, da mídia, da política nacional. Repercussões junto a autoridades governamentais e representantes de nível nacional e/ou regional; possibilidade de medidas restritivas à organização. Restrição ou revogação de uma ou múltiplas licenças de funcionamento. Também tende a mobilizar grupos de ação. Atenção para possíveis reações de sindicatos de trabalhadores e de redes sociais. Repercussão nacional no ambiente organizacional.	4

Repercussão regional: Preocupação pública, da mídia, da política dentro do estado. Pode haver envolvimento adverso de grupos de ação e/ou do governo local. Atenção para possíveis reações de sindicatos de trabalhadores e de redes sociais. Repercussão local no ambiente organizacional.	3
Repercussão local: Envolve algum interesse público local do município e/ou alguma atenção política local e/ou mídia local, com possíveis aspectos adversos para as operações. Repercussão limitada no ambiente organizacional.	2
Sem repercussão: Situações nas quais não há o conhecimento do público, mas não existe interesse público. A ocorrência não ultrapassa os limites internos da organização e/ou de suas Unidades.	1
Orçamentário	Pontuação
Catastrófica: Acima de R$ 1.500.000,00	5
Crítica: De R$ 1.000.000,01 a R$ 1.500.000,00	4
Grave: De R$ 500.000,01 a R$ 1.000.000,00	3
Moderada: De R$ 100.000,01 a R$ 500.000,00	2
Leve: Até R$ 100.000,00	1
Operacional	Pontuação
Massivo: Impacta muito fortemente macroprocessos finalísticos.	5
Severo: Impacta macroprocessos finalísticos de forma direta.	4
Moderado: Impacta levemente macroprocessos finalísticos.	3
Leve: Impacta somente macroprocessos de apoio e gerenciamento.	2
Insignificante: Não impacta nada.	1
Conformidade	Pontuação
Catastrófica: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na Instituição, havendo descumprimento nos procedimentos ou legislação e ainda em que não há argumentos e provas para inibir a aplicação de multas ou pagamentos e indenizações, havendo também possibilidade da suspensão das atividades da empresa, prisão de servidores. Uma ou múltiplas ações judiciais e multas de valor alto. Ação judicial muito séria incluindo ações populares. Encerramento legal das operações.	5
Crítica: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na Instituição, havendo descumprimento dos procedimentos ou legislação e ainda em que não há argumentos e provas para inibir a aplicação de multas ou pagamentos e indenizações.	4
Graves: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na Instituição, havendo pequenas falhas nos procedimentos ou legislação e ainda em que há argumentos e provas para inibir parcialmente a aplicação de multas ou pagamentos indenizações.	3
Moderada: Questões legais em que há possibilidade de abertura de fiscalização/investigação/processo na Instituição, porém há argumentos e provas contundentes para inibir a aplicação de multas ou pagamento de indenizações.	2
Leve: Questões legais sem qualquer impacto.	1

Quadro 2: Cálculo do Nível de Impacto

Determinação do nível de impacto		
$\text{Nível de impacto} = \frac{\text{Imagem/Reputação + Orçamentário + Operacional + Conformidade}}{\text{16 (soma dos pesos 4+4+4+4)}}$		
Nível de impacto		
Grau de Impacto	Escala	Nível de Impacto
4,51 – 5,00	5	Massivo
3,51 – 4,50	4	Severo
2,51 – 3,50	3	Moderado
1,51 – 2,50	2	Leve
1,00 – 1,50	1	Muito leve

Como parte da avaliação do impacto, estimou-se por quanto tempo o processo analisado poderia ficar indisponível. No Quadro a seguir consta a escala de valoração que foi utilizada.

Quadro 3: Escala de Valoração

Avaliação do tempo de tolerância	Pontuação
Até 1 mês	6
De 1 a 3 meses	5
De 3 a 6 meses	4
De 6 a 9 meses	3
De 9 a 12 meses	2
Mais de 12 meses	1

O resultado do cruzamento do nível de impacto com o nível de avaliação da tolerância ao tempo é uma matriz, que define o nível de criticidade de cada processo.

