Guia para Gestão de Riscos na UFCSPA

Auditoria Interna - AUDIN
Coordenação de Desenvolvimento Institucional - CDI
Núcleo de Qualidade Interna - NQI
Pró-reitoria de Planejamento - PROPLAN

Porto Alegre
Agosto/2021

Autor:
Leandro Gomes Amaral

Organizadora:
Evelise Fraga de Souza Santos

Colaboradores:
Andressa Luiza Bortolaso de Oliveira
Cláudio Moacir Marques Corrêa
Juliana Silva Herbert

Guia para Gestão de Riscos na UFCSPA

1ª edição

Porto Alegre
Agosto
2021

Universidade Federal de Ciências da Saúde de Porto Alegre
Professora Dra. Lucia Campos Pellanda
Reitora

Pró-Reitoria de Planejamento
Professora Dra. Alessandra Dahmer
Pró-Reitora

Coordenação de Desenvolvimento Institucional
Evelise Fraga de Souza Santos
Coordenadora

Núcleo de Qualidade Interna
Professora Dra. Juliana Silva Herbert
Coordenadora

Auditoria Interna
Cláudio Moacir Marques Corrêa
Auditor

Autor:
Leandro Gomes Amaral

Contato:
cgr@ufcspa.edu.br

Dados Internacionais de Catalogação na Publicação (CIP)

A485g Amaral, Leandro Gomes

Guia para gestão de riscos na UFCSPA / Leandro Gomes Amaral ; organizadora Evelise Fraga de Souza Santos ; colaboradores Andressa Luiza Bortolaso de Oliveira, Cláudio Moacir Marques Corrêa e Juliana Silva Herbert. – Porto Alegre : Edição do autor, 2021.
37 p. : il.

1. Administração. 2. Tomada de decisão. 3. Gestão de risco I. Santos, Evelise Fraga de Souza. II. Oliveira, Andressa Luiza Bortolaso de. III. Corrêa, Cláudio Moacir Marques. IV. Herbert, Juliana Silva. V. Título.

CDD 658.403
CDU 005.53

UFCSPA - Biblioteca Paulo Lacerda de Azevedo

SUMÁRIO

1.	**INTRODUÇÃO**	4
2.	**FUNDAMENTOS TEÓRICOS E NORMATIVOS**	5
3.	**FALSOS CONCEITOS**	6
4.	**O QUE SE ENTENDE POR RISCO?**	10
5.	**QUAL O PROPÓSITO DA GESTÃO DE RISCOS?**	13
6.	**COMPONENTES DA GESTÃO DE RISCOS**	15
7.	**METODOLOGIA ADOTADA PELA UFCSPA**	22
8.	**TÉCNICAS DE DIAGNÓSTICO APLICÁVEIS**	27
9.	**ESTRUTURA PARA GERIR RISCOS NA UFCSPA**	31
REFERÊNCIAS		36

1. INTRODUÇÃO

Este guia tem o objetivo de apresentar um referencial para a implementação dos procedimentos de Gestão de Riscos na Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA). O documento contempla conhecimentos teóricos, fundamentos normativos, aspectos metodológicos e sugestões de ferramentas práticas, a fim de nortear os gestores das áreas acadêmicas e administrativas nas tarefas inerentes à identificação, avaliação e ao tratamento adequado dos riscos que podem impactar os objetivos nos níveis estratégico, tático e operacional da gestão.

O Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da Administração Pública Federal, prevê, em seu artigo 17, que os órgãos e entidades devem estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos. Entende-se por Gestão de Riscos, à luz do referido Decreto, o:

> processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos (BRASIL, 2017).

O gerenciamento de riscos nos órgãos e entidades que compõem o setor público está intimamente ligado ao conceito de governança pública, uma vez que se os riscos forem geridos de maneira adequada, com a adoção de controles capazes de mitigá-los, aumenta a chance de as políticas e serviços públicos atenderem aos interesses da sociedade. Desta forma, a implantação da Gestão de Riscos incorporada aos demais processos organizacionais pode, entre outros benefícios:

- ✓ **auxiliar no alcance dos objetivos;**
- ✓ **minimizar prejuízos financeiros;**
- ✓ **proteger ativos tangíveis e intangíveis;**
- ✓ **melhorar a qualidade das decisões;**
- ✓ **contribuir para o uso racional dos recursos;**
- ✓ **propiciar a melhoria contínua.**

Recentemente, o Plano de Desenvolvimento Institucional 2020-2029 foi concebido de maneira a possibilitar, ao longo de seus dez anos de vigência, o desdobramento dos objetivos, metas, políticas e diretrizes em ações institucionais. No tocante às políticas para a área administrativa, destacam-se os objetivos de reorganizar e qualificar processos internos, no intuito de adequá-los às melhores práticas voltadas para eficiência e transparência no uso dos recursos públicos, bem como de promover melhorias nos controles internos e na gestão por processos.

Os esforços para implantação da Gestão de Riscos na UFCSPA tiveram início com a elaboração da Política de Gestão de Riscos, aprovada pelo Conselho Universitário mediante a Resolução nº 39/2017. No documento, foram definidas diretrizes e a estrutura interna para gerir riscos, que envolve a alta administração, gestores das áreas, o Comitê de Governança Riscos e Controles, a Comissão de Gestão de Riscos e a Auditoria Interna (AUDIN), cada qual com sua responsabilidade.

No que tange à gestão por processos, o Núcleo de Qualidade Interna (NQI) desenvolve ações para a implantação da gestão por processos na UFCSPA, motivando os setores a mapear, revisar e identificar possibilidades de melhoria de seus processos. Para isso, foi publicado o Guia de Aplicação do M3P – Modelo de Maturidade em Mapeamento de Processos. O modelo, descritivo e prescritivo, prevê níveis de maturidade e critérios para o alcance dos níveis, para que os setores da UFCSPA sejam avaliados quanto ao mapeamento de seus processos. Dentre os critérios, um deles está diretamente relacionado à identificação e à gestão dos riscos relacionados aos processos.

A ideia de aproximar mapeamento de processos e gerenciamento de riscos contribui para o aperfeiçoamento da gestão, uma vez que tal sinergia proporciona maior eficiência na abordagem dos dois temas. O conhecimento das etapas de um processo de trabalho favorece a identificação de riscos e dos pontos de controle existentes, assim como a necessidade de revisão das medidas de tratamento para o risco podem sugerir ajustes nos fluxos, de modo a torná-los mais adequados para geração dos resultados almejados pela gestão.

Este Guia está organizado em nove seções mais as referências. Na seção dois, são apresentados os principais fundamentos teóricos e normativos no tocante à Gestão de Riscos. Em seguida, são abordados alguns falsos conceitos atrelados ao senso comum, os quais merecem um exame mais aprofundado. As seções quatro, cinco e seis tratam do que se entende por risco, do propósito de geri-los, bem como dos componentes e etapas do processo de Gestão de Riscos, respectivamente.

Ademais, são explicitados, na seção sete, a metodologia adotada na UFCSPA e os critérios norteadores para a avaliação de riscos. A seção oito, por sua vez, contempla um rol de técnicas e ferramentas que podem ser empregadas com a finalidade de refinar o gerenciamento de riscos. Por fim, a seção nove descreve a estrutura para gerir riscos na UFCSPA e os papéis atribuídos aos atores organizacionais.

2. FUNDAMENTOS TEÓRICOS E NORMATIVOS

A título de referenciais externos relativos ao assunto, são sugeridos os seguintes:

- Decreto nº 9.203, de 22 de novembro de 2017: dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional;

- Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016: dispõe sobre controles internos, Gestão de Riscos e governança no âmbito do Poder Executivo Federal;
- NBR ISO 31000:2009 (atualizada em 2018);
- Estrutura COSO ERM - Gerenciamento de Riscos Corporativos;
- Estrutura COSO 2013 - Controle Interno;
- Estrutura COSO ERM 2017 - Gerenciamento de Riscos Corporativos Integrado com Estratégia e Performance;
- As 3 Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles.

3. FALSOS CONCEITOS

Quando se faz menção às palavras "risco", "controle" ou até mesmo à expressão "Gestão de Riscos", interpretações equivocadas podem ocorrer caso o interlocutor não esteja familiarizado com os conceitos. Alguns erros comuns podem ser evidenciados na Figura 1.

FALSOS CONCEITOS

- ✖ Só existem riscos de acidentes ou na área financeira
- ✖ Gestão de riscos é feita apenas uma vez
- ✖ Risco é com o setor de riscos
- ✖ Controle é com a Auditoria Interna
- ✖ Controle de riscos traz mais burocracia

Figura 1 - Falsos conceitos à Gestão de Riscos.
Fonte: Elaborada pelo autor.

Desmistifiquemos então cada um desses falsos conceitos.

- *Só existem riscos de acidentes ou na área financeira*

De fato, alguns tipos de eventos, como acidentes de avião, catástrofes naturais, rompimentos de barragens e incêndios, podem ocasionar enormes danos, inclusive perdas de vidas humanas. Por essa razão, acontecimentos assim adquirem ampla repercussão no noticiário e sensibilizam um grande número de pessoas em torno do assunto.

A possibilidade de um acidente com aeronave, de rompimento de uma barragem ou de incêndio num ambiente frequentado por várias pessoas caracteriza riscos certamente relevantes, devido ao impacto potencialmente catastrófico decorrente. Outro exemplo seria a emergência de novas crises de natureza financeira, tal como a ocorrida em 2008, a qual teve reflexos na economia em diversos países e gerou instabilidade no mercado financeiro.

