MINISTÉRIO DA EDUCAÇÃO
FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO

Relatório de Auditoria nº 01/2022

Avaliação da maturidade da gestão baseada em riscos no Fundo Nacional de Desenvolvimento da Educação – FNDE

Brasília - DF, outubro de 2022

Missão

Aumentar e proteger o valor organizacional, com foco no fortalecimento da governança, do gerenciamento de riscos e dos controles.

Propósito

Oferecer serviços de avaliação e consultoria, de forma objetiva e independente, adicionando valor e melhorando as operações da organização para o alcance de seus objetivos.

Relatório de Auditoria – Avaliação

O Relatório de Auditoria é um dos produtos previsto nos fluxos de trabalho da Auditoria Interna do FNDE (Audit) e consiste na obtenção e na análise de evidências com o objetivo de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria. Objetiva também avaliar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos relativos ao objeto e à Unidade Auditada, e contribuir para o seu aprimoramento.

RESUMO

Trata-se de avaliação de maturidade da gestão baseada em riscos realizada no Fundo Nacional de Desenvolvimento da educação (FNDE). O presente Relatório teve como objetivo avaliar o grau de maturidade da *arquitetura de gestão de riscos*, considerando a conformidade dos princípios, das estruturas e dos processos colocados em prática na Autarquia em relação aos principais normativos e às boas práticas sobre o tema.

Nesse contexto, os exames concentraram-se em quatro dimensões (Ambiente, Processos, Parcerias e Resultados) e focaram na análise normativa, no exame documental e na análise de percepção da Alta Administração e dos servidores lotados no FNDE.

O trabalho de auditoria, previsto no Plano Anual de Auditoria (Paint) 2021 com prosseguimento no Paint 2022, foi iniciado a partir da relação dos temas prioritários a serem desenvolvidos pela Auditoria Interna (Audit) do FNDE – levantada a partir de mapeamento do universo auditável, com base em fatores de riscos –, bem como do alinhamento com as ações dos órgãos de controle interno e externo.

Assim, espera-se agregar valor aos processos de governança, gerenciamento de riscos e controles internos, contribuindo com subsídios para o processo de implementação, por parte da Alta Administração, de mecanismos e práticas de gestão baseada em riscos na organização.

Como resultados dos exames, verificou-se que a maturidade global do FNDE para a gestão de riscos é Inicial, apurada em 11,42%, considerando as capacidades existentes em termos de liderança, políticas, estratégias e preparo das pessoas para gestão de riscos; pelo emprego dessas capacidades aos processos e parcerias; e pelos resultados obtidos na melhoria do desempenho da Autarquia.

Dessa forma, conclui-se que os princípios, as estruturas e os processos necessários não foram adequadamente colocados em prática por toda a organização. Por isso, foram emitidas recomendações visando qualificar os elementos da arquitetura de gestão de riscos, para que estes possam funcionar de forma integrada aos processos de gestão para todas as áreas, as funções e as atividades relevantes para o alcance dos objetivos-chave do FNDE.

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
Agest	Assessoria de Gestão Estratégica e Governança da Presidência do FNDE
Audit	Auditoria Interna do FNDE
BSC	*Balanced Scorecard*
CD/FNDE	Conselho Deliberativo do FNDE
CGEG	Comitê de Gestão Estratégica e Governança
CGRCI	Comitê de Gestão de Riscos, Controles Internos e Integridade
CGU	Controladoria-Geral da União
Coaud	Coordenação de Auditoria
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
COSO-CI	*framework* COSO: Controle Interno
COSO-GRC	*framework* COSO: Gerenciamento de Riscos Corporativos
COSO-GRP-EP	*framework* COSO: Gerenciamento de Riscos Corporativos integrado com Estratégia e Performance
DIGAP	Diretoria de Gestão Articulação e Projetos Educacionais
DIGEF	Diretoria de Gestão de Fundos e Benefícios
DIRAD	Diretoria de Administração
DIRAE	Diretoria de Ações Educacionais
DIFIN	Diretoria Financeira
DIRTI	Diretoria de Tecnologia e Informação
e-Aud	Sistema de Gestão da Atividade de Auditoria Interna Governamental
FNDE	Fundo Nacional de Desenvolvimento da Educação
iGG	Índice Integrado de Governança Organizacional e Gestão Pública
IIA	*Institute of Internal Auditors*
IMD	Índice de Maturidade das Dimensões
IMG	Índice de Maturidade Global
IN	Instrução Normativa
IPPF	*International Professional Practices Framework*
ISO	*International Organization for Standardization*
MOT	Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal
NA	Normas de Atributo do IPPF

ND	Normas de Desempenho do IPPF
OCDE	Organização para a Cooperação e o Desenvolvimento Econômico
Paint	Plano Anual de Auditoria Interna
PDP	Plano de Desenvolvimento de Pessoas
PEI	Plano Estratégico Institucional
PGMQ	Programa de Gestão e Melhoria da Qualidade
PNDP	Política Nacional de Desenvolvimento de Pessoas
Raint	Relatório Anual de Auditoria Interna
SEI	Sistema Eletrônico de Informações
Sipec	Sistema de Pessoal Civil da Administração Pública Federal
TCU	Tribunal de Contas da União

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

O presente Relatório apresenta os resultados da avaliação de maturidade da gestão baseada em riscos, que teve como unidade auditada o Fundo Nacional de Desenvolvimento da Educação (FNDE). Assim, foram envolvidas as seguintes áreas da organização: Presidência do FNDE, Diretoria de Administração (DIRAD), Diretoria de Tecnologia e Informação (DIRTI), Diretoria Financeira (DIFIN), Diretoria de Ações Educacionais (DIRAE), Diretoria de Gestão Articulação e Projetos Educacionais (DIGAP), Diretoria de Gestão de Fundos e Benefícios (DIGEF) e a própria Auditoria Interna (Audit).

Com base em modelo de avaliação desenvolvido pelo Tribunal de Contas da União (TCU)[1], a maturidade em gestão de riscos do FNDE foi avaliada em relação a quatro objetos, traduzidos em *Dimensões*, com foco nos processos estratégicos e nas práticas disseminadas pela organização. Tais dimensões, podem ser resumidas da seguinte forma[2]:

a) **Ambiente**: capacidades existentes na organização em termos de liderança, políticas, estratégias e preparo das pessoas;
b) **Processos**: processos de gestão de riscos adotados pela gestão, notadamente quanto a identificação, análise e avaliação de riscos; seleção e implementação de respostas aos riscos avaliados; monitoramento; controles; e comunicação;
c) **Parcerias**: gestão de riscos no âmbito de políticas de gestão compartilhadas, quando o alcance de objetivos comuns envolve outras organizações públicas ou privadas; e
d) **Resultados**: eficácia e eficiência das práticas de gestão de riscos no alcance de objetivos, qualidade dos bens e serviços ofertados, transparência, prestação de contas e conformidade.

O escopo do trabalho abrangeu a *arquitetura de gestão de riscos* colocada em prática no FNDE, considerando-se as seguintes vertentes de análise:

a) **Princípios**: conjunto compartilhado de valores, comportamentos e práticas que caracterizam como a entidade aborda o risco;
b) **Estrutura**: conjunto de componentes e arranjos organizacionais para a concepção, a implementação, o monitoramento, a análise crítica e a melhoria contínua da gestão de riscos; e
c) **Processos**: atividades de identificação, análise e avaliação de riscos; seleção e implementação de respostas aos riscos avaliados; monitoramento de riscos e controles; e comunicação sobre riscos.

As atividades foram executadas em estrita observância às normas de auditoria aplicáveis, especialmente em relação à Instrução Normativa nº 03, de 09 de junho de 2017 (Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal), e ao Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo federal (MOT), ambos da Controladoria-Geral da União (CGU). Também foram observadas as

[1] Considerando a complexidade das operações desenvolvidas no FNDE, bem como o grande volume de processos e atividades em curso na organização, optou-se pelo emprego de um modelo referencial para embasar a avaliação. Assim, utilizou-se o guia "Gestão de Riscos – Avaliação da Maturidade", do Tribunal de Contas da União (TCU, 2018a), que tem por objetivo apoiar a avaliação da maturidade da gestão de riscos nas organizações públicas, bem como identificar aspectos que necessitam ser aperfeiçoados para melhorar a entrega de produtos e serviços à sociedade.
[2] Adaptado de "Gestão de Riscos – Avaliação da Maturidade" (TCU, 2018a).

recomendações constantes da Declaração de Posicionamento do Instituto de Auditores Internos: O papel da auditoria interna no gerenciamento de riscos corporativos (IIA, 2009).

Ademais, além da Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016, que trata sobre gestão de riscos e cujas regras balizaram todo o trabalho desenvolvido, foram utilizados os seguintes *frameworks*:

a) **COSO-CI**: Controle Interno – Estrutura Integrada (COSO, 2013);
b) **COSO-GRC**: Gerenciamento de Riscos Corporativos – Estrutura Integrada (COSO, 2007);
c) **COSO-GRC-EP**: Gerenciamento de Riscos Corporativos Integrado com Estratégia e Performance (COSO, 2017);
d) **ISO 31000:2018**: ABNT NBR ISO 31000:2018 – Gestão de Riscos: Diretrizes (ABNT, 2018); e
e) **Orange Book**: *The Orange Book – Management of Risk – Principles and Concepts* (UK, 2020).

Tais referenciais, amplamente reconhecidos internacionalmente, podem ser adotados e personalizados pelas organizações, inclusive na esfera pública, para amparar a implementação e o aprimoramento da gestão de riscos. Por isso, seus conceitos, princípios e diretrizes foram utilizados também como critérios para a avaliação realizada.

Destaca-se que o presente trabalho foi executado a partir de ação prevista no Plano Anual de Auditoria Interna – Paint/2022, em conformidade com o objetivo estratégico "Fortalecer os controles internos e a gestão de riscos" definido no Plano Estratégico do FNDE 2018-2022 e em alinhamento ao Planejamento Operacional da Audit.

Nesse contexto, a avaliação de maturidade executada teve como objetivo contribuir com subsídios para o processo de implementação, por parte da Alta Administração, de mecanismos e práticas de gestão baseada em riscos no FNDE. Vislumbra-se, ainda, que os resultados dessa avaliação tendem a contribuir para a melhoria dos processos de governança, gerenciamento de riscos e controles internos da Autarquia.

Para atingimento do objetivo definido, foram formuladas as seguintes *questões de auditoria*, refletindo as quatro dimensões avaliadas:

1. Dimensão Ambiente:

    1.1. Liderança: Em que medida os responsáveis pela governança e a Alta Administração do FNDE exercem suas responsabilidades de governança de riscos e cultura?

    1.2. Políticas e estratégias: Em que medida o FNDE dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática?

    1.3. Pessoas: Em que medida as pessoas que atuam no FNDE entendem seus papéis e responsabilidades relacionados à gestão de riscos e estão preparadas exercê-los?

2. Dimensão Processos:

    2.1. Identificação e análise de riscos: Em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente a todas as operações, funções e atividades relevantes do FNDE (unidades, processos e atividades que são críticos para a realização dos objetivos-chave da organização)?

2.2. Avaliação e resposta a riscos: Em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente aos riscos identificados e analisados como significativos?

2.3. Monitoramento e Comunicação: Em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente no FNDE?

3. Dimensão Parcerias:

3.1. Gestão de riscos em parcerias: Em que medida o FNDE estabelece arranjos com clareza para assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento no âmbito das parcerias?

3.2. Planos e medidas de contingência: Em que medida são estabelecidos planos ou medidas de contingência para garantir a recuperação e a continuidade dos serviços no âmbito das parecerias realizadas?

4. Dimensão Resultados:

4.1. Melhoria dos processos de governança e gestão: Em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão do FNDE?

4.2. Resultados-chave da gestão de riscos: Em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos do FNDE?

Ainda, conforme detalhado no Anexo III deste documento, houve o desdobramento em *subquestões de auditoria* e em *objetos de análise*, construindo-se, assim, a base para aplicação dos testes de auditoria.

Os testes de auditoria foram executados de dezembro/2021 a junho/2022, por intermédio de análise normativa e de exame documental dos processos relacionados ao objeto auditado. Ainda, foi utilizada técnica de pesquisa para auditorias, com o envio de questionário à Alta Administração e aos servidores do FNDE, no intuito de coletar sua percepção acerca dos aspectos avaliados.

A metodologia utilizada para o presente trabalho foi baseada no guia "Gestão de Riscos – Avaliação da Maturidade" (TCU, 2018a), estando detalhada no Anexo II do presente Relatório. Destaca-se que, para a adequada leitura dos resultados apresentados a seguir, é importante conhecer preliminarmente as escalas de avaliação adotadas:

a) para os índices de maturidade global e das dimensões, bem como para a avaliação dos seus respectivos componentes (questões de auditoria), a escala sugerida pelo TCU varia entre **Inicial, Básico, Intermediário, Aprimorado e Avançado**, adotando-se níveis de 0 a 100% para apurar a arquitetura de gestão de riscos presente na organização e em cada dimensão avaliada; e

b) para avaliação das evidências de auditoria obtidas e, consequentemente, para avaliação dos objetos de análise selecionados, a escala adotada varia entre **Inexistente, Inicial, Básico, Aprimorado e Avançado**, com pontos atribuídos entre 0 e 4.

VISÃO GERAL DO OBJETO AUDITADO

De acordo com o Decreto nº 9.203, de 22 de novembro de 2017, considera-se "valor público":

> *Produtos e resultados gerados, preservados ou entregues pelas atividades de uma organização que representem respostas efetivas e úteis às necessidades ou às demandas de interesse público e modifiquem aspectos do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos.*

Na esfera pública, os órgãos e entidades existem para gerar valor público às partes interessadas e todas as organizações enfrentam incertezas que podem vir a afetar seus objetivos, produtos ou resultados finalísticos, impedindo o fornecimento adequado de bens públicos e a prestação eficaz de serviços públicos.

O efeito dessas incertezas caracteriza o *risco*, definido como a possibilidade de que um evento ocorra e afete a realização dos objetivos das organizações, impactando nos resultados pretendidos. Assim, o desafio dos administradores é determinar até que ponto aceitar essas incertezas, além de compreender como elas podem interferir no esforço para gerar valor às partes interessadas.

Nesse contexto, o propósito da gestão de riscos é auxiliar a criação e a proteção de valor e sua função primordial é assegurar o alcance dos objetivos, por meio da identificação antecipada dos possíveis eventos que poderiam ameaçar o atingimento dos objetivos, como: o cumprimento de prazos estabelecidos em leis e regulamentos, a execução de uma política pública ou a prestação de um serviço público.

As melhores práticas internacionais de gestão recomendam a adoção de sistemas de gerenciamento de riscos associados aos processos de planejamento, de tomada de decisão e de execução dos trabalhos relevantes, de modo a garantir que as finalidades públicas sejam alcançadas de fato, com a melhor relação custo-benefício.

Por isso, a Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016[3], estabeleceu a obrigatoriedade de os órgãos e entidades do Poder Executivo federal implementarem, manterem, monitorarem e revisarem o processo de gestão de riscos, de forma compatível com sua missão e seus objetivos estratégicos.

Para o presente trabalho, conceitua-se *gestão de riscos* como o processo estruturado, consistente e contínuo, conduzido por todos os integrantes de uma organização, por intermédio de atividades coordenadas para identificar, analisar, avaliar, tratar, monitorar e comunicar riscos, e que tem por objetivo conferir segurança razoável quanto ao alcance dos objetivos estabelecidos, melhorar o desempenho e encorajar a inovação. Enquanto *gerenciamento de riscos* refere-se às atividades aplicadas no âmbito do processo de gestão de riscos.

Ressalta-se também a diferenciação entre os papéis da Auditoria Interna e da Alta Administração nesse processo. A Alta Administração é a principal responsável por estabelecer, manter, monitorar e aprimorar o 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

[3] Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional.

Já a auditoria interna é uma atividade independente, desenhada para adicionar valor e melhorar as operações de uma organização. Seu papel é, a partir de uma abordagem sistemática e disciplinada, avaliar e melhorar a eficácia dos processos de governança, gestão de riscos e controles internos. É possível, ainda, o fornecimento de serviços de consultoria com o objetivo de aprimorar tais processos de uma organização.

Nesse contexto, o trabalho realizado buscou avaliar o FNDE a partir de abordagem relacionada à maturidade da gestão de riscos. Destaca-se que a literatura de referência mostra que modelos de avaliação de maturidade auxiliam as organizações que desejam implementar processos formais de gestão de riscos ou aprimorar os processos já existentes (HILLSON, 1997). Isto porque, ao conhecerem o seu nível presente de maturidade, as organizações são capazes de identificar metas realistas para melhoria e de desenvolver planos de ação para aprimorarem suas capacidades de gestão de riscos (*idem, ibidem*).

Assim, o presente relatório apresenta os resultados da avaliação de maturidade realizada pela Auditoria Interna do FNDE e está estruturado da seguinte forma: o capítulo denominado Resultados dos Exames, apresenta os resultados dos testes de auditoria executados, consolidados a partir do *Índice de Maturidade Global* da gestão de riscos da organização e dos *Índices de Maturidade de cada Dimensão* (Ambiente, Processos, Parcerias e Resultados); já os tópicos de 1 a 4 apresentam as conclusões obtidas em cada dimensão avaliada, com as respostas às questões e às subquestões de auditoria efetuadas, bem como com os pontos referentes a cada *componente* e às conclusões de cada *aspecto*. Ademais, apresenta-se, de forma individualizada, a pontuação obtida para cada *objeto* avaliado, bem como os principais critérios de referência utilizados; ao final, são apresentadas as recomendações de auditoria para aprimoramento dos processos; por fim, os Anexos II e III do presente relatório apresentam, respectivamente, a metodologia adotada e uma síntese dos índices de maturidade apurados.

RESULTADOS DOS EXAMES – ÍNDICES DE MATURIDADE

A. ÍNDICE DE MATURIDADE GLOBAL (IMG)

Considerando a metodologia adotada para o presente trabalho, o Índice de Maturidade Global (IMG) da gestão de riscos no âmbito do FNDE foi calculado a partir da média ponderada dos índices de maturidade das dimensões Ambiente, Processos, Parcerias e Resultados, cujos pesos adotados foram, respectivamente, 40, 30, 10 e 20.

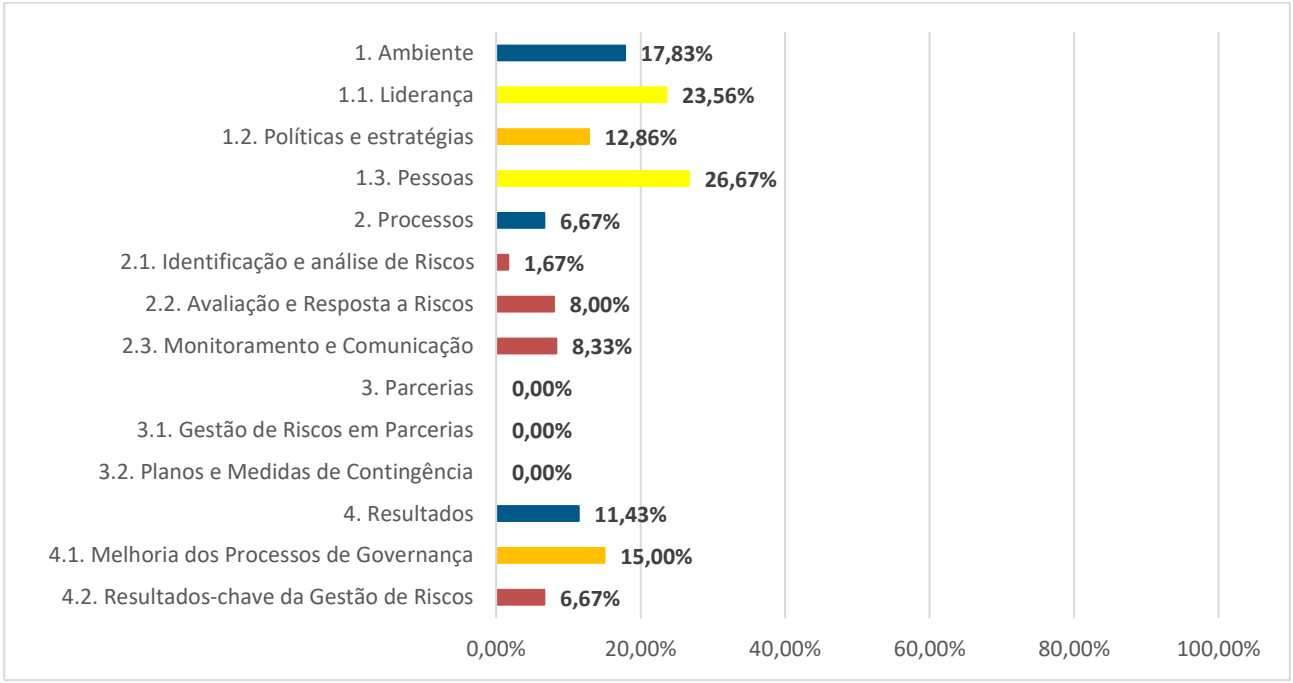
Conforme disposto no guia "Gestão de Riscos – Avaliação da Maturidade" (TCU, 2018a, p. 53):

> *O modelo tem como premissas que a maturidade da gestão de riscos de uma organização é determinada pelas capacidades existentes em termos de liderança, políticas e estratégias, e de preparo das pessoas para gestão de riscos, bem como pelo emprego dessas capacidades aos processos e parcerias e pelos resultados obtidos na melhoria do desempenho da organização no cumprimento de sua missão institucional de gerar valor para as partes interessadas com eficiência e eficácia, transparência e 'accountability', e conformidade com leis e regulamentos.*

Nesse contexto, a avaliação realizada pela Auditoria Interna do FNDE apurou um Índice de Maturidade Global de **11,42%**. Conforme a escala de avaliação detalhada no Quadro 1 do Anexo II – Metodologia, isso significa dizer que a Autarquia está no primeiro nível de maturidade da gestão de riscos: **INICIAL**.

O gráfico a seguir apresenta os índices de maturidade apurados por dimensão, detalhados a partir de seus componentes:

Gráfico 1: Índice de Maturidade em Gestão de Riscos – FNDE



Fonte: elaboração própria.

Para melhor compreensão do Índice de Maturidade Global da organização, é preciso adentrar no índice de maturidade de cada dimensão. Desse modo, é possível visualizar o grau de desenvolvimento de cada um dos aspectos que compõem a arquitetura da gestão de riscos, identificando pontos ainda não implementados, pontos já desenvolvidos, boas práticas adotadas e eventuais melhorias e ajustes necessários.

B. ÍNDICE DE MATURIDADE DAS DIMENSÕES (IMD)

1. DIMENSÃO AMBIENTE

Segundo a IN nº 01/2016, o Ambiente Interno para o desenvolvimento da gestão de riscos inclui elementos como: integridade; valores éticos; competências das pessoas; maneira pela qual a gestão delega autoridade e responsabilidades; estrutura de governança organizacional e políticas e práticas de recursos humanos. A norma esclarece, ainda, que "o ambiente interno é a base para todos os outros componentes da estrutura de gestão de riscos, provendo disciplina e prontidão para a gestão de riscos".

O COSO-CI (Estrutura e Anexos) esclarece que o ambiente é influenciado tanto por fatores internos, quanto por fatores externos, sendo esperado de uma organização que estabelece e mantém um sólido ambiente de controle:

> *[...] comportamento coerente com o compromisso existente em relação à integridade e os valores éticos; processos e estruturas adequadas de supervisão, um desenho organizacional que permite realizar os objetivos da entidade com a atribuição adequada de autoridade e responsabilidades, um alto grau de competência e um forte senso de responsabilidade em relação à realização dos objetivos (COSO, 2013b, p. 39).*

Percebe-se, portanto, que o ambiente "dá o tom" de como os riscos e controles serão vistos e abordados por uma organização e pelas pessoas que nela atuam. De acordo com o COSO-GRC:

> *Esse ambiente influencia o modo pelo qual as estratégias e os objetivos são estabelecidos, os negócios são estruturados, e os riscos são identificados, avaliados e geridos. Este influencia o desenho e o funcionamento das atividades de controle, dos sistemas de informação e comunicação, bem como das atividades de monitoramento (COSO, 2007, p. 27).*

Por isso, o ambiente de uma organização deve fornecer a base para uma *filosofia de gestão de riscos*[4], ou seja, para um conjunto de convicções e atitudes compartilhadas que caracterizam a forma pela qual a organização considera o risco em tudo o que faz: do desenvolvimento da estratégia às atividades operacionais.

Ainda em relação à importância do adequado estabelecimento do ambiente para a gestão de riscos, o COSO-GRC (COSO, 2007, p. 35) destaca que "o impacto de um ambiente interno ineficaz pode ir muito longe e talvez provocar prejuízos financeiros, desgastes da imagem pública ou, até mesmo, o fracasso".

[4] Conforme estabelecido no COSO-GRC (2007).

Nesse contexto, o objetivo desta dimensão foi avaliar as capacidades existentes no FNDE, em termos de *liderança, políticas, estratégias e preparo das pessoas*, incluindo aspectos relacionados com a cultura, a governança de riscos e a consideração do risco na definição da estratégia e dos objetivos em todos os níveis, procurando dimensionar em que medida a Autarquia detém as condições necessárias para prosperar e fornecer segurança razoável do cumprimento de sua missão institucional para geração de valor às partes interessadas.

Da avaliação realizada, verificou-se que o FNDE ainda não assume um compromisso suficientemente forte e sustentado com a cultura e o desenvolvimento de estruturas para a gestão baseada em riscos. Isso porque há fragilidades relacionadas aos mecanismos de gestão de pessoas, transparência, integridade e gestão da ética; não foram instituídas ou não funcionam adequadamente as instâncias e estruturas para gestão de riscos; e há fragilidades nos mecanismos de articulação entre os níveis estratégico, tático e operacional. Ademais, não foi instituída uma Política de Gestão de Riscos ou outro mecanismo de comprometimento das lideranças e de direcionamento para as pessoas que atuam na organização.

Consequentemente, uma consciência sobre riscos, objetivos, resultados, papéis e responsabilidades não está disseminada por todos os níveis da organização; há iniciativas esparsas e incipientes de gestão de riscos que não se encontram respaldadas em política institucional e que não cumprem um fluxo de comunicação em todos os sentidos; não há como assegurar que a gestão de riscos seja integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, as funções e as atividades relevantes para o alcance dos objetivos-chave da organização; e os responsáveis pela governança, a administração e as pessoas responsáveis em todos os níveis não têm um entendimento atual, correto e abrangente dos objetivos sob a sua gestão, de seus papéis e responsabilidades para atingimento dos resultados de cada área ou pessoa para atingir os objetivos-chave que envolvem riscos, bem como para atingir o nível de maturidade almejado para a gestão de riscos.

Adicionalmente, destaca-se que não foram identificadas políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática, de maneira formal e integrada por toda a organização. As principais causas para essa fragilidade decorrem da ausência um processo estabelecido para a gestão de riscos na Autarquia, da ausência de recursos alocados especificamente para atuar na gestão de riscos e da ausência de integração da gestão de riscos ao planejamento estratégico. Logo, não há garantia proporcionada pela gestão de riscos de que:

a) os objetivos estratégicos estão sendo alcançados na realização da missão e dos objetivos-chaves da organização;

b) os objetivos operacionais de eficiência e eficácia das operações, de qualidade de bens e serviços estão sendo alcançados;

c) a comunicação (interna e externa, em todos os níveis, *top-down* e *bottom-up*) de informações por meio de relatórios, de mecanismos de transparência e prestação de contas está sendo feita de forma confiável; e

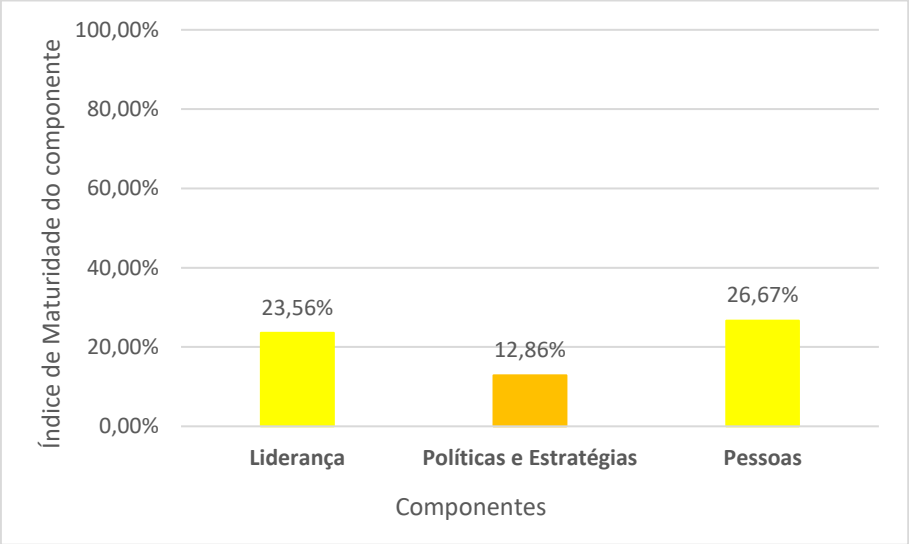
d) as leis e os regulamentos aplicáveis estão sendo cumpridos.

Ainda, como consequência da ausência de políticas e estratégias, destaca-se que há prejuízo à tomada de decisão, de modo que não é possível acompanhar se os programas, os projetos e as atividades estão sendo executados dentro das tolerâncias a risco da organização (ou das variações aceitáveis no desempenho), alinhadas aos objetivos estratégicos e ao apetite a risco.

Por fim, em que pese existirem algumas pessoas informadas e até mesmo habilitadas para exercerem papéis relacionados à gestão de riscos, não foi possível concluir que todos os integrantes da organização são capazes de reconhecer suas responsabilidades no gerenciamento de riscos e controles, não estando, ainda, adequadamente preparados para exercer essas responsabilidades. Tendo em vista que não foi estabelecido um processo para a gestão de riscos, que não foram alocados recursos para tanto e que não há mecanismos que traduzam o modelo de governança da organização, não há adequada distribuição de papéis e responsabilidades no âmbito das três linhas. Como consequência principal, uma consciência sobre riscos, objetivos, resultados, papéis e responsabilidades não é disseminada por todos os níveis da organização; há maior exposição a riscos, inclusive de integridade e ética; e há falhas no tratamento de eventos prejudiciais aos objetivos da organização.

Assim, o índice de maturidade obtido na dimensão Ambiente foi de **17,83%**, o que significa uma maturidade **INICIAL** do ambiente para desenvolvimento da gestão de riscos. O gráfico a seguir apresenta o Índice de Maturidade para cada um dos componentes relacionados à dimensão:

Gráfico 2: Índice de Maturidade por Componente – Dimensão Ambiente



Fonte: elaboração própria.

Do gráfico 2, percebe-se que, apesar de os componentes Liderança e Pessoas terem apresentado um grau básico de maturidade, o componente Políticas e Estratégias (por ter maior peso dado o número de subquestões que o compõem) tendeu o índice da dimensão para baixo[5].

Nos parágrafos a seguir, estão descritos os achados relativos a cada um dos três componentes avaliados na dimensão Ambiente (Liderança; Políticas e estratégias; e Pessoas).

[5] Para as subquestões que se desdobraram em mais de um objeto de análise, a pontuação do aspecto foi calculada a partir da média das pontuações obtidas em cada objeto que compõe o aspecto, conforme apresentado na Metodologia (Anexo II do presente Relatório).

