

SPDI Secretaria Geral de Planejamento e Desenvolvimento Institucionais

DIRC Depto. de Gestão de Integridade, Riscos e Controles Internos

Plano de Gestão de Riscos

2025-2028

PLANO DE GESTÃO DE RISCOS Universidade Federal de São Carlos VIGÊNCIA 2025-2028

UFSCar - Reitora

Ana Beatriz de Oliveira

Secretaria Geral de Planejamento e Desenvolvimento Institucional (SPDI)

Rogerio Fortunato Júnior

Departamento de Gestão de Integridade, Riscos e Controles Internos (DIRC)

Felizardo Delgado

O objetivo deste documento é conceituar riscos, gestão de riscos, estabelecer a metodologia, diretrizes e responsabilidades para o plano de gestão de riscos no âmbito da UFSCar - Universidade Federal de São Carlos e, principalmente, atender às exigências legais previstas no art. 17 do Decreto nº 9.203/2017 e ao disposto no artigo 17, inciso II, alínea e, da IN Conjunta MP/CGU n° 01/2016 e artigo 7º, inciso I e artigo 11, inciso II da Política de Gestão de Integridade, Riscos e Controles Internos da UFSCar (PGIRC-UFSCar) que estabelece as diretrizes para a gestão de riscos e define os instrumentos da Política de Gestão de Integridade, Riscos e Controles Internos da Universidade Federal de São Carlos.

Elaboração: SPDI/**DIRC – Departamento de Gestão de Integridade, Riscos e Controles Internos** com base na Metodologia de Gestão de Riscos da UFSCar – versão 5 (outubro/2024).

LISTA DE SIGLAS

Audin - Auditoria Interna

CEP - Comissão de Ética em Pesquisa em Seres Humanos

CEUA - Comissão de Ética no Uso de Animais

CGIRC - Comitê de Gestão de Integridade, Riscos e Controles Internos

CGU - Controladoria Geral da União

CIBio - Comissão Interna de Biossegurança

CIEP - Comissão de Integridade Ética na Pesquisa

CoAd - Conselho Superior de Administração

CoGMeC - Coordenadoria de Gestão e Mediação de Condutas

ConsUni - Conselho Universitário da UFSCar

CPA - Comissão Própria de Avaliação

CPADoc - Comissão Permanente de Avaliação de Documentos

CPE - Comissão Permanente de Ética da UFSCar

DIRC - Departamento de Gestão de Integridade, Riscos e Controles Internos

ECIIA - European Confederation of Institutes of Internal Auditing

e-OUV - Sistema Informatizado de Ouvidorias do Poder Executivo Federal

e-SIC - Sistema Eletrônico do Serviço de Informação ao Cidadão

EVG - Escola Virtual de Governo

FERMA - Federation of European Risk Management Associations

GR - Gabinete da Reitoria

GT-RISCO - Grupo de Trabalho do Comitê de Integridade, Riscos e Controles Internos

GUT - Matriz de Gravidade, Urgência e Tendência dos riscos

ISO - International Organization for Standardization

LAI - Lei de Acesso à Informação

MEC - Ministério da Educação e Cultura

MPOG - Ministério do Planejamento, Orçamento e Gestão (extinto em 1 de janeiro de 2019)

PDA - Plano de Dados Abertos da UFSCar

PDI - Plano de Desenvolvimento Institucional

PGIRC - Política de Gestão de Integridade, Riscos e Controles Internos

POCA - Portal de cursos abertos da UFSCar

ProAd - Pró-Reitoria de Administração

PROFIP - Programa de Fomento à Integridade Pública

ProGPe - Pró-Reitoria de Gestão de Pessoas

SEI - Sistema Eletrônico de Informações

SIC - Serviço de Informação ao Cidadão

SITAI - Sistema de Integridade, Transparência e Acesso à Informação

SPDI - Secretaria Geral de Planejamento e Desenvolvimento Institucionais

UGI - Unidade de Gestão da Integridade

UORGs - Unidades Organizacionais

CONCEITOS RELEVANTES PARA A GESTÃO DE RISCOS NA UFSCar

(Artigo 2º da PGIRC - Política de Gestão de Integridade, Riscos e Controles Internos da UFSCar1)

- 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;

¹ Disponível em: https://www.dirc.ufscar.br/legislacao-1/resolucao-consuni-78-16-08-2022.pdf/view (último acesso: 24/09/2024)

- **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 ever 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.

SUMÁRIO

APRESENTAÇÃO	2
1 - OBJETIVOS	3
2 - RISCO E GESTÃO DE RISCOS - COMPETÊNCIAS E RESPONSABILIDADES	4
2.1- Definição de risco:	4
2.2 - Definição de gestão de riscos	4
2.3 - Por que gerenciar riscos?	4
2.4 - Instâncias e responsáveis pela Gestão de Riscos na UFSCar	5
3 - ÁREAS DE IMPLEMENTAÇÃO DA GESTÃO DE RISCOS NA UFSCar	10
3.1 – Processo de gestão de riscos nos objetivos estratégicos (PDI-UFSCar)	10
3.2 – Gestão de riscos nos processos organizacionais (UORGs-UFSCar)	11
3.3 - Gestão de riscos para a integridade	14
4 – METODOLOGIA E ESTRUTURA DA GESTÃO DE RISCOS: INTEGRAÇÃO NOS PROCESSOS ORGANIZACIONAIS	16
4.1 – Recursos humanos, técnicos e operacionais	16
4.2 – Capacitação em gestão de riscos	16
4.3 – Metodologia do processo de gestão de riscos	17
5 – CUMPRIMENTO DO CRONOGRAMA DO DIRC PREVISTO NO PDI-UFSCar	27
5.1 - Demandas oriundas dos órgãos de controle interno (CGU e AudIn)	27
6 - CONSIDERAÇÕES FINAIS	29
7 - REFERÊNCIAS BIBLIOGRÁFICAS	30
Índice de Figuras	
Figura 1- As três definições de risco nas normas	4
Figura 2- As três linhas de defesa na gestão de riscos da UFSCar	9
Figura 3 - Linhas de atuação/implementação da gestão de riscos na UFSCar	10
Figura 4 - Processo de gestão de riscos da UFSCar (Adaptado ISO 31000:2009)	13
Figura 5 – Fluxo do Processo de Gestão de riscos da UFSCar	18
Figura 6 - Processo de Monitoramento em Camadas na UFSCar	26
Índice de Quadros	
Quadro 1 – Critérios de Probabilidade (tendência) e Impacto (gravidade)	21
Quadro 2 – Exemplo de priorização de riscos identificado (Matriz GUT)	22
Quadro 3 – Classificação dos riscos identificados	
Quadro 4 - Atitude perante o risco para cada classificação	23
Quadro 5 - Opções de tratamento/resposta ao risco	24
Ouadro 6 – As Recomendações da CGU RESUMIDAS (ações atualizadas em 20/10/2024)	28

