INTEGRIDADE RISCOS

DIRC UFSCAR

CONTROLES INTERNOS

METODOLOGIA DE GESTÃO DE RISCOS

UFSCar - Universidade Federal de São Carlos

*O objetivo deste documento é atender ao disposto no artigo 17, inciso II, alínea e, da **IN Conjunta MP/CGU n° 01/2016** e artigo 7º, inciso I e artigo 10º, inciso II da **PGIRC-UFSCar (Política de Gestão de Integridade, Riscos e Controles Internos**) que estabelece as diretrizes para a gestão de riscos e define os instrumentos da Política de Gestão de Integridade, Riscos e Controles Internos na Universidade Federal de São Carlos.*

Elaboração:

SPDI/DIRC – Departamento de Gestão de Integridade, Riscos e Controles Internos com base nos trabalhos da comissão constituída pela Portaria GR nº 5619 de 02/05/2022 e na PGIRC/UFSCar – Política de Gestão de Integridade, Riscos e Controles Internos.

VERSÃO 4 - JUNHO/2022

SUMÁRIO

ÍNDICE DE FIGURAS:

ÍNDICE DE QUADROS:

CONCEITOS RELEVANTES PARA A GESTÃO DE RISCOS NA UFSCar

(PGIRC-UFSCar, artigo 2º)

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

II - método de priorização de processos: classificação de processos baseada em avaliação qualitativa e quantitativa, visando ao estabelecimento de prazos para a realização de gerenciamento de riscos;

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

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

V – meta: alvo ou propósito com que se define um objetivo a ser alcançado;

VI - procedimentos de controle: políticas e procedimentos estabelecidos para enfrentar os riscos e alcançar os objetivos institucionais;

VII - procedimentos de controles internos: procedimentos que a Universidade executa para o tratamento do risco, projetados para lidar com o nível de incerteza previamente identificado;

VIII – risco: 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;

IX - risco inerente: risco a que uma organização está exposta após a implementação de medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

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

XI - riscos de imagem ou reputação do órgão: eventos que podem comprometer a confiança da sociedade ou de parceiros, de clientes ou de fornecedores, em relação à capacidade da UFSCar em cumprir sua missão institucional;

XII - riscos financeiros ou orçamentários: eventos que podem comprometer a capacidade institucional de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária;

XIII - riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da UFSCar;

XIV - riscos operacionais: eventos que podem comprometer as atividades institucionais, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

XV - nível de risco: magnitude de um risco, expressa em termos da combinação de suas consequências e probabilidades de ocorrência;

XVI - tolerância ao risco: nível de variação aceitável quanto à realização dos objetivos;

XVII - tratamento do risco: processo de estipular uma resposta aos riscos;

XVIII – apetite ao risco: nível de risco que uma organização está disposta a aceitar;

XIX - categoria de riscos: classificação dos tipos de riscos definidos pela UFSCar que podem afetar o alcance de seus objetivos estratégicos, observadas as características de sua área de atuação e as particularidades do setor público;

XX – gestão de riscos: é o conjunto de atividades coordenadas, estruturado definindo claramente os princípios, objetivos, estrutura, competências e processo para dirigir e controlar em uma organização no que se refere a riscos necessário para gerenciar riscos eficazmente;

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

XXII - processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco;

XXIII - proprietário do risco: pessoa ou unidade/setor com a responsabilidade e a autoridade para gerenciar o risco;

XXIV - probabilidade: possibilidade/chance de ocorrência de um evento;

XXV- resposta ao risco: qualquer ação adotada para lidar com risco, podendo consistir em: a) aceitar o risco por uma escolha consciente; b) transferir ou compartilhar o risco a outra parte; c) evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; ou mitigar ou reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências;

XXVI- identificação de risco: processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais, podendo envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas;

XXVII - incerteza: incapacidade de saber com antecedência a real probabilidade ou o impacto de eventos futuros;

XXVIII - impacto: efeito resultante da ocorrência do evento;

XXIX - mensuração de risco: processo que visa estimar a importância de um risco e calcular a probabilidade de sua ocorrência;

XXX - monitoramento: componente do controle interno que permite avaliar a qualidade do sistema de controle interno ao longo do tempo;

XXXI – controles internos da gestão: processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolo, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;

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

XXXIII - plano de implementação de controles: documento elaborado pelo gestor para registrar e acompanhar a implementação de ações de tratamento a serem adotadas em resposta aos riscos avaliados;

XXXIV - política de gestão de integridade, riscos e controles internos da gestão: declaração das intenções e diretrizes gerais da Universidade relacionadas à integridade, riscos e controles internos;

XXXV - Integridade pública: é o conjunto de arranjos institucionais que visam a fazer com que a Administração Pública não se desvie de seu objetivo precípuo: entregar os resultados esperados pela população de forma adequada, imparcial e eficiente;

XXXVI - programa de integridade: conjunto estruturado de medidas institucionais voltadas para a prevenção, detecção, punição e remediação de fraudes e atos de corrupção, em apoio à boa governança;

XXXVII - Risco à integridade: vulnerabilidades que podem favorecer ou facilitar a ocorrência de práticas de corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, podendo comprometer os objetivos institucionais.

1 - INTRODUÇÃO

A presente metodologia de gestão de riscos cumpre a Resolução no. 10, de 15 de outubro de 2019, que institui a PGIRC - Política de Gestão de Integridade, Riscos e Controles Internos da UFSCar.

Esse instrumento legal institui as diretrizes para a Gestão de Integridade, Riscos e Controles Internos da Gestão da Universidade Federal de São Carlos e define a metodologia ou modelo de gestão de riscos que deve ser estruturado vislumbrando como componentes o ambiente interno, a fixação de objetivos, a identificação de eventos, a avaliação de riscos, a resposta a riscos, as atividades de controles internos, a informação e a comunicação, e o monitoramento de boas práticas de gestão.

Além disso, essa metodologia tem como viés os conceitos estipulados pelo Decreto 9.203/2017 que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, bem como, se baseia também na Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016 que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Outra referência essencial foi o Manual de Gestão de Riscos do TCU - Tribunal de Contas da União que em sua primeira versão, oferece aos gestores orientações específicas e objetivas para o início da gestão interna de riscos com simplicidade de abordagem e de linguagem.

Assim, o presente documento apresenta os fundamentos, a estrutura e a metodologia de gestão de riscos da Universidade Federal de São Carlos, com o objetivo de orientar as unidades a implementá-la em conformidade com a sua Política de Gestão de Integridade, Riscos e Controles Internos, PGIRC-UFSCar

Para a UFSCar, a gestão de riscos é: *o conjunto de atividades coordenadas, estruturado definindo claramente os princípios, objetivos, estrutura, competências e processo para dirigir e controlar em uma organização no que se refere a riscos necessário para gerenciar riscos eficazmente.*

A elaboração desta metodologia de gestão de riscos iniciou-se a partir dos estudos para elaboração da PGIRC-UFSCar no ano de 2016 e, finalmente, com a publicação no Diário Oficial da União da Política de Gestão de Integridade, Riscos e Controles Internos da UFSCar em 12 de fevereiro de 2020, o DIRC – Departamento de Integridade, Riscos e Controles Internos começou a estruturar a primeira versão dessa metodologia.

Basicamente esse referencial metodológico tem a seguinte estrutura:

• **Fundamentos da Gestão de Riscos:** são apresentados os conceitos básicos, os referenciais legais e teóricos, bem como os princípios e objetivos que norteiam a Gestão de Riscos;

• **Estrutura da Gestão de Riscos:** apresenta as atribuições das instâncias da UFSCar, a forma de integração dos processos organizacionais, os recursos necessários e os mecanismos de comunicação e capacitação para a Gestão de Riscos;

• **Etapas da Metodologia de Gestão de Riscos:** estabelece as etapas do processo, incluindo o fator de gerenciamento de riscos.

2 - FUNDAMENTOS DA GESTÃO DE RISCOS

A Instrução Normativa Conjunta MP/CGU nº. 01, de 10 de maio de 2016**,** estabelece que os órgãos e entidades do Poder Executivo federal deverão instituir, pelos seus dirigentes máximos, Comitê de Governança, Riscos e Controles.

