Relatório de Auditoria 202501-01

Ação: Avaliação da conformidade e governança da Gestão de Riscos na UTFPR

17 de outubro de 2025

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
CONSELHO UNIVERSITÁRIO
AUDITORIA INTERNA

RELATÓRIO DE AUDITORIA n.º 202501-01

Unidade examinada:
REITORIA e SITAI

Período de realização:
01/01/2025 a 30/09/2025

Restrições à execução dos trabalhos:
Não houve restrições.

QUAL FOI O TRABALHO REALIZADO?

Avaliar a conformidade e governança no que tange à Gestão de Riscos no âmbito da UTFPR.

POR QUE ESTE TRABALHO FOI REALIZADO?

Este trabalho está elencado no PAINT/2025, quadro 4, item 1, como um dos trabalhos originados da avaliação de riscos e tem como escopo avaliar a gestão de processos de governança e gerenciamento de riscos da UTFPR.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUDIN? QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

A auditoria identificou que a UTFPR ainda não instituiu formalmente um processo sistematizado de gerenciamento de riscos, em conformidade com as diretrizes da IN SFC nº 01/2016. Entretanto, a instituição dispõe de elementos fundamentais que favorecem sua implementação, destacando-se o PDI e o PEP, ambos alinhados às finalidades regimentais e legais. Detectou-se uma fragilidade significativa na ausência de definição clara e formalizada da periodicidade para as etapas de identificação, avaliação, tratamento e monitoramento de riscos, o que pode comprometer a capacidade institucional de resposta a eventos que impactem os objetivos estratégicos. Além disso, a não elaboração da metodologia de gestão de riscos, prevista na PGIRC, comprometeu a efetiva sistematização do processo. Recomenda-se a revisão da Política de Gestão de Riscos e a elaboração de um plano de ação para a instituição da metodologia, especificando a periodicidade das fases do processo e as responsabilidades pelo monitoramento e análise crítica. Essas medidas são essenciais para fortalecer a governança, os controles internos, e assegurar maior integração entre a gestão de riscos, o planejamento estratégico e o alcance dos objetivos institucionais.

LISTA DE SIGLAS E ABREVIATURAS

AUDIN	Auditoria Interna
CGIRC	Comitê de Governança, Integridade, Riscos e Controles da UTFPR
CGU	Controladoria-Geral da União
IN	Instrução Normativa
GR	Gerenciamento de Riscos
OS	Ordem de Serviço
PDI	Plano de Desenvolvimento Institucional
PGIRC	Política de Governança, Integridade, Riscos e Controles
PEP	Plano Estratégico Participativo da UTFPR
UFAM	Universidade Federal do Amazonas
UTFPR	Universidade Tecnológica Federal do Paraná

SUMÁRIO

1 INTRODUÇÃO

1.1 MOTIVAÇÃO DA AUDITORIA

A presente auditoria foi realizada em cumprimento à atividade prevista no item 1 do Quadro 4 do Plano Anual de Auditoria Interna de 2025 (PAINT 2025) da Unidade de Auditoria Interna da Universidade Tecnológica Federal do Paraná (UTFPR), tendo como objetivo avaliar a gestão dos processos de governança e de gerenciamento de riscos da instituição.

A seleção desta ação de auditoria baseou-se na Metodologia do Plano de Auditoria Baseado em Riscos (PABR), elaborada pela AUDIN/UTFPR, a qual orientou a definição dos objetos de auditoria constantes no PAINT 2025.

A aplicação dessa metodologia, por meio da matriz de riscos constante no referido documento, atribuiu ao processo "Integridade e Gestão de Riscos" o nível de risco de 80 pontos. Esse resultado justificou a sua priorização como objeto da presente avaliação. De acordo com a matriz, o risco identificado decorre da inexistência ou inadequada identificação de riscos pela administração, sendo a causa principal relacionada à ausência de ferramentas e metodologias apropriadas.

Ademais, esta avaliação encontra-se alinhada aos seguintes eixos do Plano de Desenvolvimento Institucional (PDI):

> **Eixo: Planejamento e Avaliação Institucional**
>
> 1. Aperfeiçoar e ampliar os processos e as ferramentas de avaliação internos;
>
> **Eixo: Desenvolvimento Institucional**
>
> 5. Criar e fortalecer políticas institucionais;

1.2 VISÃO DO OBJETO

A Gestão de Riscos no âmbito da Administração Pública Federal é determinada pelo artigo 13 da Instrução Normativa Conjunta MP/CGU n.º 01, de 10 de maio de 2016, que prescreve que "os órgãos e entidades do Poder Executivo Federal deverão implementar, manter, monitorar e revisar o processo de gestão de riscos, compatível com a sua missão e seus objetivos estratégicos, observadas as diretrizes estabelecidas nesta instrução normativa".

No ano seguinte, o Decreto n.º 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, veio reforçar a necessidade de um sistema de Gestão de Riscos, conforme prescrição contida em seu artigo 17:

> Art. 17. 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, observados os seguintes princípios:
>
> I - implementação e aplicação de forma sistemática, estruturada, oportuna e documentada, subordinada ao interesse público;
>
> II - integração da gestão de riscos ao processo de planejamento estratégico e aos seus desdobramentos, às atividades, aos processos de trabalho e aos projetos em todos os níveis da organização, relevantes para a execução da estratégia e o alcance dos objetivos institucionais;
>
> III - estabelecimento de controles internos proporcionais aos riscos, de maneira a considerar suas causas, fontes, consequências e impactos, observada a relação custo-benefício; e
>
> IV - utilização dos resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de gerenciamento de risco, controle e governança.

Além disso, mais do que o mero cumprimento de uma conformidade normativa, a sociedade demanda uma administração pública ágil e eficiente, capaz de implementar políticas e programas governamentais que proporcionem o máximo valor à população. Nesse contexto, a adoção de práticas e estratégias eficazes de gestão requer que o gestor assuma responsabilidades claras, exercendo ações de governança e gestão nas instituições públicas, com o objetivo central de entregar o melhor valor público possível.

As incertezas que podem impactar os objetivos são inerentes à atuação de qualquer instituição e podem se originar em diferentes fatores, como econômicos, sociais, operacionais, políticos e tecnológicos.

Dessa forma, essas incertezas representam riscos aos quais a organização está sujeita e, por isso, devem ser identificadas, analisadas e tratadas, buscando sempre reduzir ao mínimo qualquer interferência sobre os objetivos institucionais.

A gestão de riscos, os controles internos e a integridade funcionam como mecanismos capazes de gerar valor às instituições e aos seus processos quando atuam de forma integrada. Eles permitem tratar as incertezas que podem impedir ou dificultar o alcance dos objetivos organizacionais, além de promover comportamentos íntegros. Tais mecanismos contribuem para aprimorar a qualidade das decisões dos gestores públicos, sempre em busca da efetivação do interesse público.

