Universidade Federal
do Acre

Manual de

GESTÃO DE RISCOS

RIO BRANCO - ACRE
JULHO DE 2021

Sumário

1. Introdução

O gerenciamento de riscos no setor público ainda é um grande desafio a ser alcançado, havendo necessidade não apenas de estruturas e processos, mas também de uma cultura de gerenciamento de riscos que contribua para a organização atingir seus objetivos de forma aprimorada. As responsabilidades e deveres do governo em relação ao bem público exigem a adoção de práticas e estratégias eficazes de gestão de riscos.

Este manual descreve a metodologia e as ferramentas de gestão a serem utilizadas na elaboração de planos de gestão de riscos na Universidade Federal do Acre (UFAC), em cumprimento ao que estabelece a Política de Governança, Gestão de Riscos, Controles e Integridade da UFAC - PGGRCI/Ufac (aprovada pelo Comitê de Governança, Integridade, Riscos e Controles da Universidade Federal do Acre e homologada pela Portaria nº 3.502, de 13 de novembro de 2019) e a Instrução Normativa Conjunta MP/CGU nº 01/2016, além da norma técnica ABNT ISO 31000:2009 e do COSO-ERM (2007).

2. Normativos Legais

Em 10 de maio de 2016, o Ministério do Planejamento, Orçamento e Gestão e a Controladoria-Geral da União publicaram a **Instrução Normativa (IN) Conjunta MP/CGU nº 01/2016**[1], instituindo a obrigatoriedade de órgãos e entidades do Poder Executivo adotarem medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança. Assim, a norma não definiu uma metodologia padrão a ser adotada, apenas delineou as orientações gerais e alguns elementos essenciais, deixando a cargo de cada órgão, dentro de sua autonomia, estruturar a metodologia e escolher as ferramentas mais adequadas à sua necessidade e contexto na gestão de seus riscos institucionais.

No âmbito da gestão de riscos, a referida IN estabelece os seguintes *princípios*:

- gestão de riscos de forma sistemática, estruturada e oportuna, subordinada ao interesse público;
- estabelecimento de níveis de exposição a riscos adequados;
- estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização;
- utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico; e
- utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais (art. 14).

Define, ainda, que os *objetivos* da gestão de riscos são:

- assegurar que os responsáveis pela tomada de decisão, em todos os níveis do órgão ou entidade, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso;
- aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis; e

[1] Fonte: CGU. Disponível em: <INSTRUÇÃO NORMATIVA -001-2016-MP-CGU>. Acesso: 28 out. 2020.

- agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos decorrentes de sua materialização (art. 15).

Com base nessa norma, o governo federal regulamentou a política de governança da administração pública direta, autárquica e fundacional por meio do **Decreto 9.203**[2], que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional e determina que:

> 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 (Decreto 9.203/2017, art. 17).

O referido Decreto também estipula alguns princípios da gestão de riscos:

- implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;
- 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;
- estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e
- utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de riscos, controle e governança (Decreto 9.203/2017, art. 17).

No que tange a referências teóricas, as principais normas utilizadas para a elaboração deste manual foram a **ABNT ISO 31000:2009**, elaborada pela Organização Internacional de Normalização e publicada pela Associação Brasileira de Normas Técnicas, que nasceu da necessidade de uma padronização da terminologia e conceitos utilizados em gestão de riscos, além do **COSO-ERM** (COSO, 2007) que trata de uma metodologia desenvolvida pelo Comitê de Organizações Patrocinadoras da Comissão Treadway, entidade privada norte-americana com atuação voltada à prevenção e inibição de fraudes em empresas por meio da gestão de riscos. Este manual foi elaborado com uma adaptação das etapas e conceitos presentes na ISO 31000:2018 e no COSO-ERM.

3. Alinhamento Estratégico

A gestão de riscos faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o Planejamento e Gestão Estratégica UFAC 2014-2023[3], o Plano de Desenvolvimento Institucional UFAC 2020-2024[4] e todos os processos de gestão de projetos e processos. Neste cenário de busca por melhoria de desempenho no

[2] Fonte: Palácio do Planalto. Disponível em: <D9203>. Acesso: 28 out. 2020.
[3] Disponível em: http://www.ufac.br/pe1423
[4] Disponível em: http://www.ufac.br/pdi2024

atendimento aos objetivos estratégicos da instituição, a gestão de riscos pode ajudar a concretizar tais objetivos, visto que poderá dar uma garantia de execução desses objetivos a partir do monitoramento dos riscos associados e desenvolver ações para tratá-los. Assim, a gestão de riscos apoiará a melhoria dos processos organizacionais e subsidiará a tomada de decisão na Instituição.

4. Abrangência

A abrangência de aplicação deste manual de gestão de riscos é de toda a estrutura da Instituição. Dessa forma, cada unidade deve elaborar seu Plano de Gestão de Riscos de forma integrada à ferramenta de planejamento adotada, para que sejam realizados os procedimentos de gestão de riscos inerentes às suas atividades.

5. Estrutura da Gestão de Riscos

5.1 Linhas de defesa

A estrutura de governança da Universidade Federal do Acre também se reflete na sua estrutura de gestão de riscos por meio do modelo de Três Linhas de Defesa elaborado e divulgado pelo Instituto dos Auditores Internos (IIA), sendo um conjunto de diretrizes que visa esclarecer e organizar as responsabilidades e papéis dos agentes públicos da instituição no gerenciamento dos riscos.

Nesse modelo, são estabelecidas três linhas de defesa, com definição clara de responsabilidades que devem ser definidas para que cada grupo de agentes públicos entenda os limites de suas responsabilidades e como seus cargos/funções se encaixam na estrutura geral de gerenciamento de riscos.