Portanto, a Universidade Federal de São Carlos instituiu a partir da publicação desta IN Conjunta a sua política de gestão de riscos, uma declaração das intenções e diretrizes gerais relacionadas à gestão de riscos. Para tanto, a Portaria GR nº. 1828/16, de 18 de julho de 2016, constituiu um Grupo de Trabalho, com a finalidade de apresentar propostas para a elaboração da Política de Gestão de Riscos da UFSCar e da constituição do Comitê de Governança, Riscos e Controles da UFSCar.

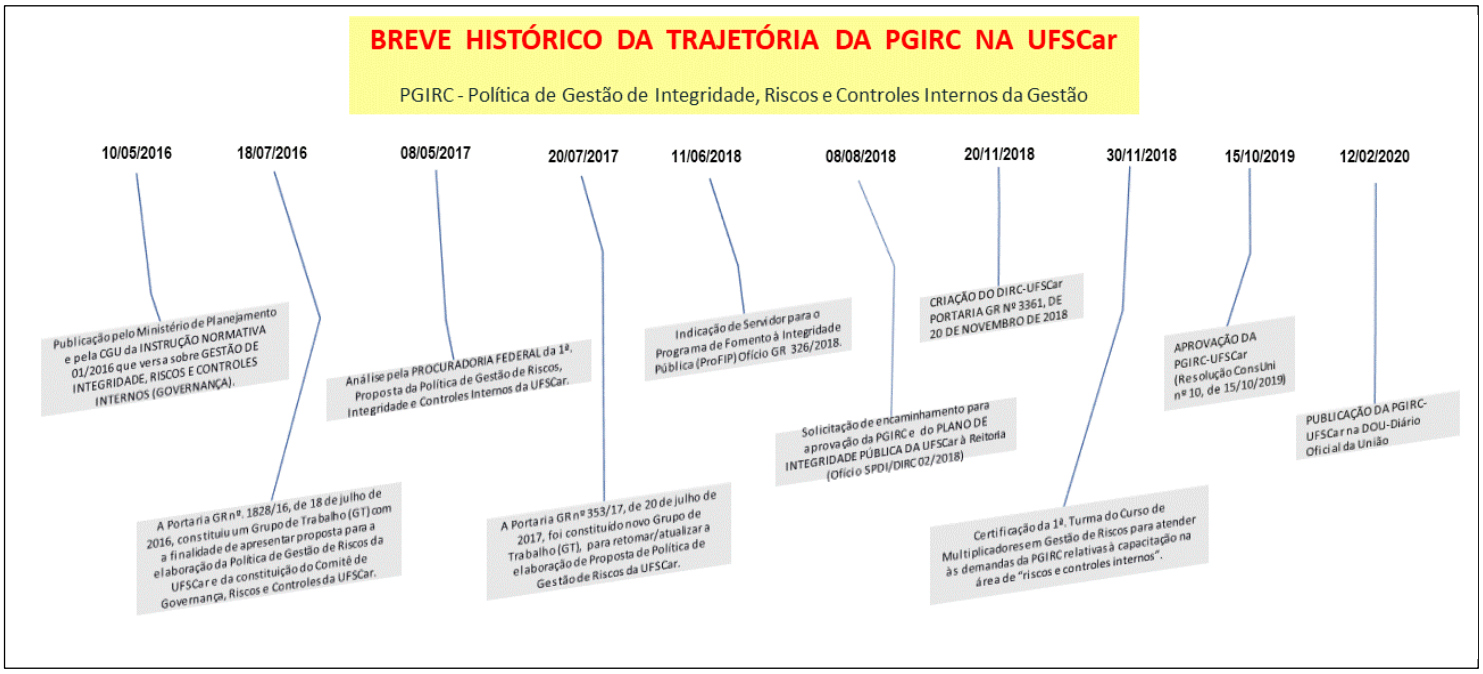

Figura 1 – Histórico da PGIRC-UFSCar (Fonte: DIRC-UFSCar)

2.1 - BREVE CRONOLOGIA DOS MODELOS DE GESTÃO DE RISCOS

A gestão de riscos com enfoque corporativo, institucional, constitui área de estudos relativamente nova, iniciando-se somente no final do século XX. Marco importante foi a publicação do artigo "*The Risk Management Revolution*", na revista *Fortune*, em 1975, o qual sugeria que se estabelecesse a coordenação das várias funções de riscos existentes em uma organização e a aceitação pela alta administração da responsabilidade por instituir políticas e manter supervisão sobre tal função coordenada.

Somente no ano de 1992 a ideia de gestão de riscos corporativos volta a ganhar foco, quando o *Committee of Sponsoring Organizations of the Treadway Commission* – COSO publica o guia *Internal Control - integrated framework (COSO-IC ou COSO I*).

Em 1995, esforço conjunto das entidades padronizadoras *Standards Australia* e *Standards New Zealand* resulta na publicação do primeiro modelo padrão oficial para a gestão de riscos, a norma técnica *Risk Management Standard,* AS/NZS 4360:1995. Normas técnicas assemelhadas logo são publicadas também no Canadá, no Reino Unido e outros países.

Em 2001, o colapso da empresa Enron revela um esquema de manipulação de balanços, ocultação de dívidas, lucros artificiais e inflados e falhas de auditorias.

Em 2004, o COSO publicou o *Enterprise Risk Management - integrated framework (COSO-ERM ou COSO II),* modelo de referência que estendeu o COSO I, tendo como foco a gestão de riscos corporativos (COSO, 2004).

Em 2009 é publicada a norma técnica ISO 31000 *Risk management – Principles and guidelines.*

Em 2013, é lançado o *COSO III* uma versão atualizada que permite às empresas desenvolver e manter sistemas de controle eficazes e eficientes no processo de adaptação às mudanças. (COSO 2013 é o modelo adotado pelo TCU).

Em 2017, "*Esta versão do COSO (...) ressalta a importância de se considerar o risco tanto no processo de definição das estratégias como na melhoria da performance. A primeira parte da publicação atualizada apresenta uma perspectiva sobre conceitos atuais e em desenvolvimento e aplicações do gerenciamento de riscos corporativos. Na segunda parte, o framework está organizado em cinco componentes que harmonizam diferentes pontos de vista e estruturas operacionais e melhoram as estratégias e a tomada de decisões*". *(Texto retirado do prefácio escrito por Robert B. Hirth Jr., COSO Chair, e Dennis L. Chesley, PwC Project Lead Partner and Global and APA Risk and Regulatory Leader).*

Em 2018 foi atualizada a ISO 31000 que fora originalmente publicada em 2009. A nova versão foi publicada em fevereiro de 2018. No entanto, a finalidade da ISO 31000 permanece a mesma – integrando a gestão do risco em um ambiente estratégico e operacional como sistema de gestão. Relevante saber que a versão da ISO 31000:2018 é muito semelhante à sua versão original.

Figura 2- Fundamentos da Gestão de Riscos – As três definições de "risco" nas normas

2.2 – REFERENCIAIS LEGAIS E TEÓRICOS

2.2.1 - COSO-IC (COSO I - 1992)

Em 1992, a gestão de riscos corporativos ganhou destaque com a publicação do guia *Internal Control – Integrated Framework, pelo Committee of Sponsoring Organizations of the Treadway Commission* – COSO, com o objetivo de orientar as organizações quanto a princípios e melhores práticas de controle interno, em especial para assegurar a produção de relatórios financeiros confiáveis e prevenir fraudes.

Nesse modelo, controle interno é definido como um "processo projetado e implementado pelos gestores para mitigar riscos e alcançar objetivos". Por sua vez, risco é definido como "a possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos" (COSO, 1992). Ou seja, para o COSO-IC, o controle interno é um processo que tem por objetivo mitigar riscos, com vistas ao alcance dos objetivos.

Em outras palavras, o COSO-IC, é um modelo de controle interno que utiliza práticas de avaliação de riscos, não tendo sido elaborado com o objetivo de ser um modelo de gestão de riscos em sentido estrito.