Além disso, a avaliação da Gestão de Riscos constitui um dos objetivos principais da auditoria interna, conforme disposto no artigo 8º do Regimento Interno da AUDIN, avaliando se os controles internos, a gestão de riscos e a governança da organização funcionam adequadamente, de forma a garantir se, entre outras atribuições, os riscos são adequadamente identificados e administrados pela gestão.

Logo, esta ação de auditoria tem por objeto a avaliação da conformidade da atual estrutura de Gestão de Riscos na UTFPR e dos pontos principais do ambiente de controle da instituição, tendo por objetivo o aperfeiçoamento desse sistema pela gestão.

2 RESULTADOS DOS EXAMES

2.1 DOS DOCUMENTOS ESTRATÉGICOS

Conforme referência anterior, o artigo 13 da IN MP/CGU n.º 01/2016 traz um preceito essencial para uma adequada implantação da Gestão de Riscos em uma instituição: **que este processo seja compatível com a sua missão e seus objetivos estratégicos**.

Esta referência normativa encontra-se alinhada ao modelo de gestão de riscos COSO ERM (*Committee of Sponsoring Organizations – Enterprise Risk Management*), em que, com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização, uma vez que, de acordo com esse modelo, não adianta as operações serem eficientes, os relatórios confiáveis e as leis e regulamentos cumpridos, se não há uma estratégia a ser alcançada.

Neste ponto, a UTFPR estabeleceu um direcionamento estratégico, que engloba sua missão, visão, valores e macro-objetivos, em consonância com suas finalidades institucionais e atribuições legais. Este planejamento se materializa no Plano de Desenvolvimento Institucional (PDI), que cobre o quinquênio de 2023 a 2027. Sobre esse documento, é possível tecer as seguintes considerações:

1. O PDI instituiu 86 macro-objetivos, divididos em cinco eixos, conforme é possível verificar na página 350 e seguintes do documento:

Quadro 1: Eixos do PDI

Eixo 1	Planejamento e Avaliação Institucional
Eixo 2	Desenvolvimento Institucional
Eixo 3	Políticas Acadêmicas
Eixo 4	Políticas de Gestão
Eixo 5	Infraestrutura

Fonte: Plano de Desenvolvimento Institucional da UTFPR 2023-2027.

2. A missão, visão e valores institucionais constam no capítulo 3.2 do PDI (p. 87 e seguintes), conforme quadro abaixo:

Quadro 2 – Missão, visão e valores da UTFPR

Missão	Desenvolver a educação tecnológica de excelência, construir e compartilhar o conhecimento voltado à solução dos reais desafios da sociedade.
Visão	Ser uma universidade reconhecida internacionalmente pela importância de sua atuação em prol do desenvolvimento regional e nacional sustentável.
Valores	Ética Tecnologia e Humanismo Desenvolvimento Humano Interação com o entorno Empreendedorismo e Inovação Excelência Sustentabilidade

	Diversidade e Inclusão Democracia e Transparência

Fonte: Plano de Desenvolvimento Institucional da UTFPR 2023-2027.

Tendo em vista que o estabelecimento de objetivos estratégicos e missão alinhados às finalidades e atribuições legais da instituição constituem o ponto de partida e um requisito fundamental para um adequado processo de gerenciamento de riscos, é possível afirmar que, em relação a esse ponto, a UTFPR estabeleceu um direcionamento estratégico adequado no que tange à observação deste requisito.

Adicionalmente, a UTFPR publicou recentemente o Plano Estratégico Participativo - PEP, documento que vem a complementar e detalhar os objetivos estratégicos da UTFPR, abrangendo o período de 2024 a 2028.

Figura 1: Missão, Visão e Objetivos Estratégicos do PEP

Fonte:PEP - UTFPR 2024-2028.

O estabelecimento dos macro-objetivos definidos no Plano de Desenvolvimento Institucional (PDI) e dos objetivos estratégicos delineados no Plano Estratégico Participativo representa a base fundamental para a consolidação de uma gestão de riscos plenamente institucionalizada e eficaz. A articulação entre esses instrumentos promove alinhamento das ações institucionais, garantindo coerência entre planejamento, execução e monitoramento, ao mesmo tempo em que fortalece os mecanismos de governança e possibilita maior capacidade de prevenção e mitigação de riscos que possam comprometer o alcance das metas institucionais.

2.2 DA POLÍTICA DE GESTÃO DE RISCOS, GOVERNANÇA E CONTROLES INTERNOS

Com a vigência da Instrução Normativa Conjunta CGU n.º 01/2016, e a prescrição, em seu artigo 17, da necessidade da formalização de uma Política de Gestão de Riscos, contendo princípios, diretrizes e responsabilidades para a gestão integrada de riscos, integridade e controles internos, os órgãos da Administração Pública Federal precisaram elaborar suas próprias políticas contendo alguns requisitos mínimos a serem observados constantes neste dispositivo, conforme segue:

> Art. 17. A política de gestão de riscos, a ser instituída pelos órgãos e entidades do Poder Executivo federal em até doze meses a contar da publicação desta Instrução Normativa, deve especificar ao menos:
>
> I - princípios e objetivos organizacionais;
>
> II - 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; e
> f) o desenvolvimento contínuo dos agentes públicos em gestão de riscos; e
>
> III - competências e responsabilidades para a efetivação da gestão de riscos no âmbito do órgão ou entidade.

Desse modo a UTFPR aprovou, por meio da Deliberação COUNI n.º 30 de 20/12/2019, a "Política de Governança, Integridade, Risco e Controle" da instituição, tendo por objetivo a estruturação da gestão de riscos e o atendimento da normativa em comento. Entretanto, como será adiante explanado, algumas das diretrizes não foram contempladas, seja de forma total ou parcial, em relação ao disposto na normativa regente.

2.2.1 Do Monitoramento da Gestão de Riscos

Sem prejuízo da observação da conformidade à norma, a definição clara da periodicidade para identificação, avaliação, tratamento e monitoramento dos riscos é elemento essencial para a efetividade da gestão de riscos na instituição. A ausência de prazos definidos pode comprometer a atualização das informações, gerar defasagem nos planos de ação e reduzir a capacidade de prevenção e resposta a eventos que possam afetar os objetivos institucionais.

O Referencial Básico de Gestão de Riscos do Tribunal de Contas da União reforça a importância da periodicidade no monitoramento, asseverando o seguinte:

> O monitoramento e análise crítica é etapa essencial da gestão de riscos e tem por finalidade: (a) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos de riscos e suas prioridades, assim como identificar riscos emergentes; (b) obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos; (c) analisar eventos (incluindo os "quase incidentes"), mudanças, tendências,

> sucessos e fracassos e aprender com eles; e (d) assegurar que os controles sejam eficazes e eficientes no projeto e na operação (ABNT, 2009). É importante observar a necessidade de segregação de funções também nas atividades de monitoramento (p. 34-35).