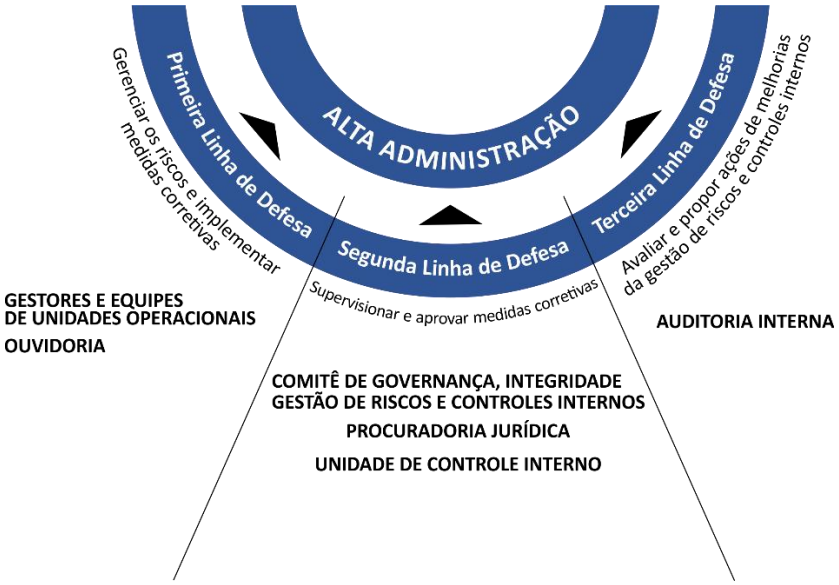
A primeira linha de defesa é composta pelas funções de gerência operacional responsáveis por monitorar e controlar os processos de trabalho, além de implementarem as ações corretivas para resolver deficiências em processos e controles. Os gerentes operacionais (gestores) devem identificar, avaliar e controlar os riscos, contribuindo para melhorar as políticas internas e assegurar que as atividades desenvolvidas estejam compatíveis com os objetivos da instituição. A primeira linha de defesa reporta-se à Alta Administração.

Na segunda linha de defesa estão as funções de gerenciamento de risco, conformidade, controle e fiscalização, para ajudar a desenvolver e/ou monitorar os controles da primeira linha de defesa. As funções da segunda linha, portanto, ajudam a primeira linha a manter as políticas e os procedimentos estabelecidos pela instituição, propondo melhorias nas estruturas e orientações. Tal qual a primeira linha, a segunda linha de defesa reporta-se à Alta Administração.

Na terceira linha de defesa encontra-se a Auditoria Interna, que tem a função de avaliar e informar a eficácia da governança, do gerenciamento de riscos e dos controles internos, incluindo a forma como a primeira e a segunda linhas de defesa alcançam os objetivos em relação ao gerenciamento de riscos e controles. Os auditores internos não elaboram ou implementam controles e não são responsáveis pelas operações da organização. Essas atividades ficam a cargo das outras duas linhas de defesa. A terceira linha de defesa reporta-se à Alta Administração, bem como ao Órgão de Governança/Conselho/Comitê de Auditoria.

A aplicação desse modelo de gerenciamento de riscos na estrutura de governança da Ufac é representada pela Figura 1.

Figura 1 – Modelo de três linhas de defesa



5.2 Competências

Detalham-se, nesta seção as competências relacionadas à gestão de riscos da Ufac, as quais estão distribuídas entre as seguintes instâncias de governança, de acordo com o Art. 16 da Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac: Comitê de Governança, Integridade, Risco e Controles; Diretoria de Controle e Gestão Institucional; Auditoria Interna; Gestores de Riscos; e Gestores de Processos.

5.2.1 Comitê de Governança, Integridade, Risco e Controles

O processo de governança da gestão de riscos será exercido pelo Comitê de Governança, Integridade, Risco e Controles (CGIRC), colegiado estratégico, permanente e de natureza deliberativa, responsável por tratar de assuntos relativos ao gerenciamento de risco, buscando sua identificação, análise, resposta e monitoramento. Sua composição engloba o(a) Reitor(a), que preside o comitê, o(a) Vice-Reitor(a), os(as) Pró-reitores(as), o(a) Diretor(a) do Núcleo de Tecnologia da Informação, o(a) Diretor(a) de Contabilidade e Finanças, o(a) Diretor(a) de Controle e Gestão Institucional e o(a) Auditor(a) Geral, na condição de assessoramento.

As competências do CGIRC estão dispostas no Art. 18 da Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac, conforme segue:

I. estabelecer e desenvolver as diretrizes de governança, de gestão de riscos, controles e de integridade da Ufac;
II. instituir a Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac;
III. aprovar o Manual de Gestão de Riscos da Ufac;
IV. aprovar o Plano de Integridade da Ufac;
V. institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos;

VI. promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de riscos, de controles internos e de integridade;
VII. garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;
VIII. promover a integração dos agentes responsáveis pela governança, pela gestão de riscos, pelos controles internos e pela integridade;
IX. promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, na transparência e na efetividade das informações;
X. aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;
XI. supervisionar o mapeamento e avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público;
XII. liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão ou entidade;
XIII. estabelecer limites de exposição a riscos globais do órgão, bem com os limites de alçada ao nível de unidade, política pública, ou atividade;
XIV. aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;
XV. emitir recomendação para o aprimoramento da governança, da gestão de riscos, dos controles internos e da integridade;
XVI. monitorar as recomendações e orientações deliberadas pelo Comitê; e
XVII. constituir Grupos Técnicos sempre que assuntos de natureza específica submetidos ao CGIRC se revestirem de interesse, importância ou de grande complexidade técnica e exigirem pesquisas, análises e detalhamentos necessários para subsidiar decisão ou encaminhamento.

5.2.2 Diretoria de Controle e Gestão Institucional

A Diretoria de Controle e Gestão Institucional (DCGI) atua como unidade administrativa responsável pela coordenação do gerenciamento dos riscos e controles, devendo prestar assessoramento às atividades do CGIRC, bem como atuar como instância de supervisão e monitoramento.