Todavia, uma série de outros riscos estão envolvidos em atividades cotidianas, sejam pessoais ou organizacionais, e podem passar despercebidos até que causem transtornos. No caso de uma instituição pública de ensino superior, existem inúmeros riscos operacionais que, na hipótese de se materializarem, podem prejudicar em algum grau os objetivos associados à promoção do ensino, da pesquisa e da extensão. O risco pode estar tanto em processos das áreas administrativas (licitações, gestão de contratos, folha de pagamento) como nos processos finalísticos ou de apoio a atividades finalísticas (matrículas, cadastro, assistência ao estudante, gestão laboratorial).

Além disso, o Decreto n° 9.203/2017 reforça o princípio de que a Gestão de Riscos deve ser **integrada ao planejamento estratégico e aos seus desdobramentos**, **às atividades e aos projetos em todos os níveis organizacionais**.

- *Gestão de Riscos é feita apenas uma vez*

Esta afirmação também é falsa, porque a Gestão de Riscos deve ser feita continuamente. Conforme dispõe o artigo 2°, IV, do Decreto n° 9.203/2017, trata-se de um processo de natureza **permanente**, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização.

- *Risco é com o setor de riscos*

Embora a existência de um setor especializado em riscos possa trazer benefícios na implantação da Gestão de Riscos, atribuir toda responsabilidade pelo processo a uma só unidade, além de ser uma ideia equivocada, prejudica a execução das ações relativas ao gerenciamento.

Cada organização tem suas particularidades e deve estabelecer uma estrutura apropriada para fazer frente aos riscos aos quais está sujeita, considerando os contextos interno e externo em que está inserida. Assim, os riscos podem diferir de natureza e magnitude entre uma instituição e outra, inclusive entre aquelas pertencentes a segmento de atuação semelhante ou até entre unidades de uma mesma organização. Isso pode ocorrer devido a fatores internos (governança, cultura organizacional, estratégia, estrutura, normas, processos, recursos, entre outros) e a fatores externos (econômicos, sociais, políticos, regionais, mercadológicos, ambientais, legais, entre outros).

Segundo o artigo 19 da IN Conjunta MP/CGU n° 01/2016, o dirigente máximo é o principal responsável por constituir a estratégia da organização e a estrutura de gerenciamento de riscos, o que inclui o estabelecimento, a manutenção, o monitoramento e o

aperfeiçoamento dos controles internos da gestão. A aludida norma prevê ainda, no artigo 20, que cada risco mapeado e avaliado deve estar associado a um agente responsável, o qual deve ser o gestor com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco.

Ademais, a instituição pode adotar "linhas de defesa" na abordagem dos seus controles internos. Os agentes responsáveis por **operacionalizar os controles correspondem à primeira linha de defesa** e as instâncias que exercem **supervisão e monitoramento dos controles são a segunda linha** (comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e *compliance*, entre outras). **Na terceira linha está a função de auditoria interna**, cujo papel é o aprimoramento da eficácia dos processos de gerenciamento de riscos, dos controles internos e da governança, por meio de **atividades independentes de avaliação e consultoria**.

- *Controle é com a Auditoria Interna*

Para esclarecer esta questão, cumpre primeiro fazer a distinção entre o Sistema de Controle Interno previsto no artigo 74 da Constituição Federal de 1988 e o controle interno preceituado na IN Conjunta MP/CGU n° 01/2016. Eis as respectivas definições:

Sistema de Controle Interno – Constituição federal

> Art. 74. Os Poderes Legislativo, Executivo e Judiciário manterão, de forma integrada, sistema de controle interno com a finalidade de:
> I - avaliar o cumprimento das metas previstas no plano plurianual, a execução dos programas de governo e dos orçamentos da União;
> II - comprovar a legalidade e avaliar os resultados, quanto à eficácia e eficiência, da gestão orçamentária, financeira e patrimonial nos órgãos e entidades da administração federal, bem como da aplicação de recursos públicos por entidades de direito privado;
> III - exercer o controle das operações de crédito, avais e garantias, bem como dos direitos e haveres da União;
> IV - apoiar o controle externo no exercício de sua missão institucional.
> § 1º Os responsáveis pelo controle interno, ao tomarem conhecimento de qualquer irregularidade ou ilegalidade, dela darão ciência ao Tribunal de Contas da União, sob pena de responsabilidade solidária.
> § 2º Qualquer cidadão, partido político, associação ou sindicato é parte legítima para, na forma da lei, denunciar irregularidades ou ilegalidades perante o Tribunal de Contas da União.

Controles internos da gestão

> 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 servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados: a) execução ordenada, ética, econômica, eficiente e eficaz das operações; b)

> cumprimento das obrigações de accountability; c) cumprimento das leis e regulamentos aplicáveis; e d) salvaguarda dos recursos para evitar perdas, mau uso e danos. O estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica;

Os trechos evidenciam as diferenças entre as duas perspectivas de controle. A primeira descreve atividades de avaliação do cumprimento das metas previstas no Plano Plurianual, da execução dos programas de governo e dos orçamentos da União e de avaliação da gestão dos administradores públicos federais, utilizando como instrumentos a auditoria e a fiscalização, sendo o órgão central do Sistema de Controle, no Poder Executivo Federal, a Controladoria-Geral da União (CGU). A segunda, por sua vez, diz respeito a um conjunto de regras, procedimentos, diretrizes, rotinas e outras medidas empreendidas pelos colaboradores de uma organização a fim de mitigar os riscos e fornecer segurança razoável de que os objetivos serão alcançados. Esta definição de controle interno é a que se pretende adotar para consecução das finalidades deste Guia.

Sobre a interpretação de que "controle é com a Auditoria Interna", não se sustenta do ponto de vista das "linhas de defesa", uma vez que cabe à auditoria interna, enquanto terceira linha, **avaliar a operacionalização e supervisão dos controles, a cargo da primeira e da segunda linhas**, respectivamente. Nesse sentido, a função de auditoria interna governamental pode ser definida como:

> atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Deve buscar auxiliar as organizações públicas a realizarem seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos (BRASIL, 2016).

- *Controle de riscos traz mais burocracia*

A associação de que controle significa necessariamente mais burocracia leva a julgamentos equivocados e pode gerar uma série de consequências negativas. O Decreto-Lei n° 200, de 25 de fevereiro de 1967, em seu artigo 14, prevê que: "o trabalho administrativo será racionalizado mediante simplificação de processos e supressão de contrôles que se evidenciarem como puramente formais ou cujo custo seja evidentemente superior ao risco (BRASIL, 1967)."

Portanto, **o controle por si só não é sinônimo de burocracia**. No entanto, pode vir a ser caso o seu custo ultrapassar o benefício proporcionado à mitigação do risco envolvido.

Cumpre ressaltar que o Decreto n° 9.203/2017 contempla enunciado semelhante ao delinear quais princípios norteiam a Gestão de Riscos. De acordo com o artigo 17, III, da referida norma, os **controles devem ser proporcionais aos riscos**, de maneira a considerar suas causas, fontes, consequências, impactos e a relação custo-benefício.

4. O QUE SE ENTENDE POR RISCO?

Há mais de uma definição de risco na literatura especializada, a exemplo das três transcritas a seguir:

IN Conjunta MP/CGU n° 01/2016

"Possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade."

ISO 31000/2018

"Efeito da incerteza nos objetivos."

COSO ERM 2004

"O risco é representado pela possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos."

Antes de continuar, é preciso esclarecer que um evento é um incidente ou uma ocorrência originária de fontes internas ou externas, que afeta a realização dos objetivos de modo negativo, positivo ou ambos. Eventos que causam impacto negativo representam riscos e os de efeito positivo são oportunidades (COSO GRC, 2004).

Segundo a ISO 31000, o evento é uma "ocorrência ou mudança em um conjunto específico de circunstâncias", que pode ter várias causas e consequências. Além disso, pode ser algo esperado que não venha a ocorrer ou algo não esperado, mas que acontece. Um evento pode ainda ser uma fonte de risco, ou seja, "um elemento que, individualmente ou combinado, tem o potencial para dar origem ao risco" (ABNT, 2018, p.2).

É interessante observar que a palavra "objetivos" está presente nas três citações, uma vez que os eventos passíveis de acontecer podem impactar o cumprimento daqueles. Por isso, **conhecer os objetivos a serem atingidos é requisito essencial para uma boa identificação de riscos**.

Outro ponto relevante é a forma de mensuração do risco. **A probabilidade expressa a possibilidade de algo ocorrer e o impacto reflete o prejuízo (ou benefício no caso de um risco positivo, também chamado de oportunidade) causado se o risco vier a se materializar.** Tanto a probabilidade como o impacto podem ser aferidos por meio de critérios qualitativos ou quantitativos pré-definidos. Por exemplo, podem ser utilizadas escalas que tenham as opções "baixo", "médio" e "alto" (método qualitativo) ou atribuir números para medir a chance associada a determinado evento e o seu impacto potencial, tais como 1 - "baixo", 2 - "médio", 3 - "alto" (método semiquantitativo) ou probabilidades de 10%, 20%, 50% e impactos de R$ 1.000.000,00; R$ 2.000.000,00; R$ 5.000.000,00; etc (método quantitativo) . A Figura 2 ilustra a ideia ora apresentada.