2.2.2 - COSO-ERM (COSO II - 2004)

Em 2004 foi publicado o modelo *Enterprise Risk Management – Integrated Framework* (Gerenciamento de Riscos Corporativos – Estrutura Integrada), também conhecida como COSO ERM ou COSO II, esse documento ainda hoje é tido como referência no tema gestão de riscos corporativos.

Vale lembrar que o COSO-ERM é uma evolução do COSO-IC, ou seja, abrange todo o escopo do modelo anterior e incorpora ferramentas complementares, como se vê na seguinte afirmação: "[o modelo COSO-ERM] não pretende substituir o modelo do controle interno [COSO-IC], mas sim incorporá-lo" (COSO, 2004).

De acordo com o COSO-ERM, a gestão de riscos corporativos é:

> *"É um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias formuladas para identificar, em toda a organização, eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatíveis com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. (COSO ERM, 2004)."*

2.2.3 - COSO – ERM (COSO - 2017)

A nova versão, *COSO ERM – Integrating with Strategy and Performance*, também denominado como Framework, destaca a importância de considerar os riscos tanto no processo de estabelecimento da estratégia quanto na melhoria da performance.

A primeira parte da publicação oferece uma perspectiva dos conceitos atuais e em desenvolvimento e aplicações do gerenciamento de riscos corporativos. A segunda parte da publicação apresenta 20 princípios organizados em 5 componentes inter-relacionados: Governança e cultura, Estratégia e definição de objetivos, Performance, Monitoramento do desempenho e revisão; e finalmente Informação, comunicação e divulgação.

Aderir a estes princípios pode conferir a organização uma razoável expectativa de que ela entende e se esforça para gerenciar os riscos associados à sua estratégia e objetivos de negócios.

2.2.4 - ISO 31000:2009 e 31000:2018

A norma técnica ISO 31000:2009 resultou do esforço da *International Organization for Standardization (*ISO) para criar um padrão internacional para a gestão de riscos corporativos,

tendo sido publicada no Brasil sob o nome ABNT NBR ISO 31000:2009 - Gestão de Riscos – Princípios e Diretrizes. O processo de gestão de riscos preconizado na ISO 31000:2018 envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos.

Convém que a natureza dinâmica e variável do comportamento humano e cultura seja considerada ao longo do processo de gestão de riscos. Embora o processo de gestão de riscos seja frequentemente apresentado como sequencial, na prática ele é iterativo.

Em 2018, a ISO 2009 foi revisada e seu conteúdo foi totalmente substituído pela nova versão. Na essência, o processo de gestão de riscos continua o mesmo incluindo as etapas relativas às atividades de comunicação e consulta, ao estabelecimento do contexto, avaliação dos riscos (identificar, analisar e avaliar os riscos), uma etapa relativa ao monitoramento e, por fim, registro e relato dos riscos.

2.2.5 - INSTRUÇÃO NORMATIVA Nº 01 MP/CGU DE 10 DE MAIO DE 2016

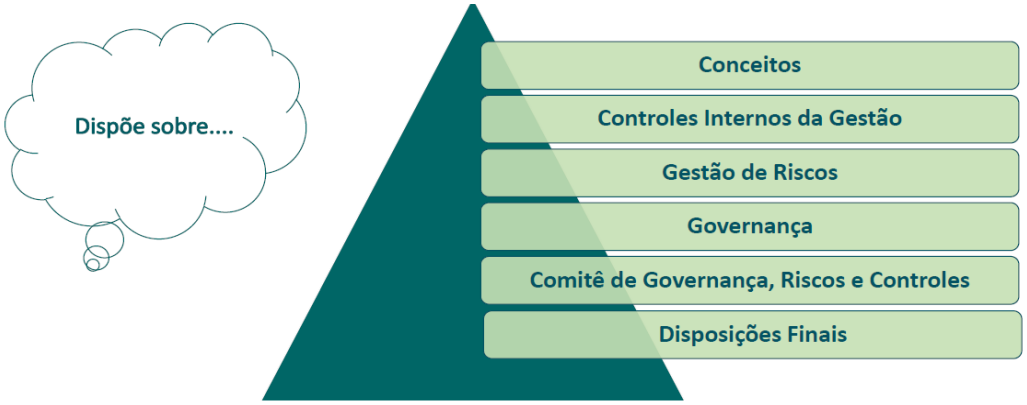

Figura 3- Conteúdos básicos da IN 01/2016

No âmbito do Poder Executivo Federal brasileiro, temos como marco regulatório a Instrução Normativa Conjunta MP/CGU nº 01 de 10/05/2016, que determina que seus órgãos adotem uma série de medidas para sistematização de práticas relacionadas à gestão de riscos, controles internos e governança e na qual são apresentados conceitos, princípios, objetivos e responsabilidades relacionados a este tema.

Com vistas ao cumprimento dessa Instrução Normativa e utilizando como parâmetros os *frameworks* citados acima, a UFSCar publicou a sua Política de Gestão de Integridade, Riscos e Controles Internos (PGIRC-UFSCar), por meio da Resolução ConsUni nº 10 de 15/10/2019. A Política de Gestão de Integridade, Riscos e Controles Internos da Gestão - PGIRC, estabelece as estruturas, as respectivas competências e atribuições referentes à governança, compreendendo as diretrizes para a Gestão de Integridade, Riscos e Controles Internos da Gestão da Universidade Federal de São Carlos – UFSCar.

A IN Conjunta MP/CGU nº 01/2016 tem como finalidades fortalecer a gestão, aperfeiçoar os processos e o alcance dos objetivos organizacionais, por meio de criação e aprimoramento dos controles internos da gestão, da governança e sistematização da gestão de riscos.

3 - ESTRUTURA DO PROCESSO DE GESTÃO DE RISCOS DA UFSCar

3.1 – PRINCÍPIOS

De acordo com a ABNT NBR ISO 31000:2018: *O propósito da estrutura da gestão de riscos é apoiar a organização na integração da gestão de riscos em atividades significativas e funções. A eficácia da gestão de riscos dependerá da sua integração na governança e em todas as atividades da organização, incluindo a tomada de decisão*.

Estreitamente ligada com os princípios, a estrutura de gestão de riscos objetiva ajudar a organização a integrar a gestão de riscos a funções e atividades importantes. Os componentes da estrutura são integração, concepção, implementação, avaliação e melhoria da gestão de riscos na organização. Todos eles funcionam em conjunto e são centrados na liderança e comprometimento, como ilustra a Figura 4 a seguir, já que para obter êxito a gestão de riscos deve estar integrada em todas atividades da organização, inclusive na tomada de decisão (ABNT NBR ISO 31000, 2018).

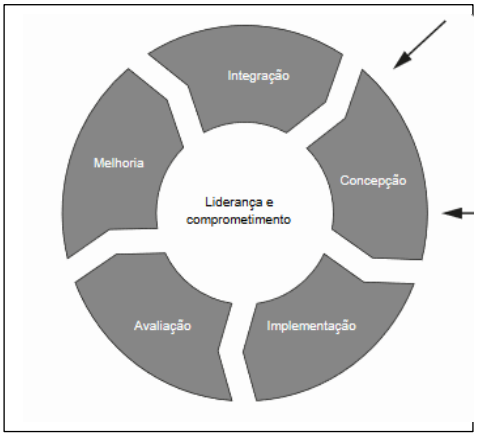

Figura 4 - Gestão de riscos (Fonte: ABNT NBR ISO 31000:2018)

O desenvolvimento da estrutura ocorre a partir da integração, concepção, implementação, avaliação e melhoria da gestão de riscos.

A começar pelos princípios, esses são critérios para a gestão de riscos eficaz. A gestão de riscos precisa ser integrada, estruturada e abrangente, personalizada, inclusiva, dinâmica, continuamente melhorada, contar com a melhor informação disponível e considerar fatores humanos e culturais.

A ISO 31000:2018 trata dos componentes Liderança e Comprometimento, Concepção da Estrutura para Gerenciar Riscos, Implementação da Gestão de Riscos, Monitoramento e Análise Crítica da Estrutura e Melhoria Contínua da Estrutura.