As competências da Diretoria de Controle e Gestão Institucional estão dispostas no Art. 22 da Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac, conforme segue:

I. auxiliar os gestores de riscos e processos na aplicação da metodologia e no uso de ferramentas e técnicas da gestão de riscos;
II. dar suporte aos gestores de riscos para a identificação, análise e avaliação dos riscos inerentes às atividades institucionais, levando em consideração a sua relevância e probabilidade de ocorrência;
III. propor, em conjunto com os gestores de riscos, as ações de tratamento (mitigação) e respostas (contingenciamento) a serem adotadas para os riscos identificados, a partir dos graus de risco definidos;
IV. contribuir com a elaboração e acompanhar a execução dos planos de ação para o tratamento dos riscos;

V. consolidar a avaliação de riscos e os controles implementados da Ifes, por meio da elaboração de relatórios periódicos a serem apresentados ao CGIRC;
VI. apoiar e conscientizar os gestores sobre a importância da gestão de riscos e sobre a responsabilidade inerente a cada servidor da Ifes;
VII. requisitar, aos responsáveis pelo gerenciamento de riscos, as informações necessárias para a consolidação dos dados e a elaboração de relatórios gerenciais;
VIII. realizar a articulação com os responsáveis pela Gestão de Riscos de cada unidade; e
IX. praticar outros atos de natureza técnica e/ou administrativa necessários ao exercício de suas responsabilidades.

5.2.3 Auditoria Interna

As auditorias internas no âmbito da Administração Pública se constituem na terceira linha ou camada de defesa das organizações, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão e da supervisão dos controles internos.

Compete à Auditoria Interna, sem prejuízo de outras competências previstas no Regimento Geral e demais normativas, no tocante à gerenciamento de riscos (Art. 28):

I. oferecer avaliações, assessoramento e consultoria ao CGIRC, destinadas ao aprimoramento dos controles internos, de forma que controles mais eficientes eficazes mitiguem os principais riscos;
II. colocar à disposição da gestão ferramentas e técnicas utilizadas pela auditoria interna para analisar riscos e controles de gestão;
III. revisar o gerenciamento dos principais riscos;
IV. avaliar os processos de gerenciamento de riscos;
V. propor melhorias para a PGGRCI/Ufac;
VI. propor metodologia para o processo de gerenciamento de riscos, capaz de subsidiar tomada de decisão no âmbito da Ufac;
VII. disseminar e dar suporte metodológico à implementação, operacionalização e avaliação do gerenciamento de riscos por parte da Diretoria de Controle e Gestão Institucional e das unidades administrativas da Ufac;
VIII. verificar se os riscos são corretamente estimados; e
IX. orientar ao CGIRC na resposta aos riscos.

5.2.4 Gestores de Riscos

São considerados gestores de riscos na Ufac, em seus respectivos âmbitos e escopos de atuação, os dirigentes das unidades acadêmicas e administrativas, responsáveis pelo gerenciamento de determinados riscos, com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco.

As competências do Gestor de Riscos estão dispostas no Art. 24 da Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac, conforme segue:

I. realizar o mapeamento dos processos de trabalho que devam ter os riscos gerenciados e tratados com prioridade em cada área técnica, à vista da dimensão dos prejuízos que possam causar;
II. realizar a seleção dos riscos que deverão ser priorizados para tratamento por meio de ações de caráter imediato, a curto, médio ou longo prazos ou de aperfeiçoamento contínuo;

III. definir as ações de tratamento a serem implementadas, bem como operacionalizar as respostas ao risco e definir o prazo de implementação e a avaliação dos resultados obtidos;
IV. assegurar que o risco seja gerenciado de acordo com a PGGRCI/Ufac;
V. monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados; e
VI. garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da Instituição.

5.2.5 Gestores de Processos

São considerados gestores de processos os servidores que sejam responsáveis pelos processos de trabalho, projetos e ações desenvolvidas nos níveis estratégicos, táticos ou operacionais na Ufac.

As competências do Gestor de Processos estão dispostas no Art. 25 da Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac, conforme segue:

I. contribuir nas atividades de identificação e avaliação dos riscos inerentes aos processos de trabalho, sob sua responsabilidade ou que perpassem a sua área de atuação;
II. gerenciar os riscos inerentes aos processos de trabalho sob sua responsabilidade, de forma a mantê-los em um nível de exposição aceitável;
III. implementar os planos de ação definidos para tratamento dos riscos inerentes; e
IV. comunicar ao Gestor de Riscos sobre novos riscos inerentes aos seus processos e que ainda não fazem parte da relação de riscos institucionais.

5.3 Ferramentas

O uso de ferramentas de gestão e análise de riscos tem como objetivo auxiliar os agentes que atuam no gerenciamento de riscos a tomarem as melhores decisões, avaliando a gravidade dos riscos para evitar que seu impacto afete os processos, objetivos ou metas da instituição. Dentre essas ferramentas estão a própria Política, o Manual de Gestão de Riscos, o Plano de Gestão de Riscos e o Relatório de Acompanhamento da Gestão de Riscos.

5.3.1 Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac

A Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac tem a responsabilidade de desenvolver, disseminar e implementar metodologias de gerenciamento de risco, desenvolver e estabelecer controles internos, contribuindo para o alcance dos objetivos institucionais, estratégicos e cumprimento do propósito institucional, bem como desenvolver a gestão da integridade, contribuindo para o aprimoramento da governança institucional.

5.3.2 Manual de Gestão de Riscos

Refere-se a este documento, apresentando a metodologia de gerenciamento de riscos na UFAC. A metodologia tem por finalidade orientar a identificação, a avaliação e a adoção de respostas aos eventos de riscos dos processos da unidade, bem como instruir sobre o monitoramento e reporte. Assim, reúne nesse documento as orientações a serem seguidas para a operacionalização da gestão de riscos, os procedimentos a serem empregados na aplicação da metodologia, além de apresentar os conceitos utilizados, papéis e responsabilidades, classificação dos eventos de riscos e controles básicos, em consonância com a Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac e com a IN Conjunta MP/CGU nº 01/2016.