Ao se analisar a Política de Governança, Integridade, Risco e Controle da UTFPR, tais requisitos não ficaram claros e objetivos no documento vigente, em dissonância com o prescrito pelas normativas e manuais apresentados. Logo, faz-se relevante que a UTFPR, na oportunidade de adequação deste dispositivo, proceda à revisão dessas diretrizes em sua Política, não apenas em busca da conformidade normativa, mas sim como medida para fortalecimento dos controles internos e do próprio alcance de seus objetivos institucionais quando do processo de gerenciamento dos riscos.

2.3 DA METODOLOGIA DA GESTÃO DE RISCOS DA UTFPR

Embora a Política de Governança, Integridade, Risco e Controle da UTFPR tenha previsto, em seu artigo 18, que a metodologia de Gestão de Riscos deveria ser aprovada em até 12 meses após a publicação da referida política, o documento ainda não foi elaborado, evidenciando uma inconformidade em razão da ausência de identificação dos riscos e, consequentemente, de sua avaliação e respostas a possíveis eventos danosos.

Analisando-se a Política de Governança, Integridade, Risco e Controle da UTFPR , verifica-se que, normativamente, a atribuição e competência para a sistematização da metodologia foi atribuída ao Subcomitê de Apoio à Governança, Integridade, com a posterior análise e aprovação do próprio Comitê de Governança, Integridade, Riscos e Controles, conforme se verifica na transcrição abaixo:

> Art. 10. Compete ao Subcomitê de Apoio à Governança, Integridade, Riscos e Controles (CGIRC), instituído pela Portaria UTFPR nº 1.384, de 01/08/2018:
> a) auxiliar o Comitê de Governança, Riscos e Controles na definição e nas atualizações da estratégia de implementação da Gestão de Riscos;
> b) auxiliar na definição dos níveis de apetite a risco, dos responsáveis e da periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;
> c) apoiar a identificação de pontos de controles nos processos organizacionais, favorecendo a Gestão de Riscos;
> d) propor metodologia de Gestão de Riscos e suas revisões;
> e) avaliar os requisitos funcionais necessários às ferramentas de tecnologia de suporte ao processo de gerenciamento de riscos;
> f) auxiliar o CGIRC na avaliação do desempenho da Gestão de Riscos institucional e da efetividade das medidas adotadas, recomendando melhorias aos gestores dos processos, quando necessário;
> g) assessorar a implementação das metodologias e instrumentos para a gestão, governança, riscos e controles internos, de forma integrada aos processos organizacionais.
> h) promover ações de capacitação aos servidores para entendimento e aplicação das políticas e metodologias de gestão de riscos, proporcionando a formação de multiplicadores sobre o tema.

Desse modo, infere-se que uma das causas para a não implementação e formalização do processo de Gerenciamento de Riscos na UTFPR estão ligadas diretamente à ausência de engajamento e atuação proativa do Comitê e Subcomitê de Governança da UTFPR.

O PDI 2023-2027, em sua página 293, esclarece, em síntese, que a gestão de riscos se encontra devidamente integrada e alinhada ao Planejamento Estratégico, ao PDI e em todas as áreas da instituição, com a priorização dos processos organizacionais que impactam diretamente nos objetivos da instituição e que possuem maior probabilidade e impacto de ocorrer.

Entretanto, sem haver uma sistematização, revisão e acompanhamento formalizados, não há como consolidar um processo de gerenciamento de riscos institucional de forma eficaz e eficiente, deixando a instituição vulnerável a esses riscos não gerenciados e causando um possível impacto no alcance de seus objetivos institucionais.

É necessário que haja um endosso claro pela alta governança da UTFPR no sentido de se estabelecer um plano de ação para revitalizar a atuação do comitê e subcomitê de Governança, Integridade, Riscos e Controles para que a cultura de gerenciamento de riscos seja formalmente implementada de acordo com o previsto nas normativas internas e externas já elencadas neste relatório.

Esse é o papel da alta administração, assumindo seu papel de liderança que é fundamental para a implementação e operação da gestão de riscos. Essa questão é fortemente sustentada pelo modelo de gerenciamento de riscos COSO GRC, que prescreve que, para que uma organização alcance uma gestão de riscos realmente eficaz, é indispensável que a postura e o compromisso da alta administração sejam claros, firmes e disseminados por toda a instituição.

2.4 MODELOS PARA A ARQUITETURA DA GESTÃO DE RISCOS INSTITUCIONAL

2.4.1 Apresentação dos modelos (Frameworks) de Gestão de Riscos mais utilizados

Conforme anteriormente exposto, tendo em vista que a UTFPR já estabeleceu seus objetivos estratégicos, a escolha de um modelo constitui o passo seguinte para institucionalizar o processo de gestão de riscos.

Desse modo, a instituição deve priorizar uma **metodologia plenamente alinhada ao contexto interno e externo da instituição, bem como ao seu perfil de risco**, conforme determina a normativa ABNT NBR ISO 31000:2018 – Gestão de Riscos – Diretrizes.

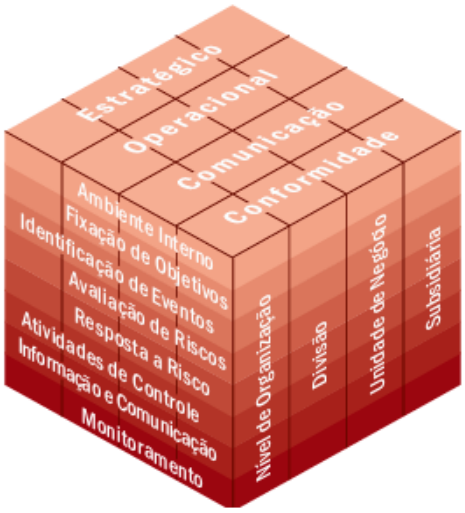
Internacionalmente, existem **quatro modelos** mais utilizados por instituições públicas e privadas, que precisam ser avaliados e conhecidos previamente à instituição da metodologia de gestão de riscos da instituição. São eles: 1) COSO II - Gerenciamento de Riscos Corporativos - Estrutura Integrada; 2) COSO GRC 2016 - Alinhando Risco com Estratégia e Desempenho; 3) ISO 31000 - Gestão de Riscos - Princípios e Diretrizes; 4) Orange Book e Risk Management Assessment Framework.

2.4.1.1 COSO II - Gerenciamento de riscos Corporativos - Estrutura Integrada

Este modelo representa uma abordagem amplamente adotada internacionalmente na gestão corporativa de riscos, com destaque especial para a América do Norte. Seu objetivo principal é oferecer uma estratégia acessível às organizações para avaliação e aprimoramento contínuo da gestão de riscos.

Visualmente, a metodologia se expressa por meio de uma matriz tridimensional, conhecida como o cubo COSO, que integra, em um único modelo, os elementos essenciais para o gerenciamento eficaz dos riscos, alinhados aos objetivos e à estrutura específica de cada entidade.