1.1. Liderança

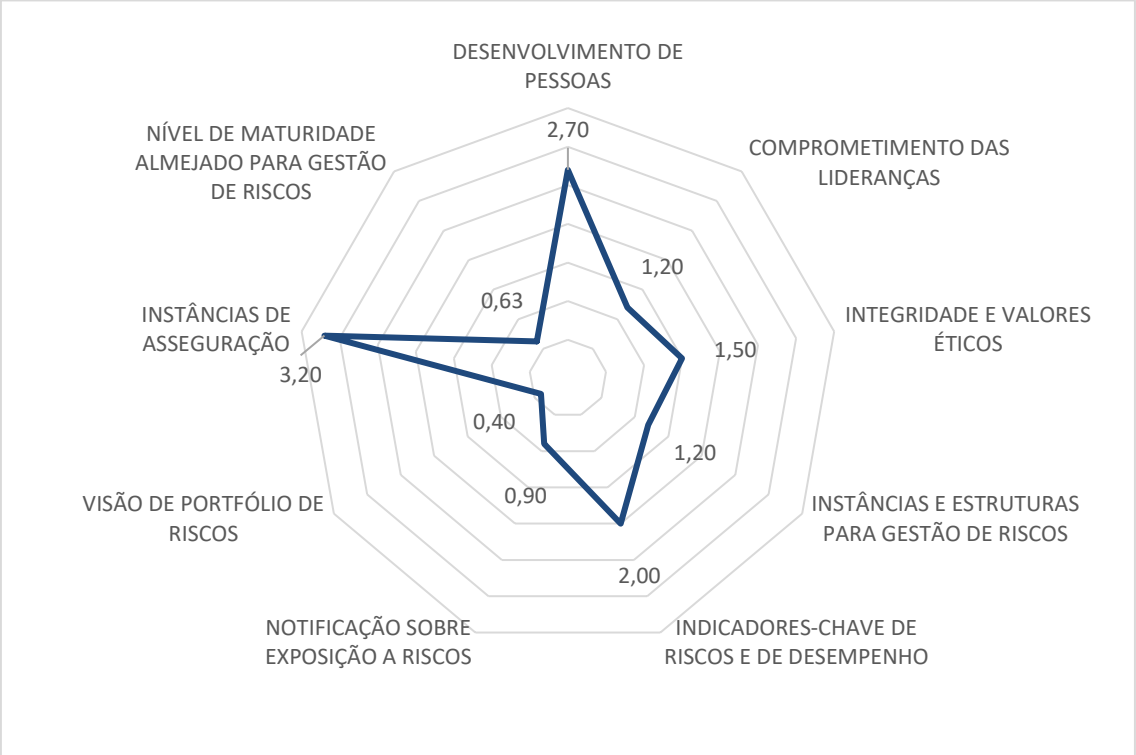
Nesse componente, apurou-se a seguinte questão: em que medida os responsáveis pela governança e a Alta Administração do FNDE exercem suas responsabilidades de governança de riscos e cultura?

Buscou-se, para tanto, avaliar se a Alta Administração do FNDE assume um compromisso forte e sustentado e se exerce supervisão adequada para obter comprometimento com a gestão de riscos em todos os níveis da Autarquia, a partir de três aspectos: 1.1.1 Cultura; 1.1.2. Governança de riscos; e 1.1.3. Supervisão da governança e da Alta Administração.

No FNDE, o resultado do componente "Liderança", a partir da avaliação dos seus aspectos, demonstrou uma maturidade **BÁSICA**, apurada em **23,56%**.

O gráfico a seguir apresenta o resultado consolidado do componente, a partir dos resultados apurados dos objetos analisados:

Gráfico 3: Resultado da avaliação dos objetos – Componente Liderança



Fonte: elaboração própria.

A partir do gráfico 3, podem ser identificadas as áreas que precisam de maior atenção. A maior parte dos objetos desse componente foram avaliados como "inexistente" ou "inicial". No entanto, destacam-se os temas *desenvolvimento de pessoas* e *instâncias de asseguração*, que obtiveram, respectivamente, classificações "básico" e "aprimorado", indicando processos mais bem estruturados e aderentes aos critérios relevantes.

A seguir apresentam-se os aspectos avaliados no componente Liderança, bem como os objetos relacionados a cada aspecto.

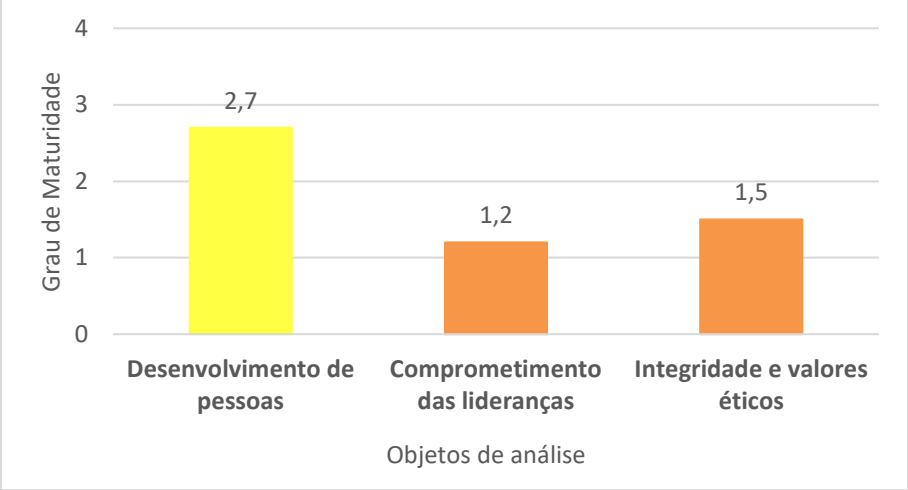
1.1.1. Cultura

A Alta Administração e os responsáveis pela governança reconhecem a importância da cultura, da integridade, dos valores éticos e da consciência de riscos como aspectos-chave para o reforço da *accountability*?

Com vistas a avaliar este aspecto, foram previstos testes relacionados a três objetos de análise: 1.1.1.1. Desenvolvimento de pessoas, 1.1.1.2. Comprometimento das lideranças e 1.1.1.3. Integridade e valores éticos.

A avaliação realizada mostrou que, em que pese a Alta Administração reconhecer a importância da integridade, dos valores éticos e da consciência de riscos, por intermédio do fornecimento de normas e orientação, estes pontos-chave apresentam fragilidades que impactam o adequado comprometimento com a cultura de gestão baseada em riscos.

Gráfico 4: Resultado da avaliação dos objetos – Aspecto Cultura



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir dos objetos de análise selecionados:

1.1.1.1. Desenvolvimento de pessoas

Buscando avaliar se o FNDE fornece normas e orientações sobre desenvolvimento de pessoas, bem como se foram instituídos mecanismos para apoiar as ações de desenvolvimento, procedeu-se a análise dos principais normativos que regulamentam as ações de gestão de pessoas publicados no âmbito da Autarquia, bem como a análise dos mecanismos instituídos. Além disso, coletou-se a percepção dos servidores e da Alta Gestão sobre o tema.

As boas práticas relacionadas ao tema gestão de riscos destacam alguns princípios que se aplicam à temática desenvolvimento de pessoas. Nesse sentido: as organizações devem demonstrar compromisso com a competência, atraindo, desenvolvendo e retendo talentos competentes e em alinhamento com seus objetivos e sua estratégia (COSO-CI, 2013; e COSO-GRC-EP, 2017); a

competência das pessoas que atuam na organização deve refletir o conhecimento e as habilidades necessárias para a execução das tarefas designadas (COSO-GRC, 2007); e as normas que tratam de gestão de pessoas devem conduzir os níveis previstos de integridade, comportamento ético e competência (COSO-GRC, 2007).

Portanto, a existência de diretrizes associadas à gestão e ao desenvolvimento de pessoas é um dos aspectos-chave para que uma organização alcance seus objetivos e desenvolva uma cultura de gestão de riscos, pois fatores humanos "influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio" (ISO 31000:2018).

Nesse contexto, a equipe de auditoria avaliou a existência e o funcionamento de ações relacionadas ao desenvolvimento de pessoas, especialmente a partir da estruturação de uma Política de Capacitação e Desenvolvimento no âmbito do FNDE. Para tanto, consideraram-se principalmente os critérios e procedimentos do Decreto nº 9.991/2019 e da IN SGP-ENAP/SEDGG/ME nº 21, de 1º de fevereiro de 2021, que tratam da Política Nacional de Desenvolvimento de Pessoas – PNDP, a ser observada pelos órgãos integrantes do Sistema de Pessoal Civil da Administração Pública Federal (Sipec).

As análises realizadas demonstraram que o FNDE:

- estabeleceu formalmente sua política de desenvolvimento de pessoas (Portaria FNDE nº 411, de 03 de julho de 2020);
- estabeleceu formalmente critérios e procedimentos para a concessão de incentivos educacionais (Portaria FNDE nº 439, de 21 de julho de 2020);
- publica, anualmente, Plano de Desenvolvimento de Pessoas – PDP, com ações previstas para todas as Diretoria e unidades equivalentes, bem como acompanha a execução a partir de revisões periódicas (bimestrais);
- dispõe de um fluxo padronizado para levantamento das necessidades de capacitação, com a participação de representantes de todas as unidades dirigentes e coordenação da Coordenação-Geral de Gestão de Pessoas e Organizações – CGPEO, bem como busca orientar seus servidores por intermédio do "Guia de Ações de Desenvolvimento de Pessoas do FNDE";
- possui ações para estímulo à participação em capacitações, com divulgação periódica de cursos disponibilizados pelas escolas de governo, de acordo com as necessidades listadas no PDP; e
- adotou metodologia do Sipec para organização das necessidades de desenvolvimento, havendo, portanto, diretriz para alinhamento das capacitações a objetivos pré-definidos.

Dentre as fragilidades encontradas nesse objeto de análise, observou-se que na prática nem todos os objetivos estratégicos do Plano Estratégico Institucional (PEI-FNDE 2018-2022) tiveram a execução de ações de desenvolvimento relacionadas durante o exercício de 2021. Assim, do rol de capacitações listado no PDP, não foram encontradas ações de desenvolvimento diretamente relacionadas aos objetivos estratégicos "Financiamento estudantil" e "Incentivar a gestão socioambiental".

Observou-se, ainda, a partir do rol de capacitações listado nos PDP 2020 e 2021, baixa realização de cursos relacionados às temáticas integridade, ética e gestão de riscos. Assim, a equipe de auditoria identificou que, no exercício de 2020, não foram executadas capacitações nos temas "integridade" e "ética", mas foram executados cursos que têm relação com o tema "gestão de riscos". Já em 2021, novamente não foram realizados cursos no tema "integridade", tendo havido realização de cursos no tema "ética" e no tema "gestão de risco" em algumas unidades.

Outro ponto de fragilidade identificado e que tem potencial de impactar o funcionamento das práticas relacionadas ao desenvolvimento de pessoas está relacionado à ausência de um mecanismo de mapeamento para definir os níveis de competência necessários para a ocupação dos postos de trabalho, conforme relatado pela própria organização. Atualmente, as competências a serem desenvolvidas são definidas pelas lideranças das unidades do FNDE e registradas em sistema, mas sem uma diretriz que guie esse processo.

Consequentemente, dado que não há conhecimento prévio das competências que precisam ser desenvolvidas, prejudica-se o alcance dos objetivos das unidades e da organização como um todo, podendo haver o não alinhamento entre a previsão de necessidades a serem desenvolvidas e as ações de desenvolvimento efetivamente executadas e, ainda, o não alinhamento entre conhecimentos, habilidades e competências dos servidores com os postos de trabalho ocupados. Essa fragilidade pode prejudicar, por exemplo, o adequado levantamento de necessidades de capacitação para compor o rol do PDP e até mesmo a disseminação de capacitações direcionadas ao perfil de cada servidor.

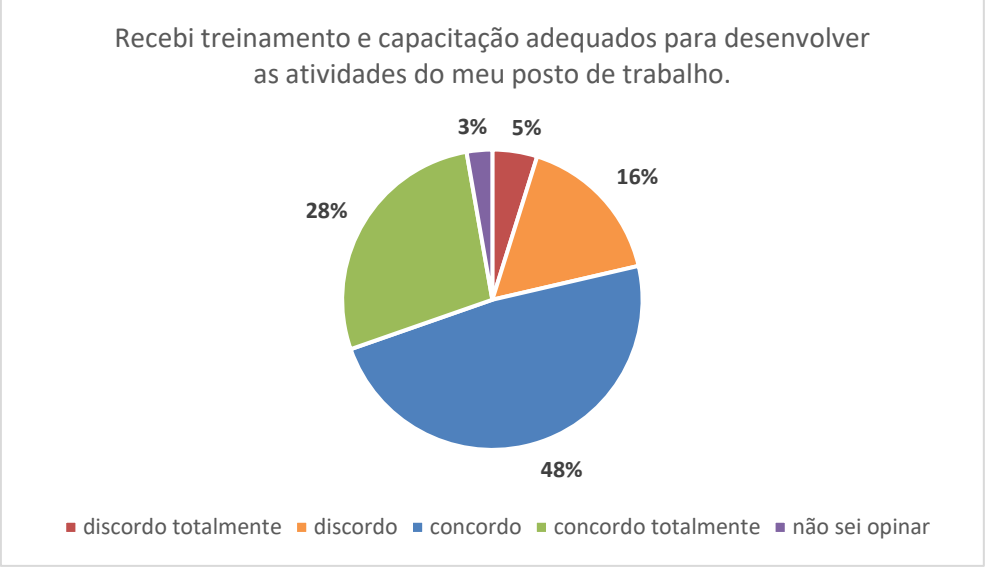
Nessa temática, a organização auditada informou que há intenção de proceder o dimensionamento da força de trabalho e que já foi firmada parceria com o Ministério da Economia e com a Universidade de Brasília com vistas a implementação do "Projeto Dimensionamento da Força de Trabalho" (DFT), atualmente desenvolvido como projeto-piloto na CGPEO (Coordenação-Geral de Gestão de Pessoas e Organizações) e na CGAME (Coordenação-Geral de Apoio à Manutenção Escolar) e com previsão de implantação da metodologia para todo o FNDE a partir de 2022.

Também foi observada a ausência de mecanismos expressivos para atrair e reter talentos. Levantamento datado de abril/2022, a partir do Sistema de Gestão por Competência (SGC), mostrou que o FNDE tem 79 servidores cedidos, o que representa 18,5% da sua força de trabalho. Dado que a organização já adota algumas boas práticas relacionadas ao tema (como Política de Desenvolvimento de Pessoas, Programa de Gestão de Competências e Programa de Qualidade de Vida, por exemplo), entende-se que estas podem ser formalizadas em políticas e mecanismos específicos para atração e retenção talentos. Outro ponto de melhoria, seria o planejamento e a preparação para a sucessão, por intermédio de planos de contingência para os responsáveis por atividades importantes, garantindo a continuidade das atividades no caso de vacância dos postos de trabalho.

Por fim, um ponto relevante a ser considerado, sendo caracterizado por sua desconformidade com o disposto pelo art. 5º, § 1º, inciso II, da Lei nº 13.346/2016, é o fato de que não há uma Política de Desenvolvimento da Alta Administração, ou seja, de um programa de desenvolvimento gerencial para ocupantes de cargos em comissão e funções comissionadas. Também não há ações destinadas à habilitação de servidores para a ocupação desses postos.

Em relação à percepção coletada junto aos servidores da Autarquia, por intermédio de questionário eletrônico, verificou-se resultado positivo sobre o tema "desenvolvimento de pessoas" no âmbito do FNDE. Obteve-se alto grau de concordância quanto ao recebimento de treinamento e capacitação adequados para desenvolvimento de atividades do posto de trabalho ocupado, conforme se observa do gráfico a seguir, e acerca do incentivo dos superiores para se capacitarem em temas relacionados a gestão de riscos.

Gráfico 5: Percepção dos servidores – Desenvolvimento de pessoas



Fonte: elaboração própria.

Ademais, 94% dos servidores "concordaram" ou "concordaram totalmente" que suas competências e habilidades estão alinhadas com o posto de trabalho ocupado. Apesar da percepção positiva, destaca-se que o FNDE ainda não dispõe de mecanismos adequados para garantir com segurança razoável esse alinhamento, especialmente considerando a ausência de mecanismos de mapeamento de postos de trabalho e de dimensionamento da força de trabalho.

Pelo exposto, verifica-se que o FNDE fornece normas e orientações sobre desenvolvimento de pessoas, bem como institui mecanismos para apoiar as ações relacionadas à gestão de pessoas, mas que há fragilidades que precisam ser trabalhadas, além de boas práticas que podem ser internalizadas, com vistas a dar maior segurança de que as necessidades de desenvolvimento relevantes para o alcance dos objetivos da organização estejam sendo contempladas.

1.1.1.2. Comprometimento das lideranças

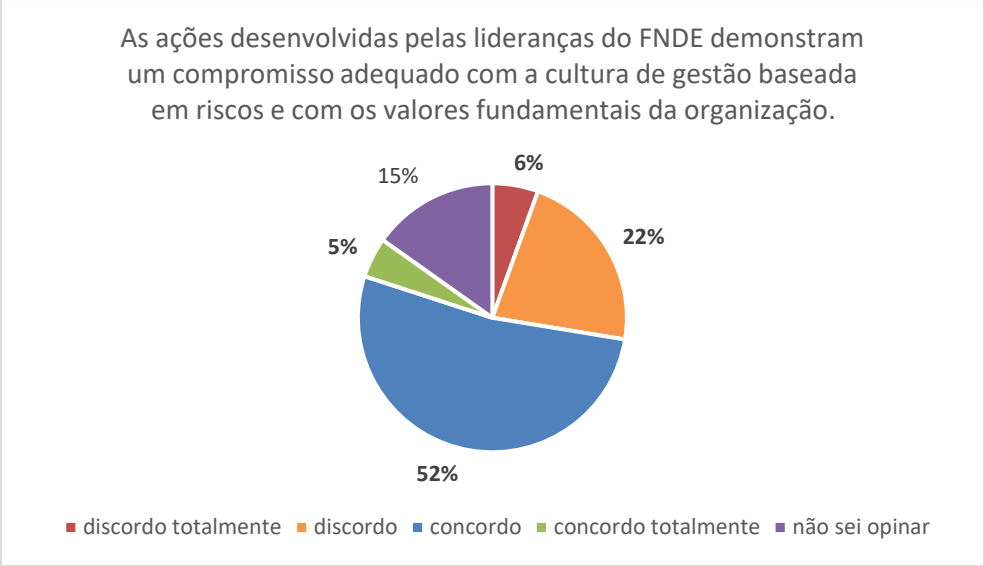
Buscando avaliar se o FNDE reforça o comprometimento das lideranças com a cultura de gestão baseada em riscos e com os valores fundamentais da organização, foram analisados os temas Política de Gestão de Riscos e Transparência Ativa. Também foi coletada a percepção dos servidores quanto aos instrumentos de transparência ativa.

Destaca-se inicialmente que o papel desempenhado pelas lideranças na gestão de riscos é fundamental, pois a atitude e o interesse da Alta Administração devem permear toda a organização como forma de fomentar a cultura da gestão de riscos. A ISO 31000:2018, ao tratar do comprometimento com a gestão de riscos, recomenda que, onde aplicável, seja estabelecida "uma política, uma declaração ou outras formas que claramente transmitam os objetivos e o comprometimento com a gestão de riscos de uma organização". No mesmo sentido, a IN nº 01/2016 estabeleceu, em seu artigo 17, a obrigatoriedade de órgãos e entidades do Poder Executivo federal instituírem políticas de gestão de riscos em até 12 meses da publicação do normativo em questão.

Assim, dado que o FNDE ainda não publicou sua Política de Gestão de Riscos tem-se uma desconformidade com a legislação vigente. Desse modo, a ausência de uma política, além de fragilizar o comprometimento das lideranças, impede a integração dos princípios, das estruturas e dos processos de gestão de riscos em todas as áreas relevantes da organização, dado que não foram definidas as diretrizes e os objetivos relacionados ao tema.

Nesse contexto, 51% dos servidores "discordaram" ou "discordaram totalmente" quando perguntados se a Alta Administração demonstra um compromisso adequado com a cultura de gestão baseada em riscos e com os valores fundamentais da organização, conforme gráfico a seguir:

Gráfico 6: Percepção dos servidores – Comprometimento das lideranças



Fonte: elaboração própria.

Outro fator que aponta o comprometimento das lideranças com a cultura da gestão baseada em riscos são as ações relacionadas à transparência ativa. Conforme preconizado pelo artigo 8º, da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), os órgãos e entidades públicas têm o dever de promover a divulgação de informações de interesse coletivo ou geral. Isso porque, a transparência é um dos princípios da *nova governança pública*[6] – que incorpora a governança, a gestão de riscos e a integridade – auxiliando a aprimorar os resultados das organizações e elevar sua responsividade perante a sociedade.

As análises realizadas pela equipe de auditoria evidenciaram que, em que pese a existência de aba de "Acesso à Informação" no portal do FNDE[7] na *internet* e a estruturação conforme os 12 itens[8] solicitados pelo Guia de Transparência Ativa da CGU, o FNDE não cumpre os requisitos mínimos de transparência ativa, dado que há informações obrigatórias não disponibilizadas, como, por exemplo, principais metas, indicadores e principais resultados no item "Ações e Programas". Também não foram disponibilizadas as informações sobre audiências públicas, conselhos, órgãos

[6] Conforme destacado em "Governança, Gestão de Riscos e Integridade" (ENAP, 2019).
[7] Em processo de migração para o gov.br quando da execução dos testes de auditoria.
[8] A saber: 1 - Institucional; 2 - Ações e Programas; 3 - Participação Social; 4 - Auditorias; 5 - Convênios e transferências; 6 - Receitas e despesas; 7 - Licitações e contratos; 8 - Servidores; 9 - Informações classificadas; 10 - Serviço de informação ao cidadão; 11 - Perguntas frequentes; 12 - Dados abertos.

colegiados e conferências no item “Participação Social”. Ainda, há *links* que não estão funcionando, como no caso de alguns *links* que encaminham para o Portal da Transparência no item “Receitas e Despesas”. Dessa forma, tem-se um descumprimento com o Decreto nº 7.724/2012.

Outra desconformidade encontrada foi a ausência de divulgação da Carta de Serviços ao Usuário, exigida pela Lei nº 13.460/2017, e que tem por objetivo informar os usuários sobre os serviços prestados pela entidade, as formas de acesso a esses serviços e seus compromissos e padrões de qualidade de atendimento ao público.

Quanto à percepção dos servidores, 71% daqueles que responderam ao questionário “concordaram” ou “concordaram totalmente” que as ações do FNDE são adequadamente reportadas às partes interessadas por meio de instrumentos de transparência ativa e de divulgação no site do FNDE.

Assim, as análises realizadas mostram que, considerando especialmente a ausência de uma Política de Gestão de Riscos e as falhas nos mecanismos de transparência, o comprometimento com a cultura de gestão de riscos e com os valores fundamentais da organização carecem de aprimoramentos, visando desenvolver um ambiente propício para gerenciar riscos.

1.1.1.3. Integridade e valores éticos

Buscando avaliar se o FNDE institui políticas, programas e medidas definindo padrões de comportamento desejáveis e se avalia a aderência destes à integridade e aos valores éticos, foram analisados o Plano de Integridade e as ações de fomento à integridade na Autarquia, bem como foram verificados pontos relacionados com a gestão da ética. Além disso, foi coletada a percepção dos servidores, da Alta Administração e da Comissão de Ética do FNDE.

Destaca-se que o comprometimento com a integridade e com os valores éticos é um dos princípios do COSO-CI (2013), cujos pontos de foco são: liderar pelo exemplo; estabelecer normas de conduta; avaliar a adesão às normas de conduta; e tratar desvios de forma oportuna. Nesse sentido, a IN nº 01/2016, em seu art. 16, inciso I, estabelece que todos os atores da organização (Alta Administração, servidores e funcionários) devem observar o componente ambiente interno, que inclui, dentre outros elementos, integridade e valores éticos.

Em consonância com o princípio acima exposto, a Portaria CGU nº 57, de 4 de janeiro de 2019, orienta sobre a estruturação, a execução e o monitoramento do Programa de Integridade dos órgãos e entidades da administração pública federal, estabelecendo também a base para a elaboração do Plano de Integridade.

Da análise realizada, verificou-se que o FNDE fornece políticas, programas e medidas de integridade e valores éticos, especialmente a partir da instituição do seu Programa de Integridade (Portaria nº 208, de 22 de abril de 2019) e do seu Plano de Integridade (SEI 1403999), bem como da instituição de uma Unidade de Gestão da Integridade (Portaria nº 202, de 18 de abril de 2019), em aderência ao que preconiza a Portaria supracitada. Ainda, verificou-se a existência de Código de Ética próprio (Portaria FNDE nº 283, de 5 de dezembro de 2002) e de Comissão de Ética instituída, cujos membros são designados em portarias específicas, em conformidade com as orientações do Decreto nº 1.171/1994.

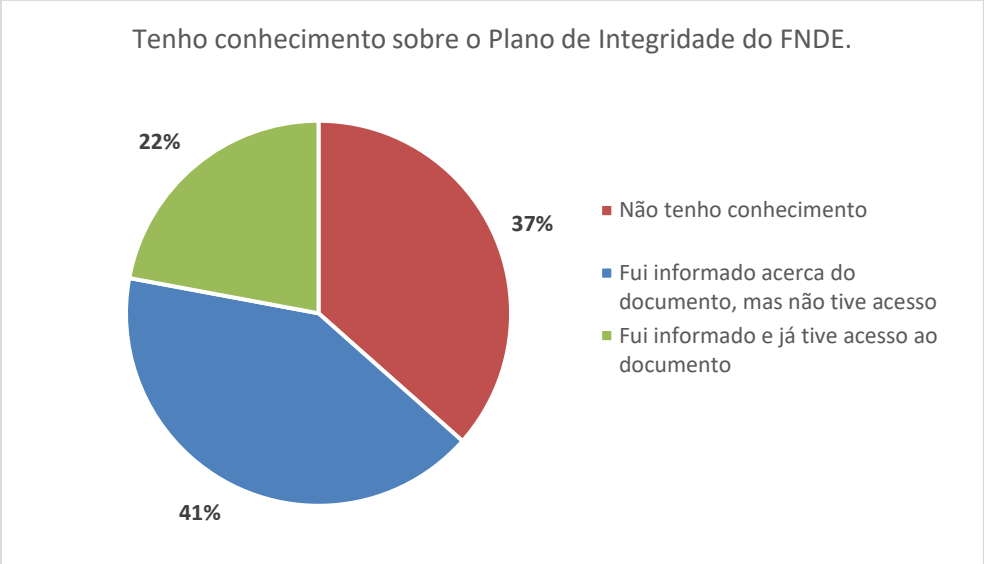
Contudo, em que pese a existência de Plano de Integridade para a Autarquia, foram observadas fragilidades e possibilidades de melhoria. Nesse sentido, verificou-se que:

- o Plano de Integridade não está publicizado no Portal do FNDE, prejudicando a transparência e a adequada divulgação do instrumento aos servidores que atuam na organização e à sociedade;
- não foram identificadas ações recentes de promoção da integridade (as últimas capacitações fornecidas pela Autarquia foram realizadas em 2019); e
- não existem mecanismos e/ou ações para articular o Plano de Integridade às estratégias do FNDE, o que tem potencial de prejudicar a eficácia do plano.

Além disso, foram identificadas desconformidades relacionadas ao conteúdo do Plano de Integridade do FNDE: não foi feito o levantamento de riscos para a integridade, contrariando o art. 5º, III, da Portaria CGU nº 57/2019; e não há previsão expressa quanto à forma e à periodicidade do seu monitoramento, nem quanto à sua atualização periódica, contrariando o art. 5º, IV, da Portaria já citada. Nesse ponto, o FNDE informou que estão sendo realizadas reuniões periódicas sobre o tema, mas que, em decorrência de instabilidades no período de 2020/2021, não houve êxito em estabelecer um mecanismo de acompanhamento contínuo.

No tocante à percepção dos servidores, 55% responderam que não recebem orientações periódicas sobre integridade. Além disso, 37% afirmaram desconhecer o Plano de Integridade do FNDE e 41%, apesar de terem sido informados sobre o documento, não tiveram acesso a ele, conforme demonstrado no gráfico a seguir:

Gráfico 7: Percepção dos servidores – Integridade e valores éticos



Fonte: elaboração própria.

Quanto à percepção da Alta Administração, 71% dos respondentes disseram que desenvolvem ações para o reforço da integridade e que levantaram riscos para a integridade e medidas para seu tratamento no âmbito de seus processos e atividades. Assim, entende-se a necessidade de coletar essas ações e os riscos já mapeados para comporem o Plano de Integridade do FNDE. Destaca-se também que 50% dos respondentes afirmaram não ter se capacitado nos temas integridade, ética e gestão de riscos em 2021 e 43% afirmaram não ter promovido a participação dos servidores que atuam em suas unidades nesses temas.

Em relação à gestão da ética, observaram-se possibilidades de melhorias, em aderência às boas práticas preconizadas pela Organização para a Cooperação e o Desenvolvimento Econômico – OCDE[9] para o tema, como:

- a inserção no Código de Ética de diretrizes sobre tratamento de conflito de interesses e nepotismo; de sanções cabíveis no caso de seu descumprimento; de mecanismos de monitoramento e avaliação; e de papéis e responsabilidades dos envolvidos no monitoramento e na avaliação do comportamento de seu público-alvo;
- a realização de ações de intercâmbio com outras comissões para compartilhamento de conhecimento e boas práticas;
- a realização de ações periódicas de fomento às práticas de gestão da ética;
- a finalização e a publicação de plano de trabalho específico para a Comissão de Ética do FNDE; e
- a instituição de modelo de monitoramento do cumprimento do Código de Ética.

Ainda, 96% dos servidores que participaram do questionário declararam conhecer a Comissão de Ética, mas 50% afirmaram não conhecer os papéis por ela desenvolvidos. Ademais, 93% dos servidores declararam conhecer o Código de Ética do FNDE. Porém, 28% declararam não conhecer os valores, princípios e comportamentos esperados no FNDE quanto à ética.

Já em relação à percepção da Alta Administração, 100% dos dirigentes que participaram do questionário declararam conhecer o Código de Ética, mas 28% destes afirmaram não conhecer os papéis desenvolvidos pela Comissão de Ética.

Nesse objeto, também foi coletada a percepção dos servidores que atuam na Comissão de Ética do FNDE. No entanto, dado que a amostra coletada não foi estatisticamente significante, os resultados do questionário não foram utilizados para fins de cálculo da percepção e de composição da pontuação do presente objeto. Porém, as respostas obtidas permitem analisar qualitativamente a atuação da Comissão e eventuais possibilidades de melhoria.

Nesse contexto, destaca-se que 75% dos membros da Comissão de Ética do FNDE que responderam ao questionário discordaram quando perguntados se foram definidas diretrizes claras para a atuação da Comissão e se há entendimento de quais atividades e ações precisam ser executadas, o que reforça a necessidade de aprimoramento dos mecanismos de gestão da ética no FNDE. Ainda, foi indicada pelos respondentes a necessidade de revisão do Código de Ética, de campanhas sobre integridade e valores éticos e de capacitação dos servidores e colaboradores da organização.

Assim, em que pese a instituição formal de políticas, programas e medidas de integridade e valores éticos, existem fragilidades e desconformidades que prejudicam o reconhecimento desses valores como aspectos-chave para o reforço da *accountability* e para a gestão de riscos.

1.1.2. Governança de Riscos

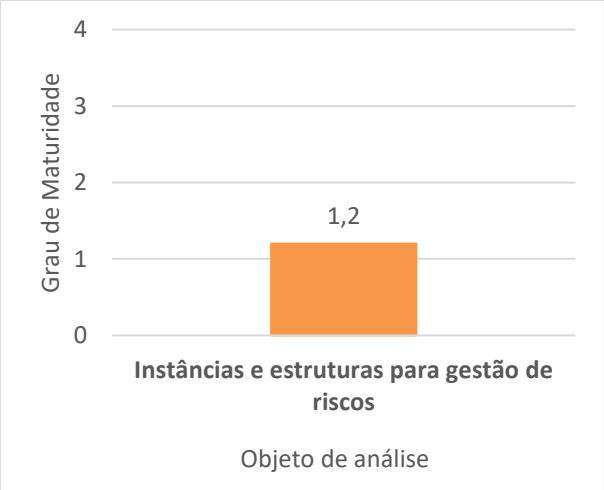
Existem estruturas e processos definidos para apoiar as responsabilidades de governança de riscos e assegurar que a gestão de riscos seja integrada aos processos de gestão?