5.3.3 Plano de Gestão de Riscos

O Plano tem como foco a operacionalização da gestão de riscos, seguindo a metodologia definida por este manual. O Plano aborda os riscos que impactam nas atividades, processos e objetivos das unidades da Ufac, por meio de um mapa de riscos que descreve os processos de análise do ambiente, identificação e classificação dos riscos, bem como avaliação e respostas aos riscos que, posteriormente, serão controlados e monitorados pelos gestores de riscos.

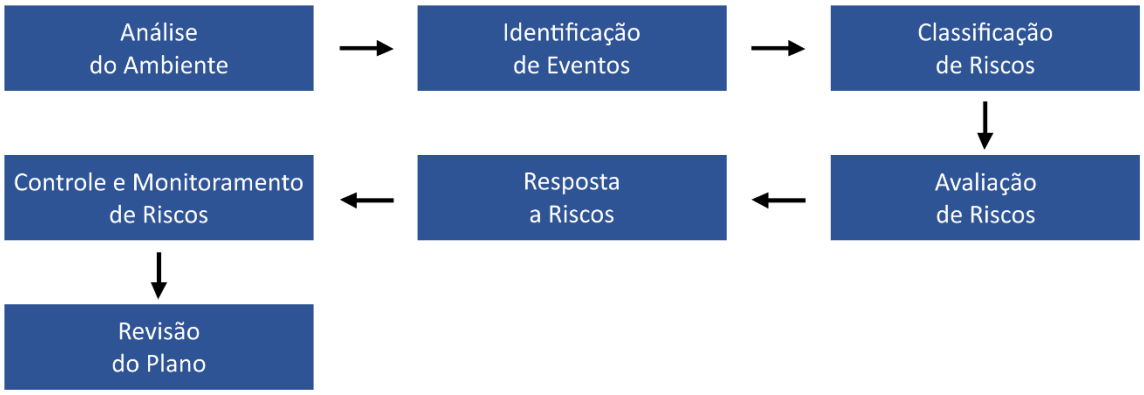
5.3.4 Relatório de Acompanhamento da Gestão de Riscos

O Relatório de Acompanhamento tem a finalidade de avaliar e monitorar a operacionalização da gestão de riscos definida pelo Plano de Gestão de Riscos da unidade a que se refere, descrevendo as atividades que foram executadas durante o período estabelecido, para eliminar e/ou mitigar os riscos identificados.

6. Metodologia de Elaboração do Plano de Gestão de Riscos

Para a aplicação da metodologia, faz-se necessário a definição de um fluxo de macroprocessos a serem seguidos. Os macroprocessos da Universidade Federal do Acre são baseados nas metodologias COSO II, ABNT ISO 31000:2009 e na IN Conjunta MP/CGU nº 01/2016, e estão representadas na Figura 2.

Figura 2 – Macroprocessos de gestão de riscos da Ufac



Tal metodologia foi dividida em 7 etapas, sendo melhor explicitada no decorrer das sessões subsequentes, orientando a forma como o Plano de Gestão de Riscos deve ser elaborado. Sua estrutura deve conter, portanto, os seguintes tópicos:

6.1 Análise do Ambiente

No processo de elaboração do Plano de Gestão de Riscos, a análise do ambiente tem a finalidade de colher informações para apoiar a identificação de eventos de riscos, elaborar um diagnóstico sobre o setor ou a instituição, bem como contribuir para a escolha de ações mais adequadas para assegurar o alcance dos objetivos do macroprocesso/processo.

No que se refere a identificação de forças e fraquezas (pontos fortes e fracos), que irão contribuir para a identificação de riscos, sugere-se a elaboração de uma matriz semelhante à apresentada no Quadro 1.

Quadro 1 – Análise do ambiente interno

Matriz SWOT – Ambiente Interno		
Objetivo Estratégico/ Macroprocesso	**Pontos Fortes**	**Pontos Fracos**
Objetivo Estratégico	1.	1.
	2.	2.
Macroprocesso	1.	1.
	2.	2.

A análise do ambiente é a base para todas as outras etapas, porque auxilia o setor/instituição a identificar os pontos fracos que podem ser minimizados e pontos fortes que podem ser potencializados.

6.2 Identificação de Eventos de Riscos

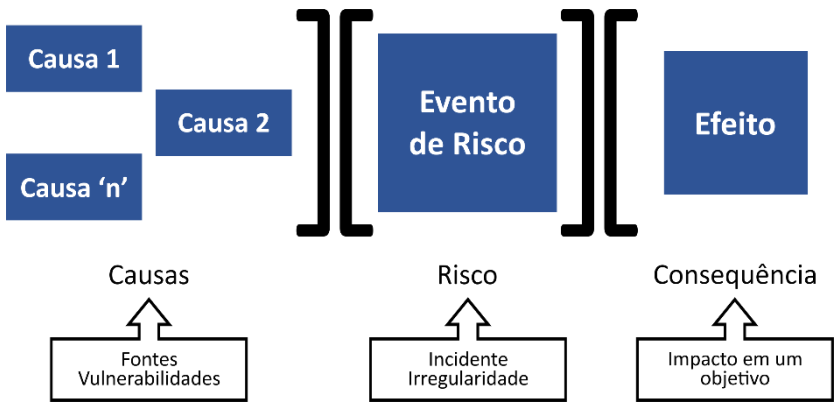
Esta etapa tem por finalidade identificar e registrar tanto os eventos de riscos que comprometem o alcance dos objetivos estratégicos ou dos macroprocessos, assim como as causas e efeitos/consequências de cada um deles.