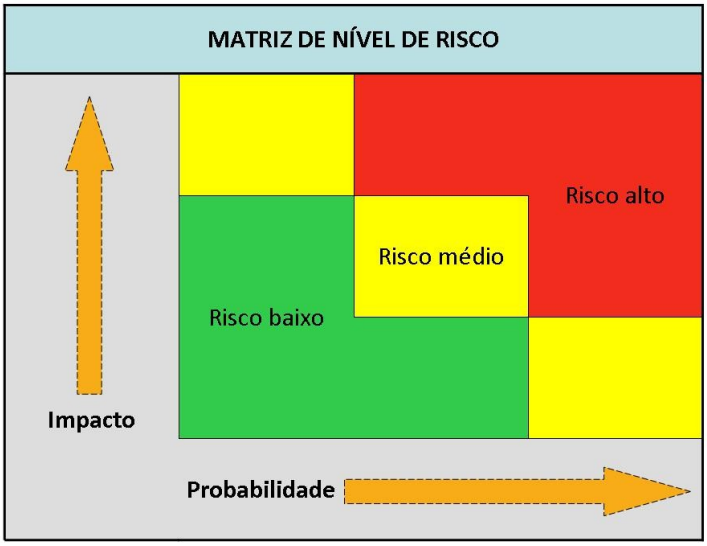

Figura 2 - Probabilidade, impacto e nível de risco.
Fonte: Elaborada pelo autor.

A combinação da probabilidade e do impacto determina o nível do risco, o qual também pode ser expresso em termos qualitativos ou quantitativos. Na UFCSPA, os critérios a serem seguidos na mensuração do risco estão descritos na Política de Gestão de Riscos da instituição.

NÍVEL DO RISCO = PROBABILIDADE X CONSEQUÊNCIA (IMPACTO)

Quando se aborda a magnitude de um risco, deve-se fazer a distinção entre os conceitos de risco inerente e risco residual, bem como explicar o significado de apetite a riscos. A IN Conjunta MP/CGU n° 01/2016 assim os define:

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

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

Apetite a risco: *"nível de risco que uma organização está disposta a aceitar".*

(BRASIL, 2016).

Portanto, o que diferencia as duas perspectivas é que o **risco residual contempla a implementação de ações gerenciais para tratamento do risco, enquanto o risco inerente as desconsidera**. Dessa forma, se um determinado risco, hipoteticamente, for considerado "alto" sob o ponto de vista do risco inerente, medidas gerenciais sobre a probabilidade e o impacto poderão reduzi-lo a um patamar residual "médio" ou "baixo", a depender da eficácia do tratamento implementado e da escala utilizada.

Se mesmo com a adoção de medidas gerenciais o risco residual superar o nível de aceitação estabelecido pela administração, será necessário rever o tratamento ou implementar novas ações com vistas a **reduzir o risco até o patamar desejável pela organização**. O apetite a risco estabelece este nível e atua como parâmetro para gestão avaliar qual resposta ao risco é mais adequada. A Figura 3 retrata a relação entre risco inerente, controle, risco residual e apetite a risco.

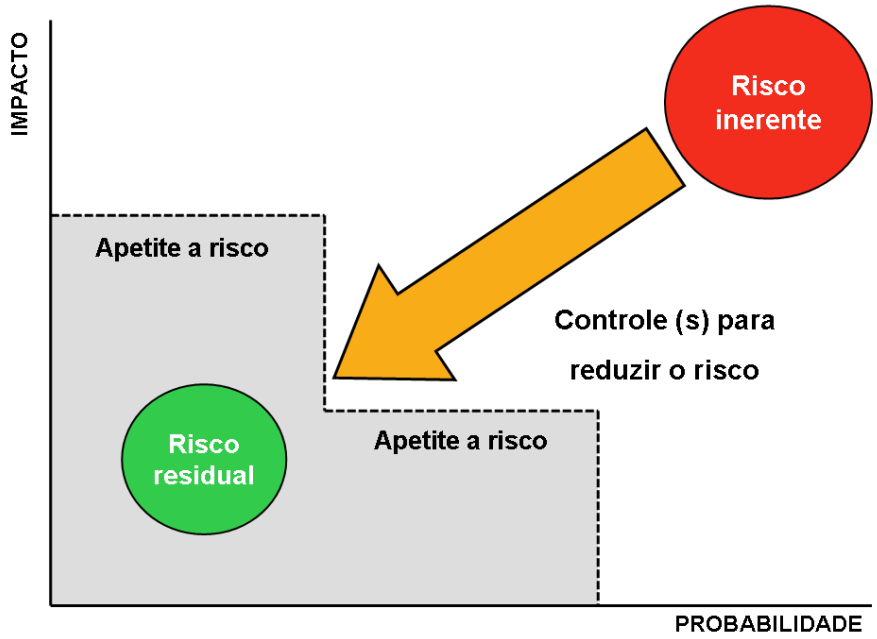

Figura 3 - Risco inerente, risco residual e apetite a risco.
Fonte: Elaborada pelo autor.

Os riscos organizacionais podem ser classificados em diversas categorias, tais como operacionais, econômicos, legais, de imagem, de integridade, políticos, ambientais entre outras. A IN Conjunta MP/CGU n° 01/2016 sugere quatro tipologias:

Riscos operacionais: *"eventos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas"*.

Riscos de imagem/reputação do órgão: *"eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional"*.

Riscos legais: *"eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade"*.

Riscos financeiros/orçamentários: *"eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros*

necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações".

(BRASIL, 2016).

E quanto à origem, podem ser classificados como:

Riscos externos: *"são os 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."*

Riscos internos: *"são os riscos associados à própria estrutura da organização, seus processos, governança, quadro de pessoal, recursos ou ambiente de tecnologia."*

(UFCSPA, 2017).

5. QUAL O PROPÓSITO DA GESTÃO DE RISCOS?

A princípio, deve-se considerar que a Gestão de Riscos se destina a **melhorar o processo de tomada de decisão, bem como fornecer razoável segurança quanto ao cumprimento da missão e dos objetivos institucionais**, na contramão de alguns conceitos falaciosos ainda presentes em segmentos da administração pública, a exemplo da noção de que o controle de risco só traz mais burocracia.

Por outro lado, é necessário ter em mente que a Gestão de Riscos e os controles internos não são um fim em si mesmos, mas um meio para a concretização da missão institucional. Assim, as **medidas de controle devem ser compatíveis com os riscos** e focar o benefício gerado para o alcance dos objetivos da organização.

A ISO 31000 ressalta que o **propósito da Gestão de Riscos é a criação e proteção de valor**, por vias da melhoria do desempenho, do incentivo a inovações, bem como do apoio ao alcance dos objetivos. A norma sugere a adoção de alguns princípios como base para gerenciar riscos de forma eficiente e eficaz, os quais devem ser considerados no momento de estabelecer a estrutura e o processo de Gestão de Riscos na organização. Os princípios destacados pela ABNT (2018) são:

- ✓ **gestão de riscos integrada:** parte integrante de todas as atividades organizacionais;
- ✓ **gestão de riscos estruturada e abrangente:** contribui para resultados consistentes e comparáveis;
- ✓ **gestão de riscos personalizada:** estrutura e processo personalizados e proporcionais aos contextos interno e externo da organização;

- ✓ **gestão de riscos inclusiva:** com o envolvimento oportuno e apropriado das partes interessadas;
- ✓ **gestão de riscos dinâmica:** antecipa, detecta, reconhece e reage a mudanças e eventos de forma oportuna e apropriada;
- ✓ **gestão de riscos baseada na melhor informação disponível:** informações históricas, atuais e em expectativas futuras, considerando explicitamente quaisquer limitações e incertezas relacionadas às informações e expectativas;
- ✓ **gestão de riscos considera fatores humanos e culturais:** comportamento humano e cultura influenciam todos os aspectos da gestão de riscos em cada nível e estágio;
- ✓ **gestão de riscos busca a melhoria contínua:** é melhorada continuamente a partir do aprendizado e das experiências.

O Decreto n° 9.203/2017 descreve a Gestão de Riscos por meio **destas características**:

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

Ainda com fundamento no Decreto n° 9.203/2017, a Gestão de Riscos deve **observar os seguintes princípios**:

- ✓ *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 risco, controle e governança.*

6. COMPONENTES DA GESTÃO DE RISCOS

Assim como há definições distintas para o que é risco, existem modelos referenciais produzidos por diferentes fontes no que tange ao gerenciamento de riscos. A Política de Gestão de Riscos da UFCSPA faz menção à IN Conjunta MP/CGU n° 01/2016 e à ISO 31000 como bases conceituais utilizadas para definir o modelo de gerenciamento de riscos na instituição.

O artigo 16 da IN Conjunta MP/CGU n° 01/2016 enumera os componentes da Gestão de Riscos a serem considerados pela alta administração e pelos servidores ou funcionários.

Ambiente interno: "*inclui, entre outros elementos, integridade, valores éticos e competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, estrutura de governança organizacional e políticas e práticas de recursos humanos. O ambiente interno é a base para todos os outros componentes da estrutura de gestão de riscos, provendo disciplina e prontidão para a gestão de riscos*".

Fixação de objetivos: "*todos os níveis da organização (departamentos, divisões, processos e atividades) devem ter objetivos fixados e comunicados. A explicitação de objetivos, alinhados à missão e à visão da organização, é necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução".*

Identificação de eventos: "*devem ser identificados e relacionados os riscos inerentes à própria atividade da organização, em seus diversos níveis".*

Avaliação de riscos: "*os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. A avaliação de riscos deve ser feita por meio de análises qualitativas, quantitativas ou da combinação de ambas. Os riscos devem ser avaliados quanto à sua condição de inerentes e residuais"*.

Resposta a riscos: "*o órgão/entidade deve identificar qual estratégia seguir (evitar, transferir, aceitar ou tratar) em relação aos riscos mapeados e avaliados. A escolha da*

estratégia dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco".

Atividades de controles internos: "*são as políticas e os procedimentos estabelecidos e executados para mitigar os riscos que a organização tenha optado por tratar. Também denominadas de procedimentos de controle, devem estar distribuídas por toda a organização, em todos os níveis e em todas as funções. Incluem uma gama de controles internos da gestão preventivos e detectivos, bem como a preparação prévia de planos de contingência e resposta à materialização dos riscos*".