APRESENTAÇÃO

O Plano de Gestão de Riscos da Universidade Federal de São Carlos (UFSCar) visa atender às exigências legais previstas no art. 17º do Decreto nº 9.203/2017 que determina: "A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional".

Atender ao disposto no artigo 17, inciso II, da IN Conjunta MP/CGU n° 01/2016 que dispõe: A política de gestão de riscos deve especificar diretrizes sobre:

- A. como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização;
- B. como e com qual periodicidade serão identificados, avaliados, tratados e monitorados os riscos;
- C. como será medido o desempenho da gestão de riscos;
- D. como serão integradas as instâncias do órgão ou entidade responsáveis pela gestão de riscos;
- E. a utilização de metodologia e ferramentas para o apoio à gestão de riscos;
- F. o desenvolvimento contínuo dos agentes públicos em gestão de riscos.

Busca cumprir também, ao que estabelece o artigo 7º, inciso I e artigo 10º, inciso II da Política de Gestão de Riscos, Integridade e Controles Internos da UFSCar (PGIRC-UFSCar), que estabelece as diretrizes para a gestão de riscos e define os instrumentos da Política de Gestão de Integridade, Riscos e Controles Internos da instituição.

A construção deste instrumento teve como base as orientações da Instrução Conjunta nº 01/MP/CGU/2016, assim como as diretrizes e objetivos do Plano de Desenvolvimento Institucional (PDI) 2024-2028, com o intuito de consolidar e melhorar a governança corporativa e transparência na Universidade, **assegurando o cumprimento de sua missão institucional e o alcance dos objetivos estratégicos do eixo 4 - Gestão**, a saber:

- → Objetivo 4.1 Melhorar a governança corporativa e transparência;
- → Ação 4.1.4 Aumentar a maturidade de Gestão de Riscos;
 - Meta 1: Mapear todos os riscos altos e extremos dos processos de todas as unidades organizacionais;

Meta 2: Implementar ações de monitoramento dos riscos identificados e redução de riscos extremos em todas as unidades organizacionais.

Dessa forma, pretende-se com esse Plano, que a implementação da gestão de riscos deverá traduzir-se em resultados satisfatórios à instituição, por meio de respostas ágeis, da otimização de recursos, e da melhoria dos serviços prestados junto à comunidade acadêmica e à sociedade, e principalmente, assegurar que os responsáveis pela tomada de decisão, em todos os níveis do órgão ou entidade, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a instituição.

No artigo 5º da PGIRC está previsto que 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, previstas no Plano de Desenvolvimento Institucional (PDI) e nos Princípios da Administração Pública. Razão pela qual o plano de gestão de riscos alinha-se continuamente com os objetivos organizacionais e está focado nas incertezas que podem impactar nos resultados.

1 - OBJETIVOS

O objetivo primordial desse plano é orientar a operacionalização da Gestão de Riscos na Universidade em cumprimento e consonância às diretrizes da Política de Gestão de Riscos (PGIRC) estabelecidas na Resolução CONSUNI nº 78, de 16 de agosto de 2022. Compreende também o planejamento da continuidade de sua implementação dentro do período de vigência do PDI (2024-2028).

Além disso, o plano segue a metodologia de gestão de riscos da UFSCar, 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.

Pretende-se que este plano de ações de gestão de riscos seja atualizado constantemente considerando-se a natureza dinâmica da gestão (PGIRC, artigo 7º inciso I). Assim a atuação da gestão de riscos deve ser dinâmica e formalizada por meio da metodologia expressa neste plano. Dessa forma pretende-se uma evolução com o decorrer do tempo de forma que incorpore, paulatinamente, diversas análises de riscos oriundas de pró-reitorias, secretarias, áreas, setores e unidades acadêmicas que ainda não implementaram suas análises de riscos até o momento (PGIRC, artigo 22).

Todas instituições desempenham atividades administrativas para atingir o cumprimento de seus objetivos, estas atividades existem graças aos processos inerentes à sua execução. A UFSCar não é exceção e está exposta a diferentes fatores ou eventos que chamamos de "riscos" decorrentes dos ambientes interno e externo e que tornam incerto se os processos de gestão das atividades administrativas atingirão efetivamente seus objetivos e/ou quando isso ocorrerá.

Conscientes da diversidade da Universidade, esse documento nunca será um trabalho definitivo, quer quanto à identificação dos riscos, quer quanto às medidas de gestão dos mesmos. O Plano de Gestão de Riscos deve ser visto, essencialmente, como um processo de construção e de reforço da Política interna de Gestão de Integridade, Riscos e Controles Internos (PGIRC).

2 - RISCO E GESTÃO DE RISCOS - COMPETÊNCIAS E RESPONSABILIDADES

2.1- Definição de risco:

No artigo 2º inciso VIII da PGIRC, risco é a 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.

Figura 1- As três definições de risco nas normas



2.2 - Definição de gestão de riscos

Para a UFSCar, a gestão de riscos é o conjunto de atividades coordenadas, estruturadas definindo claramente os princípios, objetivos, estrutura, competências e processo para dirigir e controlar uma organização no que se refere a riscos necessários para gerenciá-los eficazmente.

Quanto ao processo de gestão de riscos é: a 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.

2.3 - Por que gerenciar riscos?

Quando gerenciamos riscos, a palavra fundamental é "objetivo". Pois se há objetivo, há um risco de não o alcançar, daí a necessidade de gerenciarmos esse risco.