[9] Sintetizadas no documento intitulado "*Towards a Sound Integrity Framework: Instruments, Processes, Structures and Conditions for Implementation*" (OCDE, 2009) e abordadas no Acórdão 581/2017-TCU-Plenário.

Com vistas a avaliar este aspecto, foram previstos testes relacionados ao seguinte objeto de análise: 1.1.2.1. Instâncias e estruturas para gestão de riscos.

A avaliação realizada mostrou que não foram adequadamente definidas e não estão em funcionamento as estruturas e os processos necessários para apoiar as responsabilidades de governança de riscos. Também não se pode falar em integração da gestão de riscos aos processos de gestão, dada a ausência de diretrizes formais sobre esse tema.

Gráfico 8: Resultado da avaliação dos objetos – Aspecto Governança de riscos



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

1.1.2.1. Instâncias e estruturas para gestão de riscos

Os testes previstos buscaram avaliar se os responsáveis pela governança e a Alta Administração do FNDE utilizam instâncias internas (como comitês de governança, riscos e controles, auditoria, coordenação de gestão de riscos etc.) e outras medidas para apoiar suas responsabilidades de governança de riscos. Ainda, buscou-se avaliar se os responsáveis pela governança e a Alta Administração do FNDE asseguram que a gestão de riscos seja integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, as funções e as atividades relevantes para o alcance dos objetivos-chave da organização.

O COSO-GRC (2007) destaca que "a estrutura organizacional de uma entidade provê arcabouço para planejar, executar, controlar e monitorar as suas atividades". Nesse contexto, devem ser definidas responsabilidades relacionadas à gestão de riscos, bem como estabelecidas linhas apropriadas de comunicação. No mesmo sentido, a ISO 31000:2018 recomenda que sejam determinados os responsáveis pela gestão de riscos e os papéis de supervisão, como partes integrantes da governança da organização. Por isso, a IN nº 01/2016, em seus artigos 19, 20 e 23, trata das instâncias e estruturas para a gestão de riscos, prevendo a atribuição do dirigente máximo como principal responsável pelo estabelecimento da estratégia da organização e da estrutura de gerenciamento de riscos.

Dentre as instâncias existentes no âmbito do FNDE, destacaram-se:

- Comitê de Gestão Estratégica e Governança (CGEG) – Portaria FNDE nº 546, de 18 de outubro de 2019 (SEI 1591280), e Comitê de Gestão de Riscos, Controles Internos e Integridade (CGRCI) – Portaria nº 541, de 16 de outubro de 2019 (SEI 1591280), que abarcam parte das competências exigidas pelo art. 23, § 2º, II, da IN nº 01/2016;
- Conselho Deliberativo, órgão colegiado e de deliberação superior, cujas competências estão dispostas na Resolução/CD/FNDE nº 31, de 30 de setembro de 2003;
- a atribuição de competência regimental para a Agest de apoiar o desenvolvimento de metodologia de governança; e
- unidade de Auditoria Interna, operando enquanto terceira linha, com base nos preceitos do Modelo de 3 Linhas do IIA.

No entanto, ainda que tenham sido formalmente instituídos, evidenciou-se que não houve atuação dos Comitês acima referidos durante os exercícios de 2020 e 2021 e que não há alinhamento dessas instâncias com a cultura e com o desenho geral da organização, conforme destacado pela própria organização auditada. Além disso, não estão atribuídas nem para o CGEG nem para o CGRCI algumas competências exigidas pela IN nº 01/2016, como a prevista pelo art. 23, § 2º, II.

Outra fragilidade encontrada foi o fato de que, com exceção da DIRTI (no âmbito da Coordenação-Geral de Governança de TI – CGGOV), não há competências regimentalmente formalizadas que envolvam a gestão de riscos.

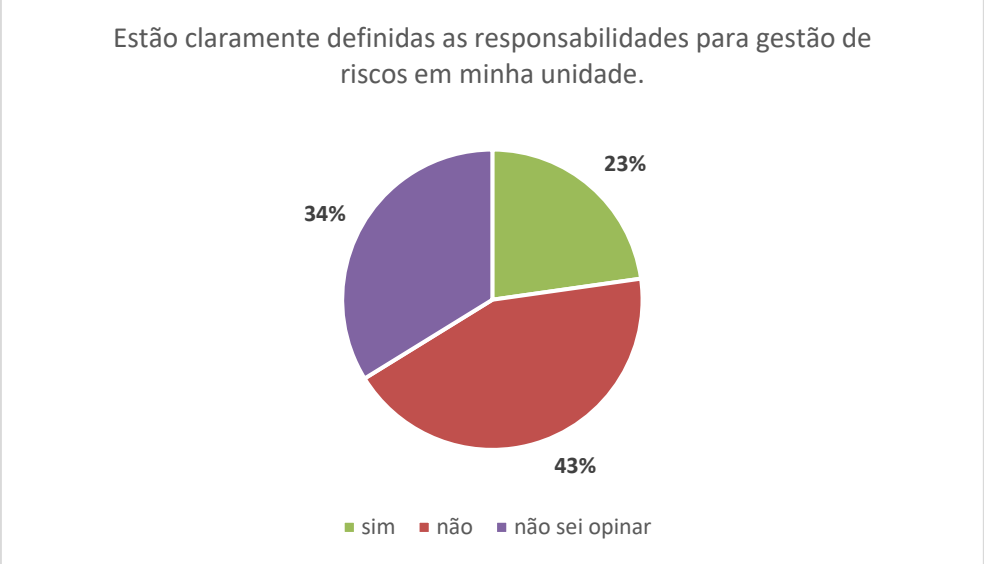
Também não existe uma unidade regimentalmente responsável pelo monitoramento e pela supervisão da gestão de riscos da organização operando enquanto segunda linha. Ademais, os Comitês existentes que poderiam auxiliar nesse processo apresentam fragilidades e não desempenham suas funções de apoio à gestão de riscos, com base nos preceitos do Modelo de 3 Linhas do IIA.

Já em relação às estruturas para gestão de riscos, ressalta-se que não foram encontradas estruturas formalizadas, disseminadas e em funcionamento por toda a organização. Isso porque:

- não há políticas e procedimentos padronizados, tampouco metodologia definida para a gestão de riscos no FNDE;
- não há sistemas ou ferramentas específicas para subsidiar a gestão de riscos;
- não existem pessoas alocadas especificamente para a realização de atividades de gestão de riscos (como “gestores de riscos”); e
- não há fluxos ou canais formalizados exclusivamente para a gestão de riscos.

A percepção dos servidores mostrou que 41% “discordou” ou “discordou totalmente” e 16% não souberam opinar quando questionados se existe uma estrutura adequada para gestão de riscos em suas unidades, a partir de procedimentos definidos, responsabilidades atribuídas, bem como sistemas ou outros mecanismos de acompanhamento de riscos. Ainda, somente 23% dos servidores entenderam que estão claramente definidas as responsabilidades para a gestão de riscos em suas unidades, conforme demonstrado no gráfico a seguir:

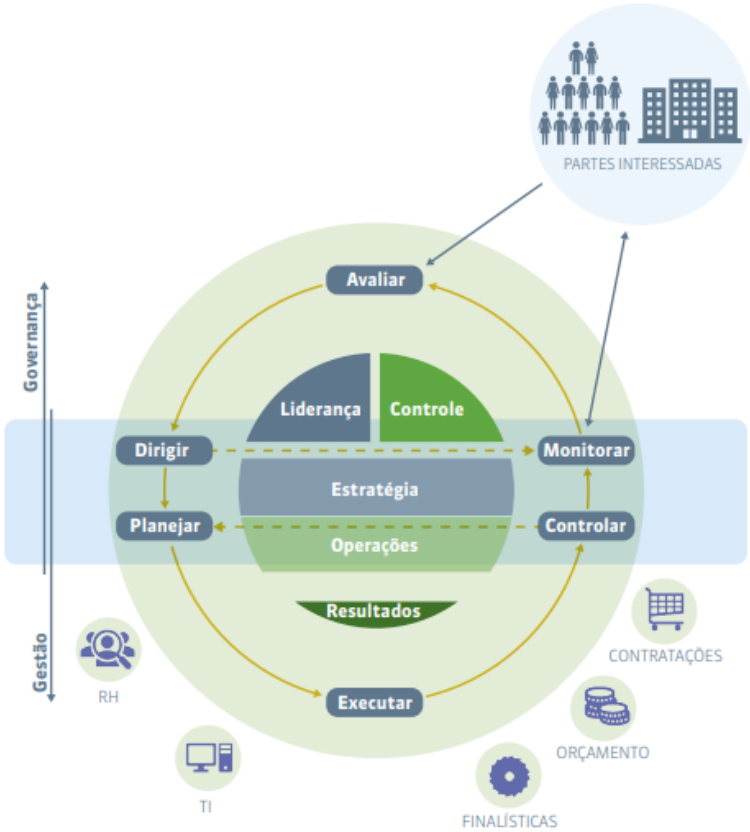
Gráfico 9: Percepção dos servidores – Instâncias e estruturas para gestão de riscos



Fonte: elaboração própria.

Complementarmente, concluiu-se que, no âmbito de um modelo de governança do FNDE, não estão claramente identificadas as instâncias internas e de apoio à governança, conforme recomendado pelo Referencial Básico de Governança e Gestão (TCU, 2020), cujo modelo de Governança e Gestão explicita-se na figura a seguir:

Figura 1: Modelo de governança e gestão



Fonte: TCU (2020).

Destaca-se que a formalização desse modelo pode auxiliar a definir as diretrizes para as atividades de governança, além de possibilitar que a organização "alinhe seus objetivos ao interesse público, gerencie seus riscos e entregue o valor esperado de forma íntegra, transparente e responsável" (TCU, 2020).

Por fim, em relação à integração da gestão de riscos ao planejamento e à gestão, verificou-se que, dada a ausência de uma Política de Gestão de Riscos, não há um normativo que defina as diretrizes para a integração da gestão de riscos ao planejamento estratégico. De acordo com a organização auditada, o Plano Estratégico do FNDE para o período 2018-2022 teve a gestão de riscos em seu radar de objetivos, "mas sem desdobrar em iniciativas que concretizassem. [...] O diagnóstico é de que alguns elementos precedentes não foram cobertos".

A partir das análises realizadas, conclui-se que existem instâncias que podem apoiar as responsabilidades de governança de riscos, mas não há efetivo funcionamento, tampouco integração e coordenação dessas instâncias, para os processos de gestão. Além disso, não há uma diretriz (a exemplo de uma Política de Gestão de Riscos) que permita a obtenção de segurança razoável quanto ao alcance de objetivos da organização.

1.1.3. Supervisão da Governança e da Alta Administração

Os responsáveis pela governança e a Alta Administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos?

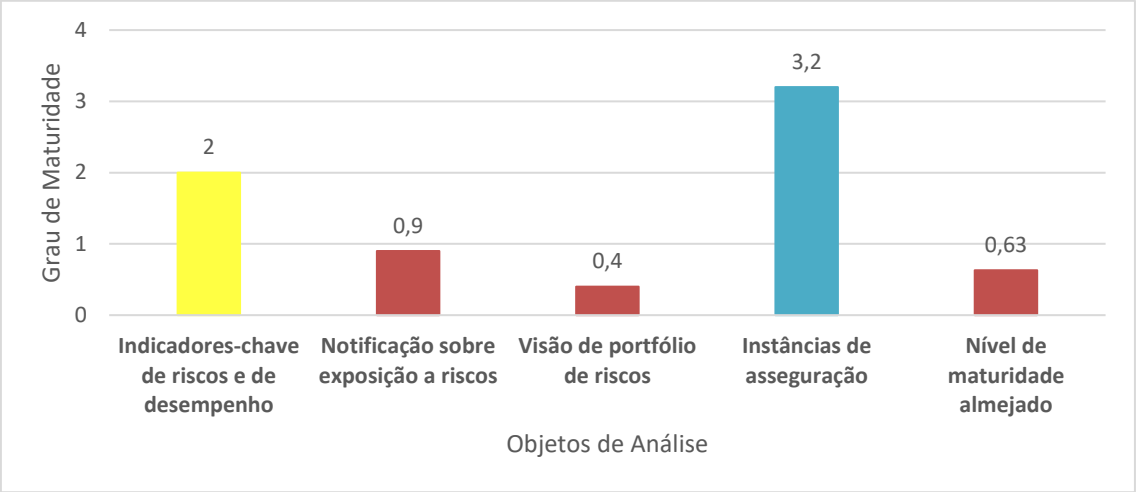
Com vistas a avaliar este aspecto, foram previstos testes relacionados a cinco objetos de análise: 1.1.3.1. Indicadores-chave de risco e de desempenho; 1.1.3.2. Notificação sobre exposição a riscos; 1.1.3.3. Visão de Portfólio de Riscos; 1.1.3.4. Instâncias de Asseguração; e 1.1.3.5. Nível de maturidade almejado para a gestão de riscos.

A avaliação realizada mostrou que a Alta Administração não dispõe de instrumentos adequados para supervisionar a estratégia e exercer suas responsabilidades de governança de riscos, visto que não há indicadores de risco definidos, não há mecanismos estabelecidos para notificação regular e oportuna sobre as exposições da organização a riscos e não foi estabelecido um nível de maturidade almejado para a gestão de riscos.

No entanto, destaca-se que a organização conta com o funcionamento de instância interna de asseguração, por intermédio da Auditoria Interna, e que a gestão tem utilizado essa instância para se certificar acerca dos processos de gerenciamento de riscos e controles.

Adicionalmente, destaca-se que, dadas as fragilidades existentes em outros aspectos – como a ausência de Política de Gestão de Riscos, de sistemas/ferramentas e metodologias que auxiliem a gerir riscos, de pessoas alocadas especificamente para funções relacionadas à gestão de riscos, de fluxos/canais formalizados para a gestão de riscos e de definição de apetite a risco – não se identificou a existência de uma visão de portfólio, contemplando todos os riscos relevantes que perpassam o FNDE.

Gráfico 10: Resultado da avaliação dos objetos – Aspecto Supervisão da governança e da Alta Administração



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir dos objetos de análise selecionados:

1.1.3.1. Indicadores-chave de riscos e de desempenho

Os testes previstos buscaram avaliar se os responsáveis pela governança e a Alta Administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos mediante incorporação explícita e monitoramento regular de indicadores-chave de risco e de desempenho nos seus processos de governança e gestão.

No que se refere à concepção de uma estrutura de gestão de riscos, a ISO 31000:2018 preconiza que, após entendimento da organização e seu contexto, a organização deve articular o comprometimento com a gestão de riscos com base em indicadores de desempenho. Ainda sobre esse tema, a IN nº 01/2016 dispõe que os órgãos e entidades do Poder Executivo Federal devem especificar diretrizes sobre como será medido o desempenho da gestão de riscos.

Nesse contexto, o Guia Técnico de Gestão Estratégica (SEGES/ME) define indicadores como "instrumentos que permitem observar, identificar e mensurar aspectos relacionados à evolução de um determinado objeto [...]".

Da análise realizada, observou-se que os responsáveis pela governança e a Alta Administração dispõem de mecanismos para supervisionar a estratégia e exercerem suas responsabilidades de governança, mediante:

- a incorporação explícita e o monitoramento regular de indicadores-chave de desempenho detalhados no Plano Estratégico Institucional (PEI-FNDE 2018-2022). Foram estabelecidos nesse plano 29 indicadores estratégicos de desempenho relacionados aos 20 objetivos estratégicos definidos;
- a pactuação de metas globais e intermediárias de desempenho, associadas aos objetivos estratégicos, por intermédio da Portaria nº 90, de 26 de fevereiro de 2021, atualizada pela Portaria no 355, de 1º de julho de 2021, em cumprimento ao Decreto nº 7.133/2010

e à Portaria FNDE nº 1.073, de 24 de agosto de 2010. Tais normativos apresentam as metas globais e intermediárias para os exercícios 2021 e 2022, bem como os índices a serem atingidos em cada período, para todas as unidades dirigentes da Autarquia. Além disso, para fins de avaliação de desempenho individual, as chefias imediatas e os servidores pactuam anualmente metas de desempenho individual; e

- o monitoramento periódico dos indicadores globais e intermediários, com a realização de apurações quadrimestrais de desempenho e a divulgação, no site do FNDE, de Painel de Indicadores Institucionais.

No entanto, há fragilidades associadas aos indicadores de desempenho definidos:

- há objetivos estratégicos sem indicadores globais associados e sem unidades responsáveis pela sua realização, conforme será demonstrado no aspecto 1.2.1.;
- conforme reconhecido pela própria organização auditada[10], há avanços que devem ser feitos em relação ao monitoramento de seu desempenho, sendo este um desafio para os próximos exercícios, com "a implantação de uma gestão estratégica voltada para potencializar o resultado [...]" e a "gestão estratégica monitorada e articulada com os níveis tático e operacional e voltada para resultados"; e
- há possibilidade de aprimoramento dos atuais indicadores[11], a partir da atualização das metas individuais, processo a ser conduzido pela CGPEO/DIRAD e que pode, eventualmente, identificar a necessidade de pactuar outras metas intermediárias.

Por isso, conclui-se que, da forma como foi desenhado o atual modelo, não houve a adequada articulação entre metas globais, intermediárias e individuais. Assim, entende-se que o próximo Plano Estratégico precisa avançar no sentido de prover ações que permitam a adequada articulação entre a gestão estratégica e os níveis táticos e operacional. Entende-se, ainda, que a recente revisão da Cadeia de Valor do FNDE possibilitará uma visão mais fidedigna dos macroprocessos de governança e gestão, permitindo a adequada formulação do direcionamento estratégico.

Por fim, verificou-se que o FNDE não conta com indicadores-chave de risco para apoiar seus processos de governança e gestão. Assim, observa-se a necessidade de estabelecer esse tipo de indicador, de modo a possibilitar o monitoramento da exposição aos riscos que a organização está exposta. Destaca-se, no entanto, que esse processo depende em grande parte da definição do apetite a risco e da tolerância a risco, que, conforme será demonstrado no aspecto 1.2.2., também não foram estabelecidos.

1.1.3.2. Notificação sobre exposição a riscos

Os testes previstos tinham como principal objetivo avaliar se os responsáveis pela governança e a Alta Administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos mediante notificação regular e oportuna sobre as exposições da organização a riscos, sobre os riscos mais significativos e sobre como a administração está respondendo a esses riscos.

[10] Relatório de Gestão – FNDE (2021).
[11] Conforme destacado na Nota Técnica nº 2255956/2021/AGEST/GABIN.

No que se refere à notificação sobre exposição a riscos, o COSO-GRC (2007) preconiza em seus princípios que a estrutura organizacional deve estabelecer linhas de comunicação. Nesse sentido, a ISO 31000:2018, no item 5.4.5, afirma que a "comunicação e a consulta sejam oportunas e assegurem que a informação pertinente seja coletada, consolidada, sintetizada e compartilhada, como apropriado, e que o retorno seja fornecido e as melhorias sejam implementadas".

Na mesma linha, a IN nº 01/2016 prevê que todos os atores envolvidos na organização desenvolvam determinados componentes da estrutura de gestão de riscos, como o componente "informação e comunicação", que estabelece que as informações relevantes para a gestão de riscos sejam identificadas, coletadas e comunicadas, permitindo que as pessoas cumpram suas responsabilidades e possibilitando o gerenciamento de riscos e a tomada de decisão.

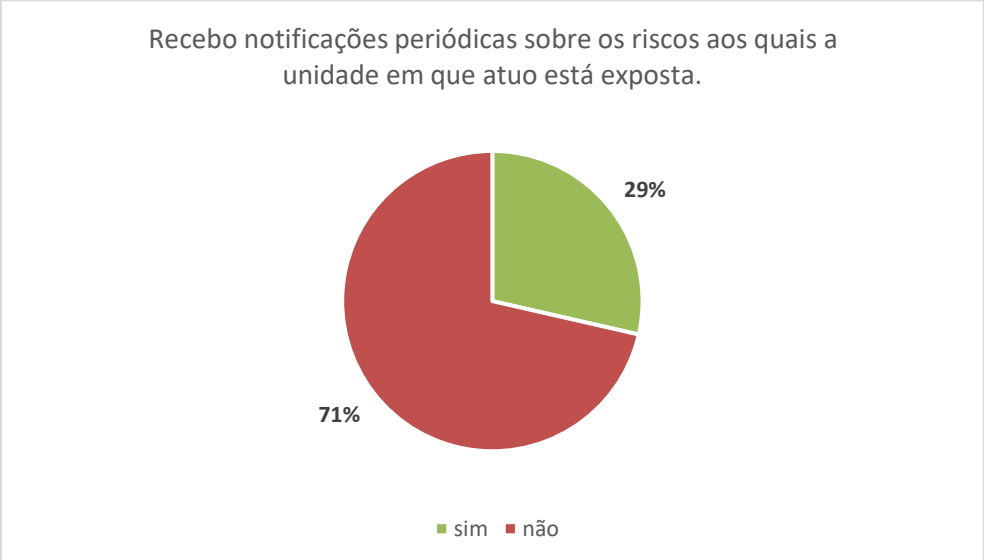
Das análises realizadas, verificou-se que o FNDE não dispõe de fluxos e canais formais e padronizados para comunicação de informações sobre riscos.

No entanto, a organização informou que há canais que podem ser utilizados com essa finalidade, a exemplo da Plataforma Integrada de Ouvidoria e Acesso à Informação - Fala.BR. Em que pese a existência destes, entende-se que, para a adequada estruturação do processo de gestão de riscos, é necessário criar canais claros e abertos que permitam que a informação relativa a riscos aos quais a organização está exposta flua em todos os sentidos (*top-down* e *bottom-up*), em conformidade com o que é recomendado pela IN nº 01/2016 e pelos principais *frameworks* sobre gestão de riscos.

Da percepção coletada junto aos servidores, verificou-se que 47% acreditam que a Alta Administração acompanha os riscos mais significativos aos quais suas unidades estão expostas e 72% "concordaram" ou "concordaram totalmente" que têm conhecimento quanto à forma e a quem devem comunicar eventuais exposições a riscos.

A percepção da Alta Administração, mostra, no entanto, que 71% dos dirigentes não recebem informações periódicas sobre riscos em suas unidades:

Gráfico 11: Percepção da Alta Administração – Notificação sobre exposição a riscos



Fonte: elaboração própria.

Assim, a avaliação realizada demonstrou que o FNDE não dispõe de mecanismos para notificação regular e oportuna sobre as exposições da organização a riscos, sobre os riscos mais significativos e sobre como a administração está respondendo a esses riscos, o que prejudica a supervisão da estratégia e o exercício das responsabilidades de governança de riscos.

1.1.3.3. Visão de portfólio de riscos

Os testes previstos tinham como principal objetivo avaliar se os responsáveis pela governança e a Alta Administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos mediante revisão sistemática da visão de portfólio de riscos em contraste com o apetite a riscos e mediante fornecimento de direção clara para gerenciamento dos riscos.

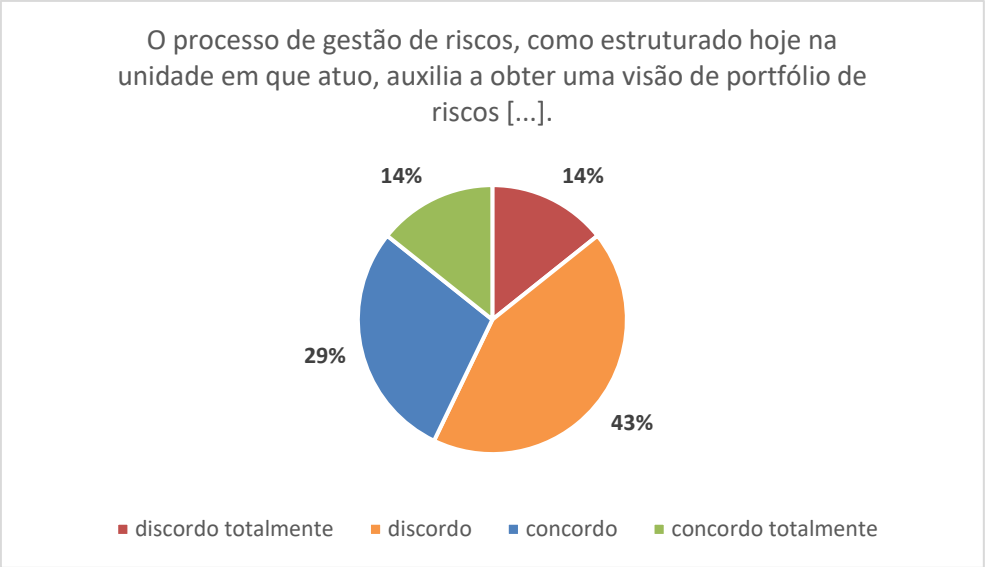
Como um dos princípios do COSO-GRC-EP (2017), a visão de portfólio de riscos diz respeito ao alinhamento do gerenciamento de riscos com os objetivos estratégicos, levando em conta os riscos combinados em uma visão de carteira, ou seja, uma visão da Alta Administração sobre os riscos selecionados e priorizados, de forma global e integrada (e não de forma isolada).

A partir das análises realizadas em outros objetos, verificou-se que o FNDE não possui uma visão de portfólio de riscos. Tal situação é agravada especialmente pela ausência de:

- Política de Gestão de Riscos ou de uma metodologia comum para gerir riscos no âmbito da organização, bem como a não utilização de sistemas ou ferramentas que auxiliem a gestão de riscos, conforme exposto nos tópicos 1.1.1.2 e 1.2.7.1;
- alocação específica de pessoas para funções relacionadas à gestão de riscos, conforme abordado no tópico 1.2.7.1; e
- fluxos e canais formalizados para a gestão de riscos, conforme tópico 1.1.3.2.

Em relação à percepção coletada junto à Alta Administração, destaca-se que 57% dos dirigentes respondentes “discordam” ou “discordam totalmente” que o processo de gestão de riscos estruturado em suas unidades auxilia a obter uma visão de portfólio de riscos:

Gráfico 12: Percepção da Alta Administração – Visão de portfólio de riscos



Fonte: elaboração própria.

Assim, entende-se que os responsáveis pela governança e a Alta Administração não detêm os instrumentos necessários que assegurem a revisão sistemática da visão de portfólio de riscos (em contraste com o apetite a risco), o que prejudica o fornecimento de direção clara para gerenciamento dos riscos. Ademais, destaca-se que os avanços relacionados a esse objeto dependem em grande parte do estabelecimento de um processo estruturado e integrado de gestão de riscos na organização.

1.1.3.4. Instâncias de asseguração

Os testes previstos tinham como principal objetivo avaliar se os responsáveis pela governança e a Alta Administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos mediante utilização dos serviços da auditoria interna ou de outras instâncias de asseguração para se certificarem de que a administração tem processos eficazes de gerenciamento de riscos e controle.

O Modelo das Três Linhas do IIA (2020) atribui à auditoria interna o papel de prestar avaliação e assessoria, de forma independente e objetiva, sobre a adequação e eficácia da governança e do gerenciamento de riscos.

Em consonância a essa ideia, a Declaração de Posicionamento do IIA "O papel da auditoria interna no gerenciamento de riscos" afirma que um dos principais requerimentos do Conselho da organização, ou de seu equivalente, é obter a avaliação (*assurance*) de que os processos de gerenciamento de risco estão funcionando eficazmente e de que os principais riscos estão sendo gerenciados em um nível aceitável. Essa asseguração advém de fontes diversas, sendo a auditoria interna uma das fontes principais.

Os testes realizados demonstraram que a Auditoria Interna do FNDE, enquanto terceira linha, tem auxiliado a gestão na asseguração dos processos de gerenciamento de riscos e controles do FNDE e tem sido instada pela Alta Gestão. Assim, destaca-se:

- da análise dos Planos Anuais de Auditoria Interna (Paint) publicados pela Auditoria Interna do FNDE nos últimos 3 exercícios, verificou-se que a maior parte dos trabalhos realizados teve como origem a avaliação de riscos realizada pela própria Audit ou alguma obrigação legal. Ocorreram, no entanto, trabalhos decorrentes de solicitação da Alta Gestão, como a auditoria de Acompanhamento das Recomendações do Relatório de Auditoria nº 19/2017 (RA nº 02/2020) e a avaliação do Programa Nacional de Formação Continuada a Distância nas Ações do FNDE – Formação pela Escola (RA nº 821081/2021). Houve também um trabalho de Consultoria sobre o Programa de Integridade do FNDE (Nota Técnica nº 1/2019/COAUD/AUDIT); e
- o Estatuto da Audit, Resolução nº 09, de 29 de setembro de 2022, prevê a possibilidade de recebimento de trabalhos decorrentes de demandas da Alta Administração, em seu artigo 29, que dispõe que essas demandas extraordinárias sejam avaliadas em relação ao impacto e à pertinência do atendimento, considerando a capacidade operacional, os trabalhos prioritários definidos e os riscos envolvidos.

Adicionalmente, destaca-se que tem havido esforço da gestão para se apropriar das recomendações de auditoria emitidas. Da análise das recomendações em monitoramento durante os exercícios de 2020, 2021 e 2022, verifica-se a existência de 53 recomendações classificadas nas

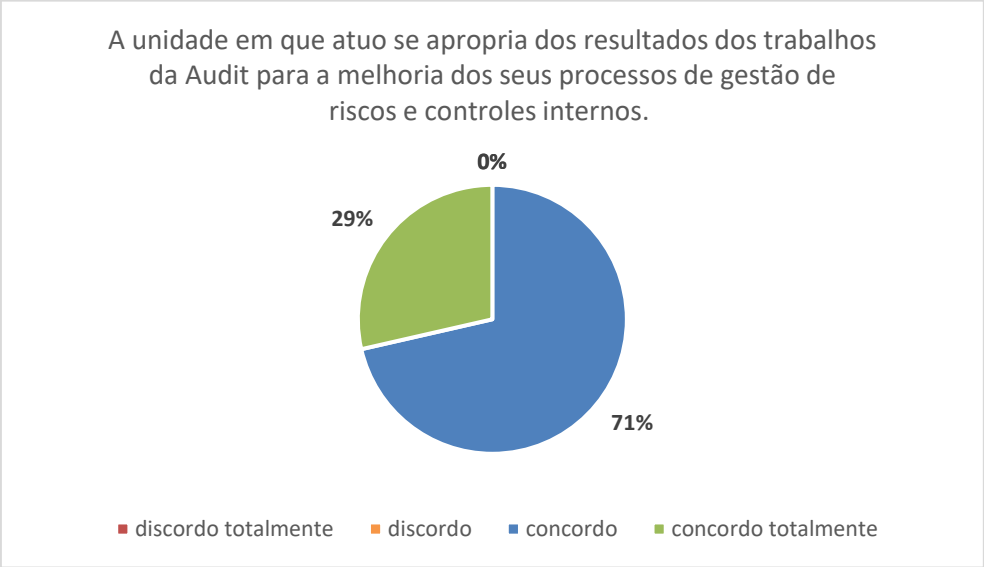
categorias “controles internos” e “gestão de riscos”, das quais 53% já foram implementadas ou implementadas parcialmente.

Ademais, a partir do início da utilização do Sistema e-Aud para monitoramento das recomendações, houve cadastro de todas as Diretorias da Autarquia, que passaram a receber notificações sobre novas recomendações, além de poderem acompanhar os prazos limites de atendimento e encaminharem providência via sistema.