Quadro 4: nível de criticidade

Críticos	Moderados	Leves
Prioritário: Não pode parar, é primordial e deve possuir uma atenção especial dos gestores.	Segunda prioridade: Possui um nível de importância média, devendo cada gestor ter um senso de urgência no tratamento.	Terceira prioridade: Pode ser considerado como suporte para os processos, atividades ou áreas consideradas críticas e moderadas.

MAPEAMENTO E MODELAGEM DE PROCESSOS

O mapeamento e a modelagem de processos na Unipampa segue metodologia definida pelo Escritório de Processos, setor responsável por definir as diretrizes, coordenar e auxiliar o desenvolvimento das atividades. A etapas que as áreas devem seguir para realizar o mapeamento e a modelagem de seus processos são:

Elaboração da carta de serviços: a carta visa informar aos cidadãos quais os serviços prestados pelo setor, como acessá-los e obtê-los. Além disso, contempla os padrões e os compromissos de atendimento.

Definição e priorização dos processos: nessa etapa deverá ser feita a definição dos processos do setor, sendo necessária a organização dos mesmos em uma ordem que permita identificar aqueles que deverão ser trabalhados de forma prioritária. Nesse momento, podem ser priorizados os processos que o setor entende que oferecem mais riscos.

Mapeamento do processo: consiste em descrever as atividades que o processo possui, bem como identificar questões que interferem no processo, os atores, a dependência de outros processos, questões legais, regimento e resoluções internas.

Modelagem do processo: o processo é representado, com auxílio de software específico e tomando como padrão a notação BPMN. Inicialmente trabalha-se na modelagem As Is, que representa o estado atual do processo. Após, faz-se a modelagem To Be, que representará o processo com as melhorias e otimizações identificadas pelos atores.

Validação do processo: a validação do processo será realizada pelo Escritório de Processos, em conjunto com a área responsável, contemplando os padrões textuais e de notação do BPM.

Manualização e publicação: consiste em elaborar toda documentação relativa ao mesmo, tais como: fluxo do processo, procedimentos, instruções de trabalho, documentação utilizada e atribuições sobre o trabalho a ser desenvolvido.

Acompanhamento do processo: o acompanhamento do processo se dará através de análise contínua por parte da área e periodicamente com o apoio do escritório de processos.

ELABORAR/REVISAR PLANO DE GESTÃO DE RISCOS

O Plano de Gestão de Riscos da unidade, deve estar de acordo com a metodologia de gestão de riscos institucional e contemplar os Planos de Tratamento (Anexo II) nos processos de gerenciamento de riscos e associado às iniciativas do PDI que impactam no processo definido.

Nesse momento o gestor da Unidade Organizacional deverá indicar a equipe técnica que atuará no processo de gestão de riscos, bem como o responsável pela gestão do risco na unidade.

ENTENDER O CONTEXTO

Nesta etapa, o processo organizacional e seus objetivos são analisados à luz de seus ambientes interno e externo, identificando ao 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;
- Modelagem 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. Para identificação dos objetivos, pode-se buscar responder à questão "O que deve ser atingido nas diversas dimensões para se concluir que o processo ocorreu com sucesso?";
- Relação de Objetivos Estratégicos da Unipampa alcançados pelo processo;
- Periodicidade máxima do ciclo do processo de gerenciamento de riscos. A unidade deve propor o prazo de revisão para um novo gerenciamento de riscos do processo organizacional, seguindo normativas internas, ou na falta dessas, atendendo o limite máximo de 1 ano.
- Unidade demandante do processo de gerenciamento de riscos no processo organizacional (a própria unidade ou o Comitê de Gestão Estratégica, por exemplo);
- 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, regulamentos e normativas internas relacionadas 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;

IDENTIFICAÇÃO E ANÁLISE DOS RISCOS

Considerando o resultado da etapa de Entendimento do Contexto, o fluxo do processo organizacional e a partir da experiência da equipe técnica designada deve-se construir 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 da seguinte pergunta:

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

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;
- Categoria do risco, dentre as definidas para a UNIPAMPA:
  - Riscos operacionais: podem comprometer as atividades da instituição ou de algum setor. Além de estarem relacionados com processos externos, podem ser associados a possibilidade de perdas resultantes de problemas nos processos internos, pessoas, infraestrutura e sistemas.
  - Riscos de conformidade: associados ao cumprimento da legislação brasileira e das normas e resoluções internas.
  - Riscos estratégicos: estão relacionados ao insucesso na aplicação das estratégias institucionais que visam o atingimento dos objetivos estratégicos, a missão e as metas da instituição.
  - Riscos orçamentários/financeiros: situação em que a instituição pode ficar sem recursos orçamentários, prejudicando assim a realização das suas atividades.
  - Riscos de imagem/reputação: relacionam-se com a imagem e reputação da instituição perante a sociedade, podem prejudicar a capacidade do órgão de atingimento dos seus objetivos.
  - Riscos de integridade: eventos relacionados com a corrupção, fraude, irregularidades ou desvio de conduta por parte do servidor.
  - Riscos de Tecnologia da Informação: relacionados aos recursos de Tecnologia da Informação e Comunicação e que podem comprometer o funcionamento da instituição ou comprometer a segurança das informações.
- 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.

Para realizar o registro de identificação e análise de riscos, a unidade organizacional deverá utilizar o Anexo I deste documento, até que haja a definição de outra ferramenta.

AVALIAÇÃO DA IDENTIFICAÇÃO DOS RISCOS

Nesta etapa, o gestor responsável pela unidade organizacional irá verificar se a etapa anterior, de identificação e análise dos riscos está de acordo com as necessidades estratégicas, táticas ou operacionais do setor e da instituição, se os riscos foram categorizados corretamente e se há necessidade de complementação quanto às causas, consequências, controles preventivos e controles de atenuação e recuperação dos riscos.

Caso haja necessidade de melhorias, o gestor deverá retornar para a equipe técnica complementar com as informações necessárias. Por outro lado, estando de acordo, o gestor

solicita à equipe técnica a continuidade do processo, passando para a etapa de avaliação dos riscos e controles.

AVALIAÇÃO DOS RISCOS E CONTROLES

Nesta etapa, são calculados os níveis dos riscos identificados pela equipe técnica designada, a partir de critérios de probabilidade e impacto. Os quadros 5 e 6 trazem as escalas de probabilidade e impacto, respectivamente:

Quadro 5: Escala de Probabilidade

Probabilidade	Escala de 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, as circunstâncias indicam claramente essa possibilidade.	10

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

Quadro 6: Escala de Impacto

Impacto	Escala de Impacto Descrição do impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	1
Baixo	Pequeno impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	2
Médio	Moderado impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	5
Alto	Significativo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade), porém recuperável.	8
Muito alto	Catastrófico impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade), de forma irreversível.	10

Fonte: Metodologia de Gestão de Riscos (CGU, 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.

RI = NP x NI

em que:

RI = nível do risco inerente

NP = nível de probabilidade do risco

NI = nível de impacto do risco

A partir do resultado do cálculo, o risco pode ser classificado dentro das seguintes faixas: Quadro 7: Classificação do Risco

Quadro 7: 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

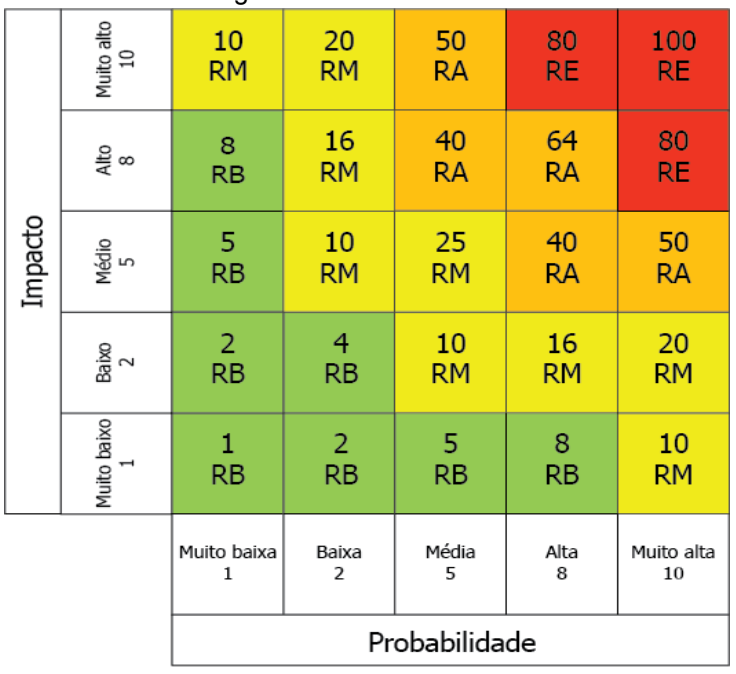
Fonte: Metodologia de Gestão de Riscos (CGU, 2018).