Um bom gerenciamento de riscos permite que a organização melhore sua gestão a alcançar os resultados esperados, planejados e desejados. Dessa forma tomando decisões claras e conscientes das oportunidades.

2.4 - Instâncias e responsáveis pela Gestão de Riscos na UFSCar

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 Universidade.

Nos artigos 14 e 15 estão explícitas as *responsabilidades e atribuições do Comitê de Gestão de Integridade, Riscos e Controles Internos (CGIRC)* na implementação da Política de Gestão de Integridade, Riscos e Controles (PGIRC), bem como, fica claro os atores que a compõem:

- I Reitor;
- II Vice-reitor;
- III Pró-reitores de Graduação, Pós-graduação, Pesquisa, Extensão, Assuntos Comunitários e Estudantis, Gestão de Pessoas e Administração;
- IV Diretores de Campi;
- V Prefeitos Universitários:
- VI Secretários Gerais de Planejamento e Desenvolvimento Institucional, Informática, Relações Internacionais, Gestão Ambiental e Sustentabilidade, Ações Afirmativas, Diversidade e Equidade e Educação a Distância, Gestão do Espaço Físico;
- VII Diretores do Sistema Integrado de Bibliotecas, Coordenadoria de Comunicação Social, Unidade Saúde Escola;
- VIII Ouvidor;
- IX Coordenador do Departamento de Gestão de Integridade, Riscos e Controles Internos da Gestão;
- X Representante da Comissão de Ética no Uso de Animais (CEUA);
- XI Representante da Comissão de Ética em Pesquisa em Seres Humanos (CEP);
- XII Representante da Comissão de Integridade Ética na Pesquisa (CIEP);
- XIII Representante da Comissão Permanente de Ética (CPE);
- XIV Representante da Comissão Interna de Biossegurança (CIBio);
- XV Representante da Comissão Permanente de Avaliação de Documentos (CPADoc);
- XVI Representante da Comissão Própria de Avaliação (CPA);
- XVII Representante da Coordenadoria de Gestão e Mediação de Condutas (CoGMeC)

No artigo 18, compete aos 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.

No artigo 19, compete a todos os servidores da UFSCar o monitoramento da gestão de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento.

No artigo 21, a Secretaria Geral de Planejamento e Desenvolvimento Institucionais – 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.

2.4.1 – RESPONSABILIDADES DO COMITÊ DE GESTÃO DE INTEGRIDADE, RISCOS E CONTROLES INTERNOS (CGIRC)

Na PGIRC estão previstas as responsabilidades do CGIRC, em seu artigo 16:

- promover práticas e princípios de conduta e padrões de comportamentos;
- institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos;
- promover o desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de riscos e de controles internos;
- garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;
- promover a integração dos agentes responsáveis pela governança, pela gestão de riscos e pelos controles internos;
- promover a adoção de práticas que institucionalizam a responsabilidade dos agentes públicos na prestação de contas, na transparência e na efetividade das informações;
- aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;
- supervisionar o mapeamento e avaliação dos riscos-chave que podem comprometer a prestação de serviços de interesse público;
- liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão ou entidade;
- estabelecer limites de exposição a riscos globais do órgão, bem com os limites de alçada ao nível de unidade, política pública, ou atividade;
- emitir recomendação para o aprimoramento da governança, da gestão de riscos e dos controles internos;
- monitorar as recomendações e orientações deliberadas pelo Comitê;
- definir e atualizar as estratégias de implementação da Gestão de Riscos, considerando os contextos interno e externo;
- definir os níveis de apetite ao risco dos processos organizacionais;
- definir os responsáveis pelo gerenciamento de riscos dos processos organizacionais;
- definir a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;
- aprovar as respostas e as respectivas medidas de controle a serem implementadas nos processos organizacionais;
- aprovar o Plano de Gestão de Riscos e suas revisões;
- aprovar os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
- monitorar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas;
- acompanhar a avaliação da Gestão de Riscos pelos órgãos de controle interno e externo;
- definir indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho institucional da UFSCar;
- garantir 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;
- garantir o alinhamento da Gestão de Riscos aos padrões de ética e conduta e integridade, em conformidade com o Plano de Integridade da UFSCar,
- supervisionar a atuação das demais instâncias da Gestão de Riscos;
- aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão.

2.4.2 RESPONSABILIDADES DO DIRC

O Departamento de Gestão de Integridade, Riscos e Controles Internos, com a sigla DIRC, é um órgão técnico, vinculado provisoriamente à SPDI, que tem como finalidade orientar os gestores da Universidade em relação à política de integridade pública, *compliance*², identificar e gerenciar riscos, mapear e acompanhar os processos, planejar, coordenar e orientar matérias relacionadas à Gestão de Riscos nos quatro campi da UFSCar, com o objetivo de alinhar os processos e riscos de gestão com os objetivos da Instituição previstos no PDI e suas necessidades, por meio da identificação, análise e gerenciamento de riscos.

As atribuições pertinentes ao Departamento de Integridade e Riscos incluem, dentre outras:

- propor o Plano de Gestão de Riscos e suas revisões;
- propor o Plano de Integridade da Instituição e revisá-lo periodicamente;
- monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;

² Compliance: conjunto de procedimentos e regras que tem como objetivo manter a organização em linha com as normas vigentes, sejam elas legais ou internas.

- dar suporte à identificação, análise e avaliação de riscos dos processos organizacionais selecionados para a implementação da Gestão de Riscos;
- elaborar estratégia de Comunicação de Gestão de Riscos;
- medir o desempenho da Gestão de Riscos objetivando a sua melhoria contínua;
- coordenar a disseminação de informações sobre o Programa de Integridade Universidade;
- planejar e participar de ações de treinamento e/ou capacitação relacionadas ao Programa de Integridade na Universidade.
- consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los ao Comitê de Integridade,
 Riscos e Controles Internos.
- realizar interlocução com órgãos de controle externos(por ex.: CGU, TCU, MGI e outros) e internos (AudIn).

Além disso, o DIRC disponibiliza aos servidores de toda Universidade a oferta gratuita de capacitação na área de Gestão de Riscos Corporativos e Gestão de Riscos para a Integridade no setor público disponível no portal de cursos abertos da Universidade (PoCA-UFSCar).