Informação e comunicação: "*informações relevantes devem ser identificadas, coletadas e comunicadas, a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas, que possibilitem o gerenciamento de riscos e a tomada de decisão. A comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos que permitam que a informação flua em todos os sentidos*".

Monitoramento: "*tem como objetivo avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos*".

(BRASIL, 2016).

A ISO 31000, por sua vez, aborda o processo de Gestão de Riscos baseado nas etapas de: *estabelecimento do contexto, identificação de riscos, análise de riscos, avaliação de riscos, tratamento de riscos, comunicação e consulta, monitoramento e análise crítica, registro e relato* (ABNT, 2018). A Figura 4 retrata as interações entre os elementos do processo de Gestão de Riscos.

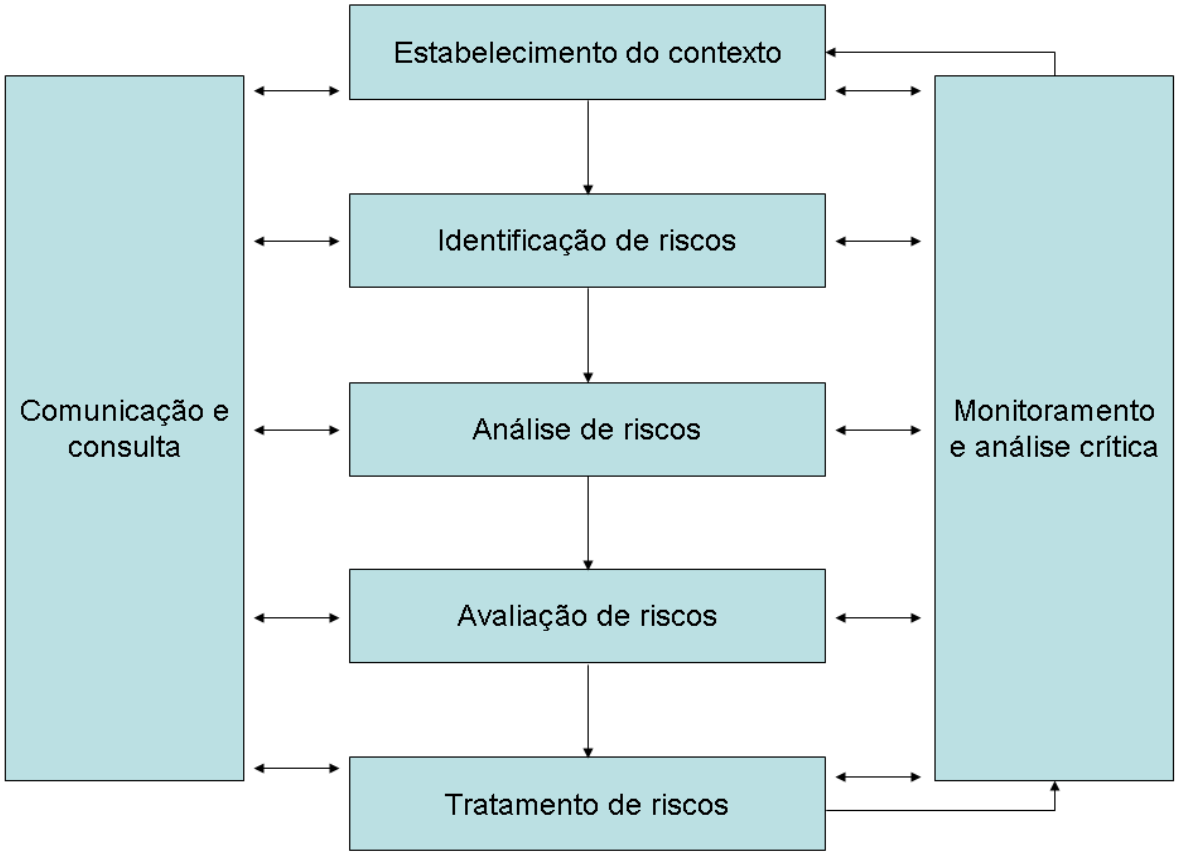

Figura 4: Processo de Gestão de Riscos.
Fonte: adaptado de ABNT, 2009.

A metodologia descrita no Plano de Gestão de Riscos da UFCSPA está alinhada ao processo de Gestão de Riscos sugerido pela ISO 31000, conforme detalhamento a seguir.

- *Avaliação do contexto*

Abrange a análise dos **ambientes externo e interno** que podem influenciar no cumprimento dos objetivos definidos no Planejamento Estratégico, bem como a identificação do escopo e dos demais critérios norteadores do processo de Gestão de Riscos. Compreender o contexto no qual a organização está inserida é fundamental para que a avaliação e o tratamento dos riscos sejam apropriados, uma vez que fatores associados à instituição podem potencializar determinados riscos.

O **contexto externo** diz respeito aos ambientes cultural, social, político, legal, regulatório, financeiro, tecnológico e econômico, bem como às relações com as partes interessadas externas, suas percepções e valores, além de tendências que tenham impacto sobre os objetivos da instituição.

Por outro lado, o **contexto interno** compreende a missão, visão e valores; a governança; a estrutura organizacional; funções e responsabilidades; recursos humanos, financeiros e tecnológicos; fluxos de informação e processos de tomada de decisão; relações

com as partes interessadas internas, suas percepções e valores; cultura organizacional; normas internas, diretrizes e modelos adotados.

A construção de uma *Matriz SWOT*, cujas iniciais são originárias das palavras inglesas *Streghts* (forças), *Weaknesses* (fraquezas), *Opportunities* (oportunidades) e *Threats* (ameaças), pode ser útil na etapa de avaliação do contexto. As forças e fraquezas pertencem ao ambiente interno de uma organização, enquanto as oportunidades e ameaças derivam do ambiente externo. A Figura 5 detalha o significado de cada uma delas.

Ambiente interno	
Streghts (S)	*Weaknesses (W)*
Características **positivas internas** que podem ser exploradas pela organização. Referem-se às habilidades, capacidades e competências básicas envolvidas para ajudá-la no alcance de suas metas e objetivos. **Exemplos:** servidores jovens e qualificados; instalações modernas; especialização em saúde; etc.	Características **negativas internas** que podem dificultar o desempenho da organização. Referem-se à ausência de capacidades ou de habilidades. São, portanto, deficiências que tratadas para que a instituição possa atingir o desempenho desejado. **Exemplos:** problemas de comunicação; ausência de mapeamento de processos críticos; espaço físico limitado e mal distribuído; etc.
Ambiente externo	
Opportunities (O)	*Threats (T)*
Características **positivas externas, não controláveis pela organização**, com potencial para impulsioná-la a crescer e atingir ou exceder as metas planejadas. **Exemplos:** financiamentos internacionais; parcerias público-privadas; *cluster* da saúde; etc.	Características **negativas externas, não controláveis pela organização**, que podem dificultar o alcance das metas planejadas e comprometer o crescimento da instituição. **Exemplos:** crise econômica; conjuntura política; congelamento dos planos de carreira; etc.

Figura 5: Dimensões da Matriz SWOT.
Fonte: adaptado de BRASIL, 2003. Exemplos extraídos de UFCSPA, 2019.

- *Identificação do risco*

Tem por finalidade buscar, reconhecer e descrever os riscos que possam vir a impactar o alcance dos objetivos nos mais variados níveis da organização. Envolve a **identificação das fontes de risco, dos eventos, suas causas e consequências potenciais**. É pertinente frisar que um mesmo evento pode estar associado a várias causas e consequências.

Nesta fase, sessões de *brainstorming* (tempestade de ideias) podem trazer diversas contribuições espontâneas dos participantes, por meio de visões distintas sobre um mesmo objeto, o que favorece a elucidação dos riscos. Sugere-se buscar a opinião de pessoas com conhecimento sobre o processo, atividade, projeto ou assunto relativo ao escopo do processo de Gestão de Riscos, a fim de se obter informações apropriadas e atualizadas. Os gestores podem também utilizar dados históricos e evidências técnicas (relatórios de auditoria, por exemplo) para subsidiar a identificação de riscos.

O emprego de técnicas para explorar relações de causa e efeito (Diagrama de Ishikawa, "5 Porquês", Análise "*Bow tie*", entre outras), a aplicação de questionários, o uso de *checklists* e a realização de entrevistas podem auxiliar na tarefa de descrever o risco.

- *Análise do risco*

Visa **compreender a natureza do risco e determinar o seu nível**. É nesta fase que ocorrem, por exemplo: a apreciação das causas e das fontes do risco, o exame das consequências (impacto) e a estimativa da probabilidade (a partir de dados históricos, da opinião de especialistas, de apontamentos de auditorias, etc.). A análise fornece a base para avaliação dos riscos e tomada de decisão quanto ao tratamento a ser adotado perante cada evento de risco.

O nível do risco é obtido pela combinação da probabilidade e do impacto associados a um evento, que podem ser aferidos por meio de critérios qualitativos ou quantitativos pré-definidos. Os parâmetros para mensuração dos riscos na UFCSPA serão apresentados oportunamente em seção específica deste guia.

- *Avaliação do risco*

Trata da **comparação dos resultados da análise de riscos com os critérios estabelecidos**, com base nos objetivos estratégicos e no contexto externo e interno, considerando as normas, leis, políticas e outros requisitos, a fim de determinar se o risco e sua magnitude são aceitáveis para a instituição, se os controles existentes são desnecessários, suficientes ou se precisa de novas formas de tratamento.

Caso o risco necessite de tratamento, deve-se avaliar também **o grau de prioridade e a relação custo/benefício de implementar novos controles**.