3.1.1 – LIDERANÇA E COMPROMETIMENTO

Em relação ao componente **Liderança e Comprometimento** deve haver integração da gestão de riscos com todas atividades da organização, a qual deve ser assegurada pela alta direção e órgãos de supervisão. Convém que esses também estipulem uma política de gestão de riscos, personalizem os componentes da estrutura para a organização ao implementá-los e garantam a alocação dos recursos necessários. Também, cabe definir responsabilidades e seus responsáveis dentro da organização (ABNT NBR ISO 31000, 2018).

Na UFSCar, a liderança e comprometimento é demonstrado pelas ações da alta administração em promover a Política de Gestão de Integridade, Riscos e Controles Internos (PGIRC-UFSCar).

3.1.2 – INTEGRAÇÃO

Quanto ao **componente integração** há o princípio que a gestão de riscos deve ser integrada. Esse componente evidencia que a gestão de risco não deveria ser separada, mas sim integrar o propósito, a governança, a liderança e o comprometimento, a estratégia, os objetivos e as operações da organização (ABNT NBR ISO 31000, 2018).

A **integração** da gestão de riscos apoia-se em uma compreensão das estruturas e do contexto organizacional. Estruturas diferem, dependendo do propósito, metas e complexidade da organização. O risco é gerenciado em todas as partes da estrutura da organização. Todos na organização têm responsabilidade por gerenciar riscos.

3.1.3 – CONCEPÇÃO

Na **concepção da estrutura** para gerenciar riscos, além da publicação da sua Política de Gestão de Riscos, a UFSCar definiu a responsabilização das suas unidades e agentes, a forma de integração dos processos organizacionais, os recursos necessários e as formas de comunicação no âmbito de sua gestão de riscos. Este componente é o projeto ou a elaboração da gestão de riscos, a qual precisa considerar a organização diante de seus contextos interno e externo. A alta direção e órgãos de supervisão idealmente devem distribuir as responsabilidades pela gestão de riscos, incumbindo as competências e definindo autoridades e funções, como também assegurar a alocação dos recursos (pessoas, habilidades, ferramentas, treinamentos, etc.) onde forem necessários (ABNT NBR ISO 31000, 2018).

3.1.4 – IMPLEMENTAÇÃO

A **implementação** é a colocação em prática da estrutura de gestão de riscos. Uma implementação bem-sucedida da estrutura requer o engajamento e a conscientização das partes interessadas. Isso permite que as organizações abordem explicitamente a incerteza na tomada de decisão, enquanto também asseguram que qualquer incerteza nova ou posterior possa ser levada em consideração à medida que ela surja. Adequadamente concebida e implementada, a estrutura de gestão de riscos assegurará que o processo de gestão de riscos é parte de todas as atividades da organização, incluindo a tomada de decisão, e que as mudanças nos contextos externo e interno serão adequadamente capturadas.

3.1.5 – AVALIAÇÃO

Para **avaliar** a eficácia da estrutura de gestão de riscos, convém que a organização:—mensure periodicamente o desempenho da estrutura de gestão de risco sem relação ao seu propósito, planos de implementação, indicadores e comportamento esperado; determine se permanece adequada para apoiar o alcance dos objetivos da organização.

3.1.6 - MELHORIA

Convém que organização **melhore** continuamente a adequação, suficiência e eficácia da estrutura de gestão de riscos e a forma como o processo de gestão de riscos é integrado. Na medida que lacunas ou oportunidades de melhoria pertinentes são identificadas, convém que a organização desenvolva planos e tarefas e os atribua àqueles responsabilizados pela implementação. Uma vez implementadas, convém que estas melhorias contribuam para o aprimoramento da gestão de riscos.

3.2 - COMPETÊNCIAS

Na UFSCar o gerenciamento de riscos corporativos é realizado por inúmeros atores nos quatro campi da Universidade e cada um deles com responsabilidades e obrigações em seus processos de trabalho.

Na PGIRC estão previstas as responsabilidades de cada um desses atores atuantes na gestão de riscos da UFSCar:

- No artigo 14º, o Comitê de Integridade, Riscos e Controles Internos e o Departamento de Integridade, Riscos e Controles Internos são responsáveis pela PGIRC;

- No artigo 19º, **compete a todos os servidores da UFSCar** o monitoramento a gestão de riscos.

- No artigo 21º, a Secretaria Geral de Planejamento e Desenvolvimento Institucional – SPDI observará as responsabilidades da Integridade, Riscos e Controles Internos da Gestão enquanto o Departamento de Gestão de Integridade, Riscos e Controles Internos – DIRC/UFSCar estiver em estruturação.

3.3 – LINHAS DE DEFESA

No sentido de esclarecer as responsabilidades de cada um dos vários atores envolvidos nas ações de gestão de riscos e controles a UFSCar adota a estrutura das "três linhas de defesa".

Esse modelo foi amplamente difundido a partir da Declaração de Posicionamento do The Institute of Internal Auditors (IIA) em setembro de 2010. O ponto significativo neste modelo é a transparência sobre quais são as responsabilidades de cada uma das partes interessadas na condução dos negócios e operação da organização, de forma a organizar o processo para que não existam lacunas.

Para coordenar os papéis dos atores envolvidos na Gestão de Riscos, a IN MP/CGU nº 01/2016 apresenta a estrutura de três linhas de defesa, conforme proposto pelo The Institute of Internal Auditors (IIA) da seguinte forma:

1ª linha de defesa: controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio dos órgãos e entidades do Poder Executivo Federal;

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

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

Assim, resumidamente a **primeira linha de defesa na UFSCar** são os gestores que tem como responsabilidade o gerenciamento de riscos de seus processos, a supervisão e o alinhamento do sistema de controle interno com os riscos inerentes. Em outras palavras são os controles internos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio dos órgãos e entidades do Poder Executivo Federal.

Como **segunda linha de defesa** estão as áreas de apoio que auxiliam os gestores a executar suas responsabilidades. Na UFSCar o DIRC executa esse papel como órgão de controle para tratar de riscos, controles internos, integridade e *compliance*.

E como **terceira linha de defesa** temos a auditoria interna a qual tem a responsabilidade de realizar um monitoramento periódico através de uma avaliação independente do processo de

governança, gestão de riscos e sistema de controles internos que os gestores da primeira e segunda linhas de defesa são responsáveis.

Seria adequado afirmar que o DIRC não faz controles internos e não faz controle, mas ajuda o gestor a ter um sistema de controles internos efetivo e otimizado. O mesmo acontece com a gestão de riscos; o DIRC serve de apoio aos gestores para fazerem a análise de riscos de seus processos.

3.4 - INTEGRAÇÃO NOS PROCESSOS ORGANIZACIONAIS E DO FLUXO DE INFORMAÇÃO

Em relação aos processos organizacionais, a Política de Gestão de Integridade e Riscos da UFSCar (PGIRC-UFSCar), bem como seus instrumentos resultantes, observa os seguintes princípios para apoiar a melhoria dos processos organizacionais, subsidiar a tomada de decisão e melhorar o fluxo de informação em todos os campi da Universidade:

- ✓ *A gestão de riscos deverá estar integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional da UFSCar, e sua execução deverá considerar o Plano Estratégico da UFSCar e os Princípios da Administração Pública.*
- ✓ *A metodologia, o modelo de gestão de riscos da UFSCar devem ser estruturado vislumbrando como componentes o ambiente interno, a fixação de objetivos, a identificação de eventos, a avaliação de riscos, a resposta a riscos, as atividades de controles internos, a informação e a comunicação, e o monitoramento de boas práticas;*
- ✓ *A gestão de riscos dever ser parte integrante dos processos organizacionais, apoiando a melhoria contínua e a inovação;*
- ✓ *A integração e sinergia das instâncias de supervisão, em todos os seus níveis, estabelecida por meio de modelos de relacionamento que considerem e compartilhem, quando possível, as competências, responsabilidades, informações e estruturas de supervisão;*
- ✓ *A integração e utilização das informações e dos resultados gerados pela gestão de integridade, riscos e controles internos da gestão na elaboração do planejamento estratégico, na tomada de decisões e na melhoria contínua dos processos organizacionais;*
- ✓ *Todos os responsáveis pelo gerenciamento de riscos dos processos organizacionais deverão manter fluxo regular e constante de informações entre si.*

Cada unidade da UFSCar deve colaborar na elaboração do Plano de Gestão de Riscos, com a identificação dos riscos nos processos organizacionais em que atua e que serão objeto da gestão de riscos, interagindo com a Gestão de Processos.