Destaca-se, ainda, o estabelecimento de indicadores para o acompanhamento dos trabalhos realizados pela Audit, medindo a atuação dos gestores, da própria unidade de auditoria interna e da efetividade dos trabalhos. Conforme observado no Relatório Anual de Auditoria Interna (Raint) 2021, estabeleceu-se como meta global o “Índice de apropriação dos trabalhos de auditoria”, que, em 2021, atingiu o valor apurado de 75% e desempenho final de 157%, considerando a meta de 48% estabelecida.

Da análise do questionário enviado à Alta Administração, verificou-se que 100% dos respondentes afirmaram entender que a Auditoria Interna pode atuar na asseguração da gestão de riscos do FNDE, a partir da execução de trabalhos de avaliação e consultoria. Ainda, 100% dos respondentes entenderam que os resultados dos trabalhos da Audit têm potencial para contribuir com a melhoria dos processos de gestão de riscos do FNDE e para o atingimento de objetivos da organização. Por fim, 43% dos respondentes informaram que costumam solicitar trabalhos à Audit para obter asseguração acerca dos processos de gestão de riscos e controles internos de sua unidade e 100% dos respondentes concordaram que a unidade em que atuam se apropria dos resultados dos trabalhos da Audit para a melhoria dos seus processos de gestão de riscos e controles internos.

Gráfico 13: Percepção da Alta Administração – Instâncias de asseguração



Fonte: elaboração própria.

Desse modo, entende-se que os responsáveis pela governança e a Alta Administração dispõem de instância de asseguração interna e costumam utilizá-la para se certificarem sobre os processos de gerenciamento de riscos e controle.

1.1.3.5. Nível de maturidade almejado para a gestão de riscos

Os testes previstos tinham como principal objetivo avaliar se os responsáveis pela governança e a Alta Administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos mediante definição do nível de maturidade almejado para a gestão de riscos e mediante monitoramento do progresso das ações para atingir ou manter-se no nível definido.

O *Orange Book* destaca que a maturidade da gestão de riscos precisa ser periodicamente avaliada, de modo a identificar áreas de melhoria. Além disso, é preciso entender que o nível de maturidade almejado pode mudar ao longo do tempo, do mesmo modo que a organização deve melhorar continuamente a adequação e a eficácia da sua estrutura de gerenciamento de riscos.

O Tribunal de Contas da União (TCU, 2018a) também ressalta a importância da avaliação de maturidade para identificar aspectos que necessitam ser aperfeiçoados no âmbito da gestão de riscos das organizações públicas, subsidiando-se, assim, a elaboração e a colocação em prática de planos de ação para aperfeiçoamento das práticas de gestão de riscos.

A organização auditada informou que ainda não definiu um nível de maturidade almejado para a gestão de riscos, mas que adotou como referência os resultados do Perfil Integrado de Governança Organizacional e Gestão Pública (iGG), elaborado pelo TCU, no qual já foi identificada como fragilidade a gestão de riscos do FNDE.

Assim, em que pese a utilização do resultado da análise realizada pelo TCU como referência, cabe à unidade definir o nível de maturidade a partir de avaliação própria e do estabelecimento de linhas prioritárias de atuação.

1.2. Políticas e estratégias

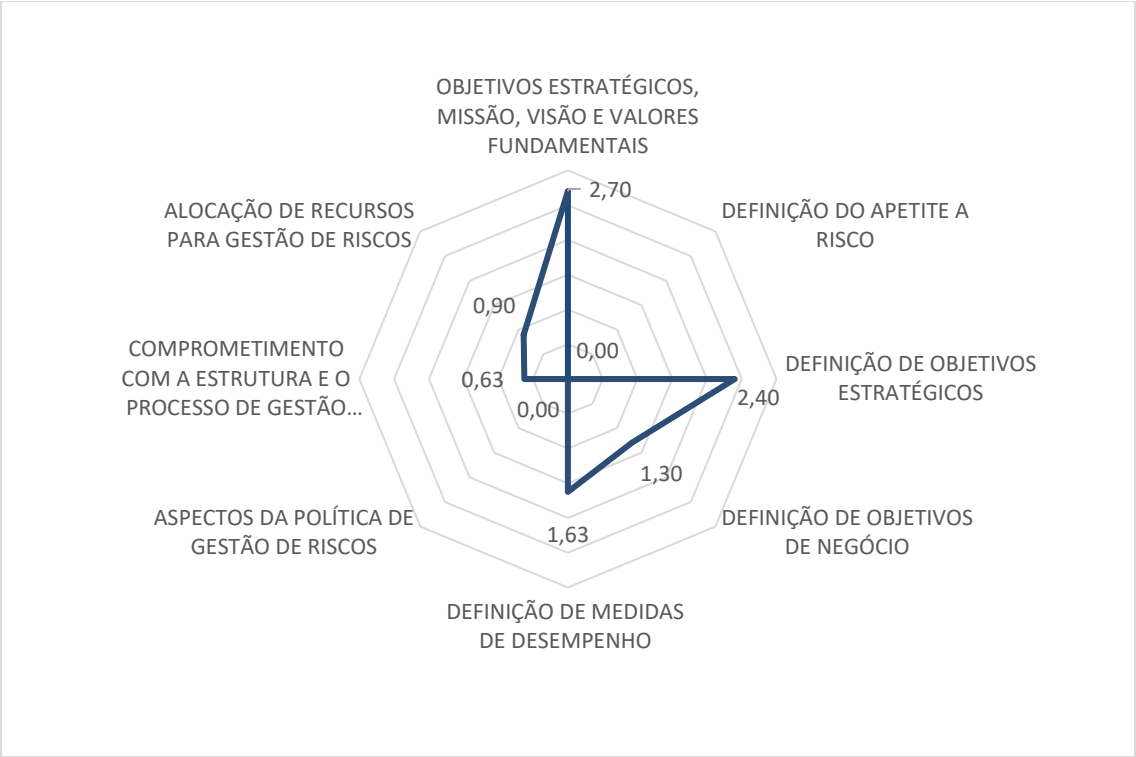
Nesse componente, apurou-se a seguinte questão: em que medida o FNDE dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática.

Buscou-se, para tanto, avaliar de que maneira o risco é considerado na definição da estratégia, dos objetivos e planos em todos os níveis críticos da entidade, e como é gerenciado nas operações, funções e atividades relevantes das diversas partes da organização. A avaliação do componente foi feita a partir de cinco aspectos: 1.2.1. Direcionamento estratégico; 1.2.2. Apetite a risco; 1.2.3. Integração da gestão de riscos ao processo de planejamento; 1.2.4. Medidas de desempenho; 1.2.5. Política de Gestão de Riscos; 1.2.6. Comprometimento da gestão; e 1.2.7. Alocação de recursos.

No FNDE, o resultado do componente “Políticas e estratégias”, a partir da avaliação dos seus aspectos, demonstra uma maturidade **INICIAL**, apurada em **12,86%**.

O gráfico a seguir apresenta o resultado consolidado do componente, a partir dos resultados apurados dos objetos analisados:

Gráfico 14: Resultado da avaliação dos objetos – Componente Políticas e estratégias



Fonte: elaboração própria.

A partir do gráfico 14, percebe-se a inexistência dos objetos relacionados à Política de Gestão de Riscos e ao apetite a risco da organização. Por outro lado, aspectos relacionados ao direcionamento estratégico, obtiveram pontuação maiores, o que demonstra uma estruturação mais adequada do Planejamento Estratégico da Autarquia. Ainda, as baixas pontuações relativas ao comprometimento com a estrutura e o processo de gestão de riscos e à alocação de recursos refletem os resultados do componente anterior, Liderança.

A seguir apresentam-se os aspectos avaliados no componente Políticas e Estratégias, bem como os objetos relacionados a cada aspecto.

1.2.1. Direcionamento estratégico

A Alta Administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico?

Com vistas a avaliar este aspecto, foram previstos testes relacionados ao objeto de análise 1.2.1.1. Objetivos estratégicos, missão, visão e valores fundamentais.

A avaliação realizada mostrou que o direcionamento estratégico foi estabelecido a partir da definição da missão, da visão e dos valores fundamentais da organização, bem como da definição de objetivos estratégicos. No entanto, não foram identificadas iniciativas que demonstrem a consideração do risco no estabelecimento da estratégia.

Gráfico 15: Resultado da avaliação dos objetos – Aspecto Direcionamento estratégico

Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

1.2.1.1. Objetivos estratégicos, missão, visão e valores fundamentais

Os testes previstos buscaram avaliar se o direcionamento estratégico é estabelecido de modo explícito e alinhado com as finalidades e as competências legais da entidade. Ainda, se este é traduzido em uma expressão inicial do risco aceitável (apetite a risco) para a definição da estratégia e a fixação de objetivos estratégicos e de negócios, bem como para o gerenciamento dos riscos relacionados.

O plano estratégico institucional dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, por determinação do art. 3º da Instrução Normativa ME nº 24, de 18 de março de 2020, deve conter, no mínimo, a cadeia de valor da instituição e sua identidade estratégica, que engloba missão, visão de futuro, valores e mapa estratégico.

Ainda, no que se refere à relação do direcionamento estratégico com a gestão de riscos, o COSO-GRC 2007, em seu componente Fixação de Objetivos, indica que “os objetivos devem existir antes que a administração possa identificar os eventos em potencial que poderão afetar a sua realização”. Assim, para estabelecer o gerenciamento de riscos corporativos, é necessário que a organização disponha de um processo de estabelecimento de objetivos que estejam alinhados com a sua missão e sejam compatíveis com o seu apetite a riscos.

Das análises realizadas em relação ao direcionamento estratégico do FNDE, verificou-se que houve estabelecimento formal, por intermédio: do PEI 2018-2022, que formaliza a definição da missão, da visão de futuro e dos valores da Autarquia; do estabelecimento de 20 objetivos

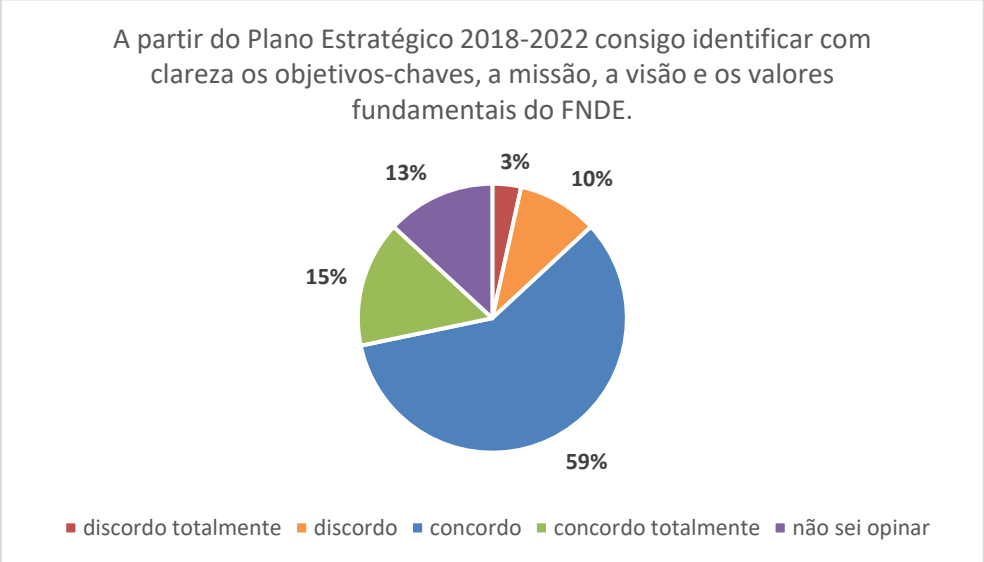
estratégicos; e da definição do Mapa Estratégico[12] para o período 2018-2022 e da Cadeia de Valor[13] da organização.

Destaca-se, no entanto, que foram observadas possibilidades de melhoria nesse objeto, com vistas a contribuir para a integração da gestão de riscos ao processo de planejamento, a saber:

- a partir da análise dos objetivos estratégicos e de suas descrições expostas no PEI-FNDE 2018-2022, da análise do Painel de Acompanhamento dos Indicadores[14], que correlaciona os objetivos estratégicos com indicadores globais, e da análise dos responsáveis pelas metas globais estabelecidos na Portaria FNDE nº 90/2021, pode-se concluir que todas as Diretorias estão vinculadas a pelo menos um objetivo estratégico, o que atende ao disposto no Decreto 10.382/2020. Porém, observou-se que há objetivos sem indicadores associados, a saber: "Assistência técnica aos entes governamentais e demais atores do sistema educacional", "Incentivar a gestão socioambiental", "Otimizar a força de trabalho" e "Promover a gestão de competências"; e
- quanto ao desdobramento do mapa estratégico, verificou-se que o documento desdobra 3 das 4 perspectivas do *Balanced Scorecard* (BSC) recomendadas pelo Guia de Gestão Estratégica[15] (ME): 1. Resultados institucionais (ou "Resultados para a sociedade"); 2. Processos internos; e 3. Aprendizado e crescimento (ou "Infraestrutura e aprendizagem"). Assim, não foi detalhada a perspectiva "Resultados para clientes, usuários, beneficiários e partes interessadas".

Ressalta-se o resultado da percepção coletada junto aos servidores do FNDE, na qual 74% dos respondentes declararam conseguir enxergar com clareza os objetivos-chave, a missão, a visão e os valores fundamentais do FNDE a partir do PEI 2018-2022:

Gráfico 16: Percepção dos servidores – Objetivos estratégicos, missão, visão e valores



Fonte: elaboração própria.

[12] e [14] Disponíveis em: https://www.gov.br/fnde/pt-br/acesso-a-informacao/transparencia-e-prestacao-de-contas-2/relatorio-de-gestao-1/relatorio-de-gestao-2021-1/estrategia.

[13] A Cadeia de Valor passou por processo de atualização em 2022. Destaca-se que a nova versão, validada em julho/2022, ainda não foi disponibilizada no Portal do FNDE.

[15] Destaca-se que a elaboração do PEI é anterior ao Guia Técnico, de 2020, no entanto, a divisão em 4 perspectivas já é tradicional do modelo BSC.

Já em relação à percepção coletada junto à Alta Administra-se, verificou-se que 100% dos respondentes entendem que os objetivos estratégicos do Plano Estratégico 2018-2022 refletem as atividades, processos e projetos desenvolvidos nas suas unidades de atuação. Ainda, 100% "concordaram" ou "concordaram totalmente" que os objetivos estratégicos definidos estão alinhados às finalidades e competências legais de suas unidades.

Como fragilidade identificada e com vistas à melhoria do direcionamento estratégico – especialmente considerando publicação de novo Plano Estratégico no próximo exercício –, cabe destacar que, dada a ausência de um processo estabelecido para gestão de riscos no FNDE (inclusive com a formalização de uma Política sobre o tema), não é possível dizer que há integração do gerenciamento de riscos com a estratégia da organização. Assim, a partir do conteúdo do PEI-FNDE, não foram identificadas iniciativas que levem em consideração o risco no processo de definição da estratégia, conforme recomendado pelo COSO-GRC-EP 2017[16].

Conclui-se, portanto, que a Alta Administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico (objetivos-chave, missão, visão e valores fundamentais da organização), alinhado com as finalidades e as competências legais da entidade. Entretanto, não foi possível identificar práticas de gestão dos riscos relacionadas ao processo de planejamento.

1.2.2. Apetite a risco

A Alta Administração, com a supervisão e a concordância dos responsáveis pela governança, define, comunica, monitora e revisa o apetite a risco?

Com vistas a avaliar este aspecto, foram previstos testes relacionados ao seguinte objeto de análise 1.2.2.1. Definição, comunicação e monitoramento do apetite a risco.

A avaliação realizada mostrou a inexistência da definição do apetite a risco no FNDE. Consequentemente, podem ocorrer prejuízos relacionados a: definição de objetivos por toda a organização; seleção de estratégias para realizá-los; alocação de recursos entre as unidades e iniciativas estratégicas; e identificação entre o planejamento e a gestão de riscos.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

1.2.2.1. Definição, comunicação e monitoramento do apetite a risco

Os testes previstos buscaram avaliar se a Alta Administração define, comunica, monitora e revisa o apetite a risco do FNDE.

Nos termos da IN nº 01/2016, apetite a risco é o "nível de risco que uma organização está disposta a aceitar". O estabelecimento de níveis de exposição a riscos adequados é, conforme o art. 14 do normativo, um princípio a ser observado na gestão de riscos.

[16] Trata especificamente da integração do gerenciamento de riscos corporativos com estratégia e performance.

Ainda, o COSO-GRC-EP 2017 estabelece a definição do apetite a risco e a avaliação de estratégias alternativas dentre os princípios que podem trazer segurança de que a organização é capaz de gerenciar de modo aceitável os riscos associados à sua estratégia e aos seus objetivos.

A organização auditada informou que não foi definido o nível de apetite a risco. Assim, entende-se que esses princípios ainda não estão disseminados pela organização.

Cabe destacar que a definição, a comunicação, o monitoramento e a revisão do apetite a risco, na forma de uma expressão ampla, porém suficientemente clara, de quanto risco a organização está disposta a enfrentar na implementação da estratégia para cumprir sua missão institucional e agregar valor para as partes interessadas, permite orientar: a definição de objetivos por toda a organização; a seleção de estratégias para realizá-los; a alocação de recursos entre as unidades e iniciativas estratégicas; e a identificação e o gerenciamento dos riscos, alinhados com o apetite a risco (TCU, 2018a).

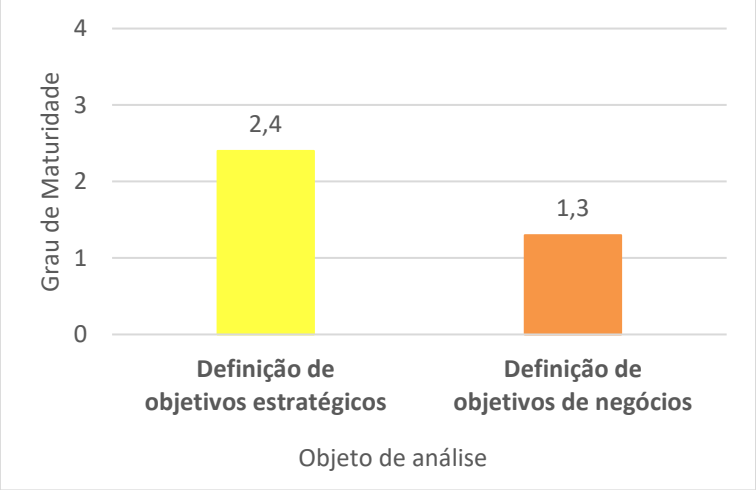
1.2.3. Integração da gestão de riscos ao processo de planejamento

A gestão de riscos é integrada ao processo de planejamento estratégico implementado no FNDE e aos seus desdobramentos?

Com vistas a avaliar este aspecto, foram previstos testes relacionados aos seguintes objetos de análise: 1.2.3.1. Definição de objetivos estratégicos; e 1.2.3.2. Definição de objetivos de negócio.

A avaliação realizada mostrou que houve a definição de objetivos estratégicos de alto nível, alinhados ao direcionamento estratégico para dar suporte à missão, à visão e aos propósitos da organização, especialmente a partir do processo de construção PEI 2018-2022. No entanto, não houve a definição de objetivos de negócios específicos nas categorias operacional, de divulgação e de conformidade. Assim, também não foram definidas as respectivas tolerâncias a risco (ou variações aceitáveis no desempenho), alinhadas aos objetivos estratégicos e ao apetite a risco (que também não foi estabelecido).

Gráfico 17: Resultado da avaliação dos objetos – Aspecto Integração da gestão de riscos ao processo de planejamento



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir dos objetos de análise selecionados:

1.2.3.1. Definição de objetivos estratégicos

Os testes previstos buscaram avaliar se os objetivos estratégicos de alto nível estão alinhados e dão suporte à missão, à visão e aos propósitos da organização e se são selecionadas as estratégias para atingi-los, considerando as várias alternativas de cenários e os riscos associados. Avaliaram, ainda, se esses objetivos são capazes de estabelecer uma base consistente para a definição dos objetivos de negócios específicos em todos os níveis da organização.

Conforme preconizado pelo COSO-GRC 2007, os objetivos devem existir antes que as organizações possam identificar eventos em potencial que afetem a sua realização. Desse modo, a fixação de objetivos é um pré-requisito para o processo de gerenciamento de riscos, ou seja, para a identificação eficaz de eventos, a avaliação de riscos e a resposta aos riscos. Ademais, os objetivos estabelecidos devem estar alinhados com o apetite a risco da organização.

A IN nº 01/2016 estabelece que a estrutura do modelo de gestão de riscos deve observar a fixação de objetivos em todos os níveis da organização e que esses objetivos precisam ser explicitados, comunicados e alinhados à missão e à visão da organização.

Da análise do PEI-FNDE 2018-2022, verificou-se que:

- foram definidos vinte objetivos estratégicos "responsáveis pelo alinhamento entre as diretrizes institucionais e seu referencial estratégico" e que "determinam o que deve ser feito para que a organização cumpra sua missão e alcance sua visão de futuro";
- além disso, de acordo com a organização, esses objetivos "traduzem os desafios a serem enfrentados pelo FNDE no cumprimento do papel institucional que lhe é reservado" e sua comunicação é feita por intermédio do próprio PEI e do Mapa Estratégico do FNDE;
- foram utilizados mecanismos para alinhar os objetivos estratégicos ao direcionamento estratégico. Um desses mecanismos foi a utilização do instrumento *Balanced Scorecard* (BSC). Segundo o PEI-FNDE, o BSC "tem por objetivo traduzir o caminho (estratégia) para se alcançar a visão do futuro e realizar a missão", por intermédio da articulação dos objetivos em perspectivas (Resultados Institucionais; Processos internos; e Aprendizado e Crescimento); e
- foram definidos metas e indicadores para mensuração dos objetivos estratégicos. Ainda, conforme demonstrado nos testes feitos no aspecto 1.1.3, o FNDE definiu indicadores de desempenho com vistas à aferição do desempenho institucional, tendo sido definidas metas globais e intermediárias para 2021 e 2022, bem como índices a serem atingidos em cada período para todas as Diretorias/equivalentes.

No entanto, a organização auditada informou que não existem planos de ação ou outros mecanismos/estratégias formalmente definidos para garantir o atingimento dos objetivos estratégicos. Entende-se que a existência desses planos tende a contribuir para a eficácia e a efetividade do planejamento estratégico.

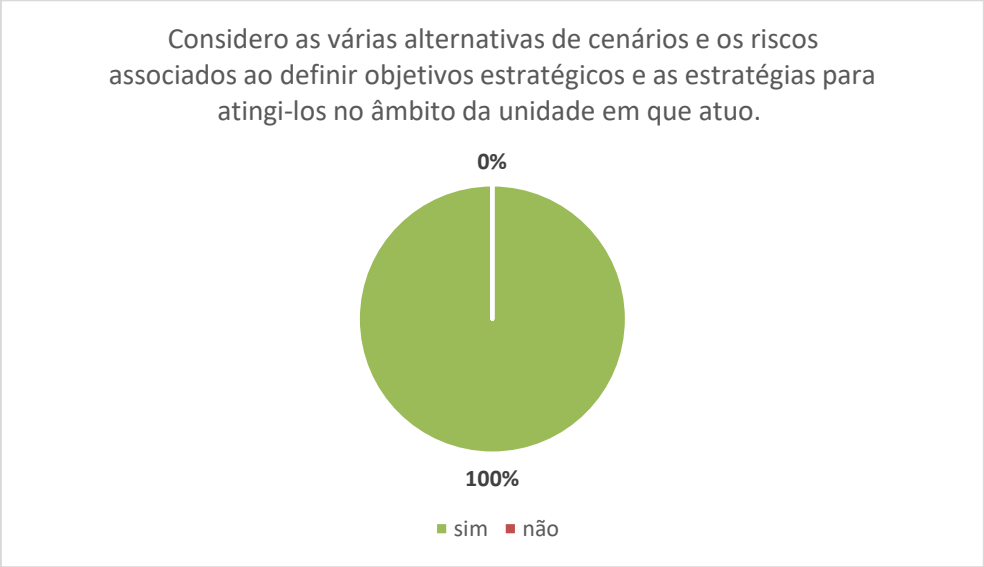
Ainda, verificou-se que não existe no âmbito da Autarquia um sistema específico para a gestão da estratégia, dada a descontinuidade do Portal da Estratégia. A existência de uma

ferramenta/sistema também tende a contribuir para a execução do planejamento estratégico e sua ausência pode prejudicar o acompanhamento das ações correlatas ao atingimento desses objetivos.

Adicionalmente, dado que não foi definido o apetite a risco do FNDE, conforme exposto no tópico 1.2.2.1, os objetivos estratégicos atualmente existentes não levam em consideração a definição de quanto risco a Autarquia está disposta a assumir na realização de seus objetivos. Sobre o tema, a organização indicou que não houve identificação de riscos relacionados aos objetivos estratégicos e que, na prática, tem-se optado trabalhar por projetos, nos quais são identificados riscos relacionados à sua execução.

Em relação à percepção coletada junto à Alta Administração, 100% dos respondentes afirmaram que consideram as várias alternativas de cenários e os riscos no processo de definição de objetivos estratégicos de suas unidades de atuação:

Gráfico 18: Percepção da Alta Administração – Definição de objetivos estratégicos



Fonte: elaboração própria.

Adicionalmente, destaca-se do Relatório de Gestão do FNDE (2021) que:

> *O FNDE vem enfrentando muitos desafios nas suas diferentes áreas de atuação. Um deles, que de certo modo se assemelha ao de outras grandes organizações, inclusive governamentais, é a implantação de uma gestão estratégica voltada para potencializar o resultado. Para que isso ocorra faz-se necessário o correto e tempestivo desdobramento das estratégias gerenciais com o seu permanente monitoramento e contínuas correções dos desvios e das não conformidades. Assim, este é o grande desafio para os próximos exercícios: gestão estratégica monitorada e articulada com os níveis tático e operacional e voltada para resultados.*

Conclui-se, portanto, apesar da definição dos objetivos estratégicos de alto nível, não foram definidas estratégias para atingi-los, considerando as várias alternativas de cenários e os riscos associados, de modo a estabelecer uma base consistente para a definição dos objetivos de negócios específicos em todos os níveis da organização. Tal situação, prejudica a integração da gestão de riscos ao planejamento estratégico da organização.

1.2.3.2. Definição de objetivos de negócio

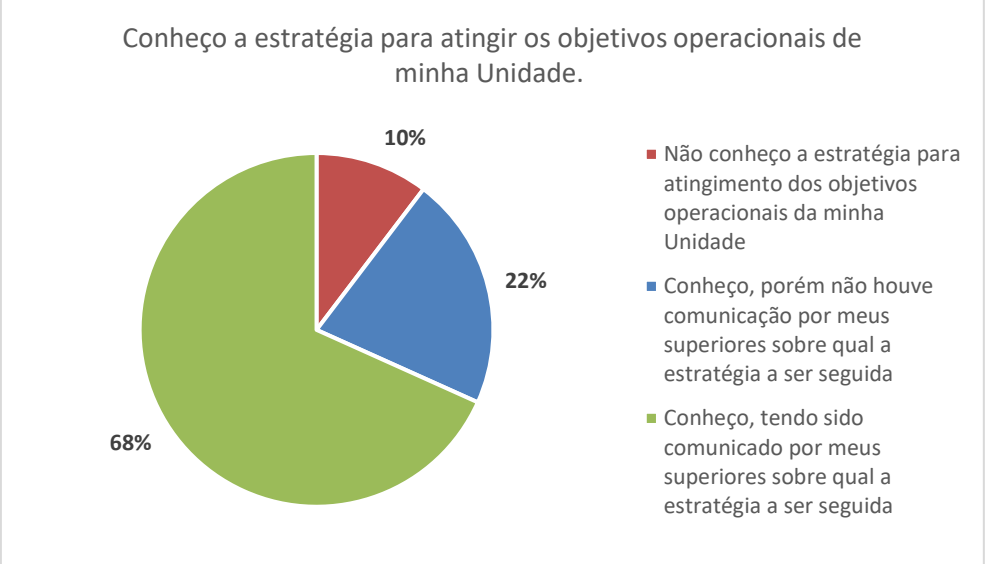
Os testes previstos buscaram avaliar se há objetivos de negócios específicos associados a todas as atividades, em todos os níveis, nas categorias operacional, de divulgação (transparência e prestação de contas) e de conformidade e as respectivas tolerâncias a risco (ou variações aceitáveis no desempenho), bem como se há alinhamento dos objetivos de negócio aos objetivos estratégicos e ao apetite a risco estabelecidos.

De acordo com o COSO ERM 2007, a partir da fixação de objetivos estratégicos, tem-se uma base para a fixação dos objetivos correlatos (de negócio). Esses dividem-se em:

> ***Objetivos Operacionais*** *– relacionam-se com a eficácia e a eficiência das operações da organização, inclusive metas de desempenho e de lucro, bem como reservas de recursos contra prejuízos. Variam de acordo com a decisão da administração em relação à estrutura e ao desempenho.*
>
> ***Objetivos de Comunicação*** *– relacionam-se com a confiabilidade dos relatórios. Incluem relatórios internos e externos e podem, ainda, conter informações financeiras e não financeiras.*
>
> ***Objetivos de Conformidade*** *– relacionam-se com o cumprimento de leis e regulamentos. Em alguns casos dependem de fatores externos e tendem a ser semelhantes em todas as organizações, e em outros casos em todo um setor industrial.*

Da percepção coletada, observou-se que 91% dos servidores "concordaram" ou "concordaram totalmente" que as ações desenvolvidas em sua unidade são direcionadas para o atingimento de objetivos previamente definidos. Além disso, 68% afirmaram conhecer a estratégia para atingimento dos objetivos operacionais de sua unidade. Ainda, 75% dos servidores disseram conhecer e terem sido comunicados acerca dos objetivos operacionais de sua unidade, enquanto 19% dizem conhecer, mas sem terem sido comunicados:

Gráfico 19: Percepção dos servidores – Definição de objetivos de negócio



Fonte: elaboração própria.

Já a partir da análise documental realizada, verificou-se que o FNDE não desdobrou formalmente os objetivos estratégicos em objetivos de negócio, por exemplo nas categorias operacional, de divulgação e de conformidade, o que seria uma boa prática conforme o COSO-CI e o COSO-GRC e uma obrigação dada pela IN 01/2016, art. 16, II.

Verificou-se que o PEI foi associado a um Portfólio de Projetos Estratégicos, no entanto, não se pode dizer que estes projetos sejam um desdobramento dos objetivos estratégicos em objetivos de negócio da organização. Em decorrência, também não foram definidas as respectivas tolerâncias a risco (ou variações aceitáveis no desempenho), alinhadas aos objetivos estratégicos e ao apetite a risco (que também não foi estabelecido).

Pelo exposto, entende-se que os objetivos estratégicos definidos no PEI 2018-2022 carecem de desdobramento em objetivos de negócio associados a todas as atividades e níveis da organização, considerando as categorias relevantes (operacional, divulgação e conformidade). Cabe, ainda, quando da definição de tais objetivos, considerar além dos objetivos estratégicos o apetite a risco, de modo a permitir que se identifiquem situações em potencial que podem afetar a realização da estratégia.

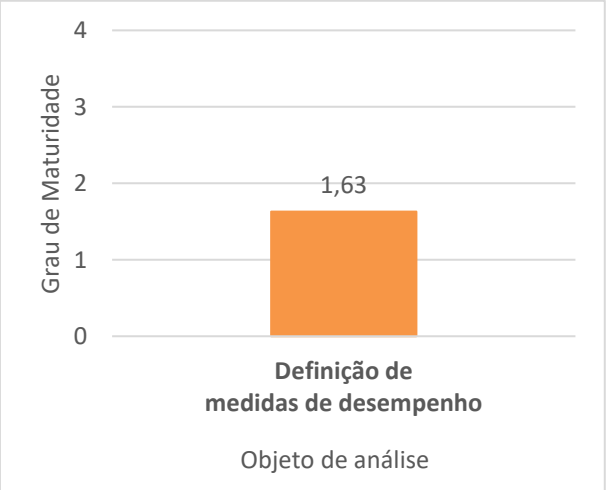
1.2.4. Medidas de desempenho

A administração define e comunica os objetivos e as respectivas medidas de desempenho em termos específicos e mensuráveis?