- *Tratamento do risco*

É etapa relativa à modificação do risco, após avaliá-lo. O risco pode ser modificado em termos de sua probabilidade ou de seu impacto (consequência), o que pode significar a adoção de novos controles ou a revisão dos existentes. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido pela organização, assim como da avaliação que se fez do risco. As respostas ao risco previstas no Plano de Gestão de Riscos da UFCSPA são:

Evitar: "*as atividades que geram os riscos são suspensas, produtos são substituídos ou até mesmo projetos são descontinuados*".

Reduzir ou Mitigar: "*são adotadas medidas para reduzir a probabilidade ou o impacto dos riscos, ou, até mesmo, ambos, levando-os à limites aceitáveis*".

Transferir ou Compartilhar: "*redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção dos riscos para outra parte, mas sem eliminá-los*".

Aceitar: "*nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos, ou não se conseguiu identificar outra estratégia de resposta adequada*".

(UFCSPA, 2018).

Cabe ressaltar que **existirá um nível remanescente do risco mesmo após o tratamento (risco residual)**, exceto se a resposta escolhida for de evitar o risco, pois esta consiste na suspensão ou descontinuidade das atividades que geram riscos. No entanto, no caso de uma universidade, por exemplo, certas atividades relacionadas ao ensino, à pesquisa e à extensão não poderão deixar de acontecer, uma vez que tais macroprocessos representam a razão de ser da instituição. Logo, evitar os riscos decorrentes de atividades essenciais não parece ser uma alternativa plausível, porém é possível gerenciá-los de outras maneiras, a fim de que seu nível se torne compatível com o apetite estabelecido.

No que concerne às **atividades de controle, podem ser preventivas (reduzir a ocorrência de eventos de risco) ou detectivas (possibilitar a identificação dos eventos de risco), bem como executadas de forma manual ou automatizada**. Alguns exemplos de atividades de controle, previstos na IN Conjunta MP/CGU n° 01/2016, são:

- *procedimentos de autorização e aprovação;*
- *segregação de funções (autorização, execução, registro, controle);*
- *controles de acesso a recursos e registros;*
- *verificações;*
- *conciliações;*
- *avaliação de desempenho operacional;*
- *avaliação das operações, dos processos e das atividades;*
- *supervisão; etc.*

Se houver necessidade de aprimoramento dos controles existentes ou de criação de novos controles em determinado processo organizacional, os setores envolvidos devem elaborar um plano de ação (Figura 6), o qual deve contemplar a atribuição de responsabilidades

sobre o controle dos riscos, bem como a definição de prazos e estratégias para a implantação das medidas que tratarão os riscos mapeados.

Para tanto, sugere-se adotar uma versão adaptada do método 5W2H, de modo a constituir um plano de ação que considere os principais aspectos da resposta ao risco, conforme modelo previsto no Plano de Gestão de Riscos da UFCSPA.

WHAT	O que será feito?	Descrever claramente a ação que será realizada.
WHY	Por que será feito?	Indicar o objetivo da ação e justificar a necessidade de sua realização.
WHO	Quem fará?	Nominar e individualizar responsabilidade para cada ação do plano.
WHEN	Quando será feito?	Precisar as datas previstas de início e fim de execução de cada ação.
WHERE	Onde será feito?	Local, unidade, processo, sistema, programa, etc.
HOW	Como será feito?	Maneira, método ou solução adotada.

Figura 6: Modelo de Plano de ação.
Fonte: adaptado de UFCSPA, 2018.

- *Informação e comunicação*

São **fluxos contínuos para produzir, fornecer, compartilhar ou obter informações e dialogar com as partes interessadas**. Inclui selecionar e divulgar as informações pertinentes e adequadas para o gerenciamento de risco.

Informações relevantes comunicadas de modo eficaz podem, entre outros benefícios: auxiliar na avaliação do contexto e na identificação dos riscos; reunir diferentes conhecimentos para análise e avaliação dos riscos; garantir o apoio para implementação de um plano de tratamento; e aprimorar a gestão de mudanças durante o processo de Gestão de Riscos.

- *Monitoramento*

Consiste em **verificar, supervisionar e analisar criticamente o processo de Gestão de Riscos, a fim de identificar mudanças no nível de desempenho desejável**. O monitoramento e a análise crítica incluem ações como: detectar mudanças no contexto e no risco; verificar a efetividade dos controles; atualizar registros de riscos e documentos relacionados; documentar informações para melhoria do processo.

Se, em decorrência do monitoramento, for constatado o descumprimento das medidas preventivas e corretivas, o fato deve ser comunicado à autoridade competente, com vistas à regularização tempestiva do tratamento do risco.

Recomenda-se, pois, a adoção do processo de Gestão de Riscos analisado nesta seção, para que a prática ocorra de forma sistemática e fundamentada. Ademais, sugere-se a observância dos aspectos metodológicos abordados na seção a seguir.

7. METODOLOGIA ADOTADA PELA UFCSPA

O processo de Gestão de Riscos descrito pode ser incorporado tanto ao planejamento estratégico como aos demais processos organizacionais, às atividades e aos projetos em todos os níveis da instituição, de forma sistemática, estruturada, oportuna e documentada.

A aferição da magnitude dos riscos e a avaliação do tratamento mais adequado consideram os parâmetros dispostos na Política e no Plano de Gestão de Riscos da UFCSPA.

A probabilidade de ocorrência de um evento pode variar entre baixa, média e alta, conforme respectivas definições:

1. **Baixa:** *evento casual e inesperado, com poucas possibilidades de ocorrência.*
2. **Média:** *evento esperado, de frequência reduzida, e com histórico de ocorrência.*
3. **Alta:** *evento usual, com grandes possibilidades de ocorrência.*

De modo semelhante, a consequência ou impacto do risco pode variar entre baixo, médio e alto, sendo que:

1. **Baixo:** *não afeta o alcance dos objetivos.*
2. **Médio:** *torna incerto o alcance dos objetivos.*
3. **Alto:** *torna improvável ou inviabiliza o alcance dos objetivos.*

Dessa forma, o nível de risco pode ser obtido a partir da multiplicação da probabilidade pelo impacto, como sugere a Figura 7.

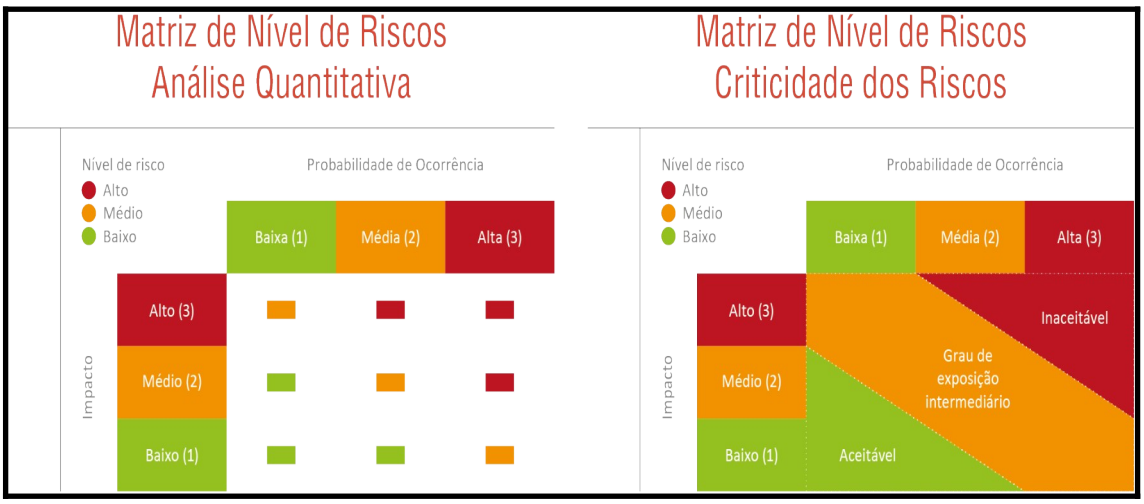

Figura 7: Matriz de Nível de Risco.
Fonte: adaptado de UFCSPA, 2018. Elaboração: Assessoria de Comunicação Social da UFCSPA.

A **Matriz de Nível de Risco ilustra os cruzamentos de probabilidade e impacto**, de maneira a possibilitar avaliação da criticidade dos riscos segundo os quadrantes em verde, amarelo e vermelho. Quanto maior a probabilidade e o impacto de um risco, maior será seu nível de criticidade.

A figura demonstra ainda os graus de exposição aos riscos, recorrendo ao conceito de apetite ao risco. Cumpre lembrar que este nada mais é do que o nível de risco ao qual a instituição está disposta a se submeter ou aceitar. Os níveis de aceitação aos riscos podem ser definidos como:

Nível de Risco Aceitável, *quando o grau de exposição atinge os valores entre 1 e 2.*

Nível de Aceitação Intermediária, *quando o grau de exposição atinge valores entre 3 e 4.*

Nível de Risco Inaceitável, *quando o grau de exposição atinge valores superiores a 4.*

O resultado da avaliação de risco nos processos organizacionais indicará se o gestor deve aperfeiçoar os controles internos existentes ou instituir novos controles, o que implicará estabelecer planos de ação, com a atribuição de responsabilidades, prazos e estratégias para a implantação ou revisão dos controles que tratarão os riscos.

É pertinente salientar que o Plano de Gestão de Riscos da UFCSPA propõe modelos de formulário para apoiar as etapas de identificação, análise, avaliação e tratamento dos riscos. A estrutura do "*Formulário de Mapeamento de Riscos*" é demonstrada no Quadro 1, juntamente com alguns exemplos hipotéticos de preenchimento.