Figura 2: Cubo COSO



Fonte: Referencial Básico de Gestão de Riscos do Tribunal de Contas da União.

Na parte superior do cubo, encontram-se as categorias de objetivos comuns a todas as organizações, indicando que o sistema de gestão de riscos deve oferecer um grau razoável de segurança em seu atingimento. A lateral esquerda do cubo ressalta os componentes fundamentais, que precisam ser implementados e operados de forma integrada à rotina institucional, garantindo a efetividade dos controles de riscos. Já a lateral direita representa as múltiplas camadas da estrutura organizacional, abrangendo diferentes níveis, funções, projetos, processos e demais atividades fundamentais para o alcance dos objetivos organizacionais.

2.4.1.2 COSO GRC 2016 - Alinhando Risco com Estratégia e Desempenho

Em 2016, o COSO apresentou uma revisão do modelo de 2004, intitulada "Alinhando Risco com Estratégia e Desempenho", com o objetivo de reforçar a integração entre a gestão de riscos, o planejamento estratégico e o desempenho das organizações.

O novo modelo, denominado COSO GRC, aprimora o alinhamento entre governança, administração e *accountability*, modernizando os conceitos anteriores e incorporando princípios que ressaltam o papel da cultura organizacional e a criação de valor. A estrutura revisada insere a gestão de riscos em três dimensões centrais: missão, visão e valores; objetivos estratégicos e de negócios; e desempenho organizacional.

A abordagem propõe que governança e alta administração assumam papel ativo na supervisão dos riscos, considerando três perspectivas principais: 1) o alinhamento entre objetivos e missão/visão/valores; 2) as implicações da estratégia adotada; 3) os riscos na execução da estratégia.

Houve também maior integração entre gestão de riscos e desempenho, destacando a necessidade de definir tolerâncias de risco como parte do processo de avaliação de resultados.

O modelo reduziu de oito para cinco os componentes da gestão de riscos:

1. Governança e cultura;
2. Estratégia e definição de objetivos;
3. Desempenho;
4. Revisão e correção;
5. Informação, comunicação e reporte.

Por fim, foram estabelecidos vinte princípios de gestão de riscos, aplicáveis a organizações de diferentes portes e setores, que possibilitam à liderança manter um nível adequado de compreensão e controle sobre os riscos relacionados à estratégia e aos objetivos corporativos.

2.4.1.3 ISO 31000 - Gestão de Riscos - Princípios e Diretrizes

A norma ISO ABNT 31000:2018 estabelece princípios e diretrizes gerais para a gestão de qualquer tipo de risco, podendo ser aplicada a organizações de todos os setores, portes ou áreas de atuação. Ela não substitui nem concorre com normas específicas, mas busca oferecer uma referência unificada para o gerenciamento de riscos.

Seu principal objetivo é servir como guia para harmonizar processos e promover uma abordagem comum aplicável a diferentes contextos organizacionais — desde a formulação de estratégias e tomada de decisões até a execução de operações, projetos, produtos, serviços e gestão de ativos.

A ISO 31000 estrutura-se em três partes interdependentes: princípios, estrutura e processo de gestão de riscos. Esse processo fornece uma metodologia sistemática para aplicar políticas, práticas e procedimentos de gestão de riscos de forma consistente e adaptável a qualquer tipo de organização, fortalecendo a governança e a tomada de decisões.

Essas características deram suporte para que este modelo seja amplamente utilizado como referência nas instituições públicas brasileiras, tendo sido escolhido pelo TCU para sistematização de processo de gerenciamento de riscos em razão de sua harmonização entre os outros modelos apresentados e o fornecimento de uma abordagem comum para a aplicação em um amplo conjunto de atividades.

2.4.1.4 The Orange Book - Princípios e Conceitos

O "*The Orange Book – Management of Risk: Principles and Concepts*", publicado pelo "HM Treasury do Reino Unido", foi a principal referência para o programa de gestão de riscos do governo britânico iniciado em 2001. Este modelo destaca-se por sua compatibilidade com

padrões internacionais como COSO e ISO 31000, além de apresentar uma introdução clara e abrangente ao tema, facilitando a compreensão de um assunto complexo.

Inspirado no Orange Book, o Ministério do Planejamento, Orçamento e Gestão do Brasil produziu um Guia de Orientação para o Gerenciamento de Riscos, que apoia o Modelo de Excelência do Sistema de Gestão Pública (GESPÚBLICA) e serve como introdução à gestão de riscos no setor público brasileiro.

Em 2009, o governo do Reino Unido lançou o *Risk Management Assessment Framework*, uma ferramenta que avalia a gestão de riscos nas organizações governamentais e identifica oportunidades de melhoria. Essa ferramenta é derivada do modelo de excelência EFQM, amplamente utilizado por diversas organizações europeias.

Em resumo, o Orange Book fornece uma estrutura simplificada e eficaz para gerenciar riscos em múltiplos níveis organizacionais (estratégico, programas, projetos e atividades), enfatizando a importância da governança, cultura e alinhamento com objetivos organizacionais no processo de gestão de riscos.

2.4.2 O Processo de Gestão de Riscos

Definido o modelo a ser utilizado pela gestão, o passo seguinte consiste na identificação, análise e avaliação dos riscos, seguido pela escolha e implementação das respostas adequadas para mitigá-los. Inclui, ainda, o monitoramento contínuo dos riscos e dos controles adotados, além da comunicação efetiva sobre os riscos com as partes interessadas, tanto internas quanto externas, durante toda a execução do processo.

Este processo é aplicável a diversas atividades da organização em todos os níveis, abrangendo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, e é sustentado pela cultura organizacional e pela estrutura de gestão de riscos vigente na entidade. Dito isso, as etapas do processo de gerenciamento de riscos consistem nas seguintes atividades, conforme demonstrado nos Quadros 3 a 9 (ABNT ISO 31000:2018 e PGIRC/UTFPR):

Quadro 3: Entendimento do Contexto

Entendimento do Contexto
Envolve entender o ambiente interno e externo onde a gestão de riscos será aplicada, identificando os parâmetros e critérios relevantes para orientar o gerenciamento dos riscos. Essa análise do contexto inclui aspectos como estruturas de governança, controles existentes, valores éticos, competências e a cultura organizacional, que vão sustentar o processo de gestão de riscos e garantir que os objetivos organizacionais sejam considerados ao identificar possíveis riscos.
Subetapas
- identificar quais objetivos ou resultados devem ser alcançados; - identificar os processos de trabalho relevantes para o alcance dos objetivos/resultados; - identificar as pessoas envolvidas nesses processos e especialistas na área; - mapear os principais fatores internos e externos que podem afetar o alcance dos objetivos/resultados (pessoas, sistemas informatizados, estruturas organizacionais, legislação, recursos, stakeholders etc.); - definir os objetos de gestão de risco mais importantes para a sua unidade ou trabalho;

- definir os objetivos/resultados de cada objeto.