2.4.3 - Missão, visão, valores do departamento de Integridade, riscos e controles internos

Missão do DIRC: Promover e aprimorar as ações de gestão de riscos, prevendo o cumprimento da integridade pública, transparência das informações e adequados controles internos, contribuindo assim, para o alcance da missão estratégica da Universidade Federal de São Carlos.

Visão do DIRC: Ser referência no aprimoramento da gestão de riscos e integridade na UFSCar e ser reconhecido pela importância do seu papel na construção do futuro da Universidade Federal de São Carlos.

Princípios e Valores do DIRC:

Profissionalismo: Atuar com proatividade, competência, ética e seriedade;

Simplificação: Desempenhar o trabalho de forma ética: direta, objetiva e efetiva;

Integração: Unir e compartilhar esforços em prol de objetivos comuns.

2.4.4 - Responsabilidades da Coordenadoria de Auditoria Interna - AudIn/UFSCar

A auditoria interna é a unidade responsável pela 3ª linha de defesa na UFSCar (vide figura 2) e por fornecer ao Comitê de Gestão de Integridade, Riscos e Controles, ao DIRC e – especialmente à alta administração avaliações objetivas e abrangentes, com o maior nível de independência dentro da organização.

De uma forma mais sintética, quanto aos riscos na gestão, cabe à AudIn:

- Emitir opinião sobre a gestão de riscos da Universidade;
- Auxiliar os gestores na melhoria da eficácia dos processos de gerenciamento de riscos, de controle e de governança, bem como na estruturação e efetivo funcionamento da primeira e segunda linhas de defesa, por meio de prestação de serviços de consultoria e avaliação;
- Buscar identificar potenciais riscos de fraude e realizar o adequado e tempestivo encaminhamento das informações às instâncias competentes, quando houver indícios suficientes de fraudes ou ilegalidades.

2.4.5 – Estrutura de responsabilidade das três linhas de defesa

A Gestão de Riscos deve ser gerida e administrada de forma integrada, por isso na UFSCar, cabe à Reitoria a responsabilidade do apoio e estabelecimento da estrutura de gestão de riscos, sempre em conformidade com o modelo das três linhas de defesa apresentadas pela IN CGU/MP nº 01/2016.

Esse modelo foi introduzido em 21 de setembro de 2010 pela Federation of European Risk Management Associations (FERMA) e pela European Confederation of Institutes of Internal Auditing (ECIIA), no documento "Guidance on the 8th EU Company Law Directive", como uma recomendação para a implementação dos requisitos

legais de monitoramento da efetividade dos sistemas de controle interno, auditoria interna e gerenciamento de riscos.

Como salienta a declaração de posicionamento do ECIIA sobre o tema:

"O modelo de Três Linhas de Defesa é uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos e controle por meio do esclarecimento dos papéis e responsabilidades essenciais".

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:

- ✓ 1º linha de defesa operacionalização: 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: supervisão e monitoramento dos controles internos executados por instâncias específicas, como o CGIRC, o DIRC ou assessorias/comissões específicas para tratar de riscos, controles internos, integridade e compliance;
- ✓ 3ª linha de defesa Avaliação: 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).

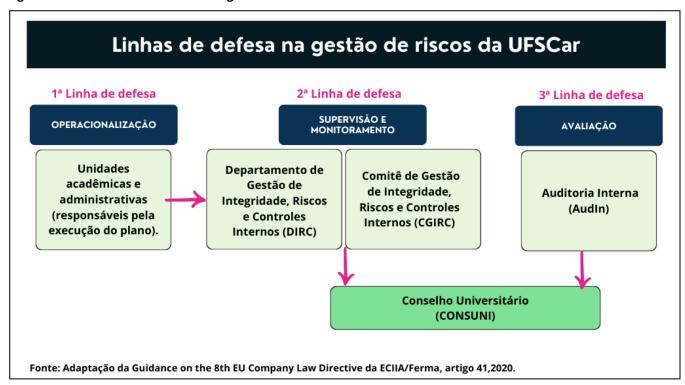
Resumidamente, a **primeira linha de defesa** na UFSCar é composta pelos gestores, responsáveis pelo gerenciamento dos riscos de seus processos, pela supervisão e pelo alinhamento do sistema de controle interno com os riscos inerentes. Em outras palavras, são os controles internos da gestão, executados por todos os agentes públicos encarregados da condução de atividades e tarefas nos 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 CGIRC, com a articulação do DIRC, desempenha esse papel como órgão de controle, responsável por tratar de riscos, controles internos, integridade e compliance (conformidade).

Como **terceira linha de defesa**, a auditoria interna é responsável por realizar monitoramentos periódicos por meio de uma avaliação independente dos processos de governança, gestão de riscos e do sistema de controles internos, pelos quais os gestores da primeira e segunda linhas de defesa são responsáveis.

É adequado afirmar que o DIRC não faz controles internos, 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 e avaliação de riscos nos seus processos organizacionais.

Figura 2- As três linhas de defesa na gestão de riscos da UFSCar



3 - ÁREAS DE IMPLEMENTAÇÃO DA GESTÃO DE RISCOS NA UFSCar

No artigo 5º da PGIRC está previsto que 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 Universidade (PDI-UFSCar) e os Princípios da Administração Pública.

Sendo assim, o gerenciamento de riscos na UFSCar será implementado de forma gradual nas áreas administrativas e acadêmicas. Este Plano, visa identificar, avaliar e tratar riscos em objetivos constantes em documentos, programas, processos, atividades entre outros que apresentam natureza crítica na instituição, de modo a priorizar as ações de riscos identificados como altos e extremos na Universidade.

Portanto, o escopo de atuação e implementação da gestão de riscos na UFSCar está delimitado em três linhas:

- Riscos nos objetivos estratégicos da Universidade (PDI-UFSCar);
- ✔ Iniciativas relacionadas à Gestão de Riscos nos processos das unidades organizacionais da UFSCar;
- ✔ Riscos nos processos das unidades organizacionais identificados como riscos para a integridade;

Figura 3 - Linhas de atuação/implementação da gestão de riscos na UFSCar



Fonte: DIRC-2024.