IDENTIFICAÇÃO DO RISCO							AVALIAÇÃO DO RISCO			TRATAMENTO DO RISCO				
#	**Processo / Subprocesso / Atividade**	**Eventos de Risco**	**Causas**	**Efeitos / Consequências**	**Classificação do Risco**	**Proprietário do Risco**	**P**	**I**	**NR**	**Resposta ao risco**	**Medidas de Tratamento (controles / ações propostas)**	**Responsável**	**Prazo**	**Situação (iniciado / em tratamento / não iniciado**
1	Gestão laboratorial	Acidente com produto químico	Descumprimento de rotinas de prevenção	Dano permanente à saúde dos atingidos	Operacional	Unidade de gestão laboratorial	1	3	3 - Médio	Reduzir ou mitigar	1. Identificar adequadamente os produtos perigosos 2. Orientar os usuários sobre cuidados a serem observados no laboratório 3. Adotar medidas de proteção individual 4. Treinar a equipe sobre ações necessárias em caso de pronto atendimento	Responsável da unidade de gestão laboratorial	1. 30/09/2021 2. 31/08/2021 3. 31/08/2021 4. 30/09/2021	Em tratamento
2	Aquisições de bens	Material não atender às necessidades	Falha na especificação dos itens a serem contratados	Prejuízo às atividades acadêmicas e administrativas	Operacional	Unidade de gestão das aquisições	2	2	4 - Médio	Reduzir ou mitigar	1. Capacitar os servidores dos setores envolvidos nas aquisições de bens	Responsável da unidade de gestão das aquisições	1. 31/10/2021 2. Imediato 3. 31/08/2021	1. Não iniciado 2. Iniciado 3. Em tratamento

IDENTIFICAÇÃO DO RISCO							AVALIAÇÃO DO RISCO			TRATAMENTO DO RISCO				
#	Processo / Subprocesso / Atividade	Eventos de Risco	Causas	Efeitos / Consequências	Classificação do Risco	Proprietário do Risco	P	I	NR	Resposta ao risco	Medidas de Tratamento (controles / ações propostas)	Responsável	Prazo	Situação (iniciado / em tratamento / não iniciado
											2. Segregar funções essenciais no processo de aquisição 3. Executar atividade de revisão dos editais e termos de referência 4. Aproveitar materiais disponíveis para atender às necessidades imediatas		4. Imediato	

Quadro 1 - Formulário de Mapeamento de Riscos.
Fonte: adaptado de UFCSPA, 2018.

Classificação do risco: operacional; de imagem; legal; ou financeiro / orçamentário. Ver detalhes na seção 4.

Probabilidade (P): 1- baixa; 2 – média ; 3 – alta.

Impacto (I): 1 – baixo; 2 – médio; 3 – alto.

Nível de risco (NR): 1 e 2 – baixo; 3 e 4 – médio; 6 e 9 – alto.

Resposta ao risco: reduzir; evitar; compartilhar (transferir); ou aceitar.

Outro modelo indicado no Plano de Gestão de Riscos é o "*Formulário de Plano de Ação*", o qual se baseia no método 5W2H, como se observa no Quadro 2.

O QUÊ?						ONDE?
#	**Processo / Subprocesso / Atividade**	**Eventos de Risco**	**Descrição**	**Tipo**	**Objetivo**	**Área Responsável pela Implementação**
1	Gestão laboratorial	Acidente com produto químico	Decorrente do descumprimento de rotinas de prevenção, com potencial dano permanente à saúde dos atingidos	Risco operacional	Realizar as atividades laboratoriais de forma segura para os usuários	Unidade de gestão laboratorial
2	Aquisições de bens	Material não atender às necessidades	Decorrente de falha na especificação dos itens a serem contratados, com potencial prejuízo às atividades acadêmicas e administrativas	Risco operacional	Prover os materiais necessários para as atividades acadêmicas e administrativas	Unidade de gestão das aquisições

Continuação

QUEM?		COMO?		QUANDO?		
#	**Responsável pela Implementação**	**Como será Implementado**	**Intervenientes**	**Data de Início**	**Data da Conclusão**	**Status**
1.1	Responsável da unidade de gestão laboratorial	Identificar adequadamente os produtos perigosos	Grupo técnico formado por especialistas no assunto	01/07/2021	30/09/2021	Em tratamento
1.2	Responsável da unidade de gestão laboratorial	Orientar os usuários sobre cuidados a serem observados no laboratório	Técnicos em laboratório	01/07/2021	31/08/2021	Em tratamento
(...)	(...)					
2.1	Responsável da unidade de gestão das aquisições	Capacitar os servidores dos setores envolvidos nas aquisições de bens	Área de gestão de pessoas	01/10/2021	31/10/2021	Não iniciado
2.2	Responsável da unidade de gestão das aquisições	Segregar funções essenciais no processo de aquisição	Não há	01/07/2021	01/07/2021	Iniciado
(...)	(...)					

Quadro 2 - Formulário de Plano de Ação.
Fonte: adaptado de UFCSPA, 2018.

Existem também as orientações emanadas do Núcleo de Qualidade Interna (NQI), no âmbito do *Modelo de Maturidade em Mapeamento de Processos da UFCSPA (M3P)*. O método apresentado pelo NQI é composto de oito níveis de maturidade, sendo 0 o menor e 7 o maior. Para alcançar determinado nível, os setores devem aplicar todos os critérios referentes ao nível desejado, assim como satisfazer os requisitos associados aos estágios de maturidade anteriores.

No intuito de integrar o gerenciamento de riscos ao mapeamento de processos, o NQI incluiu, como um dos critérios para a avaliação no M3P (Figura 8) a necessidade de os setores identificarem e realizarem a gestão dos riscos relacionados aos seus processos. Para isso, é utilizado o padrão institucional definido para o gerenciamento de riscos.

Critérios	Nível 0	Nível 1	Nível 2	Nível 3	Nível 4	Nível 5	Nível 6	Nível 7
I	O objetivo da unidade é conhecido pela equipe.	O objetivo da unidade está definido e documentado.	Os processos com **alta prioridade** estão mapeados e documentados.	Os processos com **alta e média prioridade** estão mapeados e documentados.	**Todos os processos** estão mapeados e documentados.	As ações de integração de **25% dos processos críticos** foram iniciadas e estão documentadas.	As ações de integração de **50% dos processos críticos** foram iniciadas e estão documentadas.	As ações de integração de **100% dos processos críticos** foram iniciadas e estão documentadas.
II	Os processos são executados.	A Lista de Serviços está preenchida, os processos estão codificados e priorizados.	O checklist do M3P foi aplicado em cada um dos diagramas BPMN dos processos mapeados.	A gestão dos riscos relacionados aos processos estratégicos está definida e documentada.	A relação dos processos com o Planejamento Estratégico está documentada.	A relação dos processos estratégicos com a Cadeia de Valor está definida e documentada.	O curso de Fundamentos em Indicadores de Processos foi realizado pela unidade.	As ações para garantir a implantação da melhoria contínua dos processos estão definidas, documentadas e são sistematicamente executadas.
III			Um ou mais cursos na área de Gestão por Processos oferecidos pela instituição foram realizados pela unidade.			O curso de Fundamentos em Gestão por Processos foi realizado pela unidade.	Os objetivos de medição e indicadores associados estão definidos e relacionados a processos.	

Figura 8 -: Níveis e Critérios do M3P 5ª edição.
Fonte: Herbert, J. S. et al. (2021).

Na próxima seção, serão abordadas algumas técnicas que podem auxiliar na tarefa de mapeamento dos riscos e seus tratamentos.

8. TÉCNICAS DE DIAGNÓSTICO APLICÁVEIS

Existem, na literatura sobre administração, técnicas de diagnóstico que podem auxiliar nas etapas de identificação, análise, avaliação e tratamento dos riscos. O Tribunal de Contas da União (TCU) sugere, por meio do Referencial Básico de Gestão de Riscos, a utilização de técnicas como: *brainstorming*, entrevistas, Delphi, análise de causa raiz, *What-if*, análise *bow tie*, listas de verificação (*checklists*) entre outras (BRASIL, 2018).

Embora não esteja entre as pretensões deste guia detalhar minuciosamente cada uma das técnicas para o diagnóstico de riscos, cabe descrever resumidamente, segundo o entendimento constante do Referencial Básico de Gestão de Riscos, as características daquelas que foram mencionadas.

- *Brainstorming*

Consiste em reunir pessoas que de preferência conheçam um processo ou ativo organizacional e estimular a conversa entre elas livremente, com o objetivo de identificar possíveis perigos, riscos ou controles relativos ao objeto analisado. Esta técnica é bastante indicada para identificar riscos de novas atividades, tecnologias recentes ou em situações em que não há dados disponíveis. O produto a ser gerado depende do contexto, podendo ser, por exemplo, uma lista de riscos e de controles.

- Entrevistas

Baseia-se na formulação prévia de perguntas norteadoras para o entrevistador, as quais são apresentadas oportunamente aos entrevistados. Em se tratando da gestão de riscos, o propósito da entrevista é obter informações sobre eventos de risco, fontes, consequências e controles.

Nas entrevistas estruturadas, o roteiro é totalmente pré-definido, enquanto nas semi-estruturadas o entrevistador tem maior liberdade para explorar questões que podem surgir durante a conversa. Esta técnica é indicada nas situações em que se torna complicado ou custoso reunir pessoas para análise conjunta, bem como nos casos em que é necessário ouvir opiniões pessoais sem quaisquer interferências ou influências de outros participantes.

- Técnica de Delphi

O objetivo da técnica é alcançar consenso entre opiniões de especialistas sobre determinado objeto da Gestão de Riscos, mediante uma série de questionamentos respondidos individualmente e de forma anônima, a fim de estimular a espontaneidade.