Com vistas a avaliar este aspecto, foram previstos testes relacionados ao seguinte objeto de análise: 1.2.4.1. Definição de medidas de desempenho.

A avaliação realizada mostrou que foram definidos os objetivos estratégicos da organização e as respectivas medidas de desempenho. No entanto, observaram-se fragilidades relacionadas ao objeto analisado, especialmente no tocante à articulação do nível estratégico com os níveis tático e operacional. Ademais, dado que não foram estabelecidos objetivos de negócio, não houve o estabelecimento de medidas de desempenho no que se refere às categorias operacional, de conformidade e de divulgação.

Gráfico 20: Resultado da avaliação dos objetos – Aspecto Medidas de desempenho



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

1.2.4.1. Definição de medidas de desempenho

Os testes previstos buscaram avaliar se, além dos objetivos estratégicos e de negócios, a administração define as respectivas medidas de desempenho, explicitando-as com clareza suficiente, em termos específicos e mensuráveis, e comunicando-as a todas as áreas, funções e atividades relevantes para a realização dos objetivos-chave da organização e aos responsáveis em todos os níveis, a fim de permitir a identificação e avaliação dos riscos que possam ter impacto no desempenho e nos objetivos.

Nos termos do artigo 3º, da IN ME 24/2020:

> *O plano estratégico institucional dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional deverá conter, no mínimo, os seguintes elementos: [...]*
> *III - objetivos estratégicos e respectivas metas;*
> *IV - indicadores, com seus atributos: fórmula de cálculo, periodicidade de medição, linha de base e metas; e*
> *V - projetos estratégicos a serem desenvolvidos, com seus atributos: principais entregas, com prazos e unidade responsável.*
> *Parágrafo único. Os elementos descritos no caput poderão constar do próprio plano estratégico institucional ou de outro plano que o desdobre, como o plano de gestão anual, previsto no art. 18 da Lei nº 13.848, de 25 de junho de 2019.*

A necessidade de estabelecimento de medidas de desempenho é abordada também por meio do COSO-GRC 2007, que ressalta sua importância para garantir que os resultados obtidos estejam dentro dos limites estabelecidos pela tolerância a risco. Já a norma ISO 31000:2018 destaca que a Alta Direção e os órgãos de supervisão, como demonstração de seu comprometimento com a gestão de riscos, devem promover a medição e o relato de indicadores de desempenho da organização.

A análises realizadas mostraram que o FNDE definiu objetivos estratégicos, por intermédio de seu Plano Estratégico Institucional (PEI 2018-2022), que expõe os 20 objetivos estratégicos que guiarão o ciclo, bem como os projetos estratégicos a serem desenvolvidos. Em relação às medidas de desempenho, ressalta-se que:

- houve a definição de indicadores, metas e fórmulas de cálculo para todos os objetivos estratégicos – inicialmente por intermédio do PEI e, posteriormente, com atualização por intermédio da Portaria FNDE 90/2021 –, em conformidade com a IN ME 24/2020, art. 3º, e o Guia Técnico de Gestão Estratégica (SEGES/ME);
- o acompanhamento dos indicadores é efetuado por intermédio de apurações periódicas e disponibilização de um Painel de Indicadores no site do FNDE, o qual correlaciona os objetivos estratégicos com indicadores globais definidos no âmbito da Portaria FNDE nº 90/2021; e
- foi estabelecido no PEI um portfólio de projetos estratégicos, com a lista dos projetos que o FNDE deverá implementar no âmbito do seu Planejamento Estratégico e com a indicação dos objetivos de cada um deles.

No entanto, observaram-se fragilidades em relação às medidas de desempenho dos objetivos estratégicos:

- para o objetivo “Otimizar a força de trabalho”, não foram associadas metas;
- para os indicadores existentes, não foram apresentadas linhas de base; e
- para os projetos estratégicos, não foram apresentados no PEI as principais entregas, os prazos e as unidades responsáveis, conforme preconiza a IN nº 24/2020.

Destaca-se também que a ausência de um sistema específico de gestão da estratégia prejudica o acompanhamento das medidas de desempenho definidas. Ainda, as limitações apresentadas no objeto 1.1.3.1 indicam desafios no monitoramento e na articulação do nível estratégico com os níveis tático e operacional, bem como na vinculação entre metas globais e intermediárias e metas individuais de desempenho.

Além disso, verificou-se que não foi dada a devida transparência à atualização dos indicadores e metas no site do FNDE. O Portal não informa acerca da atualização dos indicadores do PEI para os indicadores da Portaria 90/2021 e o Painel não traz os indicadores apurados nos exercícios de 2018 a 2020.

Em relação aos objetivos de negócio, dado que não houve sua definição, não há medidas de desempenho relacionadas. Assim, entende-se a necessidade de que o próximo planejamento estratégico seja desdobrado em objetivos operacionais, de conformidade e de comunicação, em atendimento às boas práticas recomendadas pelo COSO-GRC 2007 e às orientações da IN 01/2016, art. 16, II.

Por fim, como não foram definidos indicadores-chave de risco e apetite a risco, não existem medidas de desempenho que auxiliem a identificar se os resultados efetivamente obtidos estão dentro dos limites de tolerância a risco estabelecidos.

1.2.5. Política de Gestão de Riscos

O FNDE dispõe de uma política de gestão de riscos estabelecida e aprovada pela Alta Administração, apropriadamente comunicada, abordando todos os aspectos relevantes?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à avaliação da Política de Gestão de Riscos do FNDE, caso existente, ou à avaliação de outros documentos que pudessem fornecer o direcionamento da organização para abordar o risco. Assim foram selecionados cinco objetos de análise relacionados a aspectos essenciais de uma política/diretriz sobre o tema, a saber: 1.2.5.1. Princípios e objetivos; 1.2.5.2. Diretrizes para a integração; 1.2.5.3. Responsabilidades, competências e autoridades; 1.2.5.4. Plano de implementação; 1.2.5.5. Reporte; e 1.2.5.6. Monitoramento.

A avaliação realizada mostrou que a organização não dispõe de Política de Gestão de Riscos aprovada, nem de outro documento equivalente, descumprindo assim o art. 17 da Instrução Normativa MP/CGU nº 01, de 10 de maio de 2016, que estabelece que:

> *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.*

Conforme já abordado no aspecto Cultura (na análise do objeto 1.1.1.2), a ausência dessa Política também prejudica o adequado comprometimento das lideranças com a cultura de gestão de riscos e, consequentemente, fragiliza a integração da gestão de riscos por toda a organização e em todas as atividades relevantes para a consecução de seus objetivos.

Nesse sentido, a ISO 31000:2018, ao estabelecer diretrizes sobre a gestão de riscos, destaca sobre a articulação e o comprometimento com a gestão de riscos:

> *Convém que a Alta Direção e os órgãos de supervisão, onde aplicável, demonstrem e articulem o seu comprometimento contínuo com a gestão de riscos por meio de uma política, uma declaração ou outras formas que claramente transmitam os objetivos e o comprometimento com a gestão de riscos de uma organização.*

Dada a ausência de uma Política no âmbito do FNDE ou outro documento equivalente, os objetos de análise associados também foram avaliados como inexistentes. Os tópicos a seguir trazem informações e boas práticas relacionadas ao conteúdo mínimo necessário a ser observado na elaboração de uma declaração ou política que estabeleça a abordagem da gestão de riscos da organização:

1.2.5.1. Aspectos da Política de Gestão de Riscos – Princípios e objetivos

De acordo com o inciso I, do art. 17, da IN nº 01/2016, a Política de Gestão de Riscos deve especificar os princípios e objetivos organizacionais. Isso significa declarar formalmente "o propósito da organização para gerenciar riscos e vínculos com seus objetivos e outras políticas" (ISO 31000:2018).

Destaca-se que os *frameworks* costumam abordar os princípios fundamentais para a gestão de riscos:

- o COSO-GRC 2007 lista princípios para cada um dos oito componentes da estrutura;
- a ISO 31000:2018 aborda em sua estrutura sete princípios para uma gestão de riscos eficaz; e
- o *Orange Book* elenca os princípios que devem ser seguidos para o gerenciamento efetivo de riscos, atrelando esses princípios aos seus componentes e às etapas do processo de gestão de riscos.

Assim, dado que a gestão de riscos precisa ser personalizada para cada organização, considerando seu porte e seus objetivos, as orientações desses *frameworks* poderão ser utilizadas quando da elaboração da Política de Gestão de Riscos do FNDE.

1.2.5.2. Aspectos da Política de Gestão de Riscos – Diretrizes para a integração

De acordo com o inciso II, do art. 17, da IN nº 01/2016, a Política de Gestão de Riscos deve especificar diretrizes sobre: como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização; como e com qual periodicidade os riscos serão identificados, avaliados, tratados e monitorados; como será medido o desempenho da gestão de riscos; a metodologia e as ferramentas que irão apoiar a gestão de riscos; e o desenvolvimento contínuo dos agentes que irão atuar com esse tema.

Especialmente no que se refere às diretrizes para a integração, destaca-se que, para que a gestão de riscos prospere, ela precisa ser integrada em todos os processos organização, incluindo o planejamento estratégico, os projetos e as políticas de gestão em todos os níveis da organização, bem como nas parcerias[17] com outras organizações.

Sobre esse ponto, a ISO 31000:2018 recomenda:

- que o comprometimento da Alta Administração com a gestão de riscos inclua o reforço da necessidade de integrar a gestão de riscos na cultura global da organização; e
- que a gestão de riscos seja uma parte (e não separada) do propósito organizacional, da governança, da liderança e do comprometimento, da estratégia, dos objetivos e das operações.

Além disso, o COSO-GRC-EP 2017 trata especificamente da integração do gerenciamento de riscos com a estratégia e a performance, ressaltando a importância de se considerar o risco tanto no processo de definição de estratégias quanto na melhoria da performance da organização. Destaca, ainda que essa integração constrói organizações mais fortes e resilientes, na medida em que, ao conhecer os riscos de maior impacto, a entidade pode usar a gestão de riscos para criar competências que permitam sua atuação com antecedência, além de criar novas oportunidades.

1.2.5.3. Aspectos da Política de Gestão de Riscos – Responsabilidades, competências e autoridades

De acordo com o inciso III, do art. 17, da IN nº 01/2016, a Política de Gestão de Riscos deve tratar das competências e responsabilidades para a efetivação da gestão de riscos no âmbito da organização. Complementarmente, o art. 19 estabelece que o dirigente máximo é o principal responsável pelo estabelecimento da estratégia e da estrutura de gerenciamento de riscos; e o art. 20 define que cada risco mapeado e avaliado deve ser associado a um agente responsável (gestor de risco) formalmente identificado. Por fim, a IN trata em seu art. 22 do Comitê de Governança, Riscos e Controle, cujas competências incluem a promoção da integração dos agentes responsáveis pela gestão de riscos

[17] A ser tratado no aspecto 3.1 (dimensão Parcerias) do presente Relatório.

Conforme já abordado no tópico 1.1.2.1 existem instâncias que podem apoiar as responsabilidades de governança de riscos, mas para as quais não foi identificado funcionamento. Tal fragilidade decorre principalmente do fato de não existir uma Política de Gestão de Riscos que defina responsabilidades, competência e autoridades, bem como as diretrizes fundamentais para que as pessoas da organização exerçam seus papéis de gerenciamento de riscos.

A ISO 31000:2018 também ressalta que a atribuição de papéis organizacionais, autoridade, responsabilidades e responsabilizações é uma forma de a Alta Direção e os órgãos de governança demonstrarem seu comprometimento com a gestão de riscos.

Assim, eventual Política de Gestão de Riscos do FNDE deve incluir responsabilidades, competências e autoridade para gerenciar riscos no âmbito da organização como um todo e em todas as suas áreas, incluindo a responsabilidade pela implementação e manutenção do processo de gestão de riscos e de asseguração da suficiência, eficácia e eficiência de controles internos.

1.2.5.4. Aspectos da Política de Gestão de Riscos – Plano de implementação

De acordo com o inciso II, b, do art. 17, da IN nº 01/2016, devem ser definidas diretrizes sobre como e com qual periodicidade os riscos serão identificados, avaliados, tratados e monitorados. Isso pode ser feito a partir de um plano de implementação do processo de gestão de riscos, que deve abordar todos os níveis, funções e processos relevantes da organização. Esse ponto também é reforçado pela ISO 31000:2018, que indica que deve ser desenvolvido um plano apropriado, incluindo prazos e recursos.

Em *benchmarking* realizado ao longo da construção da presente avaliação de maturidade identificou-se que algumas organizações costumam elaborar planos periódicos (bienais ou quadrienais, por exemplo) que traduzam as diretrizes e os objetivos de suas políticas em ações práticas, incluindo cronograma de atividades e unidades organizacionais ou agentes responsáveis.

Assim, além da elaboração da Política de Gestão de Riscos do FNDE, considera-se uma boa prática a definição de planos de implementação, além da sua disseminação por toda a organização, de seu monitoramento periódico e da sua revisão sempre que necessário (com base nas informações decorrentes dos processos de gestão de riscos).

1.2.5.5. Aspectos da Política de Gestão de Riscos – Reporte

De acordo com o inciso II, c, do art. 17, da IN nº 01/2016, devem ser definidas diretrizes sobre como será medido o desempenho da gestão de riscos. Esse ponto também é reforçado pela ISO 31000:2018, que ressalta que o comprometimento com a gestão de riscos deve incluir a medição e o relato no âmbito de indicadores de desempenho da organização.

Conforme será abordado no tópico 2.3.1 (dimensão Processos) deste Relatório, a informação e a comunicação são dois importantes aspectos da estrutura de gestão de riscos. Isso porque é preciso que a organização disponha de informações pertinentes, obtidas de fontes internas e externa, que auxiliem as pessoas a exercerem suas responsabilidades de gerenciamento de riscos e de gestão, bem como disponha de canais e fluxos para que a comunicação flua por toda a organização.

Por isso, é importante que a organização, quando da implementação de sua Política de Gestão de Riscos, defina como serão medidos e reportados às instâncias adequadas: a adequação da estrutura, a aplicação do processo de gestão de riscos e a efetividade da política.

1.2.5.6. Aspectos da Política de Gestão de Riscos – Monitoramento

De acordo com o inciso VIII, do art. 16, da IN nº 01/2016, o monitoramento é um dos componentes da estrutura do modelo de gestão de riscos a ser implementado pelos órgãos e entidades do Poder Executivo federal. Seu objetivo é "avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes". Assim, busca-se obter segurança razoável de que a gestão de riscos e os controles internos funcionem como previsto e que sejam apropriadamente modificados quando necessário (como, por exemplo, a partir de mudanças que alterem o nível de exposição a riscos).

Esse ponto também é reforçado pela ISO 31000:2018, que recomenda que "o monitoramento contínuo e análise crítica periódica do processo de gestão de riscos e seus resultados sejam uma parte planejada do processo de gestão de riscos, com responsabilidades claramente estabelecidas".

Assim, aliado ao componente informações e comunicações, outro componente que precisa ser estabelecido na Política de Gestão de Riscos é o monitoramento, por intermédio de definição explícita de competências e responsabilidades pelo monitoramento, análise crítica e melhoria contínua da gestão de riscos, bem como das diretrizes sobre a forma e a periodicidade relacionadas a como as alterações devem ser efetivadas.

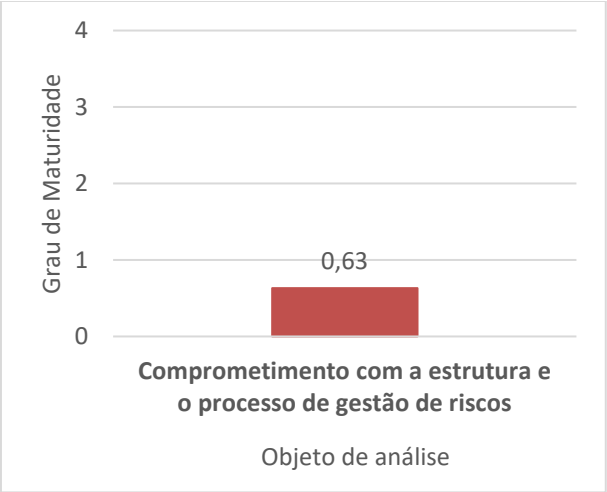
1.2.6. Comprometimento da gestão

Toda a gestão do FNDE é comprometida com a gestão de riscos?

Com vistas a avaliar este aspecto, foram previstos testes relacionados ao seguinte objeto de análise: 1.2.6.1. Comprometimento com a estrutura e o processo de gestão de riscos.

A avaliação realizada mostrou que, apesar da existência de ações pontuais, não há adequado comprometimento, por parte de toda a gestão, com o processo de gestão de riscos, principalmente em decorrência da ausência de uma Política de Gestão de Riscos aprovada e disseminada pela Autarquia.

Gráfico 21: Resultado da avaliação dos objetos – Aspecto Comprometimento da gestão



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

1.2.6.1. Comprometimento com a estrutura e o processo de gestão de riscos

Os testes previstos buscaram avaliar se Alta Administração e o corpo executivo da gestão (tática e operacional) estão completa e diretamente envolvidos em estabelecer e rever a estrutura e o processo de gestão de riscos e controles internos no âmbito de suas respectivas áreas de responsabilidade.

Acerca da estrutura de gestão de riscos, o COSO-GRC 2007 esclarece a importância da definição de áreas fundamentais de responsabilidade. Esclarece, ainda, que todos os membros da organização possuem responsabilidade pela gestão de riscos: a diretoria atribui a responsabilidade pelos procedimentos específicos de gestão de riscos corporativos aos gerentes de processos, funções ou departamentos; estes, por sua vez, exercerão um papel mais prático no planejamento e na execução do gerenciamento de riscos, além de fazer recomendações referentes a atividades de controle relacionadas, monitorar sua aplicação e relatar aos diretores o funcionamento das atividades de controle.

Dado que o FNDE não possui uma Política de Gestão de Riscos ou outra diretriz que subsidie a implementação de processos de gestão de riscos, o comprometimento da Alta Administração e do corpo executivo da gestão resta prejudicado em relação ao estabelecimento e à revisão da estrutura e do processo de gestão de riscos e controles internos no âmbito de suas respectivas áreas de responsabilidade.

Ainda, conforme destacado no tópico 1.1.2.1, não existem pessoas alocadas especificamente para a realização de atividades de gestão de riscos (“gestores de riscos”), o que também prejudica o comprometimento com a gestão de riscos.

Foram identificadas, no entanto, algumas iniciativas pontuais e esporádicas que demonstram uma intenção da gestão no tema gestão de riscos, dentre outras: o projeto Malha Fina, no âmbito da DIFIN; a construção de Mapas de Gerenciamento de Riscos, no âmbito de processos

licitatórios conduzidos pela DIRAD; e a designação de competências regimentais para gerenciamento de riscos no âmbito da DIRTI. Destaca-se, porém, que, na ausência de uma diretriz/política sobre o tema, a condução dessas ações não é integrada e não é vinculada a um processo formalizado e padronizado de gestão de riscos do FNDE.

Nesse contexto, 51% dos servidores não concordam que a Alta Administração demonstra um compromisso adequado com a cultura de gestão baseada em riscos e com os valores fundamentais da organização, conforme já relatado no tópico 1.1.1.2. Nesse contexto, destaca-se que eventuais mecanismos para reforçar o comprometimento com a gestão de riscos deverão ser previstos e associados aos controles internos da organização, por intermédio de políticas e estratégias colocadas em prática. Os Comitês de Governança, Riscos e Controles, por exemplo, possuem papéis fundamentais de segunda linha que ajudam a fomentar esse comprometimento, conforme será abordado no aspecto 1.3 deste relatório.

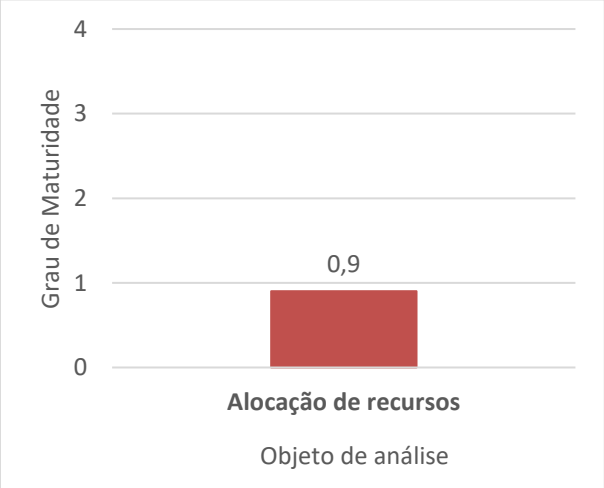
1.2.7. Alocação de recursos

A administração aloca recursos suficientes e apropriados para a gestão riscos?

Com vistas a avaliar este aspecto, foram previstos testes relacionados ao seguinte objeto de análise: 1.2.7.1. Alocação de recursos para a gestão de riscos.

A avaliação realizada mostrou que o FNDE não aloca recursos suficientes e apropriados (pessoas, estruturas, sistemas, métodos, treinamento e ferramentas) para a gestão de riscos.

Gráfico 22: Resultado da avaliação dos objetos – Aspecto Alocação de recursos



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

1.2.7.1. Alocação de recursos para a gestão de riscos

Os testes previstos buscaram avaliar se o FNDE aloca recursos suficientes e apropriados para a gestão de riscos, considerando uma relação equilibrada com o tamanho da organização, a relevância das áreas, funções e atividades críticas para a realização dos seus objetivos-chave, bem como com a natureza e o nível dos riscos.

Quanto a esse tema, a ISO 31000:2018 indica que a Alta Direção e os órgãos de supervisão devem assegurar a alocação de recursos apropriados para a gestão de riscos e cita que esses recursos podem incluir, mas não estão limitados a:

> *- pessoas, habilidades, experiência e competência;*
> *- processos, métodos e ferramentas da organização a serem usados na gestão de riscos;*
> *- processos e procedimentos documentados;*
> *- sistemas de gestão de informação e do conhecimento;*
> *- necessidades de treinamento e desenvolvimento profissional.*

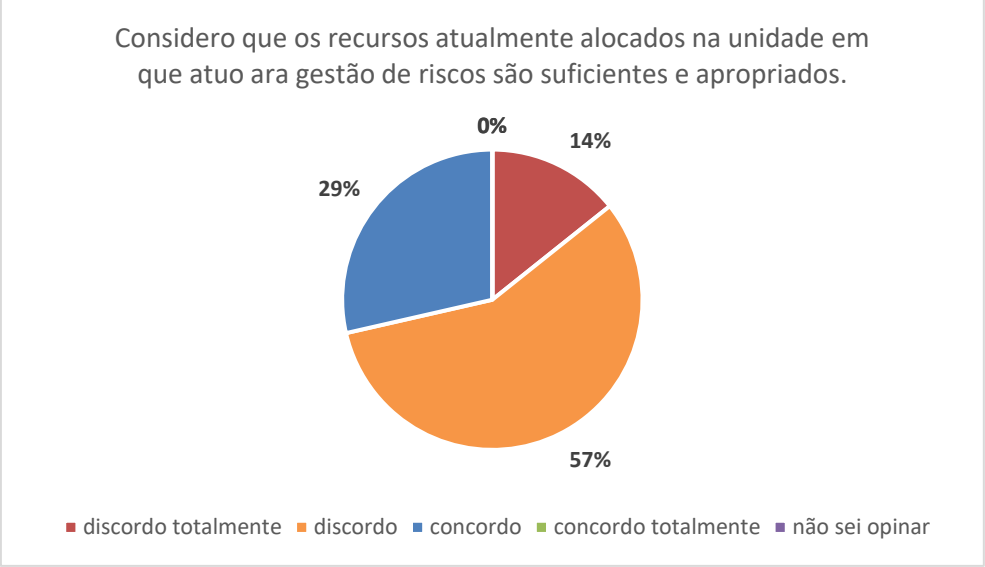
Da análise realizada, observou-se que o FNDE não aloca recursos suficientes e adequados para a gestão de riscos, especialmente devido a:

- não alocação de pessoas específicas para a realização de atividades de gestão de riscos;
- não existência de sistemas de tecnologia da informação ou de ferramentas que auxiliem no gerenciamento de riscos;
- não existência de metodologias, políticas e procedimentos formalizados para a gestão de riscos; e
- não alocação de recursos orçamentários para execução de atividades de gestão de riscos.

A percepção da Alta Administração mostrou que 71% dos dirigentes que responderam ao questionário aplicado afirmaram que não há servidores alocados especificamente para a realização de atividades de gestão de riscos e que não existem ferramentas para auxiliar na gestão de riscos de suas unidades. Ainda, 57% afirmaram que, na unidade em que atuam, não são desenvolvidas ações para fomento da gestão de riscos, como programas de treinamento e reuniões de alinhamento.

Questionados se consideram que os recursos atualmente alocados na unidade em que atuam para gestão de riscos são suficientes e apropriados, apenas 29% dos gestores manifestaram concordância com a assertiva, conforme gráfico a seguir:

Gráfico 23: Percepção da Alta Administração – Alocação de recursos para a gestão de riscos



Fonte: elaboração própria.

Assim, verifica-se que não existem pessoas, recursos, ferramentas e metodologias especificamente alocados para a gestão de riscos. Apesar disso, foi informado pela organização auditada que existem algumas iniciativas, como por exemplo linhas específicas dentro de projetos de cooperação internacional e sistemas que podem fornecer informações para subsidiar atividades de identificação, análise e avaliação de riscos. Destaca-se, no entanto, que são iniciativas pontuais e esparsas, não vinculadas a uma diretriz da organização no âmbito de um processo estruturado para a gestão de riscos.

Além disso, há que se considerar a importância de se coordenarem os esforços por toda a organização, de modo a evitar a sobreposição de eventuais alocações de recursos (por exemplo, a utilização de diversos sistemas para gestão de riscos no âmbito de diferentes unidades, sem que haja integração).

1.3. Pessoas

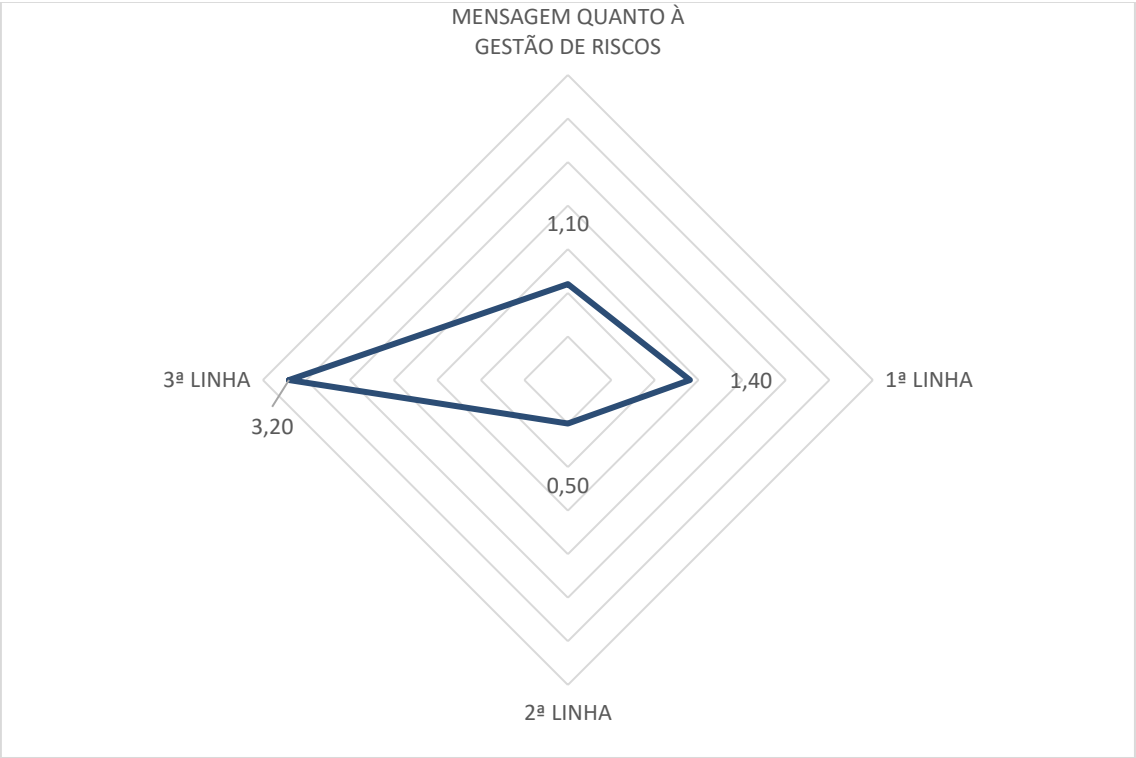
Nesse componente, apurou-se: em que medida as pessoas que atuam no FNDE entendem seus papéis e responsabilidades relacionados à gestão de riscos e estão preparadas exercê-los?

Buscou-se, para tanto, avaliar se as pessoas na organização estão informadas, habilitadas e autorizadas para exercer os seus papéis e as suas responsabilidades no gerenciamento de riscos e controles; se entendem esses papéis e os limites de suas responsabilidades; e se enxergam como os seus cargos se encaixam na estrutura de gerenciamento de riscos e controle interno da organização. A avaliação do componente foi feita a partir de dois aspectos: 1.3.1. Reforço da *accountability* e 1.3.2. Estrutura de gerenciamento de riscos e controles.

No FNDE, o resultado do componente “Pessoas”, a partir da avaliação dos seus aspectos, demonstra uma maturidade **BÁSICA**, apurada em **26,67%**.

O gráfico a seguir apresenta o resultado consolidado do componente, a partir dos resultados apurados dos objetos analisados:

Gráfico 24: Resultado da avaliação dos objetos – Componente Pessoas



Fonte: elaboração própria.

A partir do gráfico 24, percebe-se que a primeira e a segunda linhas preconizadas pelo Modelo de 3 Linhas[18] (IIA, 2020) não estão plenamente desenvolvidas para exercerem seus papéis no gerenciamento de riscos. Além disso, a gestão transmite uma mensagem ainda inicial sobre a importância da gestão de riscos, isto é, de maneira informal e esporádica, sem conseguir garantir que a comunicação flua por todas as áreas relevantes da organização.

A seguir apresentam-se os aspectos avaliados no componente Pessoas, bem como os objetos relacionados a cada aspecto:

1.3.1. Reforço da *accountability*

A gestão transmite uma mensagem clara quanto à importância de se levar a sério as responsabilidades de gerenciamento riscos e o pessoal recebe orientação e capacitação suficiente para exercer essas responsabilidades?

Com vistas a avaliar este aspecto, foram previstos testes relacionados ao objeto de análise 1.3.1.1. Mensagem da Gestão quanto à gestão de riscos.

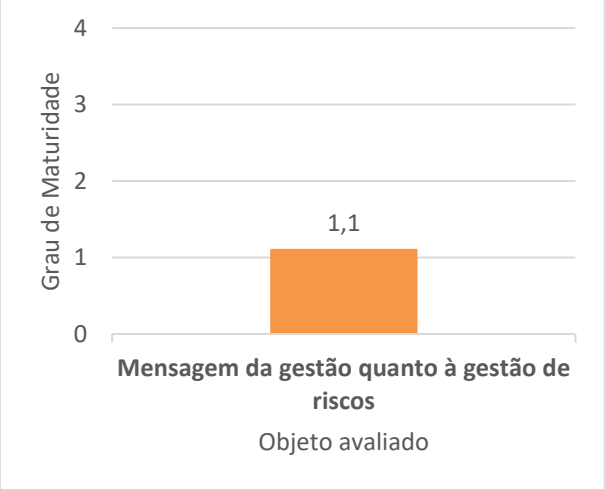
[18] Anteriormente conhecido como Três Linhas de Defesa, é um modelo que auxilia as organizações a identificarem "estruturas e processos que melhor auxiliam no atingimento dos objetivos e facilitam uma forte governança e gerenciamento de riscos". A primeira linha está mais relacionada com os papéis de entrega de produtos e/ou serviços, incluindo funções de apoio. A segunda linha, com o fornecimento de assistência no gerenciamento de riscos. A terceira linha, por sua vez, é representada pela Auditoria Interna e a prestação de serviços de avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos.