3.1 – Processo de gestão de riscos nos objetivos estratégicos (PDI-UFSCar)

A identificação, avaliação e tratamentos dos riscos nos objetivos estratégicos segue os preceitos da Política de Gestão de Integridade, Riscos e Controles Internos da Gestão - PGIRC, que estabelece em seu artigo 5º que a gestão de riscos na Universidade 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.

Além disso, objetivando a evolução da maturidade da gestão de riscos e integridade no que diz respeito ao seu Planejamento Estratégico, refletido no PDI-UFSCar recentemente aprovado (Plano de Desenvolvimento Institucional 2024-2028), no qual consta, de forma clara e bem definida em seis eixos temáticos transversais, que perpassam as Políticas Institucionais:

EIXO 1: Formação de Pessoas.

EIXO 2: Diversidade e equidade.

EIXO 3: Produção e disseminação do conhecimento.

EIXO 4: Gestão.

EIXO 5: Espaço Físico, Infraestrutura e Ambiente.

EIXO 6: Extensão, Comunicação e Inovação.

A partir desses eixos foram formulados objetivos específicos do PDI e as ações necessárias à sua consecução, bem como as metas a serem atingidas ao longo do próximo quinquênio.

Assim, o gerenciamento de riscos estratégicos consiste na identificação, na avaliação e no tratamento de riscos relacionados aos objetivos estratégicos definidos no PDI - UFSCar.

Portanto, a partir da identificação dos objetivos estratégicos, das unidades responsáveis e os processos relacionados direta ou indiretamente a cada um desses objetivos, serão priorizados os elementos críticos ou eventos mais relevantes, que impedem o atingimento dos objetivos e metas.

Recomenda-se que, para cada objetivo estratégico selecionado, as unidades responsáveis já tenham definido o mapeamento dos processos relevantes ou programas vinculados a esse objetivo, das metas esperadas e dos indicadores que mensuram o atingimento dessas metas, bem como das ações estratégicas necessárias para consecução dos mesmos.

3.2 – Gestão de riscos nos processos organizacionais (UORGs-UFSCar)

Na metodologia de gestão de riscos da UFSCar estão registradas as etapas do processo de gestão de riscos que envolve o contexto da organização, a identificação, análise, avaliação, tratamentos, monitoramento e comunicação dos riscos em todos os processos organizacionais.

O gerenciamento de riscos nos processos organizacionais visa apoiar a melhoria dos fluxos de trabalho e prevenir falhas que comprometam o desempenho dos serviços e ações da Universidade, de acordo com o art. 2º, inciso I, da PGIRC, processo é um conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido.

De acordo com o art. 2º, inciso XXII, da PGIRC, a gestão de riscos nos processos organizacionais é a 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.

Ainda citando a PGIRC, em seu artigo 22º, orienta que as iniciativas relacionadas à Gestão de Riscos existentes na UFSCar, deverão ser gradualmente alinhadas ao Plano de Gestão de Riscos aprovado pelo Comitê de Gestão de Integridade, Riscos e Controles Internos de Gestão.

Portanto, todas as unidades da UFSCar poderão tomar iniciativas quanto ao gerenciamento de riscos em seus processos organizacionais, de acordo com a política de gestão de integridade, riscos e controles internos da UFSCar. O ponto principal para a definição dos processos que serão trabalhados no âmbito da gestão de riscos na UFSCar é a sua relevância na consecução da missão da instituição. É importante destacar que os riscos identificados devem ser aqueles que impactam a instituição como um todo e que estejam alinhados aos objetivos e ações do PDI. Não devem ser confundidos com problemas locais ou questões do cotidiano de unidades específicas.

Assim, a partir da definição de objetivos institucionais, cada unidade deve identificar quais processos contribuem para o atingimento destes objetivos e terão seus riscos gerenciados. Nos processos organizacionais a identificação de riscos, isto é, o 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.

Lembrando que na UFSCar, as partes interessadas envolvidas nos processos organizacionais, são as pessoas e unidades organizacionais (UORGs) interessadas no resultado do processo. A parte interessada também pode ser tanto o público interno (outras unidades, servidores docentes ou técnico-administrativos, etc.) quanto o público externo (discentes, comunidade, órgãos externos, etc.).

Portanto, pretende-se quanto aos riscos nos processos organizacionais sejam identificados e registrados para cada unidade constante no SIORG-UFSCar, sejam incluídos em planilha de controles de riscos, onde os responsáveis são os proprietários dos riscos, ou seja os mesmos servidores lotados nas unidades com suas respectivas autoridades detentoras de Cargos de Direção (CD) e Funções Gratificadas (FG). Dessa forma, cada unidade deve definir quais processos referentes ao cumprimento dos objetivos institucionais selecionados terão seus riscos gerenciados e registrados na planilha de controle de riscos e que será disponibilizada/enviada ao DIRC-SPDI.

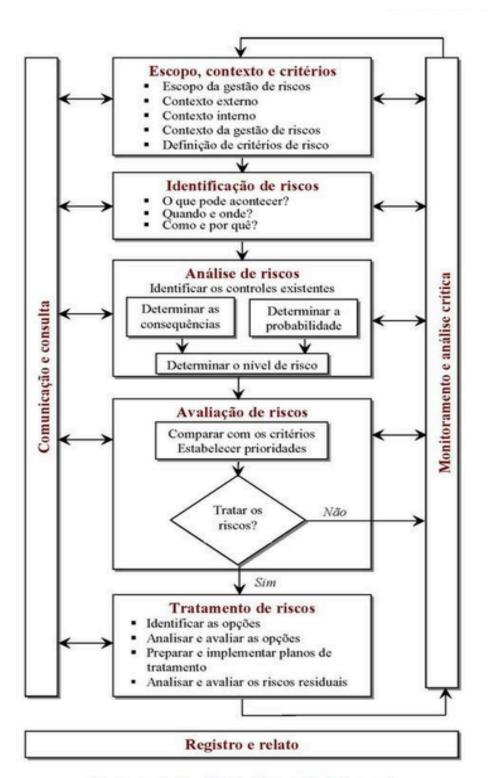
É necessário destacar que as unidades organizacionais são livres para gerenciar os riscos de qualquer elemento que for de seu interesse, apenas ficando registrado que a sugestão deste plano de gestão de riscos é que sejam priorizados os processos diretamente vinculados aos objetivos institucionais vinculados ao PDI-UFSCar ou aqueles cuja pontuação na matriz de riscos da Universidade estiverem além do apetite a riscos, ou seja, acima de 50 (cinquenta pontos) na matriz de gravidade, urgência e tendência do riscos (matriz GUT).