Fonte: Adaptado do Manual de Gestão de Riscos do TCU.

Quadro 4: Identificação dos riscos

Identificação de riscos
Envolve o reconhecimento e a caracterização dos riscos associados aos objetivos ou resultados do objeto de gestão de riscos, incluindo a identificação de potenciais fontes geradoras desses riscos. A identificação dos riscos deve ocorrer em oficinas de trabalho ou, conforme a natureza do objeto, ser conduzida diretamente pelo gestor do risco. Nesse processo, é recomendada a participação de pessoas com conhecimento aprofundado sobre o objeto de gestão. Devem ser aplicadas técnicas e ferramentas que favoreçam a ampla coleta de riscos, como brainstorming, brainwriting, entrevistas, visitas técnicas e pesquisas.
Subetapas
-Registrar de forma precisa os objetivos ou resultados previstos; -enumerar, para cada um deles, os eventos que possam afetar negativamente seu cumprimento; - detalhar o impacto de cada risco sobre o objetivo ou resultado correspondente.

Fonte: Adaptado do Manual de Gestão de Riscos do TCU.

Quadro 5: Análise de riscos

Análise de riscos
A análise de riscos consiste em compreender detalhadamente o risco e determinar seu nível, utilizando como referência uma matriz baseada na combinação entre probabilidade e impacto. A probabilidade corresponde à chance de o evento ocorrer dentro do período previsto para o alcance do objetivo ou resultado. Por exemplo, em um projeto, a avaliação considera a possibilidade de o risco se concretizar durante o prazo estipulado para a entrega do produto final. As escalas utilizadas podem variar conforme o objeto de gestão e o grau de precisão necessário para definir os níveis de probabilidade e impacto. Em geral, aplicam-se escalas qualitativas com até cinco níveis: **Escala de probabilidade (1 a 5):** 1. Raro – ocorre apenas em situações excepcionais, sem histórico conhecido ou indícios de ocorrência. 2. Pouco provável – apresenta baixa frequência de ocorrência dentro do prazo do objetivo. 3. Provável – manifesta-se com certa regularidade ou há sinais de que possa ocorrer nesse período. 4. Muito provável – tende a se repetir com alta frequência ou existem fortes indícios de ocorrência.

5. Quase certo – ocorrência praticamente garantida no prazo considerado.

Escala de impacto (1 a 5):

1. Muito baixo – afeta minimamente o alcance do objetivo, sem prejuízo prático.
2. Baixo – compromete parcialmente, mas não impede o alcance da maior parte do objetivo.
3. Médio – causa impacto moderado no alcance do resultado.
4. Alto – compromete grande parte do atingimento do objetivo pretendido.
5. Muito alto – inviabiliza total ou quase totalmente o alcance do objetivo.

Assim, a definição dos riscos seguirá a matriz abaixo:

Figura 3: matriz impacto x probabilidade

Impacto						
	Muito Alto	15 Risco (b)	19	22	24	25
	Alto	10	14 Risco (a)	18	21	23
	Médio	6	9	13	17	20
	Baixo	3	5	8	12	16
	Muito baixo	1	2	4	7	11
		Raro	Pouco provável	Provável	Muito provável	Praticamente certo
		Probabilidade				

Nível do risco (a): 14 | Nível do risco (b): 15

Fonte: Fonte: Manual de Gestão de Riscos TCU

O nível do risco é determinado diretamente pela célula correspondente na matriz, sem necessidade de cálculos matemáticos. A matriz apresenta 25 níveis possíveis, resultantes da combinação entre as estimativas de probabilidade e impacto, variando do nível 1 (evento muito raro e de impacto muito baixo) ao nível 25 (evento praticamente certo e de impacto muito alto).

Entre as principais diretrizes para uso da matriz destacam-se:

- O impacto é o fator mais relevante, devendo um evento de impacto muito alto — ainda que raro — receber maior atenção do gestor do que outro de impacto mínimo e alta probabilidade.

- Atribuições numéricas arbitrárias podem distorcer a avaliação, pois somas ou multiplicações de valores qualitativos não refletem adequadamente a gravidade dos riscos.

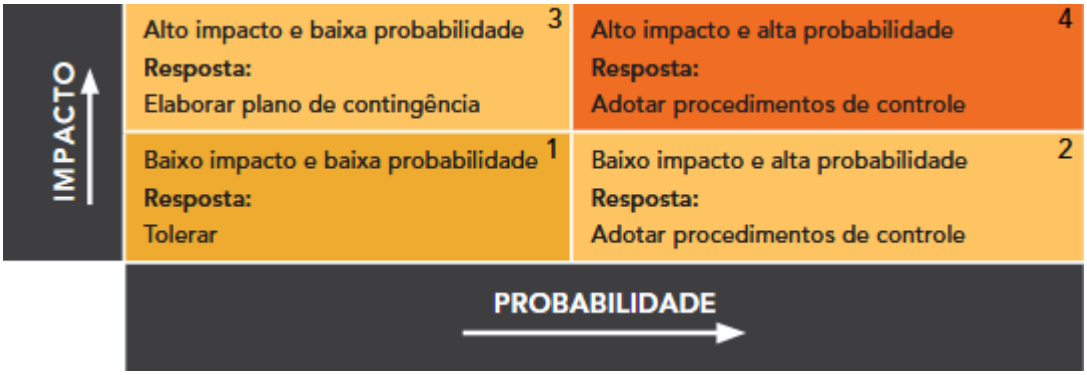
- A qualidade da avaliação depende do conhecimento técnico dos participantes sobre processos e riscos.

- É possível ajustar a escala da matriz (como 3x3 ou 5x5) para aprimorar a tomada de decisão, conforme a necessidade da análise.

- A avaliação deve considerar os controles existentes e refletir o risco real ao qual o gestor está exposto.