Revisão do processo de avaliação dos riscos

Devido à subjetividade envolvida deve-se realizar uma segunda classificação a fim de atenuar alguns erros, como por exemplo, erros de fadiga (a avaliação de vários riscos pode refletir em uma análise equivocada por parte do respondente) e de incompreensão de significado dos enunciados de riscos (causando interpretações inadequadas dos enunciados e consequentes distorções nas avaliações).

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

Figura 1: Matriz de Riscos



Fonte: Metodologia de Gestão de Riscos (CGU, 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 8 mostra os níveis de avaliação da eficácia dos controles existentes:

Quadro 8: 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
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: Metodologia de Gestão de Riscos (CGU, 2018).

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

RR = 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 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.

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: 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. Esses riscos devem passar pelo subprocesso de reavaliação do risco.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Médio	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais. Esses riscos devem passar pelo subprocesso de reavaliação do risco.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco neste nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Extremo	Nível de risco muito além do apetite a risco. Qualquer risco neste nível deve ser objeto de reavaliação, seguindo o subprocesso de reavaliação do risco.	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: Metodologia de Gestão de Riscos (CGU, 2018).

Sobre o Apetite a Risco do Processo Organizacional

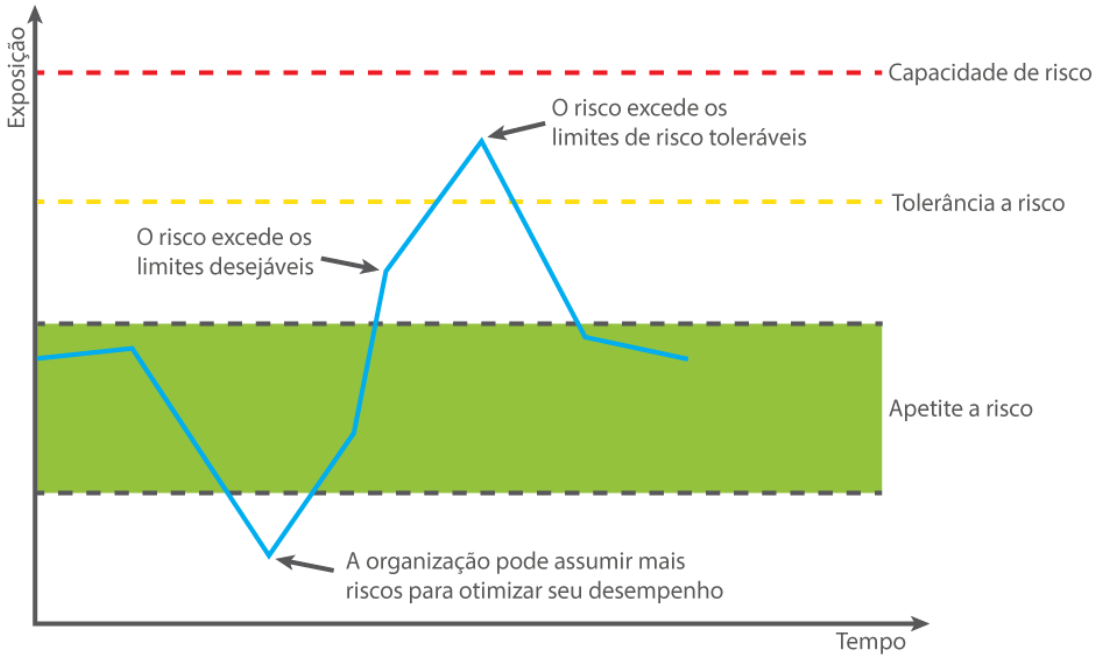
O nível de apetite a risco (nível de risco que a instituição está disposta a aceitar) deve ser definido pelo Comitê Estratégico. Uma vez definido, a unidade declara que:

- todos os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco podem ser aceitos, e uma possível priorização para tratamento deve ser justificada;

- todos os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco serão tratados e monitorados, e uma possível falta de tratamento deve ser justificada.