Portanto, quaisquer riscos identificados como acima do apetite de risco <u>devem</u> ser comunicados ao CGIRC-UFSCar (Comitê de Gestão de Integridade, Riscos e Controles). É igualmente importante e recomendado que a unidade organizacional responsável por cada processo selecionado tenha um mapeamento e uma descrição detalhada do processo. No entanto, a ausência desses artefatos não impede a execução do gerenciamento de riscos.

Enfim, esse processo de gestão de riscos é aplicado a uma ampla gama de atividades na UFSCar, abrangendo todos os níveis, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, sendo sustentado pela cultura e pela estrutura de gestão de riscos da Universidade.

Frisando que 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 como demonstrado na figura 4: Processo de gestão de riscos da UFSCar (Adaptado ISO 31000:2009).

Figura 4 - Processo de gestão de riscos da UFSCar (Adaptado ISO 31000:2009).



Processo de Gestão de Riscos - Detalhamento

3.3 - Gestão de riscos para a integridade

A gestão de riscos para a integridade consiste em ferramenta que permite aos agentes públicos mapear os processos organizacionais que integram a UFSCar, de forma a identificar fragilidades mapeadas e identificadas como "riscos à integridade que possibilitem a ocorrência de fraudes e atos de corrupção".

Segundo o **Decreto 11.529/23 que instituiu o SITAI** - Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal, considera-se:

- I programa de integridade conjunto de princípios, normas, procedimentos e mecanismos de prevenção, detecção e remediação de práticas de corrupção e fraude, de irregularidades, ilícitos e outros desvios éticos e de conduta, de violação ou desrespeito a direitos, valores e princípios que impactem a confiança, a credibilidade e a reputação institucional;
- **II plano de integridade** plano que organiza as medidas de integridade a serem adotadas em determinado período, elaborado por unidade setorial do Sitai e aprovado pela autoridade máxima do órgão ou da entidade; e
- **III funções de integridade** funções constantes nos sistemas de corregedoria, ouvidoria, controle interno, gestão da ética, transparência e outras essenciais ao funcionamento do programa de integridade.

A definição adotada na Portaria CGU nº 1.089/2018 é:

Art. 2º, II – Riscos para a integridade: riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.

Parágrafo único. Os riscos para a integridade podem ser causa, evento ou consequência de outros riscos, tais como financeiros, operacionais ou de imagem.

Já a PGIRC, define riscos à integridade como: "...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."

Portanto, na UFSCar os riscos para a integridade são tratados em um plano que contém o conjunto organizado de medidas/ações que devem ser implementadas no período de vigência do Plano de Gestão de Riscos 2025-2028, com o objetivo precípuo de prevenir, identificar, avaliar e tratar eventuais ocorrências de quebra de integridade.

Os tipos de riscos para a integridade que, segundo a CGU são mais relevantes e comuns nas organizações públicas são conforme expostos a seguir:

- Abuso de posição ou poder em favor de interesses privados;
- Nepotismo;
- Conflito de Interesses;
- Pressão Interna ou Externa Ilegal ou Antiética para influenciar agente público;
- Solicitação ou recebimento de vantagem indevida;
- Utilização de recursos em favor de interesses privados.

O plano é dividido em fases e é estabelecido após a fase de aprovação e análise e tratamento de riscos de integridade da Universidade. Portanto, **resumidamente são três fases:**

- Fase 1: Identificação da unidade de gestão de integridade na UFSCar e outras áreas presentes na Universidade relacionadas à governança e à integridade pública que buscam aproximar o cidadão dos serviços disponíveis na Universidade e, ao mesmo tempo, garantir a efetivação desses serviços.
- Fase 2: Aprovação no Conselho Superior e identificação, análise e tratamento de riscos de integridade.
- Fase 3: Atualização e monitoramento periódico do Plano de Integridade, com base nas medidas de tratamento e respostas aos riscos de integridade mapeados nas UORGs da UFSCar.

No entanto, a gestão de riscos para a integridade realizada no nível das unidades organizacionais deve ser acompanhada pelos gestores responsáveis pelos riscos de cada uma delas. O monitoramento das ações de tratamento de riscos envolve a verificação contínua ou periódica do funcionamento da implementação e dos resultados das medidas mitigadoras. O monitoramento deve considerar o tempo necessário para que as medidas mitigadoras produzam seus efeitos.

Portanto, o monitoramento consistirá na atualização da análise e avaliação dos riscos identificados, avaliados e tratados nas unidades, considerados de alto impacto e gravidade, assim como do estágio de execução das medidas de tratamento do risco e dos resultados dessas medidas. Lembrando que o monitoramento dos riscos nos processos das unidades organizacionais será realizado pelo respectivo gestor/proprietário/responsável pelo risco sendo orientado, sempre que necessário pelo DIRC-SPDI.

4 – METODOLOGIA E ESTRUTURA DA GESTÃO DE RISCOS: INTEGRAÇÃO NOS PROCESSOS ORGANIZACIONAIS

Em relação aos processos organizacionais, a Política de Gestão de Integridade, Riscos e Controles Internos da UFSCar (PGIRC), 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 deve 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.

4.1 – Recursos humanos, técnicos e operacionais

Um dos objetivos da gestão de riscos na UFSCar e que está previsto em sua política de riscos (PGIRC) é alocar e utilizar eficazmente os recursos para o tratamento de riscos. Além disso, em relação aos recursos humanos, todas as áreas participantes do 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 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).

4.2 - Capacitação em gestão de riscos

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. Estão previstas na PGIRC, 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 oferece a todos os servidores técnicos-administrativos e docentes de toda Universidade capacitação virtual na área de Gestão de Riscos Corporativos e o curso de gestão de riscos para integridade no setor público, ambos disponíveis no portal de cursos abertos da Universidade PoCA-UFSCar: https://cursos.poca.ufscar.br/login/index.php.

4.3 – Metodologia do processo de gestão de riscos

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 6 (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 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.