Inicialmente, a problemática de estudo é identificada e são elaboradas as questões para coleta de dados. O questionário é disponibilizado aos especialistas, de modo independente, e suas respostas são então sintetizadas e apresentadas ao grupo sem identificar os respondentes. Assim, em sucessivas rodadas, cada especialista tem acesso aos pontos de vista dos demais, o que torna possível a convergência de opiniões até que o consenso seja obtido.

A técnica pode ser aplicada em qualquer etapa do processo de Gestão de Riscos e gerar, entre outros produtos, uma lista de riscos identificados, níveis de riscos mensurados e opções para tratamento dos riscos acordadas.

- Análise de causa raiz

A sua finalidade é desvendar a raiz ou causas originais, em vez de lidar apenas com os efeitos imediatos e óbvios, com base na ideia de que é preferível focar o menor conjunto de causas responsáveis pela geração do risco. O exame das causas geralmente evolui de causas mais evidentes para as anteriores, relacionadas a fatores humanos, tecnológicos, materiais, ambientais, etc. A análise de causa raiz corresponde às seguintes técnicas: “Cinco Porquês“, árvore de falhas, Diagrama de Ishikawa (espinha de peixe), análise de Pareto, entre outras.

A seguir, um exemplo do uso dos porquês para se chegar à causa raiz. No caso ilustrado na Figura 9, a sequência de questionamentos "Por quê?", a partir do problema ou evento central, faz com que sejam desvendadas as causas raízes 1.2.1 e 2.1.1. Quando estas acontecem, resultam nas causas 1.2 e 2.1, respectivamente, as quais contribuem, por sua vez, para ocorrência das causas 1 e 2, imediatamente relacionadas ao problema ou evento central.

Embora a técnica faça menção a cinco indagações "Por quê?", não será necessário efetuá-las na totalidade se a causa raiz for encontrada antes.

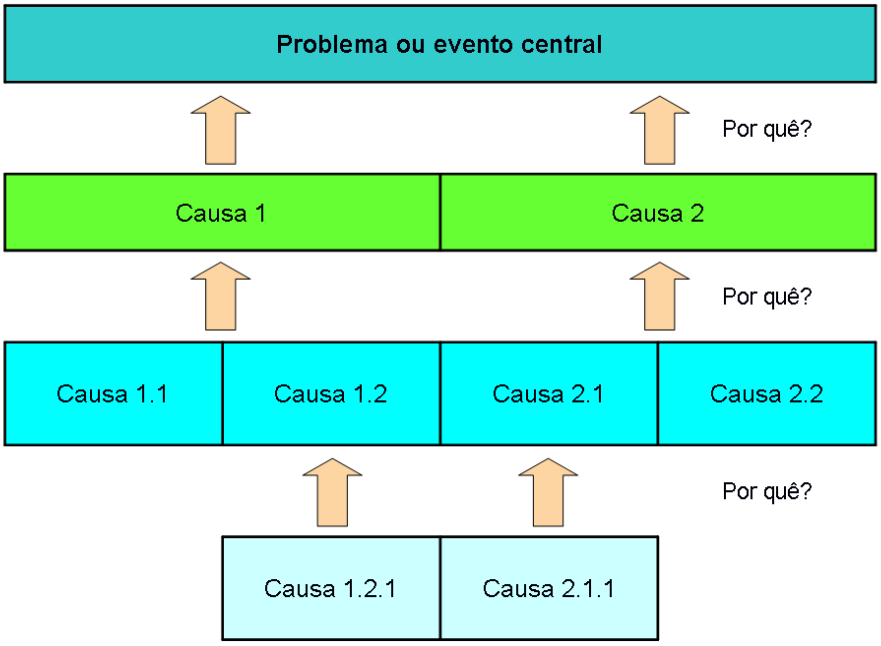

Figura 9 - Técnica dos porquês.
Fonte: Elaborada pelo autor.

- E se estruturada (What-if)

Técnica realizada em equipe, com a participação de pessoas envolvidas diretamente com o objeto examinado ou que tenham informações a respeito, mediadas por um facilitador, no intuito de identificar riscos em processos, atividades ou sistemas.

Antes do início das discussões, o facilitador define, a partir dos documentos e informações disponíveis, um plano de aplicação da metodologia e elabora um roteiro que possibilite uma análise crítica de perigos ou riscos pelos participantes. Nas oficinas ou reuniões, o facilitador estimula o grupo a refletir quanto a possíveis cenários e alternativas, experiências e incidentes, riscos associados, eventuais controles existentes e sua eficácia, bem como sobre a necessidade de medidas adicionais para tratar os riscos.

As reflexões são fomentadas por meio de questionamentos que contemplam as expressões **"e se...?"**, **"o que aconteceria se...?"**, **"alguém ou algo pode...?"**, **"alguém ou algo nunca...?"**. A técnica viabiliza a descrição de eventos, fontes de riscos, consequências,

controles, além de ações de tratamento a serem priorizadas, que devem ser confirmados com a equipe e registrados.

- Análise *bow tie*

Descreve a relação entre um evento de risco, suas causas (de um lado) e consequências (de outro), por meio de uma ilustração (Figura 10) semelhante a uma gravata borboleta (bow tie). O método considera também as barreiras entre as causas que levam ao evento de risco e as barreiras entre este e suas consequências.

A elaboração da *bow tie* deve contemplar os seguintes elementos:

- o evento de risco é o nó da gravata borboleta;
- as possíveis causas ou fontes do evento de risco são listadas no lado esquerdo e cada uma delas é conectada por uma linha ao nó da gravata;
- as barreiras que impedem ou diminuem a possibilidade da causa ou fonte produzir o evento de risco são simbolizadas como barras verticais interceptando as linhas do lado esquerdo. São controles preventivos;
- do lado direito do evento, identificam-se as possíveis consequências e cada uma delas é ligada ao nó central por uma linha;
- as barreiras que impedem ou diminuem o efeito são simbolizadas como barras verticais interceptando as linhas do lado direito. São controles reativos, visando à atenuação dos efeitos no caso de o risco se materializar.

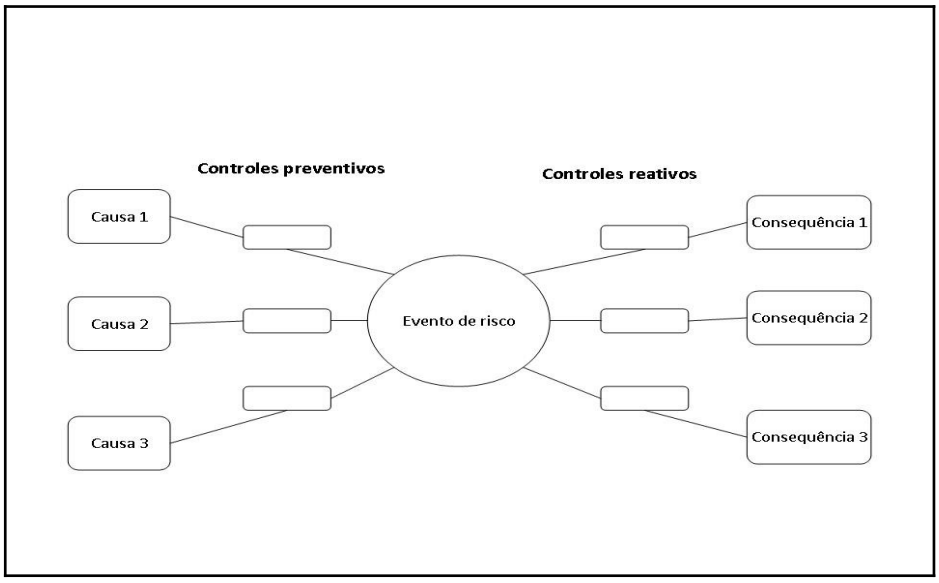

Figura 10 - Análise *Bow Tie*. Fonte: Elaborada pelo autor.

- Listas de verificação (*checklists*)

São listas pré-existentes de perigos ou riscos utilizadas como instrumento de apoio a outras técnicas de diagnóstico. As listas podem ser originárias da própria experiência, de boas práticas, de uma Análise Preliminar de Perigos, bem como de registros de incidentes.

A aplicação consiste em comparar as informações contidas na lista (eventos, fontes de risco, controles, por exemplo) e a situação ou o objeto avaliado. As constatações resultantes podem dizer respeito a riscos inaceitáveis, controles inadequados ou ausentes, entre outras.

9. ESTRUTURA PARA GERIR RISCOS NA UFCSPA

O estabelecimento de **estrutura apropriada para a Gestão de Riscos é requisito essencial à integração desta na governança, nos processos e atividades organizacionais, assim como na tomada de decisões**. Os aspectos da estrutura e o seu funcionamento podem ser mais ou menos adequados de acordo com as particularidades de cada instituição, portanto não existe formato padrão de estrutura a ser implantado indistintamente em todas as organizações.

A ISO 31000 indica que a montagem da estrutura se decompõe nas fases de: **integração, concepção, implementação, avaliação e melhoria.** A norma enfatiza a importância do papel desempenhado pela alta administração no sentido de demonstrar liderança e comprometimento para a consolidação dos componentes da estrutura de gestão de riscos. Nesse sentido, uma das ações necessárias é a definição de uma política norteadora da abordagem referente a risco na organização (ABNT, 2018).

No ano de 2017, o Conselho Universitário aprovou, mediante a Resolução nº 39/2017, a **Política de Gestão de Riscos da UFCSPA**. O referido documento veio estabelecer conceitos, diretrizes, atribuições e responsabilidades do processo de Gestão de Riscos, bem como orientar a identificação, a análise, a avaliação, o tratamento, o monitoramento e a comunicação dos riscos na UFCSPA, com vistas ao alcance dos objetivos institucionais.