3.5 – RECURSOS HUMANOS, TÉCNICOS E OPERACIONAIS

Um dos objetivos da gestão de riscos na UFSCar e que está previsto em sua PGIRC é alocar e utilizar eficazmente os recursos para o tratamento de riscos. Além disso, em relação aos recursos humanos, todas as áreas participantes de processo organizacional deverão designar uma equipe para participar das etapas do gerenciamento do processo de gestão de riscos.

Essa equipe deve ser constituída por servidores que conheçam a área, o processo, os objetivos, contextos, atores envolvidos, resultados e controles já existentes. É relevante a participação e orientação no início das ações dos servidores com conhecimento das metodologias de gestão de riscos da UFSCar, no caso o DIRC-UFSCar.

Está previsto, também na PGIRC-UFSCar que o Comitê de Integridade, Riscos e Controles Internos de Gestão garantirá o apoio institucional para promover a gestão de riscos, em especial

os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos servidores.

Quanto aos recursos operacionais e tecnológicos necessários para as ações de Gestão de Riscos da UFSCar espera-se que sejam especificados em Guias Metodológicos (planilhas, formulários, roteiros, manuais, softwares entre outros).

3.6 – CAPACITAÇÃO

Especificamente quanto à riscos, integridade e controles internos a ProGPe – Pró-Reitoria de Gestão de Pessoas e o DIRC- Departamento de Integridade, Riscos e Controles Internos indicarão ações de capacitação com o objetivo de formar multiplicadores de gestão de riscos, integridade e processos na UFSCar, conforme as necessidades. Outros treinamentos sobre a aplicação das Metodologias de Gestão de Riscos e/ou de Processos podem ser solicitados pelas unidades. Os treinamentos devem ocorrer, preferencialmente, antes do início das atividades em cada processo organizacional da UFSCar e de forma remota sempre que possível.

Estão previstas na PGIRC-UFSCar, ações de capacitação em seu artigo 7º:

> *"... a capacitação dos agentes públicos que exercem cargo, função ou emprego na UFSCar na área de gestão de riscos deve ser desenvolvida de forma continuada, por meio de soluções educacionais, em todos os níveis."*

Bem como em seu artigo 10º, inciso III:

> *III - A Política de Capacitação da UFSCar deve contemplar, no eixo temático de governança pública, competências relacionadas à capacitação sobre temas afetos à gestão de integridade, riscos e controles internos.*

Artigo 17, itens VI e XIV:

> *VI - Incentivar o desenvolvimento de estudos e oferecer capacitação continuada em Gestão de Riscos para os servidores envolvidos no processo de Gestão de Riscos;*
>
> *XIV – planejar e participar de ações de treinamento e/ou capacitação relacionadas ao Programa de Integridade na Universidade.*

Relevante informar que o DIRC- Departamento de Gestão de Integridade, Riscos e Controles Internos da UFSCar já oferece a todos os servidores técnicos-administrativos e docentes de toda Universidade capacitação virtual na área de Gestão de Riscos Corporativos com carga horária mínima de 20h (riscos/integridade) disponível no portal de cursos abertos da Universidade PoCA-UFSCar (https://cursos.poca.ufscar.br/login/index.php).

4 - ETAPAS DA METODOLOGIA DE GESTÃO DE RISCOS NA UFSCar

A construção de uma metodologia de gestão de riscos na UFSCar tem como objetivo primordial estabelecer as etapas do processo de gestão de riscos que envolve o contexto da organização, a identificação, análise, avaliação, tratamentos, monitoramento e comunicação dos riscos.

Conforme a ABNT NBR ISO 31000 (2018), o processo de gestão de riscos pode ser adotado no nível estratégico, operacional, de programas ou projetos. É iterativo e compreende a realização de práticas e procedimentos para comunicação e consulta, definição de contexto, avaliação, tratamento, monitoramento, análise, registro e relato dos riscos. A Figura 5 (abaixo) ilustra esse processo, na qual se pode notar que não consiste necessariamente em uma sequência de atividades, mas sim um conjunto de etapas iterativas e coordenadas.

A PGIRC-UFSCar contempla em seu artigo 8º, as seguintes etapas metodológicas:

A operacionalização da gestão de riscos da UFSCar deverá contemplar no mínimo, as seguintes etapas:

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

*II – **identificação de riscos:** etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais;*

*III – **análise de riscos:** etapa em que são identificadas as possíveis causas e consequências do risco;*

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

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

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

Esse processo de gestão de riscos é aplicado a uma ampla gama das atividades da UFSCar, em todos os níveis, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, e é suportado pela cultura e pela estrutura de gestão de riscos da Universidade.

A Metodologia de Gestão de Riscos da UFSCar objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da gestão de riscos por meio da definição de um processo de gerenciamento de riscos.

Os passos a serem trilhados nesta metodologia estão sintetizados na Figura 5:

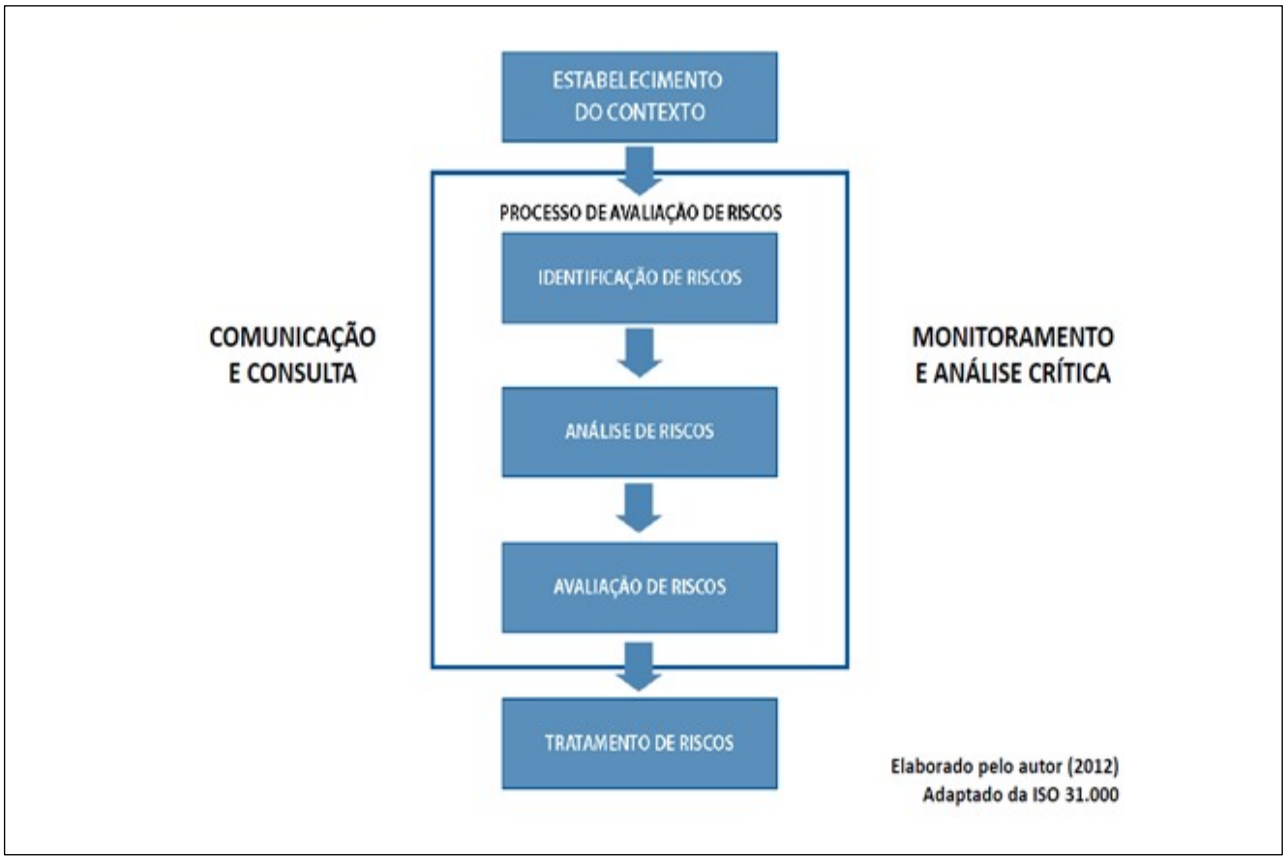

Figura 5 - Processo de Gestão de riscos da UFSCar (Adaptado ISO 31000:2009)

4.1 – ESTABELECIMENTO DO CONTEXTO

O objetivo do entendimento do contexto é adequar à realidade da UFSCar o processo de gestão de riscos, para adequá-lo aos seus determinantes (contexto) internos e externos.