Relacionados ao conceito de apetite a risco, estão os conceitos de tolerância e capacidade ao risco. O apetite é o nível de risco que a organização quer aceitar, já a tolerância é o nível aceitável de variação referente à realização dos objetivos. Por sua vez, a capacidade de assumir riscos será o nível máximo de risco que a organização pode suportar na perseguição aos seus objetivos (BRASILIANO, 2018), conforme apresentado na figura 2.

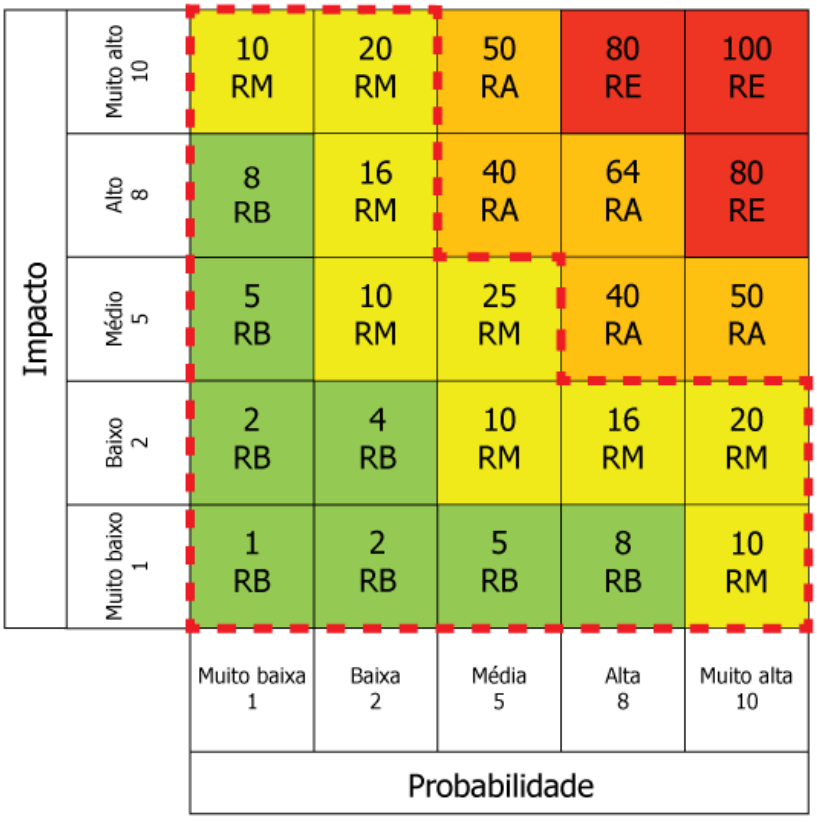
Figura 2: Apetite, Tolerância e Capacidade de Risco



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: Metodologia de Gestão de Riscos (CGU, 2018).

Sobre o Risco Extremo

Além dos riscos classificados como baixo e extremo, riscos com as outras classificações (médio e alto) podem ser objeto da reavaliação, desde que indicados pelo dirigente máximo da unidade.

O Anexo I deste documento traz o modelo de planilha para o registro de informações produzidas na etapa de Priorização de Riscos

DEFINIÇÃO DE RESPOSTAS AOS RISCOS

Esta etapa objetiva definir as opções e as medidas de tratamento (controles) para os riscos priorizados na etapa anterior.

Cada risco priorizado deve ser relacionado a uma opção de tratamento. A escolha da opção depende do nível do risco, contexto da Instituição ou custo do controle, conforme apresenta o quadro 10.

Quadro 10: 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 Comitê Estratégico.
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: Metodologia de Gestão de Riscos (CGU, 2018).