Em conformidade com a Política de Gestão de Riscos, a estrutura interna para gerir riscos (Quadro 3) envolve “linhas de defesa” das quais participam: a alta administração; os gestores das áreas; o Comitê de Governança Riscos e Controles; a Comissão de Gestão de Riscos; e a Auditoria Interna. De acordo com as funções de cada uma em relação aos controles internos da gestão, podem estar situadas em uma das três “linhas de defesa” da organização, sendo que **a primeira linha operacionaliza controles, a segunda os monitora e a terceira realiza avaliações independentes do sistema de controles da gestão**.

Camada	Função	Agentes
1ª Linha	Gerencia e tem propriedade sobre os riscos. É responsável por implementar as ações corretivas para solucionar deficiências nos processos e controles sob a sua alçada.	Gestores e suas equipes
2ª Linha	Engloba funções de gerenciamento de riscos e conformidade, com o propósito de auxiliar a 1ª linha no desenvolvimento e monitoramento dos controles da gestão. Difere da 3ª linha por não ter a prerrogativa de independência em relação à administração.	- Comitê de Governança, Riscos e Controles; - Comissão de Gestão de Riscos; - Unidade de Gestão da Integridade
3ª Linha	Fornece avaliações independentes e objetivas sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos. Reporta-se à estrutura de governança da organização.	Auditoria Interna

Quadro 3 - Modelo de 3 Linhas de Defesa na UFCSPA.
Fonte: adaptado de IIA, 2013.

- *Alta administração*

O dirigente máximo é o principal responsável por instituir a estratégia e a estrutura de gerenciamento de riscos na UFCSPA, o que inclui o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão. Ademais, a alta administração é responsável por prover os recursos necessários ao gerenciamento de riscos; identificar papéis e responsabilidades; iniciar as atividades de gestão de riscos; e aprovar pontos importantes relativos ao assunto.

- *Gestores das áreas*

A responsabilidade no plano operacional compete aos gestores. Na incidência de riscos, todos numa determinada unidade devem ter conduta pró-ativa e alertar aos responsáveis os perigos e consequências caso não sejam adotadas medidas corretivas.

No que tange a essa questão, a IN Conjunta MP/CGU n° 01/2016 dispõe em seu artigo 20:

> Art. 20. Cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente identificado.
>
> § 1° O agente responsável pelo gerenciamento de determinado risco deve ser o gestor com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco.
>
> § 2° São responsabilidades do gestor de risco:

> I — assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos da organização;
>
> II — monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos; e
>
> III — garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da organização.

Embora as ações de mapeamento, avaliação e mitigação dos riscos estejam associadas diretamente aos gestores que detêm conhecimento e alçada suficiente para tanto, a Coordenação de Desenvolvimento Institucional e o Núcleo de Qualidade Interna atuam no assessoramento técnico em questões pertinentes a gerenciamento de riscos e mapeamento de processos, respectivamente.

- *Comitê de Governança, Riscos e Controles*

É composto pelo dirigente máximo e por dirigentes de unidades a ele diretamente subordinadas, sob a presidência do primeiro. Competem a este comitê estratégico **funções associadas à "segunda linha de defesa" no sistema de controles internos da gestão**, entre as quais as previstas na Política de Gestão de Riscos da UFCSPA:

> a) designar a Comissão de Gestão de Riscos da UFCSPA;
>
> b) aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;
>
> c) promover o desenvolvimento contínuo e a integração dos agentes públicos, incentivando a adoção de boas práticas de governança, de gestão de riscos e de controles internos;
>
> d) garantir a observância às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;
>
> e) supervisionar o mapeamento e avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público e monitorar as recomendações e orientações deliberadas pelos órgãos de controle interno e externo;
>
> f) liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão ou entidade;
>
> g) estabelecer limites de exposição a riscos globais do órgão, bem como os limites de alçada ao nível de unidade, política pública, ou atividade;
>
> h) emitir recomendações para o aprimoramento da governança, da gestão de riscos e dos controles internos.

- *Comissão de Gestão de Riscos*

Segundo a Política de Gestão de Riscos da UFCSPA, trata-se de um grupo formado por representantes indicados pelas coordenações das seguintes áreas:

- Assessoria de Comunicação Social;

- Comitê de Biossegurança;
- Coordenação de Assuntos Estudantis;
- Coordenação de Desenvolvimento Institucional;
- Coordenação de Engenharia;
- Coordenação de Pesquisa;
- Departamento de Administração de Pessoas;
- Departamento de Compras e Contratos;
- Departamento de Contabilidade e Finanças;
- Departamento de Registro e Controle Acadêmico;
- Departamento de Serviços Gerais;
- Gerência de Laboratórios;
- Núcleo de Qualidade Interna;
- Núcleo de Tecnologia da Informação;
- Prefeitura; e
- Pró-reitoria de Gestão com Pessoas.

A Comissão de Gestão de Riscos é responsável pela **elaboração do Plano de Gestão de Riscos**, submetido à aprovação do Comitê de Governança, Riscos e Controles, documento que especifica, no nível operacional, os procedimentos que devem ser utilizados para alcançar a estratégia definida na Política de Gestão de Riscos. Também são atribuições da Comissão de Gestão de Riscos a **implementação do Plano de Gestão de Riscos, o tratamento e monitoramento contínuo dos riscos, bem como a divulgação, atualização e gerência sobre as questões que envolvem gestão de riscos**.

- *Auditoria Interna*

A Unidade de Auditoria Interna é vinculada ao Conselho Universitário e desenvolve **atividades independentes de avaliação e consultoria** visando agregar valor à gestão, por meio da **melhoria da governança, do gerenciamento de riscos e dos controles internos**. Integra a "terceira linha de defesa" da instituição, pois tem por incumbência a avaliação dos controles internos gerenciados pela primeira e segunda linhas.

A estrutura de Gestão de Riscos definida para a UFCSPA tem a intenção de **gerar e proteger valor na organização, a fim de melhorar os serviços prestados à sociedade**. A implantação de rotinas focadas na prevenção dos riscos, baseadas em normas e boas práticas internacionalmente reconhecidas, como as citadas na seção dois, proporciona um gerenciamento adequado de potenciais eventos adversos sobre os objetivos, por meio da adoção de medidas proporcionais à gravidade dos riscos.

Observou-se que o risco deriva da incerteza, a qual se faz presente nos mais variados tipos de organizações, assim como nos contextos da vida em geral. A ocorrência de certos eventos pode ser desastrosa para pessoas e instituições, comprometendo objetivos considerados estratégicos. Portanto, ao abordar os riscos antecipadamente e de modo explícito, é possível estabelecer ações de mitigação e/ou planos de contingência capazes de diminuir prejuízos e danos a níveis que sejam administráveis, além de viabilizar a identificação e o aproveitamento de oportunidades.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000: gestão de riscos: princípios e diretrizes**. Rio de Janeiro: ABNT, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000: gestão de riscos: diretrizes.** Rio de Janeiro: ABNT, 2018.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Presidência da República**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 22 mai. 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. **Presidência da República**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm>. Acesso em: 5 mar. 2020.

BRASIL. Decreto-Lei nº 200, de 25 de fevereiro de 1967. Dispõe sobre a organização da Administração Pública Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm>. Acesso em 22 mai. 2020.

BRASIL. Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. **Diário Oficial da União**. Ed. 89, Seção 1, P. 14, 2016; 11 mai.

BRASIL. Tribunal de Contas da União. **Referencial básico de gestão de riscos** / Tribunal de Contas da União. – Brasília; TCU, Secretaria Geral de Controle Externo (Segecex, 2018). Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/referencial-basico-de-gestao-de-riscos.htm> Acesso em: 13 abr. 2020.

BRASIL. Tribunal de Contas da União. **Técnicas de Auditoria: análise SWOT e verificação de risco** / Tribunal de Contas da União. - Brasília: TCU, Secretaria de Fiscalização e Avaliação de Programas de Governo, 2003.

Fundação Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA). **Plano de Gestão de Riscos**: versão 1.0. Porto Alegre: UFCSPA, 2018.

Fundação Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA). **Política de Gestão de Riscos**: documento aprovado pelo Conselho Universitário na sessão de 10 de agosto de 2017 - Resolução nº 39/2017. Porto Alegre: UFCSPA, 2017. Disponível em: <https://www.ufcspa.edu.br/documentos/institucional/politica-de-gestao-de-riscos.pdf>. Acesso em: 3 ago. 2020.

Fundação Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA). **Plano de Desenvolvimento Institucional – PDI 2020-2029**. Porto Alegre: UFCSPA, 2019. Disponível em: <https://www.ufcspa.edu.br/documentos/institucional/ufcspa-pdi-2020-2029.pdf>. Acesso em: 3 ago. 2020.

Herbert, J. S. et al. (2021) Guia de Aplicação do M3P (Modelo de Maturidade em Mapeamento de Processos – 5.ed. Porto Alegre: UFCSPA, 2021. 42p. : il. color. Texto eletrônico. Modo de acesso: https://www.ufcspa.edu.br/documentos/nqi/guia-m3p5ed.pdf.

THE COMMITTE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION - COSO. **Gerenciamento de Riscos Corporativos: Estrutura Integrada: Sumário Executivo e Estrutura** (COSO GRC, 2004). Tradução: PriceWatherhouseCoopers e Instituto dos Auditores Internos do Brasil, São Paulo, 2007. Disponível em: <http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Portuguese.pdf>. Acesso em 08 mai. 2020.

THE INSTITUTE OF INTERNAL AUDITORS - IIA. **Declaração de Posicionamento do IIA: As Três Linhas de Defesa no gerenciamento eficaz dos riscos e controles**. Flórida, 2013. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2013.