Eventos são situações em potencial – que ainda não ocorreram – que podem causar impacto na consecução dos objetivos da organização, caso venham a ocorrer. Podem ser positivos ou negativos, sendo que os eventos negativos são denominados riscos, enquanto os positivos, oportunidades.

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.

Componentes do Evento de Risco:

Figura 3 – Componentes do Evento de Risco



- **Causas**: condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo;
- **Risco**: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos;
- **Consequência**: o resultado de um evento de risco sobre os objetivos da organização.

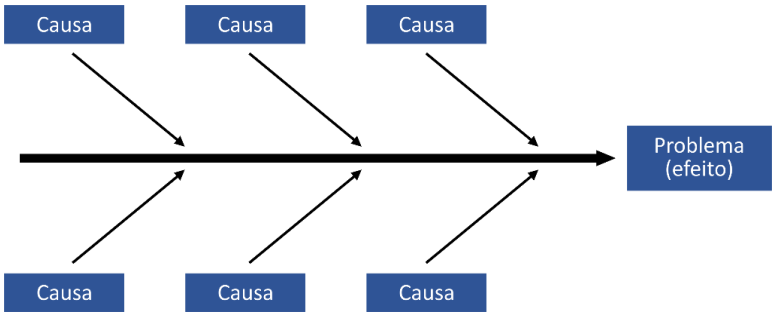
6.2.1 Técnicas e Ferramentas para Identificar Riscos

O processo de identificação de riscos requer a participação de servidores com conhecimento dos processos da unidade nos seus diferentes níveis. Cabe ao gestor de riscos identificar qual a técnica e ferramenta mais adequada a ser utilizada na identificação de eventos de risco de seu setor.

Dentre as principais técnicas e ferramentas estão: questionários e *checklist*; *workshops* e sessões de *brainstorming*; fluxogramas, diagrama de causa e efeito, *bow-tie*, etc.

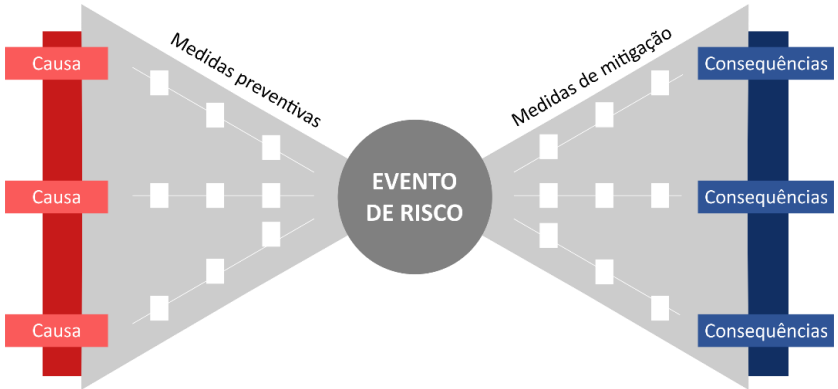
- Diagrama de causa e efeito (espinha de peixe): é uma técnica para identificação de uma possível causa raiz de um problema. No diagrama, cada espinha refere-se a uma causa e a cabeça refere-se ao problema que as causas levam. Esse método pode ser aplicado em *workshops* e *brainstorming*, partindo da identificação de um problema e em seguida as suas possíveis causas.

Figura 4 – Diagrama de causa e efeito



- *Bow-tie* (gravata borboleta): considerado uma evolução do diagrama de causa e efeito, consiste em identificar e analisar os possíveis caminhos de um evento de risco, dado que um problema pode estar relacionado a diversas causas e consequências.

Figura 5 – Diagrama bow-tie



Identificados os eventos de riscos, é necessário fazer sua compilação para o Mapa de Riscos, exposto na seção subsequente.

6.2.2 Mapa de Riscos

Para a organização das informações produzidas nesta etapa de identificação dos riscos, será utilizada uma estrutura em formato planilha (excel), denominada "**Mapa de Riscos**", contendo as colunas dos **objetivos/processos**, os **eventos de risco**, suas **causas**, ou seja, os fatores de riscos, e as **consequências**, ou seja, os impactos gerados caso o evento de risco ocorra.

Quadro 2 – Mapa de Risco

Processo/Objetivo	Identificação do Evento de Risco		
	Causa	**Evento**	**Consequência**
Processo/Objetivo 1	Causa 1	Evento 1	Consequência 1
Processo/Objetivo 2	Causa 2	Evento 2	Consequência 2

6.3 Classificação de Riscos

6.3.1 Classificar o Tipo de Risco

Esta etapa tem por finalidade categorizar os riscos identificados de acordo com as classificações e conceitos definidos na Política de Governança, Gestão de Riscos, Controles e Integridade da Ufac. Os riscos podem ser classificados em:

- **Riscos estratégicos**: estão associados à tomada de decisão que podem afetar negativamente o alcance dos objetivos estratégicos da organização;
- **Riscos operacionais**: estão associados à ocorrência de eventos que podem comprometer as atividades do órgão ou da instituição, normalmente associados a perdas, falhas, deficiências e sistemas, tecnologia, assim como eventos externos (como mudança no contexto político e econômico e etc);
- **Riscos financeiros/orçamentários**: eventos que podem comprometer a capacidade do órgão ou da instituição de contar com recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;
- **Riscos de comunicação**: estão associados a eventos que podem impedir ou dificultar a disponibilidade de informações para a tomada de decisão e para o cumprimento das obrigações de prestação de contas;
- **Riscos de conformidade**: estão associados ao não cumprimento de normas, legislações específicas ou regulamentações e procedimentos externos e internos aplicáveis, além de eventos derivados de alterações legislativas ou normativos que podem comprometer as atividades do órgão ou da instituição;
- **Riscos de imagem/reputação do órgão ou da instituição**: eventos que podem comprometer a confiança da sociedade (ou de parceiros, clientes ou de fornecedores) em relação à capacidade do órgão ou da instituição em cumprir sua missão institucional;
- **Riscos de integridade**: riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.