Se a opção de tratamento do risco for MITIGAR, devem ser definidas medidas de tratamento para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou 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:

- Iniciativa, com a proposta de projeto ou ação que implementará um conjunto de medidas de tratamento;
- Medida(s) de tratamento contemplada(s) na iniciativa e o risco relacionado que deseja tratar;
- Objetivos/benefícios esperados por medida de tratamento;
- Unidade organizacional responsável pela implementação da iniciativa;

• Unidades organizacionais corresponsáveis pela implementação da iniciativa, ou seja, unidades envolvidas na implementação da medida de tratamento;

• Servidor(es) ou cargo(s) responsáveis pela implementação;

• Breve descrição sobre a implementação;

• Custo estimado para a implementação (opcional);

• Data prevista para início da implementação;

• Data prevista para o término da implementação;

• Situação da iniciativa.

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

Se as iniciativas definidas no Plano de Tratamento envolverem mais de uma unidade, o responsável pelo processo de gerenciamento de riscos deve encaminhar a proposta de Plano para que essas unidades validem as iniciativas de que participaram.

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

ANALISAR RISCOS E MEDIDAS DE TRATAMENTO

Os resultados das etapas anteriores do processo de gerenciamento de riscos (entendimento 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 dirigente máximo da unidade organizacional (Pró-Reitor, Diretor).

Após a aprovação desses resultados, o responsável pelo processo de gerenciamento de riscos ou o dirigente da unidade deve:

• Encaminhar esses resultados à Unidade de Gestão de Riscos;

• 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.

IMPLEMENTAR O PLANO DE TRATAMENTO

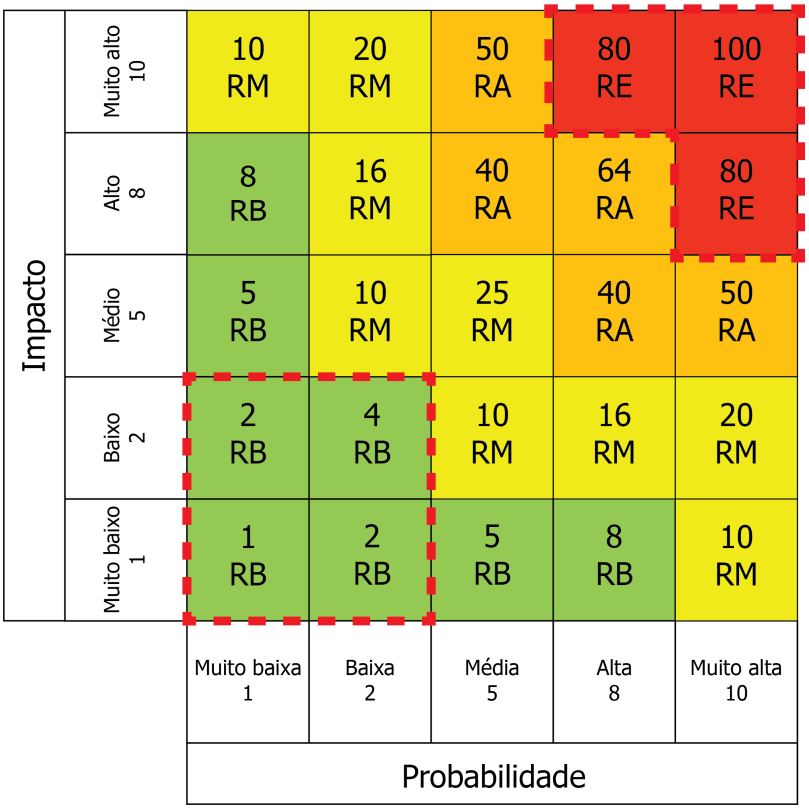
A implementação do Plano de Tratamento envolve a participação da unidade organizacional responsável pelo processo organizacional e das unidades relacionadas como corresponsáveis em cada iniciativa, se previstas.

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.

REAVALIAÇÃO DO RISCO

Riscos residuais classificados como “baixo” e “extremo” deverão ser reavaliados com a participação efetiva da Unidade de Gestão de Riscos (figura 4).