Nesta etapa, portanto, são levantadas informações básicas do processo, o seu escopo, a conexão com a estratégia e missão da Universidade, os fornecedores, servidores, alunos, funcionários, entradas e saídas, bem como, os objetivos a serem cumpridos pelo processo.

Nesta etapa, devem ser identificados, pelo menos:

- ✓ Descrição resumida do processo. A descrição é um breve relato sobre o processo que permite compreender o seu fluxo, a relação entre os atores envolvidos e os resultados esperados;
- ✓ Fluxo (mapa) do processo organizacional;
- ✓ Objetivos do processo organizacional. É importante apontar quais objetivos são alcançados pelo processo organizacional. Sendo possível, devem ser indicados o objetivo geral e os objetivos específicos do processo, considerando perspectivas como estratégicas, temporais, relacionais, financeiras, orçamentárias, metas, entre outras. Para identificação dos objetivos, pode-se buscar responder à questão "O que deve ser atingido nas diversas dimensões para se concluir que o processo ocorreu com sucesso?";
- ✓ Relação de objetivos estratégicos da UFSCar alcançados pelo processo (PDI/UFSCar);
- ✓ Leis e regulamentos relacionados ao processo organizacional;
- ✓ Sistemas tecnológicos que apoiam o processo organizacional.

4.2 - IDENTIFICAÇÃO, ANÁLISE DE RISCOS E OPORTUNIDADES

O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos ou oportunidades que possam ajudar ou impedir que uma organização alcance seus objetivos.

O objetivo é produzir uma lista abrangente de riscos, incluindo causas, fontes e eventos, que possam ter um impacto na consecução dos objetivos identificados na etapa de estabelecimento do contexto.

Primeiro, identificam-se riscos em um nível geral ou superior como ponto de partida para se estabelecer prioridades para, em segundo momento, identificarem-se e analisarem-se riscos em nível específico e/ou mais detalhado. Pode-se, por exemplo, primeiramente identificar riscos aos objetivos estratégicos e, posteriormente, riscos que afetam processos prioritários.

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

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

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

O evento é um risco que pode comprometer claramente um objetivo do processo?

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

Objetivo do processo organizacional/etapa impactado pelo risco.

Categoria do risco, dentre as definidas para a UFSCar, por exemplo:

- ✓ ***Operacional:*** *eventos que podem comprometer as atividades da UFSCar, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;*
- ✓ ***Legal****: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da UFSCar;*
- ✓ ***Financeiro/orçamentário****: eventos que podem comprometer a capacidade da UFSCar 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;*
- ✓ ***Integridade****: eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela UFSCar e a realização de seus objetivos.*

O Apêndice I deste documento traz o modelo de Formulário para o registro de informações produzidas nas etapas de Identificação e Análise de Riscos.

4.3 - AVALIAÇÃO DE RISCOS

O objetivo dessa etapa é compreender a natureza do risco e suas características, avaliando-se o nível do risco em termos da gravidade dos impactos, as incertezas, a tendência e a eficácia dos controles.

O processo de analisar qualitativamente os riscos identificados avalia a probabilidade de ocorrência e o impacto dos riscos para então priorizá-los, de modo a permitir que se direcione o

foco para os riscos de alta prioridade, essas informações vão subsidiar as decisões para o tratamento dos riscos.

A PGIRC-UFSCar prevê em seu artigo 8º sobre a operacionalização da gestão de riscos a:

> *"Priorização de riscos: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior."*

Nesta etapa, são calculados os níveis dos riscos identificados pela equipe técnica designada, a partir de critérios de probabilidade e impacto.

Existem diversas ferramentas para identificação e análise de riscos, notadamente especificadas na ISO 31010 que traz dezenas de ferramentas que apoiam e dão estrutura para a avaliação de riscos.

Na UFSCar para efeitos práticos e didáticos decidiu-se utilizar duas das ferramentas mais simples de uso e aplicação: *brainstorming/brainwriting* e a Matriz GUT (gravidade, urgência, tendência).

4.3.1 - Brainstorming/Brainwriting ou "Tempestade de Ideias"

Essa técnica tem o objetivo de captar o maior número de ideias criativas com a participação de todos os integrantes da equipe técnica. Deve-se incentivar que todos se sintam livres para expressar suas ideias: nenhum julgamento ou crítica é permitido nesse momento e nenhuma ideia deve ser rejeitada, mesmo que pareça inadequada a princípio. É desejável que as pessoas desenvolvam as ideias dadas por outros e todas as ideias devem ser anotadas para serem analisadas posteriormente. Quanto mais ideias, melhor.

Para a aplicação da ferramenta, um dos dois roteiros abaixo deve ser seguido:

***Brainstorming*:**

1. Apresentar a pergunta: "O que é um efeito indesejado ou problema no processo?";
2. Observar alguns minutos de silêncio para as pessoas pensarem sobre o assunto; e
3. Convidar os participantes a comentarem suas ideias, enquanto o facilitador toma nota.

***Brainwriting*:**

1. Observar o prazo de tempo razoável e necessários para que cada participante relacione os riscos e problemas do processo;

2. Realizar um rodízio das listagens para que, durante alguns minutos, cada pessoa desenvolva as ideias de cada listagem;

3. O líder, com a ajuda do grupo/equipe, deve consolidar todas as ideias levantadas.

O líder de cada processo deve considerar o tamanho e a diversidade da equipe técnica para decidir qual das duas técnicas é mais apropriada à análise do seu processo.

Durante essa análise é importante que se tenha clara a diferença entre problema e risco.

Os problemas são efeitos indesejados no processo. Ou seja, são eventos que não comprometem o atingimento dos objetivos, a eficácia, mas a eficiência do processo.

Riscos são eventos internos ou externos cuja ocorrência pode causar impacto no cumprimento dos objetivos organizacionais.

4.3.2 - Matriz GUT (Gravidade, Urgência, Tendência)

A matriz GUT é uma ferramenta de priorização de riscos baseada em três critérios: gravidade, urgência e tendência. Para cada um desses critérios é atribuída uma nota — de 1 a 5 — e, ao final, esses valores são multiplicados, resultando na pontuação da matriz.

Os riscos, inclusive de integridade, e problemas identificados, em geral não afetam o desempenho do processo da mesma forma ou com a mesma intensidade, sendo importante identificar quais devem ser atacados prioritariamente.

Eles diferem, principalmente, quanto ao **impacto** (gravidade), à **probabilidade** de ocorrência (ou urgência) e à tendência, caso nenhuma ação seja tomada. Para que esses aspectos de cada risco possam ser considerados, será utilizada a variação da ferramenta "Matriz GUT".

Todos os problemas e riscos levantados no *Brainstorming e/ou Brainwriting* devem ser listados, e os participantes da reunião devem graduar cada problema de acordo com três critérios:

Gravidade (Impacto): refere-se ao impacto do risco ou problema sobre os objetivos ou desempenho do processo;

Urgência : refere-se à velocidade com que as ações necessitam ser tomadas para a solução do problema. Para riscos, deve refletir a **probabilidade deste acontecer**;

Tendência (Probabilidade): refere-se à tendência do risco de ser agravado ou atenuado ao longo do tempo.