6.3.2 Definir o Gestor de Risco

Após a classificação dos riscos de acordo com a sua tipologia, é necessário informar um responsável pelo acompanhamento de cada risco identificado.

Feita a classificação dos riscos e a identificações dos gestores responsáveis, a próxima etapa é avaliar os riscos.

6.4 Avaliação de Riscos

Esta etapa tem por finalidade avaliar os eventos de riscos identificados considerando os seus componentes (causas e consequências). Os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto. Normalmente as causas se relacionam à probabilidade de o evento ocorrer. Por sua vez, as consequências referem-se ao impacto caso o evento se materialize.

6.4.1 Escala de Probabilidade

A probabilidade consiste na medição de quão provável é a ocorrência do risco. Em outras palavras, avaliar o grau de probabilidade de um risco implica em refletir sobre a frequência que ele pode ocorrer em determinado período de tempo.

- **Muito baixa (peso 1)**: não é provável que o evento aconteça;
- **Baixa (peso 2)**: possibilidade de o evento ocorrer apenas em situações excepcionais;
- **Média (peso 3)**: possibilidade de que o evento talvez ocorra em determinado momento;
- **Alta (peso 4)**: possibilidade que o evento ocorra em grande parte das situações;
- **Muito Alta (peso 5)**: esperado que o evento ocorra na maioria das situações.

6.4.2 Escala de Impacto

O impacto se refere às consequências do risco caso ele venha ocorrer, ou seja, quais serão os prejuízos ou danos causados caso o risco incida de fato.

- **Muito baixo (peso 1)**: os riscos possuem consequências pouco significativas;
- **Baixo (peso 2)**: Os riscos possuem consequências reversíveis em curto e médio prazo com custos pouco significativos;
- **Médio (peso 3)**: Os riscos possuem consequências reversíveis em curto e médio prazo com custos baixos;
- **Alto (peso 4)**: Os riscos possuem consequências graves e reversíveis em curto e médio prazo com custos altos;
- **Muito Alto (peso 5)**: os riscos possuem consequências irreversíveis ou com custos inviáveis.

6.4.3 Avaliar o Risco

A Matriz de Riscos ou Matriz de Probabilidade e Impacto é uma ferramenta de gerenciamento de riscos que permite de forma visual identificar o nível dos riscos que irão afetar menos ou mais a organização, possibilitando a tomada de decisões e a realizações de medidas preventivas para tratar esses riscos. O resultado da classificação do risco se dá em função da multiplicação da probabilidade x impacto, e indica em qual célula da matriz o risco se encaixa.

Quadro 3 – Matriz de Riscos

Nivel de Risco		Impacto				
		Muito Baixo (1)	Baixo (2)	Médio (3)	Alto (4)	Muito Alto (5)
Probabilidade	Muito Alta (5)	Médio (5)	Alto (10)	Alto (15)	Muito Alto (20)	Muito Alto (25)
	Alta (4)	Médio (4)	Médio (8)	Alto (12)	Alto (16)	Muito Alto (20)
	Média (3)	Baixo (3)	Médio (6)	Médio (9)	Alto (12)	Alto (15)
	Baixa (2)	Baixo (2)	Médio (4)	Médio (6)	Médio (8)	Alto (10)
	Muito Baixa (1)	Muito Baixo (1)	Baixo (2)	Baixo (3)	Médio (4)	Médio (5)
Probabilidade: Muito Baixa (1); Baixa (2); Média (3); Alta (4); Muito Alta (5) Impacto: Muito Baixo (1); Baixo (2); Médio (3); Alto (4); Muito Alto (5) Nível de Risco (Probabilidade x Impacto): Muito Baixo 1; Baixo 2-3; Médio 4-9; Alto 10-16; Muito Alto 20-25						

O resultado dessa classificação irá permitir fazer a avaliação do risco a partir das seguintes categorias:

- **Risco trivial**: nenhuma ação é necessária, risco deve ser aceito;
- **Risco tolerável**: risco deve ser aceito. A monitoração é necessária para assegurar que os controles sejam mantidos;
- **Risco moderado**: é necessário o planejamento e execução de ações para mitigar ou reduzir o risco;
- **Risco substancial**: é necessário o planejamento e execução de ações imediatas para reduzir o risco. Tais riscos devem ser transferidos/compartilhados;
- **Risco intolerável**: os riscos avaliados como intoleráveis não são admitidos e devem ter prioridade no gerenciamento de riscos. Tais riscos devem ser evitados.

Quadro 4 – Avaliação dos Riscos

Impacto X Probabilidade	Muito Baixo	Baixo	Médio	Alto	Muito Alto
Muito Alta	Moderado	Substancial	Substancial	Intolerável	Intolerável
Alta	Moderado	Moderado	Substancial	Substancial	Intolerável
Média	Tolerável	Moderado	Moderado	Substancial	Substancial
Baixa	Tolerável	Moderado	Moderado	Moderado	Substancial
Muito Baixa	Trivial	Tolerável	Tolerável	Moderado	Moderado

6.5 Resposta a Riscos

Feita a classificação e avaliação dos riscos, faz-se necessário apresentar as respostas necessárias que garantam segurança razoável para o alcance dos objetivos. O processo de planejar as respostas aos riscos visa definir o que será feito a respeito de cada risco que foi identificado e classificado nas etapas anteriores. No planejamento das respostas aos riscos deve-se encontrar formas de reduzir a ameaça ou eliminá-la por completo.