Nos termos da ISO 31000:2018, a Alta Direção e os órgãos de governança devem assegurar que a gestão de riscos seja integrada na organização, incluindo, dentre outros mecanismos, o estabelecimento de uma Política de Gestão de Riscos e a atribuição de responsabilidade e responsabilização.

Essa responsabilização (*accountability*[19]) traduz-se na "responsabilidade por ações e atos" (ISO 31000:2018). Para que a gestão de riscos tenha condições de prosperar, é necessário dividir os papéis: a Alta Administração é responsabilizada por gerenciar riscos, enquanto os órgãos de governança são responsabilizados por supervisionar a gestão de riscos. Para tanto, é preciso assegurar que a informação sobre a gestão de riscos seja apropriadamente comunicada por todos os níveis da organização.

A avaliação realizada mostrou que o FNDE não transmite uma mensagem clara quanto à importância da gestão de riscos. A incipiência do modelo de governança, a ausência de Política de Gestão de Riscos e a não atuação das estruturas formalizadas prejudicam esse aspecto e têm reflexos na maturidade das linhas que apoiam a gestão de riscos.

Gráfico 25: Resultado da avaliação dos objetos – Aspecto Reforço da *accountability*



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

1.3.1.1. Mensagem da gestão quanto à gestão de riscos

Os testes previstos buscaram avaliar se todo o pessoal na organização, incluindo prestadores de serviço e outras partes relacionadas, recebe uma mensagem clara da gestão quanto à importância de se levar a sério suas responsabilidades de gerenciamento riscos, bem como se é orientado e se sabe como proceder para encaminhar assuntos relacionados a risco às instâncias pertinentes.

[19] O termo "*accountability*" foi traduzido na ISO 31000:2018 como "responsabilização", com o sentido de prestação de contas. Assim, o termo "*accountable*" é entendido como "responsabilizado".

A norma ISO 31000:2018 indica que a Alta Direção e os órgãos de supervisão devem emitir uma declaração ou política que estabeleça uma abordagem, um plano ou um curso de ação da gestão de riscos, como forma de demonstrar sua liderança e comprometimento, assegurando que a gestão de riscos esteja integrada em todas as atividades da organização. Isso é feito principalmente pelo estabelecimento de uma Política de Gestão de Riscos, que representa uma declaração transparente da filosofia de gerenciamento de riscos, conforme o COSO-GRC 2007.

Espera-se ainda que os órgãos de supervisão assegurem que a informação sobre riscos e sua gestão seja apropriadamente comunicada. Nesse sentido, a IN nº 01/2016, em seu art. 16, inciso VIII, ressalta a necessidade de que informações relevantes sejam identificadas, coletadas e comunicadas, a tempo de permitir que as pessoas cumpram suas responsabilidades e a fim de possibilitar o gerenciamento de riscos e a tomada de decisão. Desse modo, todo o pessoal precisa receber "uma mensagem claramente delineada da Alta Administração, de que o gerenciamento de riscos corporativos deve ser levado a sério" (COSO-GRC-2007).

Por intermédio do Modelo das Três Linhas, o Instituto de Auditores Internos - IIA preconiza entre seus princípios, que:

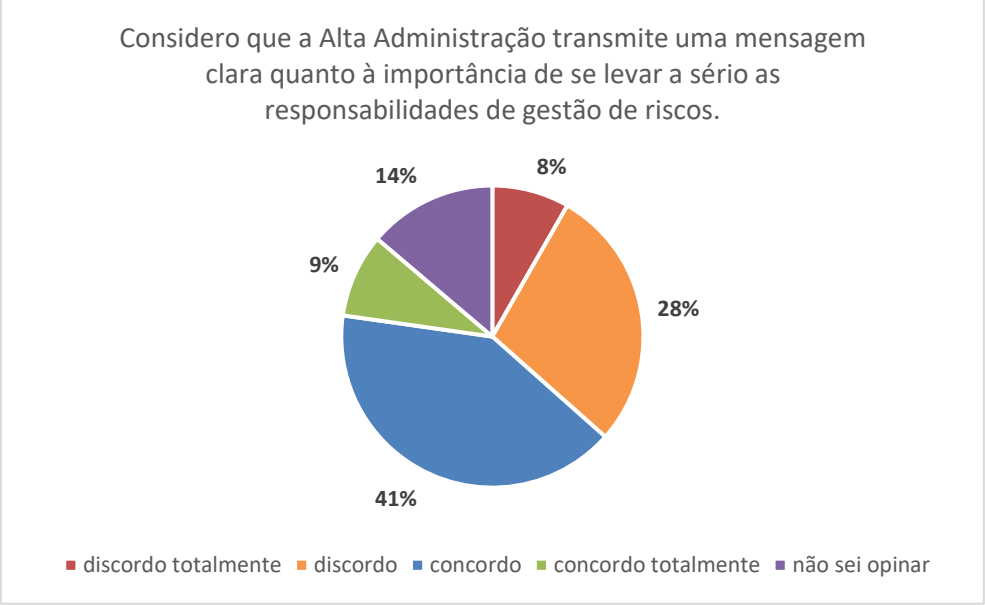
> *Todos os papéis que trabalham juntos contribuem coletivamente para a criação e proteção de valor quando estão alinhados entre si e com os interesses priorizados dos 'stakeholders'. O alinhamento das atividades é feito através da comunicação, cooperação e colaboração. Isso garante a confiabilidade, coerência e transparência das informações necessárias para a tomada de decisões baseada em riscos.*

Tomando por base esses critérios, a avaliação realizada identificou que a gestão do FNDE não transmite uma mensagem clara sobre a gestão de riscos da organização, dado que:

- conforme já abordado no tópico 1.1.2.1, não há um modelo de governança padronizado e formalmente adotado que possa servir de diretriz para a atuação do FNDE;
- nesse mesmo tópico, concluiu-se que não há estruturas formalizadas especificamente para apoiar a gestão de riscos, havendo iniciativas esparsas que poderão ser utilizadas para dar início à construção de estruturas formais no futuro. Ademais, dentre as instâncias instituídas, verificou-se que a atuação dos Comitês de Gestão Estratégica e Governança e de Gestão de Riscos, Controles Internos e Integridade está prejudicada e que suas competências e atribuições não estão sendo efetivamente exercidas;
- conforme resultados apresentados no tópico 1.2.5.3, não há responsabilidades e competências definidas em uma política que sirva de diretriz para toda a organização; e
- conforme os resultados que serão apresentados nos tópicos 2.1.3.1 e 2.2.3.1 (dimensão Processos), concluiu-se que não há definição expressa dos responsáveis pelas atividades de identificação, avaliação e tratamento de riscos no âmbito do FNDE; bem como não existem fluxos de informações formais entre as partes interessadas, para adequado desempenho de suas responsabilidades.

Da análise da percepção dos servidores, observou-se que 50% não identificam que a Alta Administração transmite uma mensagem clara quanto à importância de se levar a sério as responsabilidades de gestão de riscos ou não sabem opinar:

Gráfico 26: Percepção dos servidores – Mensagem da gestão quanto à gestão de riscos



Fonte: elaboração própria.

Assim, entende-se que, apesar das ações esparsas, a gestão do FNDE não transmite uma mensagem clara quanto à importância de se levar a sério as responsabilidades de gerenciamento de riscos, não havendo uma estruturação suficiente e adequada para que essas responsabilidades sejam exercidas.

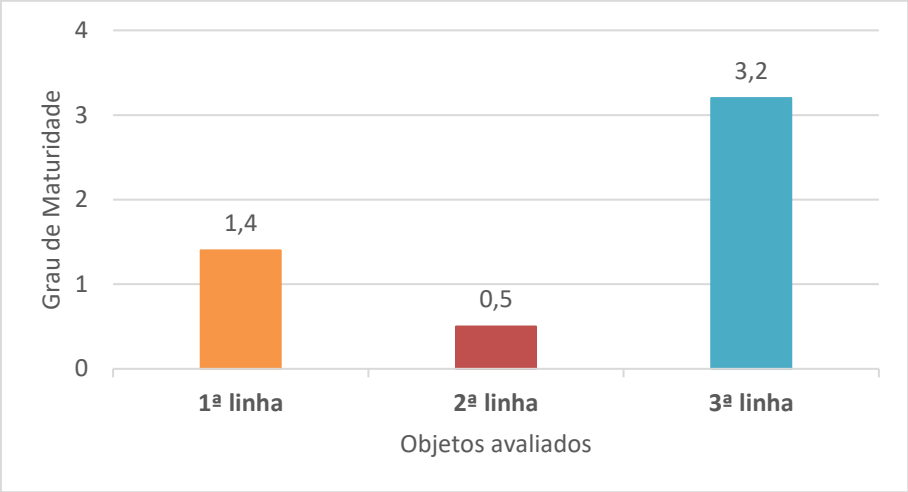
1.3.2. Estrutura de gerenciamento de riscos e controles

Os grupos de pessoas que integram as três linhas na estrutura de gerenciamento de riscos e controles por todo o FNDE têm clareza quanto aos seus papéis, entendem os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos e controles da organização?

Com vistas a avaliar este aspecto, foram previstos testes relacionados a três objetos de análise: 1.3.2.1. Primeira Linha; 1.3.2.2. Segunda Linha; e 1.3.2.3. Terceira Linha.

A avaliação realizada mostrou que, dada a ausência de uma Política de Gestão de Riscos ou documento equivalente, os papéis de primeira e segunda linhas não estão claros na organização e não há limites e responsabilidades formalmente estabelecidos no âmbito de uma estrutura geral de gestão de riscos e controles do FNDE. Os papéis da terceira linha, no entanto, foram designados no Estatuto da Auditoria Interna do FNDE, em conformidade com as normas que regem a atividade de auditoria interna governamental, além da existência de estruturas e princípios difundidos.

Gráfico 27: Resultado da avaliação dos objetos – Aspecto Estrutura de gerenciamento de riscos e controles



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

1.3.2.1. Primeira linha

Os testes previstos buscaram avaliar se, na primeira linha, os gestores:

I. Têm plena consciência de sua propriedade sobre os riscos, de sua responsabilidade primária pela identificação e gerenciamento dos riscos e pela manutenção de controles internos eficazes; e
II. São regularmente capacitados para conduzir o processo de gestão de riscos em suas áreas de responsabilidade e para orientar as suas equipes sobre esse tema.

Conforme dita a IN nº 01/2016, os controles internos da gestão se constituem na primeira linha (ou camada) de defesa das organizações públicas para propiciar o alcance de seus objetivos. Esses controles são operados 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.

Recorrendo-se ao Modelo das Três Linhas do IIA - Uma atualização das Três Linhas, por meio do Princípio 3: “Gestão e os papéis da primeira e segunda linhas”, verifica-se que a responsabilidade da gestão de atingir os objetivos organizacionais engloba os papéis da primeira e segunda linhas e que “os papéis de primeira linha estão mais diretamente alinhados com a entrega de produtos e/ou serviços aos clientes da organização, incluindo funções de apoio”.

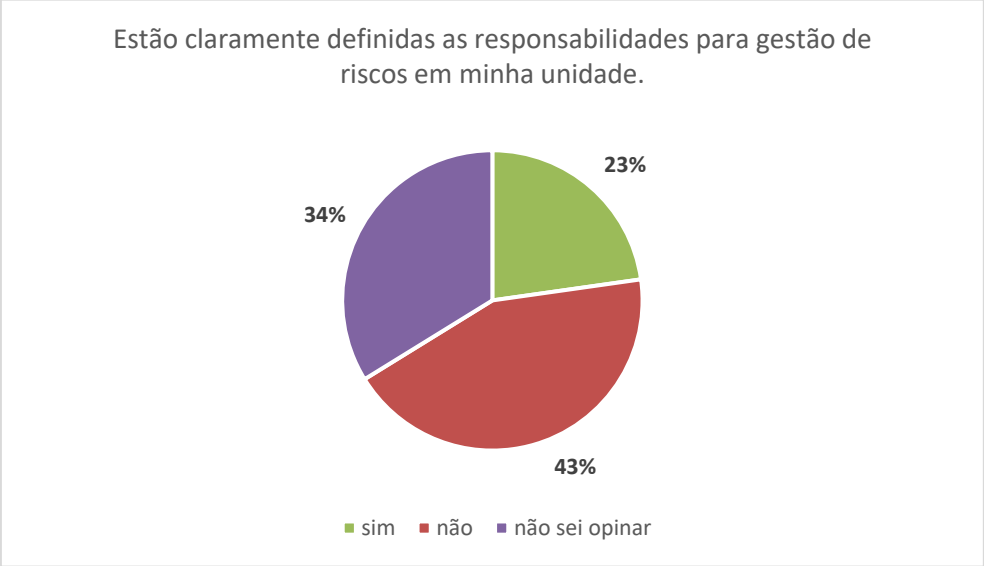
A organização auditada informou que não existem pessoas alocadas especificamente para a realização de atividades de gestão de riscos (“gestores de riscos”). Aliado a isso, a ausência de uma Política de Gestão de Riscos ou de outro documento equivalente fragiliza a atuação da primeira linha, dado que não são formalmente apontadas as responsabilidades por:

I. Liderar e dirigir ações (incluindo gerenciamento de riscos) e aplicação de recursos para atingir os objetivos da organização;
II. Manter um diálogo contínuo com o órgão de governança e reportar resultados planejados, reais e esperados, vinculados aos objetivos da organização, além dos riscos;
III. Estabelecer e manter estruturas e processos apropriados para o gerenciamento de operações e riscos (incluindo controle interno); e
IV. Garantir a conformidade com as expectativas legais, regulatórias e éticas.

A partir da análise do Regimento Interno do FNDE, verificou-se que há unidades para as quais foram estabelecidas competências específicas relacionadas à gestão de riscos, conforme já relatado no tópico 1.1.2.1. No entanto, verifica-se que não há vinculação dessas competências com uma diretriz superior para a gestão de riscos decorrente, principalmente, de uma Política de Gestão de Riscos.

Nesse sentido, o questionário enviado aos servidores mostrou que 77% dos servidores ou entenderam que não estão claramente definidas as responsabilidades para gestão de riscos em suas unidades ou não souberam opinar:

Gráfico 28: Percepção dos servidores – Primeira linha

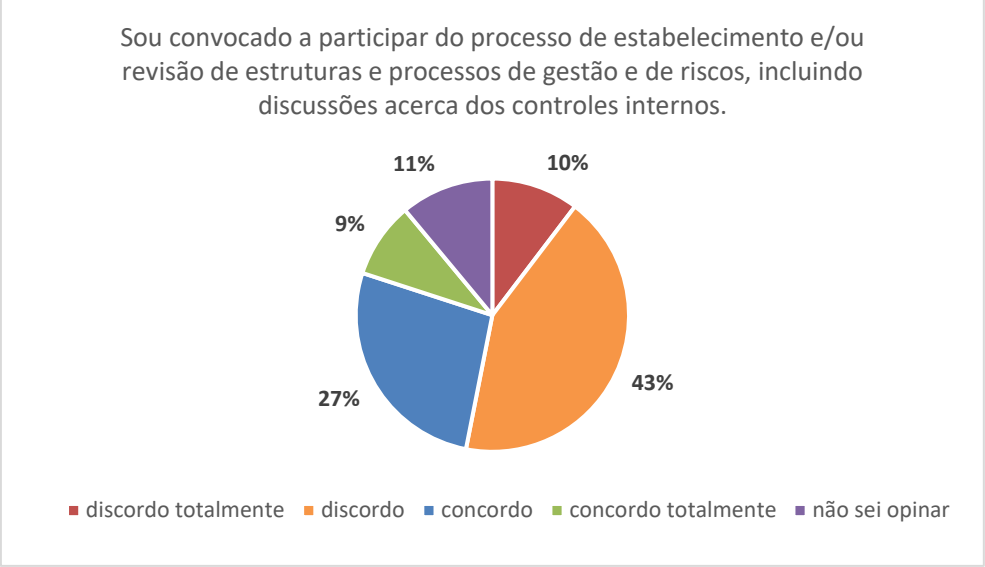


Fonte: elaboração própria.

Dentre os 23% que entenderam que as responsabilidades foram claramente definidas, 91% disseram terem sido adequadamente instruídos sobre o seu papel e suas responsabilidades na gestão de riscos dos processos de suas unidades. O mesmo percentual de respondentes afirmou ter clareza acerca de quem é responsável por liderar e dirigir as ações de gestão de riscos em sua unidade.

Destaca-se, ainda, que apenas 36% os servidores responderam que são convocados a participar do processo de estabelecimento e/ou revisão de estruturas e processos de gestão de riscos e discussões sobre controles internos:

Gráfico 29: Percepção dos servidores – Primeira linha



Fonte: elaboração própria.

Além disso, 89% afirmaram ter clareza acerca do seu papel na garantia de conformidade com as expectativas legais, regulatórias e éticas; e 66% afirmaram ter clareza acerca da forma pela qual devem reportar os riscos relacionados aos objetivos de sua unidade.

Assim, apesar das percepções apontarem certa medida de aderência na atuação da 1ª linha, os mecanismos existentes na organização não fornecem suporte para o seu correto funcionamento. Em especial, considerando que não foram formalmente atribuídos os papéis de primeira linha e não há pessoas especificamente designadas para promover ações que visem dar garantia razoável do atingimento dos objetivos organizacionais no âmbito de um processo coordenado e integrado de gestão de riscos.

1.3.2.2. Segunda linha

Os testes previstos buscaram avaliar se, na segunda linha, o pessoal que integra funções de coordenação de atividades de gestão de riscos e/ou de gerenciamento de riscos específicos por toda a organização:

I. Apoia e facilita os gestores no estabelecimento de processos de gerenciamento de riscos que sejam eficazes em suas áreas de responsabilidade;
II. Fornece metodologias e ferramentas a todas as áreas, por toda a organização, com a finalidade de identificar e avaliar riscos;
III. Define, orienta e monitora funções e responsabilidades pela gestão de riscos em todas as áreas, por toda a organização;
IV. Estabelece uma linguagem comum de gestão de riscos, incluindo medidas comuns de probabilidade, impacto e categorias de riscos;
V. Orienta a integração do gerenciamento de riscos nos processos organizacionais e de gestão, e promovem competência para suportá-la; e
VI. Comunica ao dirigente máximo e aos gestores executivos o andamento do gerenciamento de riscos em todas as áreas, por toda a organização.

Segundo a IN nº 1/2016:

> *Art. 6º Além dos controles internos da gestão, os órgãos e entidades do Poder Executivo federal podem estabelecer instâncias de segunda linha (ou camada) de defesa, para supervisão e monitoramento desses controles internos. Assim, comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e 'compliance', por exemplo, podem se constituir em instâncias de supervisão de controles internos.*

Conforme orienta o Modelo das Três Linhas do IIA, "Os papéis de segunda linha fornecem assistência no gerenciamento de riscos", podendo se concentrar em objetivos específicos do gerenciamento de riscos, como: "conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade".

Da análise realizada, verificou-se que não foram formalmente atribuídos os papéis de segunda linha, por meio de uma Política de Gestão de Riscos ou de outro documento equivalente. Assim, não existe uma unidade regimentalmente responsável pelo monitoramento e supervisão da gestão de riscos da organização – conforme já apontado no tópico 1.1.2.1 – e não há pessoas formalmente designadas para atuar no âmbito de um processo coordenado e integrado de gestão de riscos.

Corroborando esse achado, o iGG/TCU apontou fragilidade relacionada ao estabelecimento de atividades típicas de segunda linha, considerando o resultado (2112) "inicial".

Ressalta-se, por fim, que a IN nº 01/2016 prevê algumas responsabilidades de apoio à 2ª linha que poderiam ser exercidas pelo Comitê de Gestão Estratégica e Governança e pelo Comitê de Gestão de Riscos, Controles Internos e Integridade. No entanto, conforme demonstrado no tópico 1.1.2.1, esses comitês não têm sido atuantes.

1.3.2.3. Terceira linha

Os testes previstos buscaram avaliar se, na terceira linha, o pessoal que integra a auditoria interna, especialmente o dirigente dessa função:

I. Tem conhecimento dos papéis fundamentais que a função de auditoria interna deve assumir em relação ao gerenciamento de riscos, dos que não deve assumir e dos que pode assumir com salvaguardas à independência, previstos na Declaração de Posicionamento do IIA: "O papel da Auditoria Interna no gerenciamento eficaz de riscos corporativo", e de fato exerce seus papéis em conformidade com essas orientações;
II. Tem compreensão clara da estratégia da organização e de como ela é executada, incluindo objetivos, metas, riscos associados e como esses riscos são gerenciados, e alinha as atividades da auditoria interna com as prioridades da organização; e
III. Detém as competências necessárias para utilizar uma abordagem sistemática e disciplinada baseada no risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.

Conforme dispõe a IN nº 01/2016, em seu art. 2º:

> *III - [...] As auditorias internas no âmbito da Administração Pública se constituem na terceira linha ou camada de defesa das organizações, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha ou camada de defesa, executada por todos os níveis de gestão dentro da organização) e da supervisão dos controles internos (segunda linha ou camada de defesa, executada por instâncias específicas, como comitês de risco e controles internos).*

O Modelo das Três Linhas do IIA detalha que:

> *A auditoria interna presta avaliação e assessoria independentes e objetivas sobre a adequação e eficácia da governança e do gerenciamento de riscos. Isso é feito através da aplicação competente de processos sistemáticos e disciplinados, expertise e conhecimentos. Ela reporta suas descobertas à gestão e ao órgão de governança para promover e facilitar a melhoria contínua. Ao fazê-lo, pode considerar a avaliação de outros prestadores internos e externos.*

No âmbito do FNDE, os testes realizados e as evidências coletadas mostraram que a Audit tem buscado desempenhar seu papel de terceira linha a partir das orientações da Estrutura Internacional de Práticas Profissionais (*International Professional Practices Framework* - IPPF[20]), visto que:

- a Audit está posicionada de forma independente (NA[21] 1100), diretamente ligada ao Conselho Deliberativo, sem subordinação a outra unidade dirigente, conforme se observa do Regimento Interno do FNDE;
- o Estatuto da Audit (Resolução nº 09, de 29 de setembro de 2022) estabeleceu em seu art. 1º as atividades de avaliação e consultoria e em seu art. 2º o foco em governança, gerenciamento de riscos e controles (NA 1000.A1 e 1000.C1);
- foi efetuado mapeamento do universo auditável[22], o que contribui com o planejamento de auditoria baseada em risco (ND[23] 2010). O modelo adotado tem entre seus fatores de construção a associação aos objetivos estratégicos do FNDE, bem como a identidade com metas do Plano Nacional de Educação – PNE e com indicadores estratégicos definidos;
- o plano de auditoria é baseado em riscos (ND 2010), sendo feita a publicação anual do Paint da Audit/FNDE, definindo os trabalhos prioritários a serem realizados durante o exercício – também em consonância ao disposto na IN SFC/CGU nº 09, de 09 de outubro de 2018. Desde 2020, o planejamento da Audit utiliza a metodologia da análise do universo auditável para definição dos temas prioritários a serem trabalhados. Ademais, é efetuada consulta à alta gestão para identificar áreas/temas prioritários; e

[20] A Estrutura Internacional de Práticas Profissionais (*International Professional Practices Framework* – IPPF) é a base conceitual que organiza as informações oficiais promulgadas pelo *The Institute of Internal Auditors*. O IIA fornece aos profissionais de Auditoria Interna do mundo todo métodos organizados no IPPF, como as orientações mandatórias e as recomendadas.

[21] As Normas de Atributo (NA) abordam as características das organizações e das partes que realizam atividades de Auditoria Interna.

[22] Os resultados são apresentados em *dashboard* do Power BI, que permite acompanhar os temas relevantes e seus fatores de risco. Ademais, foi publicado o documento "Políticas e procedimentos – Mapeamento do universo auditável", contendo as diretrizes para o mapeamento e a classificação do universo auditável, a partir de métricas baseadas em fatores de risco.

[23] As Normas de Desempenho (ND) descrevem a natureza das atividades de Auditoria Interna e fornecem critérios que permitem avaliar o desempenho desses serviços.

- existem mecanismos de fomento à capacitação, ao treinamento e ao desenvolvimento periódicos (NA 1230). Nesse sentido, foi definida meta de capacitação para os servidores da Auditoria Interna, vinculada ao atingimento da meta de desempenho individual, cujos resultados são aferidos por meio do "Índice de Cumprimento das Tarefas dos Projetos e da Meta de Capacitação", que exige a realização de, no mínimo, 40h de capacitação por exercício. Ainda, foi elaborada trilha de capacitação que contempla as principais necessidades das unidades da Auditoria Interna, em alinhamento aos temas do Plano de Desenvolvimento de Pessoas (PDP) do FNDE. A partir da análise dos Raint 2020 e 2021, observou-se o cumprimento da meta de capacitação para todos os servidores.

Adicionalmente, foi enviado questionário específico aos servidores que atuam no serviço de auditoria na Audit/FNDE (com exceção dos servidores que atuaram no presente trabalho e do Auditor-Chefe). As percepções coletadas demonstraram que: 100% dos respondentes "concordaram" ou "concordaram totalmente" que foram adequadamente instruídos sobre os papéis fundamentais da Audit em relação ao gerenciamento de riscos; 100% dos respondentes "concordaram" ou "concordaram totalmente" que são incentivados a se capacitarem de forma periódica, em temas relevantes para o desenvolvimento de suas atividades; e 100% dos respondentes "concordaram" ou "concordaram totalmente" que, a partir dos trabalhos desenvolvidos, a Audit/FNDE exerce os papéis fundamentais de identificar oportunidades e promover a melhoria contínua dentro da organização.

Por isso, entende-se que o pessoal que integra a terceira linha (Auditoria Interna) tem clareza acerca de seu papel, demonstra conhecimento dos papéis fundamentais que a auditoria interna deve assumir, compreende as estratégias da organização, alinhando-as com o planejamento da unidade e apresenta as competências necessárias para utilizar uma abordagem sistemática e disciplinada baseada no risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.

Apesar disso, considerando a inexistência de uma política de gestão de riscos e a não definição de um cadastro de riscos da organização (conforme será tratado no tópico 2.1), o mapeamento do universo auditável e a seleção dos trabalhos de auditoria são feitos com base na avaliação de riscos realizada pela própria Audit (e não na avaliação de riscos realizada pelo FNDE). Nesse sentido, a atuação da unidade de auditoria interna poderá ser aprimorada quando os processos de gestão de riscos da Autarquia, especialmente no tocante à identificação de riscos, estiverem mais maduros e estruturados. Isso porque a definição da estratégia de auditoria depende em grande parte do grau de maturidade da gestão de riscos da unidade auditada[24], bem como da clara definição de objetivos estratégicos e operacionais para adequado alinhamento entre a estratégia da Audit com as estratégias da organização.

Outro ponto de melhoria da atuação da Audit relaciona-se ao Programa de Gestão e Melhoria da Qualidade (PGMQ). Nesse ponto, destaca-se que a unidade instituiu, por intermédio da Portaria Audit/FNDE nº 1, de 20 de agosto de 2021 o seu PGMQ, já tendo sido realizadas as primeiras atividades de monitoramento contínuo, inclusive com a coleta de *feedback* dos gestores sobre a agregação de valor da atividade de auditoria interna. Ademais, está prevista para o segundo semestre de 2022 a conclusão da primeira avaliação interna periódica para avaliar a qualidade, a adequação e a suficiência do processo de auditoria interna. Vislumbra-se que os resultados dessa

[24] Conforme disposto no MOT (CGU, 2017a).

avaliação interna subsidiarão a melhoria das atividades da Audit/FNDE, tanto no nível de trabalhos individuais de auditoria, quanto no nível mais amplo da sua atuação.

Assim, verifica-se que estão formalmente instituídas as estruturas e difundidos os princípios necessários para a regular atuação da Audit enquanto terceira linha, bem como conclui-se pelo funcionamento de todas as ações relevantes relacionadas. Ainda, verifica-se que estão previstas atividades para aprimoramento e melhoria contínua da atividade de auditoria interna.

2. DIMENSÃO PROCESSOS

Conforme já citado neste relatório, a IN nº 01/2016 estabeleceu a obrigatoriedade de os órgãos e entidades do Poder Executivo federal implementarem, manterem, monitorarem e revisarem o processo de gestão de riscos, de forma compatível com sua missão e objetivos estratégicos e observando as diretrizes estabelecidas na IN.

Nesse contexto, as organizações costumam adotar "desde abordagens informais até abordagens altamente estruturadas e sistematizadas de gestão de riscos, dependendo do seu porte e da complexidade de suas operações" (TCU, 2018a). Isso porque, a gestão de riscos precisa ser "personalizada e proporcional aos contextos externo e interno da organização relacionados aos seus objetivos" (ISO 31000:2018).

Desse modo, uma organização do porte do FNDE, que lida com diversos atores e cujos programas e serviços prestados têm grande impacto na sociedade, precisa de estruturas formalizadas e desenvolvidas que reflitam sua complexidade e permitam gerenciar adequadamente os riscos que a permeiam.

Em relação ao Processo de Gestão de Riscos, a Norma ABNT NBR ISO 31000:2018 trouxe a seguinte referência:

> *O processo de gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos.*

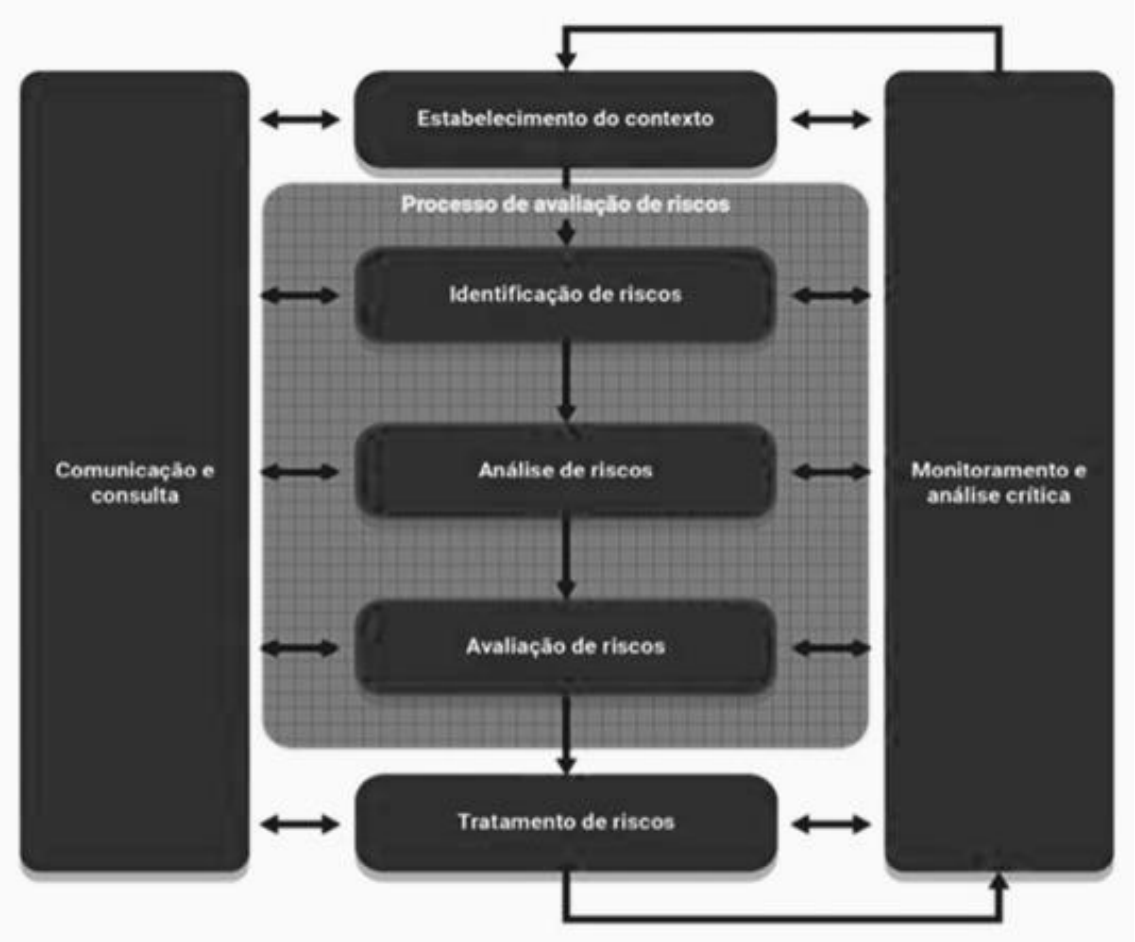
Ainda nesse contexto, o Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal, direta, autárquica e fundacional dispôs:

> *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 [...].*

De acordo com os diversos *frameworks* existentes sobre o assunto, diferentes etapas para o processo de gestão de riscos costumam ser definidas, mas, de modo geral, algumas etapas básicas são comuns a todos os modelos, como: identificação, avaliação, tratamento e monitoramento.