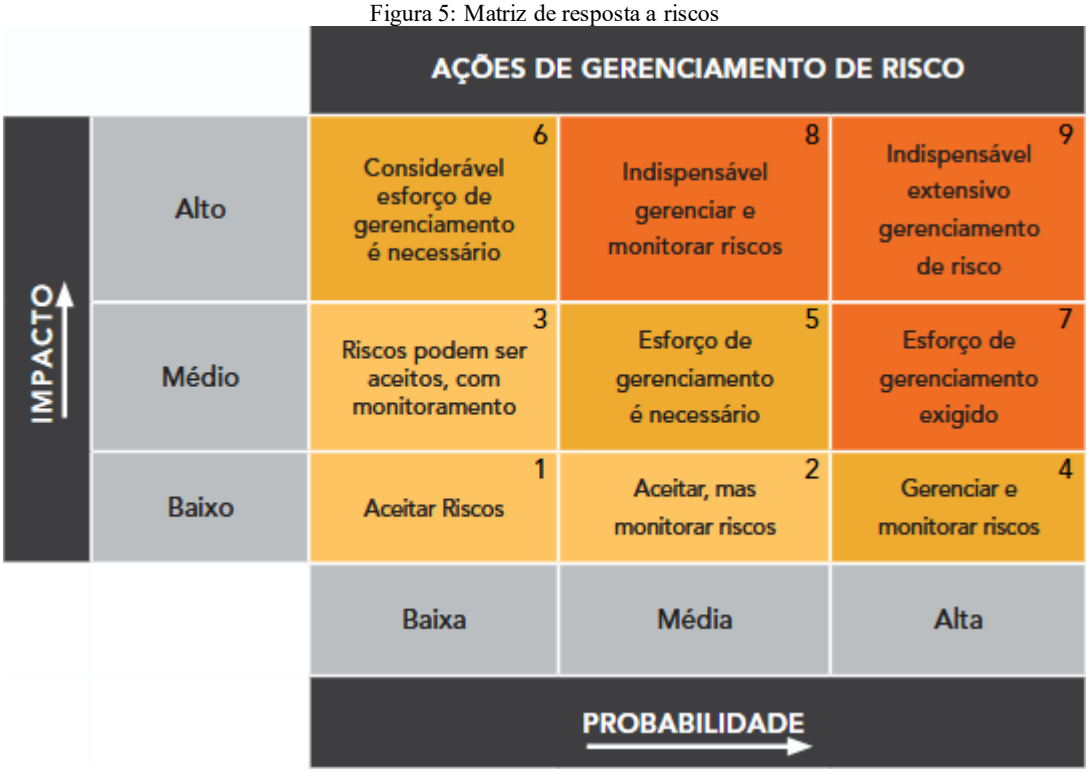
Não há modelo único de escala; o gestor deve adotar o formato que proporcione utilidade prática sem complexidade excessiva.

Figura 4: Matriz Simples de Avaliação e Resposta a riscos



Fonte: Manual de Gestão de Riscos TCU

Figura 5: Matriz de resposta a riscos



Fonte: Manual de Gestão de Riscos TCU

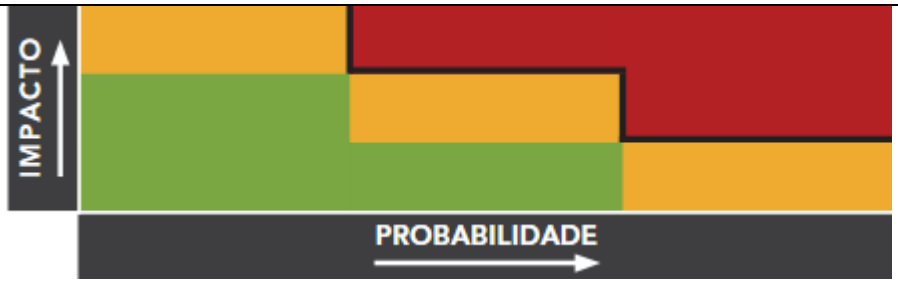
Logo, a análise dos riscos permite obter uma visão abrangente sobre os níveis associados a cada evento identificado, possibilitando sua ordenação em termos de prioridade. A responsabilidade por essa priorização recai sobre o gestor do risco, que deve determinar quais eventos demandam tratamento específico.

Subetapas
- Avaliar o impacto do risco sobre o objetivo ou resultado, considerando o grau de comprometimento potencial que ele pode causar. Um risco que possa comprometer total ou quase totalmente o alcance de um objetivo é classificado como de alto impacto. -Avaliar também a probabilidade de ocorrência do risco, entendendo como de alta probabilidade aquele evento cuja concretização seja praticamente certa. -Por fim, determinar o nível do risco a partir da combinação entre a probabilidade e o impacto, utilizando a matriz de risco correspondente.

Fonte: Adaptado do Manual de Gestão de Riscos do TCU.

Quadro 6: Avaliação dos riscos

Avaliação dos riscos
A avaliação do risco consiste em confrontar seu nível com o limite de exposição estabelecido, visando verificar sua aceitabilidade. Esse limite indica o patamar de risco a partir do qual se recomenda a adoção de medidas de tratamento. Com a implementação dessas medidas, espera-se que o nível efetivo de risco seja reduzido para abaixo do limite de exposição definido, conforme a matriz abaixo: Figura 6: Matriz Simples de Risco e Tolerância ao Risco



Fonte: UK Orange Book (adaptação)

LIMITES DE EXPOSIÇÃO AO RISCO
Riscos acima do limite de exposição: faixa vermelha
Riscos com necessidade de monitoramento: faixa amarela
Riscos que podem ser aceitos: faixa verde

A avaliação dos riscos serve como apoio ao processo decisório, não sendo, por si só, determinante para a adoção de medidas de tratamento. Assim, compete ao gestor, diante da relação de riscos organizada conforme seu nível, definir quais deverão ser objeto de ações mitigadoras.

Subetapas
-Na matriz probabilidade x impacto, devem ser destacados os riscos que ultrapassam o limite de exposição definido (faixa vermelha), identificando-se, para cada um deles, as respectivas origens, causas e potenciais efeitos sobre a organização. -Para os riscos abaixo do referido limite, aqueles situados na faixa amarela requerem avaliação quanto à necessidade de monitoramento, enquanto os enquadrados na faixa verde podem ser aceitos sem a adoção de medidas adicionais.

Fonte: Adaptado do Manual de Gestão de Riscos do TCU.

Quadro 7: Tratamento dos riscos

Tratamento dos Riscos
O tratamento de riscos envolve o planejamento e a execução de ações voltadas a modificar seu nível, por meio de medidas de resposta que podem mitigar, transferir ou evitar os riscos priorizados. A definição dessas medidas deve ocorrer em oficinas de trabalho ou pelo próprio gestor do risco, com apoio de pessoas que conheçam o processo analisado. Utilizam-se técnicas como brainstorming, entrevistas, visitas técnicas e pesquisas para identificar o maior número possível de alternativas de resposta. As medidas devem buscar, preferencialmente, atuar sobre as causas do risco (reduzindo sua probabilidade) ou sobre suas consequências (minimizando os impactos), podendo combinar ambas as abordagens. Na decisão de implantação, devem ser considerados o custo-benefício, a abrangência e o grau de redução do risco obtido. Entre as ações mitigadoras possíveis estão o fortalecimento de controles, o redesenho de processos, a capacitação de pessoal, a melhoria de soluções de TI e a adequação da estrutura organizacional.

O registro das informações, preferencialmente por meio de técnicas como o método bow-tie, contribui para uma gestão mais eficaz ao relacionar causas, consequências e as medidas preventivas e atenuantes correspondentes.
Subetapas
-Para os riscos priorizados, devem ser identificadas suas causas e possíveis consequências; -Com base nessas informações, é necessário registrar as alternativas de resposta e avaliar sua viabilidade, considerando aspectos como custo-benefício, viabilidade técnica, tempestividade e eventuais efeitos colaterais; -Após a definição das medidas a serem executadas, deve-se elaborar o respectivo plano de implementação, assegurando sua integração aos planos institucionais.