Figura 4. Riscos que devem ser reavaliados



Fonte: Comitê de Gestão de Riscos - UNIPAMPA

Essa reavaliação seguirá os passos descritos a seguir:

a) **Análise prévia da unidade de gestão de riscos:** a unidade realizará a compilação de todos os riscos identificados e os priorizará para a reavaliação de acordo com a sua classificação, respeitando a seguinte ordem de prioridade: Extremo e Baixo.
b) **Reavaliação da unidade de gestão de riscos e equipe técnica responsável:** após a priorização, a unidade de gestão de riscos se reunirá com a equipe técnica responsável e em conjunto, farão a revisão da classificação do risco.
c) **Revisão por parte do gestor da unidade:** os riscos que, após a reavaliação, mantiverem-se como Extremo, deverão passar por avaliação do gestor da unidade, que poderá subsidiar a unidade de gestão de riscos e a equipe técnica com informações que possam impactar no resultado da reavaliação.
d) **Ciência do Comitê Estratégico:** se após essas etapas, o risco se mantiver com a classificação de Extremo, será enviado ao Comitê Estratégico, que deverá indicar ações que devem ser realizadas para tratar o risco.

O sub-processo de reavaliação dos riscos pode ser acessado através do link

https://processos.unipampa.edu.br/proplan/gestao_de_riscos. Os resultados da reavaliação subsidiarão a priorização quanto à alocação de recursos para o atingimento de objetivos institucionais, que poderá refletir na revisão dos Planos de Tratamento dos riscos propostos pelas unidades.

COMUNICAÇÃO E MONITORAMENTO

Durante as etapas do processo de gerenciamento de riscos, o Comitê de Gestão Estratégica, a Unidade de Gestão de Riscos e os responsáveis pelo gerenciamento de riscos dos processos organizacionais, deverão manter fluxo constante de informações entre si.

Dentro do escopo de um processo de gerenciamento de riscos, deve ser observada a Matriz de Responsabilidade RACI apresentada no quadro 11.

A Matriz de Responsabilidade RACI, foi adaptada e define Responsável, Autoridade, Consultado, Informado e Suporte para o processo de gerenciamento de riscos na UNIPAMPA. Durante as etapas do processo de Gerenciamento de Riscos, a comunicação deve ser realizada conforme a matriz a seguir:

- Responsável (R): quem executa a atividade;
- Autoridade (A): quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade;
- 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 11: Matriz RACI

	Comitê Estratégico	Unidade de Gestão de Riscos / EPROC	Dirigente da Unidade	Responsável pelo Gerenciamento de Riscos / Equipe Técnica Designada	Servidores da Unipampa
Definir o processo organizacional	I	S	A,R	C,I	
Elaborar/Revisar o plano de gestão de riscos da unidade	I	S	A,R	C,I	I
Entender o contexto		S	A,C	R	C
Identificar e analisar riscos		S	A,C	R	C
Analisar identificação dos	I	S	A,R	C,I	

riscos					
Avaliar riscos e controles		S	A,C	R	C
Priorizar Riscos		S	A,C	R	C
Definir respostas aos riscos		S	A,C	R	C
Analisar riscos e medidas de tratamento	I	S	A,R	C,I	
Implementar o plano de tratamento		S	A,C	R	C
Realizar reavaliação do risco	A	R	C,I	C,I	
Monitorar	A	S	A,R	C,I	R

Fonte: Metodologia de Gestão de Riscos (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.

A PGR/UNIPAMPA delega também, em seu art. 9º, 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 Unidade de Gestão de Riscos, a quem compete supervisionar os resultados de todos os processos de gerenciamento de riscos já realizados nos processos organizacionais da UNIPAMPA.

Semestralmente, a Unidade de Gestão de Riscos 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 Estratégico.

Além disso, a Unidade Organizacional 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 Comitê Estratégico.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Ministério da Transparência e Controladoria-Geral da União. Metodologia de Gestão de Riscos. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf. Acesso em 02 de outubro de 2020.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. Metodologia de Gestão de Riscos - Manual. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/institucionais/arquivos/cgu-metodologia-gestao-riscos-2018.pdf. Acesso em 02 de outubro de 2020.

BRASILIANO, Antonio Celso Ribeiro. Inteligência em riscos: gestão integrada em riscos corporativos. 2. ed. revisada e ampliada. São Paulo: Sicurezza, 2018.

INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA. Caso práctico sobre apetito de riesgo. La Fábrica de Pensamiento - Instituto de Auditores Internos de España, 2015. Disponível em: https://auditoresinternos.es/uploads/media_items/150629-caso-pr%C3%A1ctico-sobre-apetito-de-riesgo.original.pdf. Acesso em 10 de março de 2021.