Para o presente trabalho, serão consideradas as seguintes etapas do processo de gestão de riscos:

Figura 2: Processo de Gestão de Riscos



Fonte: ISO 31000:2018

O modelo acima pode ser utilizado em todas as operações, funções e atividades relevantes para a realização dos objetivos-chave de uma organização. Destaca-se que algumas etapas podem ocorrer de forma sequencial (como identificação, análise e avaliação de riscos), enquanto outras ocorrem de forma contínua, ao longo de todo o processo e dando suporte às demais etapas (como "comunicação e consulta" e "monitoramento e análise crítica"). Destaca-se também que o processo é iterativo e perpassa todas as áreas e funções relevantes da organização.

Adicionalmente, destaca-se que o Decreto 9.203/2017 estabeleceu a observância dos seguintes princípios para a gestão de riscos:

> *[...] 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.*

Assim, pelo exposto, conclui-se que os processos de gestão de riscos se agregam aos processos da gestão, sendo parte integrante destes; porém, nem todas as atividades da gestão fazem parte necessariamente da gestão de riscos – ou seja, nem todas as atividades ou processos terão seus riscos gerenciados.

Conforme preconizado no COSO-GRC:

> *Os custos e os benefícios da implementação de funcionalidades de identificação de eventos, avaliação de riscos, atividades pertinentes de resposta e controle são mensurados com diferentes níveis de precisão, que variam frequentemente dependendo da natureza da organização. A questão é encontrar um ponto de equilíbrio. Da mesma forma que recursos, por serem limitados, não devem ser alocados a riscos não significativos, o controle excessivo é dispendioso e contraproducente.*

Nesse sentido, a IN 01/2016 estabeleceu em seu art. 23, § 1º, a competência do Comitê de Governança, Riscos e Controles para:

> *XI - aprovar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão.*

Destaca-se também que é recomendável que todo o processo de gestão de riscos e seus resultados sejam documentados e relatados por meio de mecanismos apropriados.

Assim, a presente dimensão examinou os processos de gestão de riscos adotados pela gestão, procurando avaliar em que medida o FNDE dispõe de um modelo de processo formal, com padrões e critérios definidos para a identificação, a análise e a avaliação de riscos; para a seleção e a implementação de respostas aos riscos avaliados; para o monitoramento de riscos e controles; e para a comunicação sobre riscos com partes interessadas, internas e externas.

Da avaliação realizada na presente dimensão, concluiu-se que o FNDE não dispõe de um processo de gestão de riscos estruturado e formalmente instituído, que permita a realização adequada das atividades de gestão de riscos, de forma consistente em relação a todas as operações, funções e atividades relevantes para a realização de seus objetivos-chave.

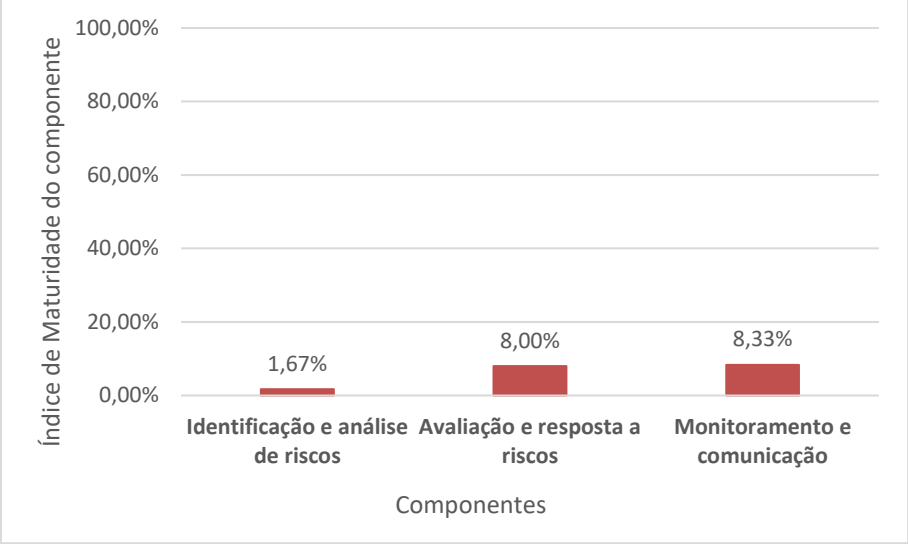
Conforme demonstrado na dimensão Ambiente, a organização não instituiu uma Política de Gestão de Riscos (ou documento equivalente) para guiar as ações de gerenciamento de riscos. Essa ausência de política impacta diretamente na existência e funcionamento da dimensão Processos. Dado que não há um processo estabelecido e não há adequada alocação de recursos (pessoas, sistemas, orçamento etc.) para a gestão de riscos, as atividades de identificação e análise de riscos, de avaliação e resposta a riscos e de monitoramento e comunicação não estão estabelecidas e não são aplicadas de forma consistente na organização.

Consequentemente, os responsáveis pela governança, a administração e as pessoas responsáveis em todos os níveis não têm um entendimento atual, correto e abrangente dos objetivos sob a sua gestão, de seus papéis e responsabilidades, tampouco sabem em que medida os resultados de cada área ou pessoa são significativos para atingir os objetivos-chave que envolvem riscos. Ademais, faltam elementos suficientes para tomada de decisões com segurança razoável por parte dos gestores e servidores.

Cabe ressaltar, ainda, que o processo de gestão de riscos é suportado pela cultura e pelo ambiente de gestão de riscos da entidade. Assim, as considerações feitas no capítulo anterior, que tratou da dimensão Ambiente, têm influência direta nas avaliações que serão realizadas no presente capítulo.

O índice de maturidade obtido na dimensão Processos foi de **6,67%**, o que significa uma maturidade **INICIAL** do seu modelo de gestão de riscos. O gráfico a seguir apresenta o Índice de Maturidade para cada um dos componentes relacionados à dimensão:

Gráfico 30: Índice de Maturidade por Componente – Dimensão Processos



Fonte: elaboração própria.

Do gráfico acima, percebe-se a baixa maturidade dos processos de gestão de riscos do FNDE. Isso porque, conforme será detalhado nessa dimensão, as atividades relacionadas às etapas do gerenciamento de riscos ainda não são estabelecidas e aplicadas de forma consistente pela organização, em todas as áreas e atividades relevantes. A ausência de uma Política de Gestão de Riscos pode ser apontada como a causa principal dessa fragilidade.

Nos parágrafos a seguir, estão descritos os achados relativos a cada um dos três componentes avaliados na dimensão Processos (Identificação e análise de riscos; Avaliação e resposta a riscos; e Monitoramento e comunicação).

2.1. Identificação e análise de riscos

Nesse componente, apurou-se a seguinte questão: em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente a todas as operações, funções e atividades relevantes do FNDE (unidades, processos e atividades que são críticos para a realização dos objetivos-chave da organização)?

Buscou-se, para tanto, avaliar se os riscos significativos para a organização são identificados e priorizados, possibilitando as atividades subsequentes de avaliação e resposta a riscos. A avaliação do componente foi feita a partir de quatro aspectos: 2.1.1. Estabelecimento do contexto; 2.1.2. Documentação do estabelecimento do contexto; 2.1.3. Identificação e análise dos riscos; e 2.1.4. Documentação da identificação e análise dos riscos.

Cabe ressaltar que, após o estabelecimento do contexto, o processo de avaliação de riscos inicia-se com a etapa de *identificação*, seguida pela *análise* e depois pela *avaliação*, conforme

modelo da ISO 31000:2018, apresentado na introdução desta dimensão. Ainda, o presente capítulo trata da identificação juntamente com a análise de riscos, dado que as duas etapas costumam ser executadas de forma bastante correlacionada.

O COSO-CI (2013) estabelece, como princípio, que a organização deve identificar os riscos relacionados à realização de seus objetivos e avaliá-los para determinar a forma como esses riscos devem ser gerenciados. Para que isso ocorra, é necessário que os objetivos da organização (estratégicos e de negócios) tenham sido fixados[25], sendo condição prévia para a execução do processo (COSO-GRC, 2007).

Na etapa de *identificação*, busca-se "encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos" (ISO 31000:2018). Assim, as organizações, a partir de diversas técnicas, identificam incertezas – sob seu controle ou não – que possam afetar os seus objetivos e as classificam como riscos ou oportunidades.

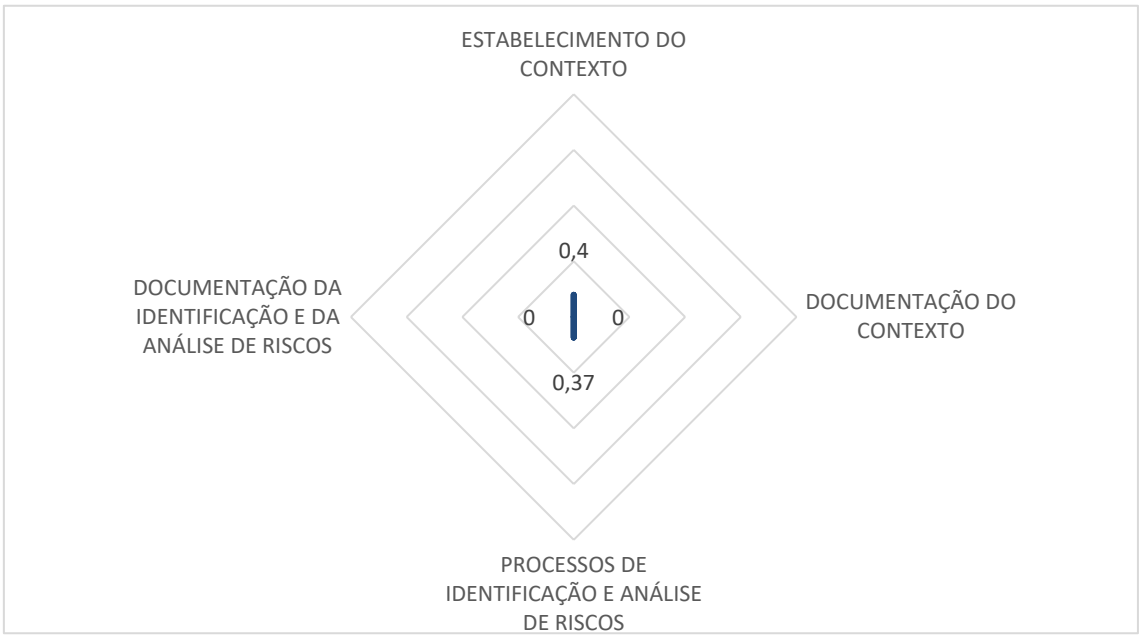
Em seguida, na etapa de *análise* dos riscos identificados, o propósito é "compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado" (ISO 31000:2018). Esse processo envolve "a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia" (*idem*, *ibidem*). Com isso, tem-se uma visão acerca de quais riscos precisarão ser tratados e como (o que ocorrerá na etapa de avaliação).

Para a adequada identificação e análise de riscos é necessário que uma série de premissas tenham sido cumpridas, inclusive no que se refere à preparação do seu ambiente interno. Ademais, é preciso lembrar que o processo de gestão de riscos precisa ser personalizado para cada organização, considerando especialmente o seu contexto de atuação e os objetivos prioritários que precisam ser alcançados.

No FNDE, o resultado do componente "Identificação e análise de riscos", a partir da avaliação dos seus aspectos, demonstra uma maturidade **INICIAL**, apurada em **1,67%**. O gráfico a seguir apresenta o resultado consolidado do componente:

[25] Conforme já abordado no tópico 1.2.3 do presente Relatório.

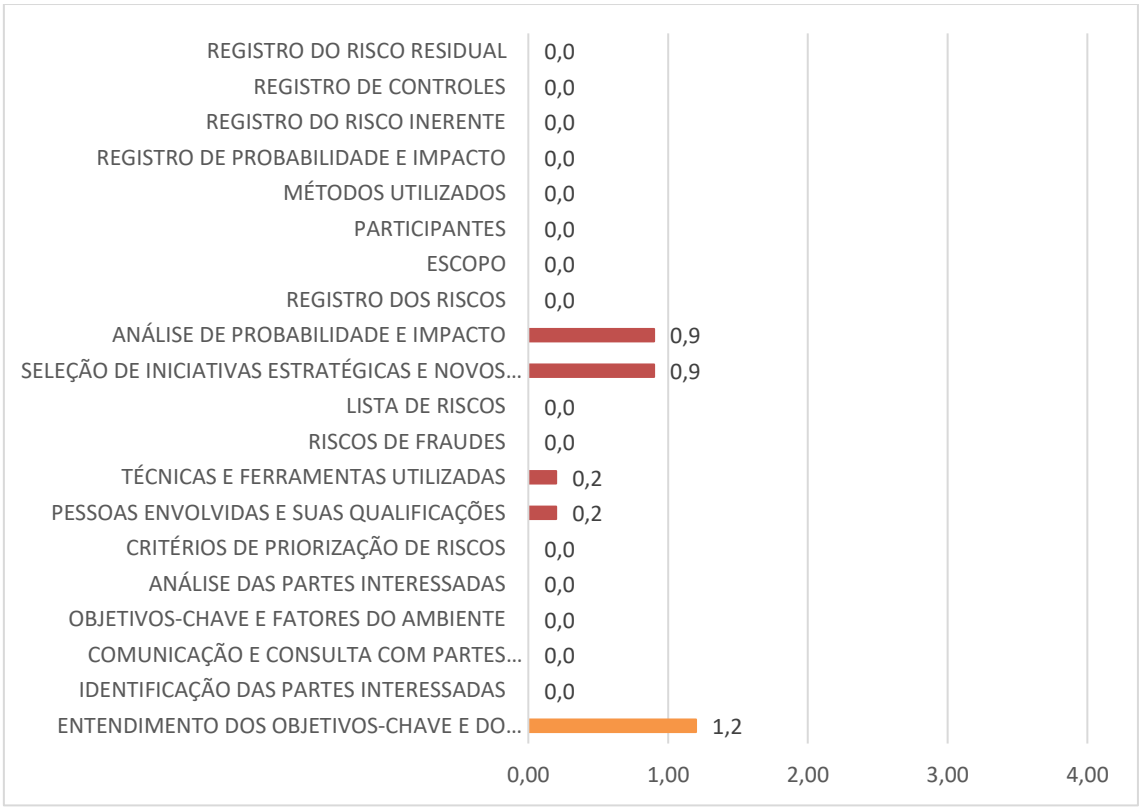
Gráfico 31: Resultado da avaliação dos objetos – Componente Identificação e análise de riscos (resultado por aspecto)



Fonte: elaboração própria.

Já o gráfico abaixo, apresenta os resultados de cada objeto analisado nos quatro aspectos que integram o componente "Identificação e análise de riscos":

Gráfico 32: Resultado da avaliação dos objetos – Componente Identificação e análise de riscos (resultado por objeto)



Fonte: elaboração própria.

Dos gráficos 31 e 32, percebe-se baixo grau de maturidade dos processos de identificação e análise de riscos no FNDE, de modo que a maior parte dos elementos mínimos necessários para o desenvolvimento dessa etapa ainda não foi instituída pela organização auditada. Nesse sentido, reforça-se que um grau maior de maturidade relacionado a essa etapa depende também de uma maior maturidade do ambiente interno da organização, especialmente no que se refere ao estabelecimento de objetivos e à definição de políticas e metodologias que permitam um processo coordenado, integrado e padronizado pela organização.

A seguir apresentam-se os aspectos avaliados no componente Identificação e análise de riscos, bem como os objetos relacionados a cada aspecto.

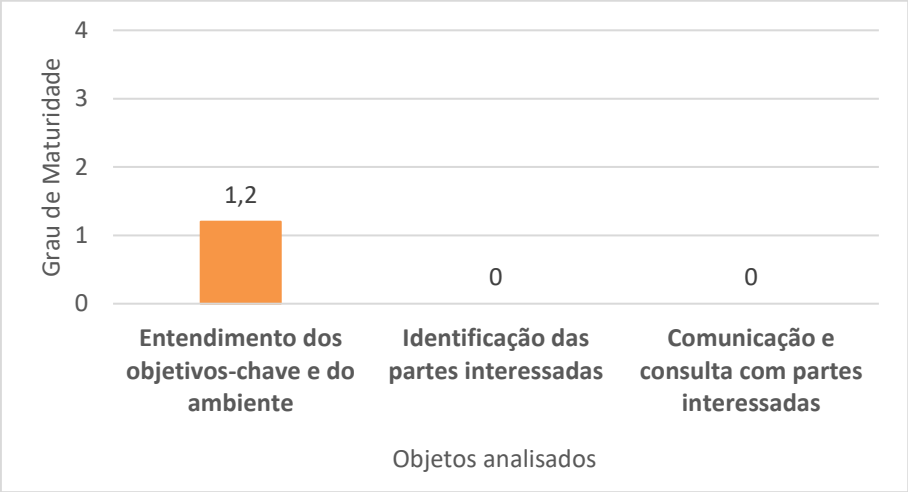
2.1.1. Estabelecimento do contexto

A identificação de riscos é precedida de uma etapa de estabelecimento do contexto?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à etapa de estabelecimento do contexto, que busca obter uma visão abrangente dos fatores internos e externos que podem influenciar a capacidade da organização de o atingir seus objetivos. Assim foram selecionados três objetos de análise como requisitos essenciais nessa etapa, a saber: 2.1.1.1. Entendimento dos objetivos-chave e do ambiente; 2.1.1.2. Identificação das partes interessadas; e 2.1.1.3. Comunicação e consulta com partes interessadas.

A avaliação realizada mostrou que não há atividades de identificação e análise de riscos sendo aplicadas de forma consistente a todas as operações, funções e atividades relevantes da organização. Observaram-se iniciativas pontuais sobre o tema, mas a ausência de uma Política de Gestão de Riscos ou de outros documento equivalente, contendo diretrizes para os processos de gerenciamento de riscos, prejudica a aplicação de atividades coordenadas e sua operação integrada.

Gráfico 33: Resultado da avaliação – Aspecto Estabelecimento do contexto



Fonte: elaboração própria.

Dessa forma, os tópicos a seguir trazem informações sobre os objetos analisados e, ainda, boas práticas relacionadas ao conteúdo mínimo a ser observado na definição de critérios relacionados às etapas de identificação e análise de riscos.

2.1.1.1. Entendimento dos objetivos-chave e do ambiente

Buscando avaliar se o FNDE compreende o contexto em que está inserido e se consegue, com base nesse contexto, identificar riscos, procedeu-se a análise da existência e do funcionamento do processo de identificação dos objetivos-chave das atividades, dos processos ou dos projetos objeto da gestão de riscos, bem como coletou-se a percepção da Alta Administração quanto ao estabelecimento do contexto para a gestão de riscos em suas unidades de atuação.

As boas práticas relacionadas à gestão de riscos destacam como princípio a especificação preliminar de objetivos, com clareza suficiente, a fim de permitir a identificação e a avaliação dos riscos associados aos objetivos (COSO-CI 2013, COSO-GRC 2007 e IN MP/CGU nº 01/2016). A partir desses objetivos, é possível estabelecer o escopo das atividades de gerenciamento de riscos – planejando, por exemplo, os objetivos e decisões a serem tomadas, os resultados esperados, os recursos requeridos e o relacionamento com outros processos, projetos e atividades (ISO 31000:2018).

Nesse sentido, entender os objetivos-chave e o ambiente da organização é um pré-requisito fundamental para a identificação dos riscos relacionados. Por isso, as organizações costumam definir preliminarmente quais processos, projetos ou atividades terão seus riscos gerenciados, documentando essa definição em Planos de Gestão de Riscos, que costumam conter, dentre outras informações: objetivos a serem alcançados pelos processos/projetos/atividades selecionados; informações relacionadas a perspectivas estratégicas, temporais, financeiras e orçamentárias; metas e indicadores associados; percepções relacionadas ao contexto externo e interno (forças, fraquezas, ameaças e oportunidades).

As análises realizadas pela equipe de auditoria nesse objeto apontaram para a ausência de diretrizes consistentes que tenham por objetivo o entendimento dos objetivos-chave e do ambiente para a gestão de riscos. Dado que não foram formalmente definidas as atividades, os projetos e os processos para serem objeto da gestão de riscos e que não há diretrizes para a etapa de identificação de riscos – especialmente em decorrência da não instituição de Política de Gestão de Riscos ou de outro documento equivalente – as práticas encontradas no FNDE foram avaliadas como esporádicas, não padronizadas e não disseminadas na organização.

Verificou-se que, no âmbito de consultoria externa[26] realizada entre 2017 e 2018, houve iniciativas relacionadas ao estabelecimento da gestão de riscos do FNDE. Com base na Metodologia de Gestão de Integridade, Riscos e Controles Internos da Gestão (desenvolvida pelo antigo MP), foram selecionados processos críticos a serem mapeados no âmbito de cada Diretoria do FNDE, tendo sido selecionada também uma atividade no âmbito de cada processo para ter seus riscos avaliados. Destaca-se, no entanto, que os resultados dessa consultoria não foram incorporados às

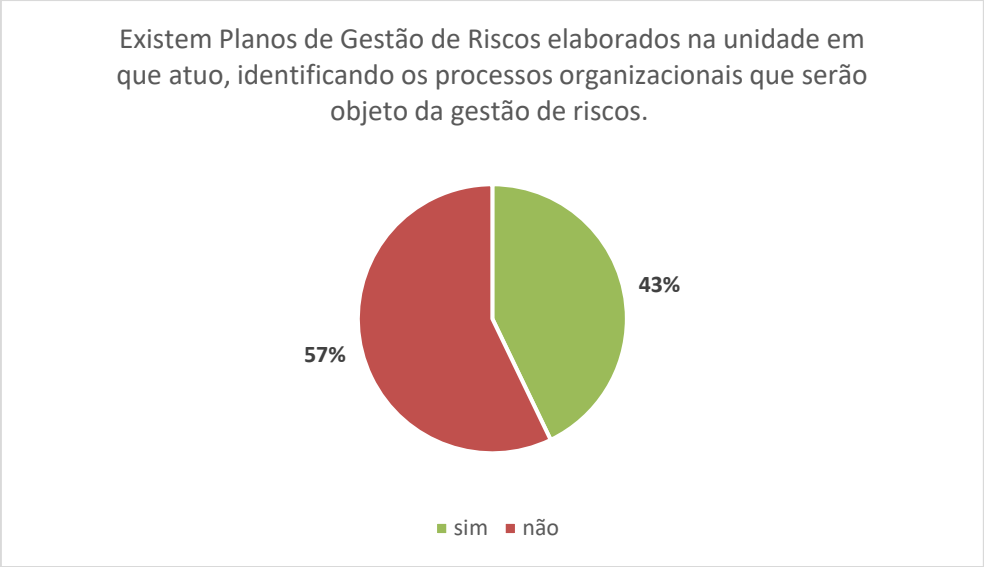
[26] Ressalta-se que tal iniciativa vai de encontro a orientações da CGU quanto à necessidade de contratação desse tipo de serviço em virtude da existência de instâncias governamentais, a exemplo das Auditorias Internas, capazes de prestar à Gestão o apoio necessário ao desenvolvimento e à implementação de metodologias de Gestão de Riscos.

práticas institucionais, de modo que não se observa uma continuidade do trabalho realizado e não se identifica a utilização, no dia a dia da instituição, dos mecanismos apresentados.

Adicionalmente, conforme informado pela organização auditada, verificou-se a existência de iniciativas pontuais e projetos estratégicos que foram selecionados para receberem um tratamento orientado à gestão de riscos, como: Malha Fina, Demandas de Órgãos de Controle e Novo Fundeb (Implantação do Valor Anual Total por Aluno – VAAT).

Da análise de percepção coletada junto à Alta Administração, verificou-se que 43% dos dirigentes afirmaram possuir planos de gestão de riscos, conforme apresentado no gráfico a seguir:

Gráfico 34: Percepção da Alta Administração – Entendimento dos objetivos-chave e do ambiente



Fonte: elaboração própria.

Assim, eventuais planos existentes precisarão ser incorporados, ou até mesmo revisados, quando da institucionalização de mecanismos estruturados para a gestão de riscos do FNDE (com base, por exemplo, numa metodologia que oriente a construção desses planos).

A partir dos projetos citados e da percepção dos dirigentes, entende-se que há uma realização esporádica do princípio, em algumas unidades relevantes, mas sem a presença de diretrizes ou de uma metodologia que possam orientar e padronizar a identificação dos objetivos-chave das atividades, dos processo ou dos projetos a serem objeto da gestão de riscos; ainda, sem considerar o contexto dos objetivos-chave da organização como um todo, de modo a assegurar que os riscos significativos de cada objeto possam ser apropriadamente identificados.

2.1.1.2. Identificação das partes interessadas

Buscou-se avaliar se o FNDE identifica as partes interessadas, bem como se identifica e aprecia necessidades, expectativas e preocupações destas, de modo a incluí-las em cada etapa do processo de gestão de riscos, por meio de comunicação e consulta.

Entende-se que, para tornar o processo de avaliação de riscos eficaz, é necessário entender as particularidades e o contexto de cada organização, de modo a personalizar esse processo. Para tanto, o estabelecimento do contexto e de um ambiente de controle e gestão de riscos deve abordar valores, necessidades, interesses e expectativas da organização e dos agentes que a compõem, bem como de partes externas interessadas, tendo o cidadão e a sociedade como principais vetores (ISO 31000:2018 e IN nº 01/2016, art. 22).

As análises realizadas apontaram que o FNDE não instituiu processos consistentes de identificação das partes interessadas e de seus interesses, especialmente em virtude de não haver uma Política de Gestão de Riscos definida (ou outro documento equivalente) e tampouco diretrizes formais para o estabelecimento do contexto da gestão de riscos.

Consequentemente, não há diretrizes ou uma metodologia que orientem e padronizem a identificação das partes interessadas (internas e externas), bem como a identificação e a apreciação das suas necessidades, expectativas legítimas e preocupações, de modo a incluir essas partes interessadas em cada etapa do processo de gestão de riscos, por meio de comunicação e consulta.

Assim, eventuais políticas e procedimentos para gestão de riscos e a serem instituídas no FNDE devem apresentar diretrizes para o estabelecimento do contexto, contemplando a identificação das partes interessadas e seus pontos de vista nesse processo.

2.1.1.3. Comunicação e consulta com partes interessadas

Esta análise buscou avaliar se o FNDE realiza comunicação e consulta com as partes interessadas (internas e externas), a fim de assegurar que as suas visões, percepções, necessidades, suposições, conceitos e preocupações sejam identificados, registrados e levados em consideração no processo de gestão de riscos.

A ISO 31000:2018 e a IN nº 01/2016 destacam que a comunicação e consulta com partes interessadas (internas e externas) devem ocorrer no âmbito de cada etapa e ao longo do processo de gestão de riscos, fluindo para todos os atores envolvidos (da organização e fora dela). Para o COSO-CI (2013), a comunicação interna permite que as informações relevantes sejam transmitidas pela organização; a comunicação externa, que informações significativas sejam recebidas das partes externas, bem como transmitidas para essas partes, com vistas a responder requisitos e expectativas.

Neste contexto e considerando os resultados do tópico 2.1.1.2, apontando que não foram previamente identificadas as partes interessadas, as análises realizadas concluíram que também não existem processos consistentes para comunicação e consulta com as partes interessadas, nem documentação sobre a análise de seus interesses.

Adicionalmente, não foram identificadas diretrizes ou uma metodologia que possam orientar e padronizar a comunicação e consulta com partes interessadas (internas e externas), de modo a assegurar que as suas visões e percepções, incluindo necessidades, suposições, conceitos e preocupações sejam identificadas, registradas e levadas em consideração no processo de gestão de riscos.

Assim, eventuais política e procedimentos para gestão de riscos a serem instituídas no FNDE devem prever diretrizes para a comunicação e consulta com as partes interessadas.

2.1.2. Documentação do contexto

A documentação da etapa de estabelecimento do contexto inclui elementos essenciais para viabilizar um processo de avaliação de riscos consistente?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à documentação dos processos de identificação e análise de riscos instituídos (ou seja, à documentação dos objetos avaliados no aspecto 2.1.1), a partir de três objetos de análise: 2.1.2.1. Objetivos-chave e fatores do ambiente; 2.1.2.2. Análise das partes interessadas; e 2.1.2.3. Critérios de priorização de riscos.

A avaliação realizada reflete a inexistência de processos e atividades relacionadas ao estabelecimento do contexto para a gestão de riscos. Portanto, inexiste também documentação dessa etapa.

Dessa forma, os tópicos a seguir trazem informações sobre as análises realizadas e, ainda, boas práticas para a adequada implementação dessa etapa.

2.1.2.1. Objetivos-chave e fatores do ambiente

Esta análise buscou verificar se o FNDE documenta a descrição dos objetivos-chave e dos fatores críticos para que se tenha êxito na gestão de riscos e se analisa os fatores do ambiente interno e externo.

Ressalta-se que o COSO-CI 2013 tem como princípio a definição clara dos objetivos para promover a melhor identificação e avaliação dos riscos associados aos objetivos.

Adicionalmente, a norma ABNT IEC 31010:2021 defende que a definição de objetivos deve ser documentada para facilitar a identificação dos riscos e a compreensão das implicações destes riscos. Como diretrizes, a norma estabelece que, na medida do possível, os objetivos devem ser:

- específicos para o objeto da avaliação;
- mensuráveis qualitativa ou quantitativamente;
- alcançáveis dentro das restrições impostas pelo contexto;
- relevantes para os objetivos ou contexto mais amplos da organização; e
- alcançáveis dentro de um prazo estabelecido

Neste sentido, verificou-se que não há a descrição dos objetivos-chave e de fatores críticos, conforme destacado no aspecto 2.1.1. Ainda que a organização auditada tenha mencionado a existência de iniciativas pontuais e projetos estratégicos que foram selecionados para receberem um tratamento orientado à gestão de riscos (como: Malha Fina, Demandas de Órgãos de Controle e Novo Fundeb), entende-se que a documentação do contexto para a gestão de riscos é inexpressiva, dado que não há uma metodologia que possa orientar e padronizar essa documentação.

2.1.2.2. Análise das partes interessadas

Esta análise buscou verificar se o FNDE documenta a análise de partes interessadas e seus interesses, a partir, por exemplo, de: análise de *stakeholder*, análise RECI (quem é o responsável, quem executa, quem é consultado e quem é informado) ou matriz de responsabilidades.