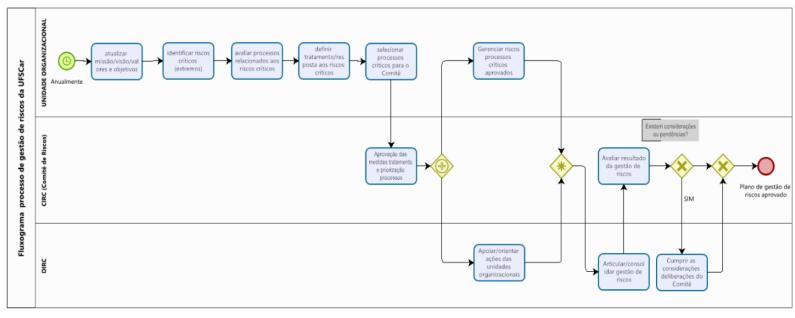
Esse processo de gestão de riscos é aplicado a uma ampla gama das atividades da UFSCar, em todos os níveis, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, e é suportado pela cultura e pela estrutura de gestão de riscos da Universidade.

O fluxo da 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 neste fluxo estão sintetizados na figura 5 a seguir:

Figura 5 – Fluxo do Processo de Gestão de riscos da UFSCar

(Adaptado ISO 31000:2009, disponivel em: https://www.dirc.ufscar.br/riscos/processo-gestao-riscos-ufscar.png/view)



4.3.1 - 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:

- **A. 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;
- B. Fluxo (mapa) do processo organizacional;
- **C. 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?";
- D. Relação de objetivos estratégicos da UFSCar alcançados pelo processo (PDI/UFSCar);
- E. Leis e regulamentos relacionados ao processo organizacional; e
- F. Existência de ferramentas tecnológicas que apoiam o processo organizacional.

4.3.2 - 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 utilizada a seguinte questão:

• 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 à 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;
- **Imagem ou reputação:** eventos que podem comprometer a confiança da sociedade ou de parceiros, fornecedores, em relação à capacidade da UFSCar em cumprir sua missão institucional.

4.3.3 - 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 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).

4.3.4 - 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. 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.

4.3.5 - 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 para a 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), quanto à urgência (tempo/prazo para resolver o risco) e à **probabilidade ou** tendência (consequências), 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 (tendência) e Impacto (gravidade)

_	Quadro 1 - Criterios de Probabilidade (tendencia) 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	Т	TOTAL	PRIORIDADE
1	COVID-19	5	5	5	125	19
2	Greve Estudantil	3	5	2	30	2º

Fonte: Adaptação própria (DIRC-2021)

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
110-125	Risco Extremo - RE
81- 109	Risco Alto - RA
31 - 80	Risco Médio - RM
1- 30	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.

4.3.6 – 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- 30 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. Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer		tratamento, essa priorização deve ser justificada pela unidade e	
		tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu Comitê de Integridade e Riscos.	
Risco Alto RA 81-109 Nível de risco além do apetite a risco. Qualquer risco neste 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.		de tratamento, a não priorização deve ser justificada pela unidade e do. aprovada pelo seu Comitê de Integridade e Riscos.	
Risco Extremo RE 110-125	Nível de risco muito além do apetite a risco. Qualquer risco neste 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.	

4.3.7 - Sobre o apetite a riscos da UFSCar no processo organizacional

Segundo a PGIRC, 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 <u>APETITE A RISCO:</u> somente serão tratados e comunicados ao CGIRC-UFSCar os riscos considerados altos e extremos ambos com impacto acima de 80 (OITENTA) 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, 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

RESPOSTA AO RISCO	DESCRIÇÃO DAS AÇÕES
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.

4.3.8 - 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 Gestão 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, 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.

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

Portanto, o monitoramento do processo de gestão de riscos é feito continuamente por todas as partes interessadas e atores envolvidos no processo na forma de camadas, com abrangência e níveis de informação específicos. Detalhadamente, em nível operacional e tático o monitoramento é feito pelos servidores da unidade organizacional e responsáveis (proprietários) dos riscos identificados cujos objetivos básicos são:

- Manter os controles internos eficientes;
- Cumprir o tratamento/respostas aos riscos identificados na unidade;
- Analisar eventuais ocorrências de novos riscos.

Em nível gerencial, o monitoramento é feito pelo CGIRC – Comintê de Gestão de Integridade, Riscos e Controles e pelo DIRC – Departamento de Gestão de Integridade, Riscos e Controles internos. Os objetivos do monitoramento nesse nível são:

- monitorar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas;
- monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas nos processos organizacionais das unidades organizacionais;
- verificar a implementação dos controles internos definidos em cada unidade;
- acompanhar a evolução dos níveis de riscos nas unidades organizacionais.

Em relação à Unidade de Auditoria Interna, no que diz respeito à sua missão cabe sinteticamente avaliar a gestão por meio de atuação independente e objetiva, prestando serviços de consultorias e agregando valor aos controles internos da Universidade, sempre buscando a eficácia nos processos de gerenciamento de riscos.

A figura 6, ilustra como é estruturado o processo de monitoramento da gestão de riscos na UFSCar

Figura 6 - Processo de Monitoramento em Camadas na UFSCar



5 – CUMPRIMENTO DO CRONOGRAMA DO DIRC PREVISTO NO PDI-UFSCar

A efetividade da aplicação deste plano, pretende-se que abranja, direta ou indiretamente, todas as áreas e unidades organizacionais da UFSCar no período abrangido pelos planos de Gestão de Riscos e Integridade previstos no cronograma do PDI-UFSCar neste período de quatro anos, desde 2025 até o final de 2028, período previsto de vigência deste plano.

O cronograma de ações do DIRC considerará as três linhas de abordagens ou áreas de atuação e implementação da gestão de riscos na UFSCar:

- ✔ Riscos nos objetivos estratégicos da Universidade (PDI-UFSCar);
- ✔ Iniciativas relacionadas à Gestão de Riscos nos processos das unidades organizacionais (UORGs);
- ✔ Riscos nos processos das unidades organizacionais identificados como riscos para a integridade;

Além disso, buscará cumprir da melhor forma possível e dentro da capacidade operacional do DIRC, as suas atribuições previstas na PGIRC, seu artigo 17º, dentre outras responsabilidades do departamento.