São respostas a riscos:

- **Aceitar o risco**: a exposição ao risco é aceita ou tolerada sem nenhuma ação específica para afetar a probabilidade ou o grau de impacto dos riscos;
- **Mitigar/Reduzir o risco**: são adotadas medidas para reduzir a probabilidade e/ou impacto de um evento de risco adverso até um limite aceitável;
- **Transferir/Compartilhar o risco**: transferência ou compartilhamento de uma parte do risco na busca da redução da probabilidade ou do impacto dos riscos;
- **Evitar o risco**: a exposição ao risco somente pode ser tratada alterando o plano, processo ou descontinuando a atividade que deu origem ao risco.

Quadro 5 – Tratamento dos Riscos

Impacto X Probabilidade	Muito Baixo	Baixo	Médio	Alto	Muito Alto
Muito Alta	Mitigar/ Reduzir	Transferir/ Compartilhar	Transferir/ Compartilhar	Evitar	Evitar
Alta	Mitigar/ Reduzir	Mitigar/ Reduzir	Transferir/ Compartilhar	Transferir/ Compartilhar	Evitar
Média	Aceitar	Mitigar/ Reduzir	Mitigar/ Reduzir	Transferir/ Compartilhar	Transferir/ Compartilhar
Baixa	Aceitar	Mitigar/ Reduzir	Mitigar/ Reduzir	Mitigar/ Reduzir	Transferir/ Compartilhar
Muito Baixa	Aceitar	Aceitar	Aceitar	Mitigar/ Reduzir	Mitigar/ Reduzir

A transferência de riscos exige a passagem do impacto negativo de uma ameaça para terceiros, juntamente com a propriedade da resposta, devendo ser reportada ao superior imediato para que sejam planejadas as ações necessárias visando à mitigação do risco. Essa transferência confere a uma outra parte a responsabilidade, parcial ou total, do gerenciamento dos riscos identificados; ela não elimina os riscos.

6.5.1 Planejar a Resposta a Riscos

Definida a resposta a riscos, faz-se necessário elaborar um plano de ação visando a redução do grau de exposição do risco inerente, ou seja, do risco identificado sem considerar quaisquer ações gerenciais. Assim, após a efetiva implementação das ações gerenciais, o risco inerente diminui o seu grau de exposição, passando a condição de risco residual. Sendo assim, além das informações apresentadas no Mapa de Riscos, o planejamento de respostas a riscos envolve a elaboração de uma segunda tabela, chamada de Plano de Respostas a Riscos.

Quadro 6 – Plano de Repostas a Riscos

PLANO DE RESPOSTAS A RISCOS									
Objetivo/ Processo	**Evento de Risco**	**Resposta**	**O QUE**	**QUANDO**	**ONDE**	**POR QUÊ**	**POR QUEM**	**COMO**	**CUSTO**

As atividades dessa etapa devem possuir uma equipe designada com atribuições e responsabilidades definidas, assim como prazos estabelecidos. Cabe ao gestor do risco o gerenciamento das atividades e o registro das ações adotadas, com vistas à construção de um histórico de melhores práticas e à elaboração do Relatório de Acompanhamento da Gestão de Riscos.

6.6 Controle e Monitoramento de Riscos

O controle e monitoramento são etapas que ocorrem durante todo o processo de gerenciamento de riscos, devendo integrar todas as instâncias envolvidas, bem como pelo monitoramento, verificação e supervisão contínuos da própria gestão de riscos, a fim de determinar a adequação, suficiência e eficácia dos controles internos estabelecidos.

Na Universidade Federal do Acre, essas etapas serão realizadas de acordo com a metodologia ForRisco, elaborada pelo Fórum de Pró-Reitores das IFES (Forplad/Andifes). Será utilizada uma ferramenta desenvolvida para este fim, desenvolvida pelo Ministério do Planejamento, Desenvolvimento e Gestão, denominada ÁGATHA, que documenta os eventuais riscos, oferecendo mecanismos de controle e de tratamento das inconformidades.

6.7 Revisão do Plano

Nesta etapa são descritas as atividades que foram executadas durante o ano, por meio de um relatório de acompanhamento, devendo ter, portanto, periodicidade anual. Cada unidade, por meio de seus gestores de riscos, deverá desenvolver um relatório que contenham informações relevantes, podendo ser utilizadas planilhas eletrônicas, tabelas, gráficos, além de textos.

Dessa forma, o relatório irá evidenciar a necessidade ou não de alteração do Plano para o próximo período, além de estimular a melhoria nos controles e promover um aprendizado para os usuários que irão trabalhar com os riscos em suas atividades.

O recomendado é que o relatório contenha, pelo menos, as seguintes seções:

- Apresentação;
- Estrutura organizacional da unidade;
- Processos avaliados na unidade;
- Período de avaliação;
- Riscos identificados;
- Avaliação dos controles;
- Ações de controle propostas;
- Parecer final sobre os riscos e controles identificados nos processos, principalmente no que se refere a riscos relevantes.

É importante que as informações apresentadas no Relatório possuam qualidade contextual, como:

- Relevância: a informação deve ser útil para o objetivo do trabalho;
- Integralidade: as informações importantes e suficientes para a compreensão devem estar presentes;
- Concisão: a informação deve ser apresentada de forma compacta;
- Clareza: a informação deve ser facilmente compreensível; e
- Adequação: volume de informação adequado e suficiente.

7. Considerações Finais

Este manual apresenta uma metodologia de elaboração do Plano de Gestão de Riscos, orientando detalhadamente as etapas necessárias para sua construção, com o objetivo de proporcionar uma base aplicável para o gerenciamento de riscos na Universidade Federal do Acre. Com o intuito de manter-se adequado às necessidades da Universidade, este manual estará em constante processo de melhoria.

Por fim, ressalta-se que o levantamento e gerenciamento de riscos devem fazer parte dos processos das unidades, assim, é necessário elaborar cronograma para a realização dos trabalhos, observados os prazos institucionais, e submeter às instâncias para aprovação e acompanhamento.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISSO 31000. **Gestão de riscos**: princípios e diretrizes, 209. Disponível em https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso em 01 dez. 2020.