Cada quesito (G, U e T) deve receber nota de 1 a 5 conforme os critérios expostos no Quadro 1:

Quadro 1 – Critérios de Probabilidade (urgência) e Impacto (gravidade)

	G – Gravidade (Impacto) Gravidade do dano ou prejuízo que pode ocorrer.	**U – Urgência** É necessária uma ação / chance de ocorrer:	**T – Tendência (probabilidade)** Se nada for feito, a situação vai:
5	Catastróficos, irreversíveis	Imediata / Quase certa	Piorar rapidamente
4	Significativos, de difícil reversão.	O mais cedo possível / Provável	Piorar em médio prazo
3	Moderados, recuperáveis.	Com alguma urgência / Possível	Piorar em longo prazo
2	Pequenos	Pode esperar um pouco / Rara	Estável
1	Mínimos	Não tem pressa / Improvável	Não vai piorar/pode melhorar

Fonte: Metodologia de Gestão de Riscos – ANP (adaptado)

A nota total de cada problema/risco será obtida pelo produto dos valores atribuídos aos critérios (GxUxT). Os problemas e riscos do processo devem ser elencados em ordem decrescente de notas, isto é, dos mais prioritários aos menos relevantes.

Quadro 2 – Exemplo de priorização de riscos identificado (Matriz GUT)

Risco	**Descrição Risco**	**G**	**U**	**T**	**TOTAL**	**PRIORIDADE**
1	COVID-19	5	5	5	125	1º
2	Greve Estudantil.	3	5	2	30	2º

O risco é uma função tanto da probabilidade como das consequências, portanto, o nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e de suas consequências, em termos da magnitude do impacto nos objetivos.

Risco = função (Probabilidade e Impacto)

O resultado final do processo de análise de riscos será o de atribuir, para cada risco identificado, uma classificação tanto para a probabilidade como para o impacto do evento, cuja combinação determinará o nível do risco. A identificação de fatores que afetam a probabilidade e as consequências também é parte da análise de riscos, incluindo a apreciação das causas e as fontes

de risco, suas consequências positivas ou negativas, expressas em termos de impactos tangíveis ou intangíveis.

No caso específico da análise de Riscos, a partir do resultado do cálculo o risco pode ser classificado dentro das faixas descritas no Quadro 3:

Quadro 3 – Classificação dos riscos identificados

Faixa de risco	Classificação
80-125	Risco Extremo - RE
50-79	Risco Alto - RA
13-49	Risco Médio - RM
1-12	Risco Baixo - RB

Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018, adaptado)

Durante o processo de identificação e análise de riscos, o líder de cada processo deve decidir a melhor maneira de conduzir a votação e ponderar as notas dos participantes juntamente com o auxílio do moderador. Lembrando que é um processo eminentemente subjetivo, por isso, é essencial o bom senso e comunicação para diminuir o grau de subjetividade.

Dependendo das circunstâncias, a análise de riscos pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas, e ser mais ou menos detalhada (ABNT, 2009). O método e o nível de detalhamento da análise podem ser influenciados pelos objetivos, pela natureza do risco, pela disponibilidade de informações e de recursos. Métodos qualitativos definem o impacto, a probabilidade e o nível de risco por qualificadores como “alto”, “médio” e “baixo”, com base na percepção das pessoas. Métodos semiquantitativos usam escalas numéricas previamente convencionadas para mensurar a consequência e a probabilidade, os quais são combinados, por meio de uma fórmula, para produzir o nível de risco (Tribunal de Contas da União. – Brasília: TCU, 2018).

O Apêndice I deste documento traz o modelo de Formulário para o registro de informações produzidas na etapa de avaliação/priorização de riscos.

4.4 – TRATAMENTO E DEFINIÇÃO DE RESPOSTAS AOS RISCOS

Essa é a etapa em que são definidos quais riscos terão suas respostas/tratamento priorizados, levando em consideração a classificação dos riscos identificados no quadro 3 (etapa anterior).

Nesse momento, serão definidos quais pontos devem ser considerados inicialmente, observando-se a ordem de prioridade. A equipe deve considerar a sua capacidade de ação e a relevância dos problemas e riscos e deve decidir quantos problemas e riscos serão trabalhados durante o ciclo.

Para fins de clareza e entendimento, deve ser elaborada uma lista com a classificação do risco e ações necessárias (atitudes perante o risco) conforme exemplo no quadro 4, abaixo:

Quadro 4: Atitude perante o risco para cada classificação

Classificação	Ação necessária	Exceção
Risco Baixo RB 1- 12	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu Comitê de Integridade e Riscos.
Risco Médio RM 13-49	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu Comitê de Integridade e Riscos.
Risco Alto RA 50-79	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao Comitê de Integridade e Riscos e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do comunicado ao Comitê de Integridade e Riscos.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu Comitê de Integridade e Riscos.
Risco Extremo RE 80-125	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser objeto de Avaliação Estratégica e comunicado ao Comitê de Integridade e Riscos e ter uma resposta imediata. Postergação de medidas só com autorização do Comitê de Integridade e Riscos.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu Comitê de Integridade e Riscos.

4.4.1 - SOBRE O APETITE A RISCOS DA UFSCar NO PROCESSO ORGANIZACIONAL

Segundo a PGIRC-UFSCar, em seu artigo 2º, inciso XVIII: Apetite a riscos é o nível de risco que uma organização está disposta a aceitar.

É importante que o apetite seja entendido/compreendido no início do processo de gerenciamento de riscos. Uma vez definido, a unidade declara que:

> *Todos os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco podem ser aceitos, e uma possível priorização para tratamento deve ser justificada;*
>
> *Todos os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco serão tratados e monitorados, e uma possível falta de tratamento deve ser justificada.*

Na UFSCar considerando a sua atual Metodologia de Gestão de Riscos, fica assim definido o seu APETITE A RISCO: **somente serão tratados e comunicados ao CGIRC-UFSCar os riscos considerados altos e extremos ambos com impacto acima de 50 (cinquenta) pontos na matriz GUT). e considerados ACIMA do apetite a riscos.**

Portanto, fica estabelecido que quaisquer riscos além do apetite a risco, classificados como ALTO ou EXTREMO na matriz GUT, obrigatoriamente devem ser comunicados ao CGIRC - Comitê de Gestão de Integridade, Riscos e Controles Internos e qualquer postergação de medidas de tratamento ocorrerá somente com autorização do mesmo Comitê.

Segundo a PGIRC-UFSCar, em seu artigo 2º, inciso XXV: Resposta ao risco: qualquer ação adotada para lidar com risco, podendo consistir em:

a) aceitar o risco por uma escolha consciente;

b) transferir ou compartilhar o risco a outra parte;

c) evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; ou mitigar ou reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências.

Tendo selecionado os riscos mais prioritários (que têm maior exposição), precisamos definir a Estratégia de resposta/tratamento:

Quadro 5: Opções de tratamento/resposta ao risco

Opção de Tratamento	Descrição
Aceitar o risco	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.
Transferir ou Compartilhar	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas a implementação de controles não apresenta um custo/benefício adequado. Na UFSCar, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar o risco	Um risco normalmente é evitado quando é classificado como "Alto" ou "Extremo", e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a UFSCAR. Evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Integridade e Riscos.
Mitigar ou reduzir o risco	Um risco normalmente é mitigado quando é classificado como "Alto" ou "Extremo". A implementação de controles, neste caso, apresenta um custo/benefício adequado. Na UFSCAR, mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.

Se a opção de tratamento do risco for MITIGAR, devem ser definidas medidas de tratamento para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro ou mais próximo possível das faixas de apetite a risco (risco "Baixo" ou "Médio", por exemplo).

Dessa forma, todos os riscos cujos níveis estejam dentro dos níveis aceitáveis (BAIXO e MÉDIO) podem ser aceitos, e uma possível priorização para tratamento deve ser justificada e todos os riscos cujos níveis estejam fora dos níveis aceitáveis (ALTO e EXTREMO) deverão ser tratados e monitorados, e uma possível falta de tratamento deve ser justificada. O Apêndice A deste documento traz um modelo de Plano de Tratamento dos riscos identificados.