Finalmente, é imprescindível registrar a busca do DIRC pelo cumprimento de seus objetivos estratégicos previstos no PDI-UFSCar 2024-2028, especificamente o alcance dos objetivos estratégicos do eixo 4 - Gestão, a saber:

- → **Objetivo 4.1** Melhorar a governança corporativa e transparência;
- → Ação 4.1.4 Aumentar a maturidade de Gestão de Riscos;
 - Meta 1: Mapear todos os riscos altos e extremos dos processos de todas as unidades organizacionais;

Meta 2: Implementar ações de monitoramento dos riscos identificados e redução de riscos extremos em todas as unidades organizacionais.

5.1 - Demandas oriundas dos órgãos de controle interno (CGU e AudIn)

Entre fevereiro e julho de 2021 a CGU fez na UFSCar, um trabalho de verificação e avaliação da maturidade da governança de riscos. O objetivo principal dos trabalhos dos auditores da CGU, foi verificar como a Universidade Federal de São Carlos identifica e administra os riscos decorrentes da execução de suas atividades e qual é a sua capacidade de implantar controles internos administrativos que possam mitigar ou neutralizar esses riscos.

Os resultados revelaram que a UFSCar ainda não possui uma estrutura adequada para a gestão de riscos de forma compatível com a sua missão e os seus objetivos estratégicos, e em todos os processos organizacionais da instituição.

Consequentemente, em 2021 foram emitidas 07 (sete) recomendações para que se adotem, dentre outras providências, a implantação de uma estrutura adequada, disponibilizando para a SPDI/DIRC os recursos necessários para a consecução dos objetivos previstos pelo art. 16, incisos I a VIII da IN MP/CGU nº 01/2016.

Em 2024, em relação às 07 (sete) recomendações originais, apenas 04 (quatro) continuam em monitoramento.

Quadro 6 – As Recomendações da CGU RESUMIDAS (ações atualizadas em 20/10/2024)

	RECOMENDAÇÕES	RESUMO DAS AÇÕES/PROVIDÊNCIAS SOLICITADAS PELA CGU
1	E-AUD # 1176259 SEI 23112.010667/2022-72	- Estabelecer e comunicar todos os indicadores necessários para monitorar o atingimento dos objetivos estratégicos estabelecidos pela UFSCar Atualizadas em 20/10/2024: ACOMPANHAMENTO PELA CGU (ENVIADA EM 10/10)
2	E-AUD # 1176297 SEI 23112.010673/2022-20	- Complementar/atualizar o plano de integridade 2023-2024 da universidade em relação aos riscos de nepotismo. Atualizadas em 20/10/2024: ACOMPANHAMENTO PELA CGU - PRAZO 13/12/24.
3	EAUD # 1176276 SEI 23112.010679/2022-05	- Implementar o processo de gestão de riscos em todos os processos organizacionais da UFSCar. Atualizadas em 20/10/2024: ACOMPANHAMENTO PELA CGU - PRORROGAÇÃO DE PRAZO DE ENVIO DAS RESPOSTAS PARA O DIA 31/10/24.
4	EAUD # 1176291 SEI 23112.010670/2022-96	-Implantar estrutura adequada para a gestão de riscos Atualizadas em 20/10/2024: ACOMPANHAMENTO PELA CGU - ENVIADA EM 09/10/24.

Fonte: Elaborada pelo DIRC com base no acompanhamento pela Auditoria Interna e CGU - Relatório de Auditoria #905610

6 - CONSIDERAÇÕES FINAIS

Este documento apresentou o Plano de Gestão de Riscos da UFSCar previsto para o período 2025-2028, bem como, explicitou os fundamentos legais e teóricos que norteiam as ações de gestão de riscos na Universidade.

Como objetivo primordial buscou 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 10, 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.

Apresentou também, a metodologia de gestão de riscos da UFSCar e suas respectivas etapas. A pretensão foi de orientar os gestores envolvidos no processo de implementar as ações de mapeamento dos riscos em suas áreas e setores em conformidade com a metodologia e explicitamente de acordo com a PGIRC-UFSCar.

Demonstrou no cronograma de ações do DIRC as três linhas de abordagens ou áreas de atuação e implementação da gestão de riscos na UFSCar: identificação dos riscos nos objetivos estratégicos da Universidade (PDI-UFSCar); registro das iniciativas relacionadas à Gestão de Riscos nos processos das unidades organizacionais da UFSCar e registro de riscos nos processos das unidades organizacionais identificados como riscos para a integridade. Buscando-se cumprir da melhor forma possível as atribuições e competências do DIRC previstas na PGIRC-UFSCar em seu artigo 17.

A relevância da padronização da implementação de uma gestão de riscos nos processos de trabalho, além de fortalecer a gestão, aperfeiçoa os processos e maximiza o alcance dos objetivos organizacionais, por meio de criação e aprimoramento dos controles internos da gestão, da governança e sistematização da gestão de riscos.

Finalmente, ressalta-se que em qualquer iniciativa de implementação de metodologias é essencial considerar o caráter dinâmico da administração (gestão), e assim, buscar a realização de acertos e ajustes para se adequar ao contexto e às necessidades da UFSCar.

O Plano de Gestão de Riscos deve ser visto, essencialmente, como um processo de construção e de reforço da política interna de governança na área de gestão de integridade, riscos e controles internos da Universidade (PGIRC-UFSCar).

7 - REFERÊNCIAS BIBLIOGRÁFICAS

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

BRASIL. Instrução Normativa Conjunta MP/CGU № 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 – CGU.

BRASIL. Universidade Federal de São Carlos. Plano de Desenvolvimento Institucional (PDI) - vigência 2024-2028. Disponível em: https://www.spdi.ufscar.br/arquivos/planejamento/pdi/pdi-2024-2028.pdf . Acesso em: 24/09/2024.

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.

UFSCar. Plano de Desenvolvimento Institucional - PDI 2024-2028. São Carlos, SP: Universidade Federal de São Carlos, out. 2024. Disponível em: https://www.spdi.ufscar.br/arquivos/planejamento/pdi/pdi-2024-2028.pdf Acesso em: 22/10/2024.