BRASIL. **Decreto nº 9.203**, de 22 de novembro de 2017. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. DF, 2017. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm. Acesso em 01 dez. 2020.

_____. **Instrução Normativa Conjunta CGU/MP Nº 001**, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Ministério do Planejamento, Orçamento e Gestão/Controladoria Geral da União: DF, 2016. 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 01 dez. 2020.

IAA. **Declaração de Posicionamento do IIA**: As três linhas de defesa no gerenciamento eficaz de riscos e controles. 2013. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/41842/12/As_tres_linhas_de_defesa_Declaracao_de_Posicionamento.pdf. Acesso em 01 dez. 2020.

COSO. Committee of Sponsoring Organizations of the Treadway Comission. **Gerenciamento de Riscos Corporativos** – Estrutura Integrada. Sumário Executivo. 2007. Disponível em: https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf. Acesso em 01 dez. 2020.

MP. Ministério do Planejamento, Desenvolvimento e Gestão. **Manual de gestão de integridade, riscos e controles internos da gestão**. 2017. Disponível em: https://www.gov.br/economia/pt-br/centrais-de-conteudo/publicacoes/planejamento/controle-interno/manual_de_girc___versao_2_0.pdf. Acesso em 01 dez. 2020.

UFAC. **Estatuto da Universidade Federal do Acre**. UFAC, Rio Branco/AC, 2013. Disponível em: http://www.ufac.br/transparencia/sobre/documentos/documentos/estatuto-ufac.pdf/@@download/file/ESTATUTO%20-%20UFAC.pdf. Acesso em 01 dez. 2020.

ANEXOS

Anexo I - Termos e Definições

Ameaça – possibilidade de que um evento afete negativamente o alcance de objetivos;

Apetite a risco – nível de risco que uma organização está disposta a aceitar;

Avaliação de risco – processo de identificação e análise dos riscos relevantes para o alcance dos objetivos organizacionais e a determinação de respostas apropriadas;

Causa – condições que dão origem à possibilidade de um evento ocorrer, também chamadas de fatores de riscos e podem ter origem no ambiente interno e externo;

Consequência – resultado de um evento que afeta positiva ou negativamente os objetivos da organização;

Controle – qualquer medida aplicada, no âmbito da Universidade, para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidas sejam alcançados;

Controles internos – processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de colaboradores da organização, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;

Evento – uma ou mais ocorrências, provenientes de ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo materializar ou não o risco, que pode ser uma ameaça ou uma oportunidade;

Gerenciamento de riscos – processo para identificar, avaliar, administrar, tratar, controlar e monitorar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização;

Gestão de riscos – conjunto de atividades coordenadas para dirigir e controlar uma organização no que se refere ao risco, contribuindo para a redução da materialização de eventos que impactem negativamente em seus objetivos ou para potencializar a materialização de eventos que aumentem as oportunidades de atingimento dos objetivos;

Gestor de riscos - os dirigentes das unidades acadêmicas e administrativas, responsáveis pelo gerenciamento de determinados riscos, com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco

Gestor de processos – agentes que sejam responsáveis pelos processos de trabalho, projetos e ações desenvolvidas nos níveis estratégicos, táticos ou operacionais na Instituição.

Governança – combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar e monitorar suas atividades, com o intuito de alcançar os seus objetivos;

Identificação de riscos – processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais. A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas;

Impacto – consequências do risco caso ele venha ocorrer, ou seja, quais serão os prejuízos ou danos causados caso o risco incida de fato.

Matriz de risco – ferramenta que permite aos gestores mensurar, avaliar e ordenar os eventos de riscos que podem afetar o alcance dos objetivos do processo da unidade e, consequentemente, os objetivos organizacionais, com base em uma escala de probabilidade versus impacto, particionada em regiões, que caracterizam os níveis de riscos dimensionados em função do apetite a risco definido pela organização;

Matriz SWOT – também chamada de FOFA (Forças, Oportunidades, Fraquezas e Ameaças), é um sistema de análise para o estudo dos ambientes interno e externo da organização, onde são identificados os pontos fortes e fracos, além das ameaças e oportunidades.

Monitoramento – é um componente do controle interno que permite avaliar a qualidade do sistema de controle interno ao longo do tempo;

Nível de risco – medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos da organização;

Política de Governança, Gestão de Riscos, Controles e Integridade da Universidade Federal do Acre - denominada PGGRCI/Ufac, tem a responsabilidade de desenvolver, disseminar e implementar metodologias de gerenciamento de risco, desenvolver e estabelecer controles internos, contribuindo para o alcance dos objetivos institucionais, estratégicos e cumprimento do propósito institucional, bem como desenvolver a gestão da integridade, contribuindo para o aprimoramento da governança institucional;

Probabilidade – possibilidade de ocorrência de um evento;

Resposta a riscos – qualquer ação adotada para lidar com risco. As respostas podem se enquadrar nos seguintes tipos: aceitar; transferir/compartilhar; mitigar/reduzir ou evitar o risco.

Risco – efeito da incerteza nos objetivos da organização. É a possibilidade de ocorrência de um evento que venha afetar o alcance dos objetivos. O risco é medido em termos de impacto e probabilidade.

Risco externo – riscos associados ao ambiente onde a organização opera. Em geral, a organização não tem controle direto sobre estes eventos, mas, mesmo assim, ações podem ser tomadas quando necessário;

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 interno – riscos associados à própria estrutura da organização, seus processos, governança, quadro de pessoal, recursos ou ambiente de tecnologia;

Risco residual – risco remanescente a que uma organização está exposta, após a implementação de ações gerenciais, controles internos, para o tratamento do risco;

Tipo de risco – classificação dos tipos de riscos definidos pela organização, que podem afetar o alcance de seus objetivos estratégicos, observadas as características de sua área de atuação e as particularidades do setor público.