Fonte: Adaptado do Manual de Gestão de Riscos do TCU.

Quadro 8: Acompanhamento

Acompanhamento
O monitoramento constitui etapa fundamental da gestão de riscos, voltada à identificação de alterações no ambiente interno e externo, atualização de critérios e priorizações, além da detecção de riscos emergentes. Também visa aprimorar a política, a estrutura e os processos de gestão, possibilitando o aprendizado a partir de eventos, tendências e resultados obtidos, e garantindo a eficácia e eficiência dos controles. Essas atividades devem possuir responsabilidades claramente definidas e observar a segregação de funções. Incluem: ● acompanhamento contínuo ou periódico dos riscos e de suas respostas, por meio de indicadores e análises de desempenho; ● autoavaliações de riscos e controles realizadas pelos gestores responsáveis; ● auditorias internas ou externas destinadas a verificar, de forma independente, a estrutura e a efetividade do processo de gestão de riscos. Os resultados dessas ações devem ser devidamente registrados e atualizados no registro de riscos institucional.

Fonte: Adaptado do Manual de Gestão de Riscos do TCU.

Quadro 9: Comunicação

Comunicação
A etapa de comunicação e consulta na gestão de riscos envolve a identificação das partes interessadas e o compartilhamento de informações pertinentes, respeitando a classificação de sigilo aplicável. Seu objetivo é assegurar que todos os envolvidos ou afetados pelos riscos conheçam as informações necessárias sobre sua natureza e tratamento, prevenindo sua materialização. O fluxo de comunicação deve ocorrer em dois sentidos: ● **Vertical**, garantindo que as unidades informem à alta administração os riscos identificados e que esta, por sua vez, divulgue aos servidores os principais riscos organizacionais;

- **Horizontal**, promovendo o intercâmbio de informações entre áreas que compartilham processos transversais, assegurando visão integrada e coordenação das ações de controle.

Fonte: Adaptado do Manual de Gestão de Riscos do TCU.

2.5 BOAS PRÁTICAS

Nesta seção serão elencadas boas práticas relacionadas ao objeto desta auditoria. Trata-se de ações, condutas, métodos ou procedimentos reconhecidamente eficazes no alcance dos objetivos na área de gestão de riscos e referenciados como exemplos para as mais diversas instituições.

2.5.1 Processo de gerenciamento de riscos na Universidade Federal do Amazonas e utilização do ForRisco como sistema de gerenciamento

A Universidade Federal do Amazonas (UFAM), por meio de sua Pró-Reitoria de Planejamento e Desenvolvimento Institucional, divulga em seu sítio institucional uma página específica para a Gestão de Riscos, contendo sua Política e seus Plano de Gestão de Riscos devidamente atualizados.

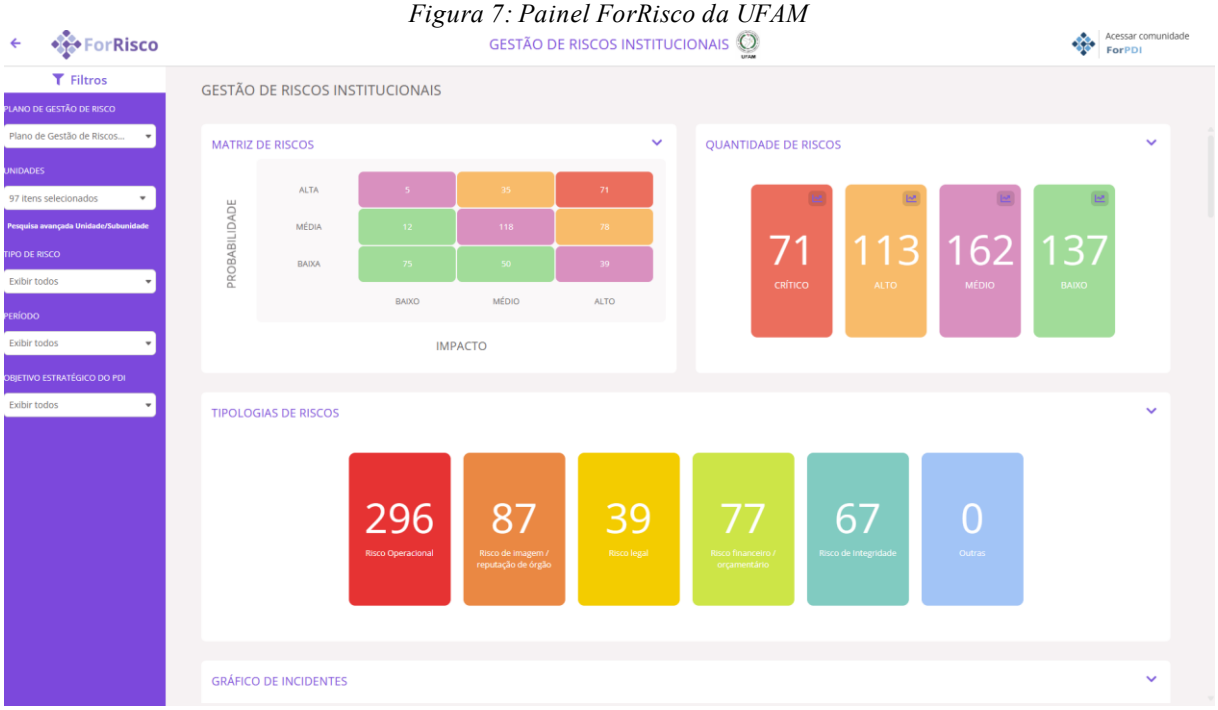
Para o gerenciamento do seu processo de Gestão de Riscos, a UFAM utiliza o ForRisco[1], uma plataforma de código aberto desenvolvida para o acompanhamento e gestão de riscos. Este sistema foi criado pela Universidade Federal de Alfenas (UNIFAL) com apoio de várias instituições, e, por ter seu código aberto, permite que equipes das instituições realizem o gerenciamento dos riscos, incluindo identificação, análise, planejamento, monitoramento e controle dos riscos, reduzindo ao mínimo os impactos negativos nos projetos, pessoas, meio ambiente e imagem da organização.

A UFAM foi uma das instituições pioneiras na implementação desta ferramenta para o gerenciamento de riscos, tendo sido premiada no 1º concurso de boas práticas do MEC na categoria "Fortalecimento da Gestão de Riscos e dos Controles Internos".

A intuitividade do sistema é um dos pontos fortes, possibilitando o acompanhamento e gerenciamento em tempo real do processo de gerenciamento de riscos da instituição, conforme se verifica na imagem abaixo.