4.5 - VALIDAÇÃO DOS RESULTADOS DAS ETAPAS DA METODOLOGIA DE GERENCIAMENTO DE RISCOS

Os resultados das etapas anteriores do processo de gerenciamento de riscos (entendimento do contexto, identificação e análise dos riscos, avaliação dos riscos, priorização dos riscos e definição de respostas aos riscos) devem ser avaliados e aprovados pelo Comitê de Integridade, Riscos e Controles Internos da UFSCar.

Após a aprovação desses resultados, o responsável pelo processo de gerenciamento de riscos ou pela unidade deve encaminhar esses resultados ao DIRC – Departamento de Integridade, Riscos e Controles Internos que é a área responsável pelo registro e articulação da gestão de riscos e integridade na Universidade.

Na PGIRC-UFSCar, em seu artigo 18º estão expressas as competências dos responsáveis pelo gerenciamento de riscos dos processos organizacionais:

I – identificar, analisar e avaliar os riscos dos processos sob sua responsabilidade, em conformidade ao que se define esta PGIRC;

II – propor respostas e respectivas medidas de controle a serem implementadas nos processos organizacionais sob sua responsabilidade;

III – monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas nos processos organizacionais sob sua responsabilidade;

IV – informar ao Departamento de Gestão de Integridade, Riscos e Controles Internos da Gestão sobre mudanças significativas nos processos organizacionais sob sua responsabilidade;

V – responder às requisições do Departamento de Gestão de Integridade, Riscos e Controles Internos da Gestão.

4.6 - COMUNICAÇÃO E MONITORAMENTO

A comunicação e consulta refere-se à identificação das partes interessadas em objetos de gestão de riscos e obtenção, fornecimento ou compartilhamento de informações relativas à gestão de riscos sobre tais objetos, observada a classificação da informação quanto ao sigilo.

De forma geral, as informações produzidas durante as etapas do processo de gerenciamento de riscos têm caráter restrito. Esse nível de restrição deve ser observado pelos servidores da UFSCar e demais partes.

A atividade de comunicação e consulta objetiva transmitir informações confiáveis e pertinentes que contribuem para a compreensão do risco e buscar *feedback* para apoiar a tomada de decisão (ABNT NBR ISO 31000, 2018).

Na IN Conjunta MP/CGU nº 01/2016, artigo 11 inciso IV explicita que:

> *"A comunicação eficaz deve fluir para baixo, para cima e através da organização, por todos seus componentes e pela estrutura inteira. Todos os servidores devem receber mensagem clara da alta administração sobre as responsabilidades de cada agente no que concerne aos controles internos da gestão. A organização deve comunicar as informações necessária ao alcance dos seus objetivos para todas as partes interessadas, independentemente no nível hierárquico em que se encontram."*

Nessa mesma IN Conjunta em seu artigo 16 inciso VII explicita que:

> *"... 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 possibilinciso 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."*

Na PGIRC-UFSCar a operacionalização da gestão de riscos da Universidade está prevista que a comunicação e monitoramento será a etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria Gestão de Riscos, com vistas à sua melhoria.

Além disso nessa mesma norma, em seu artigo 20 frisa que:

> " *O Comitê de Integridade, Riscos e Controles Internos de Gestão, o Departamento de Gestão de Integridade, Riscos e Controles Internos da Gestão e os responsáveis pelo gerenciamento de riscos dos processos organizacionais deverão manter fluxo regular e constante de informações entre si."*

Segundo a ISO 31000:2009, durante todas as etapas do processo de gerenciamento de riscos, é importante comunicar as partes interessadas.

5 - REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. **Gestão de Riscos – Princípio e diretrizes.** NBR ISO 31000. Associação Brasileira de Normas Técnicas. 2009.

BRASIL. **Instrução Normativa Conjunta MP/UFSCAR Nº 01**, de 10 de maio de 2016, que estabelece a adoção de uma série de medidas para a sistematização de práticas relacionadas a gestão de riscos, controles internos e governança.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Assessoria Especial de Controles Internos. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão.** Brasília. Brasília. V1.1.2 – 2017.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Gestão de Riscos e Controles Internos no Setor Público**. 55p. Abril de 2017.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Portaria nº 915**, de 12 de abril de 2017, que institui a Política de Gestão de Riscos – PGR – do Ministério da Transparência, Fiscalização e Controladoria-Geral da União – UFSCAR.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Portaria nº 50.223**, de 04 de dezembro de 2015, que aprova o Planejamento Estratégico da UFSCAR para o quadriênio 2016-2019.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos**. Disponível em http://portal.tcu.gov.br/gestao-e-governanca/gestao-de-riscos/. Acesso em Abril de 2017.

BRASIL. Tribunal de Contas da União. **Gestão de Riscos – Avaliação da Maturidade**. Brasília. 164 p., 2018.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission*. **Gerenciamento de Riscos Corporativos – Estrutura Integrada**. 2007. Tradução: Instituto dos Auditores Internos do Brasil (Audibra) e *Pricewaterhouse Coopers Governance, Risk and Compliance*, Estados Unidos da América, 2007.

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

APÊNDICE A

MODELO DE FORMULÁRIO DE APOIO AO PROCESSO DE GERENCIAMENTO DE RISCOS

(Identificação, análise, avaliação, priorização e resposta aos riscos)

Macroprocesso da área	*Nome da Pró-Reitoria, unidade de apoio ou unidade acadêmica*
Processo	*Nome do processo a ser utilizado como base para identificação, análise e avaliação de riscos*
Proprietário do risco	*Responsável pela Pró-Reitoria, unidade de apoio ou unidade acadêmica.*

Nº	ATIVIDADE	DESCRIÇÃO DO RISCO	CAUSA/ ORIGEM RISCO	PRIORIZAÇÃO G x U x T probab/impacto Notas de 1 A 5	CLASSIFICAÇÃO DO RISCO baixo/médio/alto/extremo
1					
2					
n					

MEDIDA(S) MITIGADORA(S) – OPÇÃO DE TRATAMENTO/RESPOSTA AO(s) RISCO(s)

RISCO	MEDIDA	RESPONSÁVEL	PROPRIETÁRIO DO RISCO
Atividade 1	*R01 – medida mitigadora do risco*	*Função e respectivo número(s) da(s) atividade(s) sob sua responsabilidade.*	*Responsável pela Pró-Reitoria, unidade de apoio ou unidade acadêmica.*
Atividade 2			
Atividade n			

MEDIDAS MITIGADORAS (Opções de tratamento/resposta ao risco)

Opção de Tratamento	Descrição
Aceitar o risco	Um risco normalmente é aceito quando seu nível está nas faixas de apetite a risco. Nessa situação, nenhum novo controle precisa ser implementado para mitigar o risco.
Transferir ou Compartilhar	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas a implementação de controles não apresenta um custo/benefício adequado. Na UFSCar, pode-se compartilhar o risco por meio de terceirização ou apólice de seguro, por exemplo.
Evitar o risco	Um risco normalmente é evitado quando é classificado como "Alto" ou "Extremo", e a implementação de controles apresenta um custo muito elevado, inviabilizando sua mitigação, ou não há entidades dispostas a compartilhar o risco com a UFSCAR. Evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pelo Comitê de Integridade e Riscos.
Mitigar ou reduzir o risco	Um risco normalmente é mitigado quando é classificado como "Alto" ou "Extremo". A implementação de controles, neste caso, apresenta um custo/benefício adequado. Na UFSCAR, mitigar o risco significa implementar controles que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.

Critérios de Probabilidade (urgência) e Impacto (gravidade)

	G – Gravidade (Impacto) Gravidade do dano ou prejuízo que pode ocorrer.	**U – Urgência (probabilidade)** É necessária uma ação / chance de ocorrer:	**T – Tendência** Se nada for feito, a situação vai:
5	Catastróficos, irreversíveis	Imediata / Quase certa	Piorar rapidamente
4	Significativos, de difícil reversão.	O mais cedo possível / Provável	Piorar em médio prazo
3	Moderados, recuperáveis.	Com alguma urgência / Possível	Piorar em longo prazo
2	Pequenos	Pode esperar um pouco / Rara	Estável
1	Mínimos	Não tem pressa / Improvável	Não vai piorar/pode melhorar

Fonte: Metodologia de Gestão de Riscos – ANP (adaptado)