[1] "A RNP apoia o Ministério da Educação (MEC) na disponibilização em nuvem da ferramenta tecnológica que auxilia na criação do Plano de Desenvolvimento Institucional e no Gerenciamento de Riscos das instituições da Rede Federal de Educação. Ela contempla um conjunto de soluções, também conhecidas como ForPDI, que uniformiza e otimiza tarefas administrativas, e a ForRisco, de gerenciamento de riscos. Ambas visam melhorar as práticas de planejamento estratégico e levam em conta questões específicas da Rede Federal de Educação e as legislações que a regem." Plataforma For - RNP

Figura 7: Painel ForRisco da UFAM



Fonte: Plataforma ForRisco UFAM, acesso em 15/10/2025.

O ForRisco é integrante da plataforma For, que integra também o ForPDI, voltado para o planejamento institucional, uma vez que, conforme discorrido neste relatório, a gestão de riscos deve estar alinhada ao planejamento estratégico institucional, possibilitando uma interlocução sistematizada entre essas atividades.

O ForRisco foi concebido para fomentar as boas práticas de gestão de riscos no setor público, com suporte de metodologia própria, material de capacitação e acessibilidade gratuita. Além disso, o sistema é utilizado para facilitar a tomada de decisão dos gestores e estruturar o uso eficiente dos recursos institucionais, sendo utilizada atualmente por 58 IFES, sendo 39 Universidades Federais e 19 Institutos Federais.

3 RECOMENDAÇÕES E PLANOS DE AÇÃO

Após as análises evidenciadas no presente relatório, sugere-se a implementação da seguinte recomendação:

Recomendação 3.1: Sob a coordenação do SITAI e ASDIT, que procedam a institucionalização do gerenciamento de riscos da UTFPR, com fulcro na Instrução Normativa Conjunta CGU nº 01/2016, bem como na Política de Governança, Integridade, Risco e Controle da UTFPR, ajustando-a conforme as necessidades e alinhamentos institucionais.

4 CONCLUSÃO

A auditoria permitiu concluir que a UTFPR ainda não formalizou um processo sistematizado de gerenciamento de riscos, em conformidade com as diretrizes da Instrução Normativa Conjunta CGU n.º 01/2016. Verificou-se, entretanto, que a instituição dispõe de condições favoráveis à sua institucionalização, destacando-se a existência de um Plano de Desenvolvimento Institucional e de um Planejamento Estratégico recentemente publicado, os quais apresentam missão, valores e objetivos estratégicos alinhados às suas finalidades regimentais e legais. Esses instrumentos constituem fundamentos adequados para a integração sistêmica da gestão de riscos aos processos de governança, planejamento e tomada de decisão da universidade.

A análise evidenciou que, embora a Política de Governança, Integridade, Risco e Controle da UTFPR forneça os elementos principais para a gestão de riscos, a ausência de definição clara da periodicidade para as etapas de identificação, avaliação, tratamento e monitoramento representa uma fragilidade relevante para a efetividade desse processo. Tal lacuna pode comprometer a atualização tempestiva das informações, ocasionar defasagens na execução dos planos de ação e reduzir a capacidade institucional de prevenção e resposta a eventos que possam afetar o alcance dos objetivos estratégicos.

Também se constatou que a ausência de elaboração da metodologia de gestão de riscos, prevista na Política de Governança, Integridade, Risco e Controle da UTFPR, configura fragilidade relevante no processo de gestão de riscos da instituição. A não atuação do Comitê e Subcomitê de Governança comprometeu a efetiva sistematização da gestão de riscos, em desconformidade com as diretrizes normativas da própria PGIRC. Dessa forma, faz-se necessária atuação assertiva da alta administração para promover o engajamento das instâncias de governança e garantir a institucionalização do processo, condição essencial para o fortalecimento da governança e o alcance dos objetivos estratégicos da universidade.

Por essa razão recomendou-se que a UTFPR promova revisão e aprimoramento de sua Política de Gestão de Riscos e da elaboração de um plano de ação para a elaboração da Metodologia de Gestão de Riscos, conforme consta no item 3 deste relatório, com vistas a explicitar a periodicidade das etapas do processo e a definir de forma detalhada as responsabilidades pelo monitoramento e pela análise crítica. Tal medida contribuirá não apenas para a conformidade normativa, mas principalmente para o fortalecimento do sistema de governança e de controles internos, assegurando maior integração entre a gestão de riscos, o planejamento estratégico e a consecução dos objetivos institucionais.

Vale acrescentar que a AUDIN, por força da lei, não realiza e não se responsabiliza pelos atos de gestão. As ações da AUDIN, que visam fortalecer os controles internos, não elidem, sobremaneira, a incessante responsabilidade de cada chefia em produzirem e executarem os seus próprios controles de gestão (Art. 17 do Decreto n.º 3.591/2000 e Art. 7º da IN Conjunta PR/CGU n.º 1/2016).

É o relatório.

Roberto Miyashiro Junior
Auditor

De acordo:

Tiago Hideki Niwa
Chefe da Auditoria Interna

ANEXOS

1.1 MANIFESTAÇÕES DA UNIDADE EXAMINADA

Conforme o Ofício n.º 3/2025-SITAI, documento SEI n.º 5318133, no processo SEI n.º 23064.051799/2025-10, a unidade auditada apresentou a seguinte manifestação:

> *Em respeito ao Relatório Preliminar de Auditoria 202501-01 (5293455), manifesto que após análise, não há crítica, alteração ou sugestão da parte desta Assessoria, a ser inserida no referido.*

1.2 ANÁLISE DA AUDITORIA INTERNA

Uma vez que a unidade auditada manifestou sua concordância com os termos do relatório preliminar e não apresentou propostas de alteração, procede-se à publicação do relatório definitivo.

1.3 CONTABILIZAÇÃO DE BENEFÍCIOS

A contabilização de benefícios financeiros e não financeiros é realizada conforme preconiza a IN CGU n.º 10/2020 CGU, que aprova a Sistemática de Quantificação e Registro dos Resultados e Benefícios da Atividade de Auditoria Interna Governamental do Poder Executivo Federal.

BENEFÍCIOS FINANCEIROS:	
Valor de Gastos Indevidos Evitados ou Receitas Obtidas:	-
Valores Recuperados:	-
Valor Total de Benefícios Financeiros:	**-**
BENEFÍCIOS NÃO FINANCEIROS:	
Missão, Visão e/ou Resultado - Repercussão Transversal	
Missão, Visão e/ou Resultado - Repercussão Estratégica	
Missão, Visão e/ou Resultado - Repercussão Tático/Operacional	
Pessoas, Infraestrutura e/ou Processos Internos - Repercussão Transversal	
Pessoas, Infraestrutura e/ou Processos Internos - Repercussão Estratégica	3.1
Pessoas, Infraestrutura e/ou Processos Internos - Repercussão Tático/Operacional	
Total dos Benefícios Não-Financeiros	**01**

Fonte: Audin.