A ISO 31000:2018 entende que a gestão de riscos acontece no contexto dos objetivos e atividades da organização. Sendo os ambientes interno e externo espaços no qual a organização define e alcança seus objetivos, é imprescindível compreender as partes afetadas para melhor analisar em que contexto a gestão de riscos está sendo aplicada.

Ademais, a ABNT IEC 31010:2021 afirma que o envolvimento das partes interessadas deve assegurar que as informações a que os riscos estejam relacionados sejam válidas e aplicáveis e que essas partes compreendam melhor as razões por trás das decisões tomadas. Nesse contexto, a norma apresenta algumas técnicas para obter opiniões de partes interessadas, como: *brainstorming*, técnica Delphi, técnica de grupo nominal, entrevistas estruturadas ou semiestruturadas e pesquisas. Além disso, também são convencionais na literatura sobre o tema as técnicas de análise de *stakeholder*, análise RECI ou matriz de responsabilidades.

Nesse objeto, verificou-se que, na ausência de Política de Gestão de Riscos do FNDE e de diretrizes que tratem da identificação das partes interessadas, também não há definição formal de atividades, projetos e processos para serem objeto da gestão de riscos, conforme destacado no aspecto 2.1.1. Consequentemente, não há diretrizes nem um processo formalmente definido para documentar a análise das partes interessadas.

2.1.2.3. Critérios de priorização de riscos

Esta análise busca verificar se o FNDE documenta os critérios com base nos quais os riscos serão analisados, avaliados e priorizados, incluindo, por exemplo: como serão definidos a probabilidade e o impacto; como será determinado se o nível de risco é tolerável ou aceitável; quais os critérios de priorização para análise, avaliação e tratamento dos riscos identificados.

A ISO 31000:2018 entende que a organização deve definir a quantidade e o tipo de risco que podem ou não assumir em relação aos seus objetivos, bem como definir critérios para melhor entender a significância dos riscos e para embasar a tomada de decisão. Recomenda-se que tais critérios reflitam os valores, objetivos e recursos da organização e estejam em conformidade com a Política da Gestão de Riscos.

Ademais, o *framework* preleciona que, para estabelecer os critérios de risco, deve-se considerar a natureza e o tipo de incertezas que podem afetar resultados e objetivos e a forma pela qual as consequências e as probabilidades serão definidas e medidas. Além disso, é importante que haja fatores referentes ao tempo, que haja consistência no uso de medidas e que seja definido como o nível de risco será determinado. Adicionalmente, deve-se definir quais combinações e quais riscos serão levados em consideração e qual a capacidade da organização.

Assim, verificou-se que, considerando a ausência de Política de Gestão de Riscos do FNDE (ou de documento equivalente) e de estruturação da etapa de estabelecimento do contexto, não há diretrizes sobre o tema e não foram formalmente definidos os critérios de priorização de riscos.

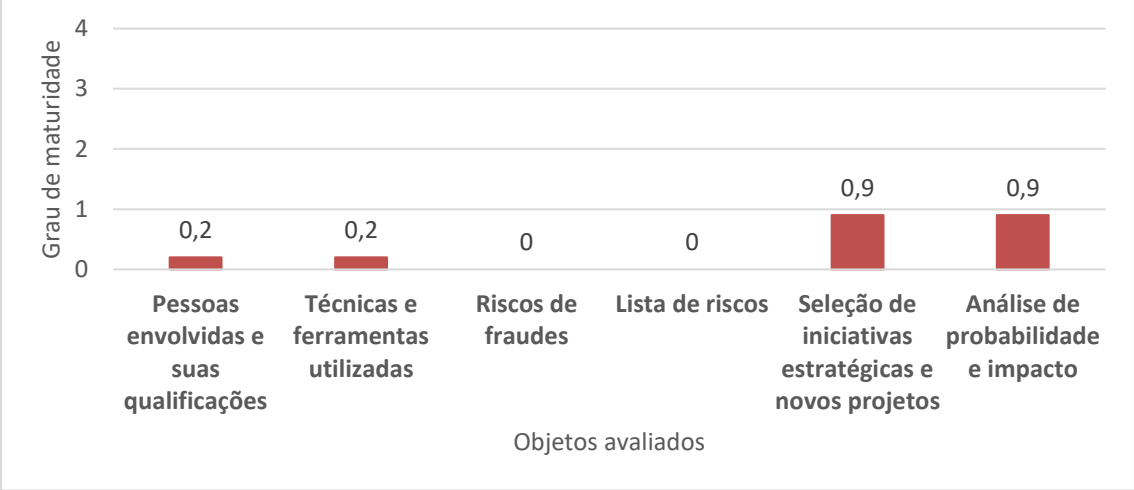
2.1.3. Processos de identificação e análise de riscos

Os processos de identificação e análise de riscos envolvem pessoas e utilizam técnicas e ferramentas que assegurem a identificação abrangente e a avaliação consistente dos riscos?

Com vistas a avaliar este aspecto, foram previstos testes relacionados às atividades que fazem parte dos processos de identificação e análise de riscos instituídos. Assim foram selecionados seis objetos de análise que contemplam requisitos essenciais nessa etapa, a saber: 2.1.3.1. Pessoas envolvidas e suas qualificações; 2.1.3.2. Técnicas e ferramentas utilizadas; 2.1.3.3. Riscos de fraudes; 2.1.3.4. Lista de riscos; 2.1.3.5. Seleção de iniciativas estratégicas e novos projetos; e 2.1.3.6. Análise de probabilidade e impacto.

A avaliação realizada mostrou que a organização ainda não dispõe de processos padronizados e disseminados para as etapas de identificação e análise de riscos. Em que pese haver iniciativas que podem conter elementos deste aspecto, estas estão restritas a projetos e processos específicos sem, contudo, vincular-se a elementos estratégicos da organização inseridos na lógica de um processo de gestão de riscos integrado.

Gráfico 35: Resultado da avaliação – Aspecto Processos de identificação e análise de risco



Fonte: elaboração própria.

A ausência de uma Política de Gestão de Riscos e, consequentemente, de diretrizes sobre como e com qual periodicidade os riscos devem ser identificados e analisados, reflete em uma baixa maturidade dos objetos avaliados no presente aspecto. Por isso, os tópicos a seguir trazem informações sobre as análises realizadas e, ainda, boas práticas no tocante ao conteúdo mínimo necessário a ser observado na etapa de identificação e análise de riscos.

2.1.3.1. Pessoas envolvidas e suas qualificações

Esta análise buscou verificar se o FNDE envolve pessoas com conhecimento adequado, bem como os gestores executivos das respectivas áreas, no processo de identificação e análise de riscos.

Além disso, foi coletada a percepção, por meio de questionário direcionado aos servidores, acerca de sua participação em atividades de identificação e análise de riscos.

A IN nº 01/2016, em seu artigo 19, estabelece que o dirigente máximo da organização é o principal responsável pelo estabelecimento da estratégia da organização e da estrutura de gerenciamento de risco. Ainda, que cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente identificado.

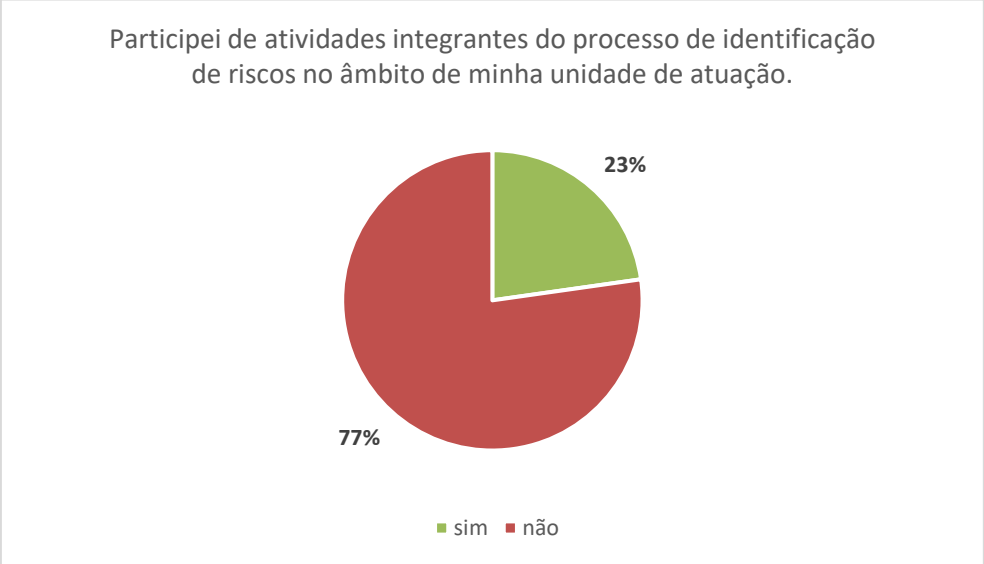
Na mesma linha, os *frameworks* que tratam do tema gestão de riscos destacam a importância de serem distribuídas responsabilidades e de serem envolvidas todas as partes da organização no processo. Ainda sobre este ponto, a ISO 31000:2018 recomenda:

- que sejam atribuídas e comunicadas a toda organização as responsabilidades e responsabilizações sobre o gerenciamento de riscos; e
- que sejam identificados os indivíduos que possuam responsabilização e tenham autoridade para gerenciar riscos.

Contudo, pela falta de diretrizes formalmente definidas, observou-se que não há, no FNDE, uma clara definição das pessoas envolvidas na gestão de riscos. Conforme destacado nos tópicos 1.1.2.1, 1.2.5.3, 1.2.6.1 e 1.2.7.1, não foram definidos gestores de riscos e não foram formalmente atribuídas responsabilidades, competências e autoridade para gerenciar riscos. Consequentemente, as etapas de identificação e análise não preveem o envolvimento de pessoas adequadamente capacitadas e que detenham conhecimento adequado para a realização de suas responsabilidades em gestão de riscos.

A partir da análise de percepção dos servidores, quando perguntados acerca da sua participação em processos de identificação e análise de riscos, apenas 23% dos respondentes disseram já ter participado de atividades do tipo.

Gráfico 36: Percepção dos servidores – Pessoas envolvidas e suas qualificações



Fonte: elaboração própria.

Por isso, entende-se que a realização do princípio é inexpressiva, de modo que ainda não se tem garantia de que, nas etapas de identificação e análise de riscos, são envolvidas pessoas com conhecimento adequado e os gestores executivos das respectivas áreas.

2.1.3.2. Técnicas e ferramentas utilizadas

Esta análise buscou verificar se o FNDE utiliza técnicas e ferramentas adequadas, considerando especialmente os objetivos e tipos de riscos, no processo de identificação e análise. Novamente, coletou-se a percepção dos servidores quanto à sua participação em atividades de identificação e análise de riscos. Ademais, coletou-se a percepção da Alta Administração em relação às técnicas e ferramentas utilizadas em suas unidades para dar suporte à gestão de riscos.

De acordo com a ISO 31000:2018, o principal objetivo da gestão de riscos é encontrar, reconhecer e descrever riscos capazes de influenciar o alcance dos objetivos da organização. O documento segue afirmando que é possível utilizar diferentes técnicas para identificar incertezas, a partir de análises qualitativas, quantitativas ou da combinação destas. Ademais, é necessário alocar recursos para a gestão de riscos, o que inclui a adoção de processos, métodos e ferramentas adequados.

Destaca-se, ainda, que o COSO-GRC (2007) apresenta, em seu Anexo 4.1, exemplos de técnicas de identificação de eventos. Na mesma linha, a ABNT IEC 31010:2021, ressalta as seguintes técnicas de identificação de riscos: *checklists*; classificações e taxonomias; análise de modos e efeitos de falha (FMEA); análise de modos; efeitos e criticidade de falha (FMECA); estudos de perigos e operabilidade (HAZOP); análise de cenário; e técnica *"what if*" (SWIFT).

Com base nestes critérios, verificou-se que o FNDE não definiu formalmente técnicas e ferramentas para identificação e análise de riscos. Conforme já destacado no tópico 1.2.7.1, não há sistemas ou ferramentas específicos para a gestão de riscos.

Além disso, verificou-se que, no âmbito da consultoria realizada entre 2017 e 2018, houve iniciativas relacionadas ao estabelecimento da gestão de riscos do FNDE. Com base na Metodologia de Gestão de Integridade, Riscos e Controles Internos da Gestão, desenvolvida pelo antigo MP, foi apresentada planilha em Excel para fins de registro da priorização de processos para gerenciamento de riscos. Porém, como já relatado, os resultados da referida consultoria não foram incorporados às práticas institucionais.

Adicionalmente, da análise de percepção coletada junto à Alta Administração, verifica-se que 71% dos dirigentes que responderam ao questionário enviado afirmaram que suas unidades possuem ações de identificação e análise de eventos e riscos. Destes, 100% afirmam que os riscos identificados e analisados estão registrados em sistemas, planilhas ou matrizes.

Já em relação aos servidores, apenas 19% afirmaram já ter participado de atividades de análise de riscos em suas unidades de atuação. Dentre esses 19%, 70% concordam que foram envolvidas pessoas com conhecimento adequado e foram utilizadas técnicas/ferramentas adequadas.

Do cenário analisado, entende-se que, apesar da percepção acerca da existência de ações e da utilização de ferramentas para registro de riscos, considerando que não foram instituídos os processos de identificação e análise de riscos na organização, tais ações ocorrem de forma de isolada, não estando respaldadas em diretrizes organizacionais.

Ademais, cumpre ressaltar que eventuais iniciativas pontuais precisarão ser incorporadas, ou até mesmo revisadas, quando da institucionalização de mecanismos estruturados para a gestão de riscos do FNDE. Por fim, é necessário considerar que as técnicas e ferramentas escolhidas precisam ser compatíveis com a filosofia de gestão de riscos da organização, conforme recomenda o COSO-GRC (2007).

2.1.3.3. Riscos de fraudes

Esta análise buscou verificar se, no processo de identificação e análise de riscos, o FNDE considera explicitamente a possibilidade de fraudes, burla de controles e outros atos impróprios, além dos riscos inerentes aos objetivos de desempenho, divulgação (transparência e prestação de contas) e de conformidade com leis e regulamentos.

O COSO-CI (2013) estabelece como princípio que a organização deve considerar o potencial de fraude na avaliação dos riscos para a realização dos objetivos. Complementarmente, o Referencial de Combate a Fraude e Corrupção (TCU, 2018c) afirma que a gestão de riscos de fraude deve estar integrada à gestão de riscos da organização, tendo em vista que os diferentes riscos podem se interseccionar.

Nesse contexto, entende-se como fraude qualquer "ato intencional praticado por um ou mais indivíduos, entre gestores, responsáveis pela governança, empregados ou terceiros, envolvendo o uso de falsidade para obter uma vantagem injusta ou ilegal"[27]. Dada a complexidade da identificação desse tipo de risco, o referencial supracitado recomenda que seja criada uma equipe para essa identificação, incluindo "indivíduos de diversas áreas de conhecimento, por exemplo o pessoal das áreas de compras, de finanças, recursos humanos, contabilidade, do setor jurídico, relacionamento com o público, consultores" (TCU, 2018c).

Considerando que o FNDE não definiu formalmente um processo para identificação e análise de riscos, logo, a avaliação realizada também não identificou um processo formal para a identificação do risco de fraudes.

Ademais, outras fragilidades identificadas ao longo deste trabalho podem prejudicar a estrutura de mecanismos de combate à fraude, como as fragilidades relacionadas a(o): gestão da ética e da integridade; transparência; e modelo de governança da organização. Vale destacar, ainda, que a não existência de uma Política de Gestão de Riscos institucionalizada (ou outro documento equivalente) e a não alocação de pessoas especializadas para gestão de riscos na organização prejudicam a identificação de riscos associados a fraudes e burla de controles.

Assim, eventuais políticas e procedimentos para gestão de riscos a serem instituídos no FNDE devem prever diretrizes relacionadas aos processos de identificação e análise de riscos de fraudes, para melhor atender as necessidades de transparência e prestação de contas, bem como do cumprimento dos requisitos legais.

[27] Conforme a norma ISA 240 do *International Auditing and Assurance Standards Board* (Iaasb).

2.1.3.4. Lista de riscos

Esta análise buscou verificar se eventual processo de identificação de riscos instituído no FNDE produz uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução dos objetivos da organização identificados na etapa de estabelecimento do contexto.

A IN nº 01/2016 afirma que a organização deve observar alguns componentes para a gestão de riscos como, por exemplo, a identificação de eventos, contemplando o reconhecimento e o relacionamento dos riscos inerentes à própria atividade da organização, em seus diversos níveis. No mesmo sentido, os principais *frameworks* sobre o tema recomendam que as organizações identifiquem e classifiquem riscos e oportunidades.

Da análise realizada, observou-se que o FNDE não definiu formalmente um processo para identificação e análise de riscos, de modo que não há atualmente uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução dos objetivos da organização.

Conforme destacado pela organização auditada, a análise é realizada em cada caso particular. Mencionou-se, ainda, iniciativa relacionada à integridade, com a instituição do Plano de Integridade do FNDE (no entanto, conforme descrito no tópico 1.1.1.3, o Plano não trouxe a identificação de riscos para a integridade).

Adicionalmente, no âmbito da consultoria realizada entre 2017 e 2018, verificou-se que foram identificados e categorizados alguns eventos de riscos. Porém, como já mencionado, os resultados da referida consultoria não foram incorporados às práticas institucionais.

Assim, observa-se que a identificação de riscos é efetuada de forma pontual e não padronizada, sem que haja políticas ou metodologias que orientem o processo e permitam a construção de uma lista abrangente de riscos em todos os níveis e unidades organizacionais.

2.1.3.5. Seleção de iniciativas estratégicas e novos projetos

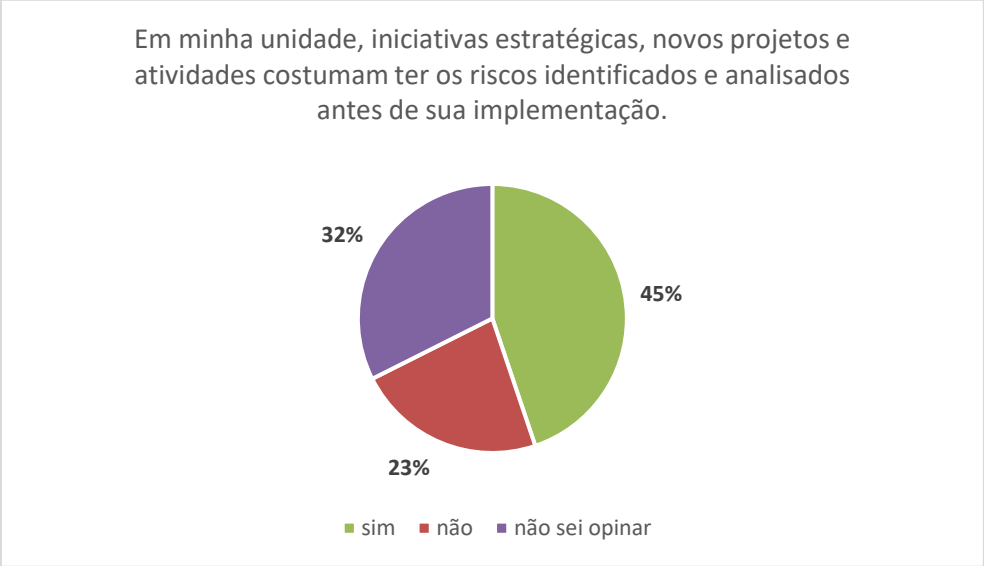
Esta análise buscou verificar se o FNDE identifica e analisa riscos quando da seleção de iniciativas estratégicas, novos projetos e atividades, bem como se esses riscos são incorporados ao processo de gestão de riscos da organização. Além disso, coletou-se a percepção dos servidores quanto ao seu conhecimento sobre riscos relacionados a iniciativas estratégicas, novos projetos e atividades.

Neste sentido, o *Orange Book* estabelece que o risco deve ser considerado como parte do fluxo normal de informações de gestão das atividades da organização e das decisões sobre estratégia, novos projetos, bem como compromissos relativos à alocação de recursos. A norma Intosai GOV 9130/2004 também recomenda que a administração precisa considerar na estrutura de gestão de riscos definida novas iniciativas e projetos.

Sobre o objeto analisado, a organização auditada informou que há iniciativas voltadas para a gestão de riscos dos projetos estratégicos, sem que haja, no entanto, uma metodologia formalmente definida ou normativos internos que tratem da matéria. Citou-se, ainda, que o termo de abertura utilizado para o início desses projetos traz a identificação de eventos com potencial de prejudicar os objetivos relacionados.

Em relação à percepção coletada, quando questionados acerca da identificação e análise de riscos relacionados a iniciativas estratégicas, novos projetos e atividades, 55% dos servidores discordaram ou não souberam opinar acerca da realização dessa atividade nas unidades em que atuam, conforme gráfico a seguir:

Gráfico 37: Percepção dos servidores – Processos de identificação e análise de riscos



Fonte: elaboração própria.

Com base nos critérios acima referidos e considerando que o FNDE ainda não definiu formalmente processos para identificação de riscos, concluiu-se que a realização do princípio é inicial e informal, dado que não foram estabelecidos diretrizes e protocolos que possam orientar o processo de identificação de riscos, inclusive em novos projetos e iniciativas. Ainda, não se pode falar em padronização ou em incorporação e integração dessas iniciativas ao processo de gestão de riscos.

Por isso, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever diretrizes relacionadas aos processos de integração de iniciativas estratégicas e novos projetos à gestão de riscos. Ademais, as iniciativas pontuais relatadas poderão ser incorporadas, quando da institucionalização de mecanismos estruturados para a gestão de riscos do FNDE.

2.1.3.6. Análise de probabilidade e impacto

Esta análise buscou verificar se eventuais riscos identificados e analisados no âmbito do FNDE são analisados em termos de probabilidade e impacto nos objetivos, fornecendo, assim, uma base para a avaliação e tomada de decisões sobre as respostas para o tratamento dos riscos. Também foi coletada a percepção da Alta Administração sobre o objeto.

As boas práticas da gestão de riscos apontam para o fato de que a organização necessita classificar os riscos com base no impacto (magnitude das consequências) que terão e na probabilidade de que ocorram. Nesse contexto, é recomendável que seja estabelecida uma

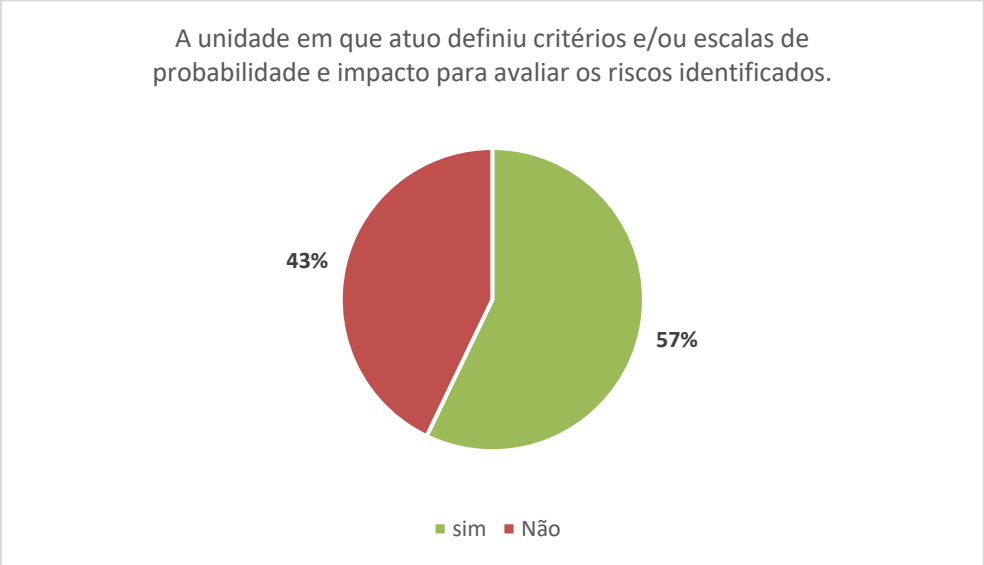
linguagem uniforme de gestão de riscos, que inclua medidas comuns, como, por exemplo, a criação de escalas padronizadas para medir de probabilidade e impacto (TCU, 2018a).

As análises realizadas demonstram que o FNDE não definiu formalmente métrica para medir a probabilidade de ocorrência de riscos relacionados aos seus objetivos nem o impacto nestes, especialmente considerando a ausência de uma Política ou uma metodologia para gestão de riscos que trate do processo de análise de riscos.

Contudo, observou-se que já houve iniciativa relacionada a esse tema, como no âmbito da consultoria realizada entre 2017 e 2018, que enquadrou alguns riscos a partir de escalas de probabilidade e impacto. Ademais, a organização auditada informou que, no âmbito de alguns projetos estratégicos, como no projeto do Malha Fina, é feita análise de riscos.

Complementarmente, a percepção coletada junta à Alta Administração mostrou que 57% dos dirigentes respondentes afirmaram que definiram critérios e/ou escalas de probabilidade e impacto para avaliarem os riscos identificados em suas unidades.

Gráfico 38: Percepção da Alta Administração – Análise de probabilidade e impacto



Fonte: elaboração própria.

A partir do exposto, entende-se que há uma realização esporádica do princípio, mas sem a presença de diretrizes ou de uma metodologia que possam orientar e padronizar a identificação dos objetivos-chave da atividade, do processo ou do projeto a ser objeto da gestão de riscos e sem a adoção formal de escalas padronizadas em todo o FNDE para a avaliação de probabilidade e impacto.

Por isso, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever escalas padronizadas para medir de probabilidade e impacto, de modo a se definirem medidas comuns para análise de riscos.

2.1.4. Documentação da identificação e análise dos riscos

No registro de riscos, a documentação da identificação e análise de riscos contém elementos suficientes para apoiar o adequado gerenciamento dos riscos?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à documentação do processo de identificação e análise de riscos. Assim foram selecionados oito objetos de análise entendidos como requisitos essenciais nessa etapa, a saber: 2.1.4.1. Registro dos riscos; 2.1.4.2. Escopo; 2.1.4.3. Participantes; 2.1.4.4. Métodos utilizados; 2.1.4.5 Registro de probabilidade e impacto; 2.1.4.6. Registro do risco inerente; 2.1.4.7. Registro de controles; e 2.1.4.8. Registro do risco residual.

De acordo com a ISO 31000:2018 é de suma importância que o processo de gestão de riscos e seus resultados sejam documentados e relatados por meio de mecanismos adequados. Esses registros objetivam comunicar atividades e resultados de gestão de riscos de toda a organização, fornecer informações para a tomada de decisão, aprimorar as atividades de gestão de riscos e auxiliar no relacionamento com as partes interessadas. Além disso, o relato serve para dar suporte à Alta Administração e para o cumprimento das responsabilidades pelo órgão de supervisão.

Nesse sentido, a documentação da identificação e análise de riscos deve conter, no mínimo: partes interessadas e suas necessidades; custo, frequência e pontualidade do relato; método do relato; e pertinência da informação para os objetivos e para a tomada de decisão.

Em primeiro lugar, destaca-se que o FNDE não definiu formalmente atividades, projetos e processos para serem objeto da gestão de riscos, conforme já abordado no tópico 2.1.1.1. Também não há diretrizes nem um processo formalmente definido para identificação de riscos. Por isso, verificou-se que não são utilizadas técnicas e ferramentas específicas para a gestão de riscos na organização. Assim, a avaliação realizada mostrou que não há registro dos riscos identificados, o que é refletido na baixa maturidade desse aspecto.

Dessa forma, os tópicos a seguir trazem informações sobre as análises realizadas e, ainda, boas práticas e diretrizes para a adequada documentação dessa etapa.

2.1.4.1. Registro dos riscos

Esta análise buscou avaliar se o FNDE possui documentação da etapa de identificação e análise dos riscos que contenha o registro dos riscos identificados e analisados em sistema, planilha ou matriz de avaliação de riscos, bem como se são descritos os componentes de cada risco separadamente com, pelo menos: suas causas, o evento e as consequências e/ou impactos nos objetivos identificados na etapa de estabelecimento do contexto.

Sobre o tema, o documento *Risk Management Assessment Framework* (RMAF) recomenda o registro, de maneira estruturada, dos riscos e das oportunidades identificadas, abrangendo os seguintes aspectos: as relações de dependência entre os riscos apurados; as relações entre os riscos de maior e menor nível de ocorrência; a identificação dos riscos-chave; e a atribuição de propriedade sobre o risco para aqueles que tenham autoridade para gerenciá-lo.

Diante da análise apresentada nos 1.2.7.1 e 2.1.3.2, verificou-se que atualmente não são utilizadas técnicas e ferramentas para a gestão de riscos. Assim, não é feito o registro dos riscos em sistemas ou planilhas. Trata-se, portanto, de prática não implementada na organização.

Nesse contexto, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever a forma de registrar os riscos identificados e analisados, bem como orientar sobre os componentes a serem descritos para cada risco (probabilidade de ocorrência, causas, consequências e/ou impactos, dentre outros).

2.1.4.2. Escopo

Esta análise buscou avaliar se, no registro de riscos eventualmente adotado, o FNDE inclui o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise de riscos.

De acordo com a ISO 31000:2018, dado que o processo de gestão de riscos pode ser aplicado em diferentes níveis (estratégico ou operacional; em programas, projetos ou atividades) é conveniente que a organização defina um escopo para o gerenciamento dos riscos, de modo a deixar claro: os objetivos pertinentes a serem considerados e o seu alinhamento aos objetivos organizacionais.

Contudo, em virtude de a análise apresentada nos tópicos 1.2.7.1 e 2.1.3.2 ter concluído pela inexistência de registro de riscos em planilhas/sistemas, avalia-se que a documentação do escopo dos processos de gestão de riscos também é uma prática não implementada no FNDE.

Assim, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever a forma de registrar o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise de riscos.

2.1.4.3. Participantes

Esta análise buscou avaliar se o FNDE possui documentação da etapa de identificação e análise dos riscos que contenha o registro dos participantes das atividades dessa etapa.

De acordo com a ISO 31000:2018, a Alta Administração deve assegurar a alocação de recursos apropriados para a gestão de riscos. Desse modo, também é necessário documentar quem são os participantes das atividades de identificação e análise de risco.

No entanto, diante do fato de a análise dos tópicos 1.2.7.1 e 2.1.3.2 ter concluído pela inexistência de registro de riscos em planilhas/sistemas, não há que se falar em documentação dos participantes das atividades de identificação e análise. Trata-se, portanto, de prática não implementada no FNDE.

Assim, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever a forma de registrar os participantes das atividades de gestão de riscos.

2.1.4.4. Métodos utilizados

Esta análise buscou avaliar se o FNDE possui documentação da etapa de identificação e análise dos riscos que contenha a descrição das abordagens ou dos métodos utilizados, bem como as classificações de probabilidade e impacto adotadas e as fontes de informação consultadas.

A ISO 31000:2018 também trata do assunto, orientando que a Alta Administração, onde aplicável, assegure o uso de processos, métodos e ferramentas adequados para a gestão de riscos.

Em *benchmarking* realizado ao longo da construção da presente avaliação de maturidade identificou-se que algumas organizações costumam elaborar metodologias para a gestão de riscos, orientando suas unidades sobre como implementar as políticas de gestão de riscos instituídas.

Diante da análise realizada nos tópicos 1.2.7.1 e 2.1.3.2 ter concluído pela inexistência de registro de riscos em planilhas/sistemas, não há que se falar em documentação dos métodos de identificação e análise utilizados. Trata-se, portanto, de prática não implementada na organização.

Assim, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever adicionalmente a abordagem ou o método de identificação e análise de riscos, considerando também as boas práticas já abordadas no tópico 2.1.3.6.

2.1.4.5 Registro de probabilidade e impacto

Esta análise buscou avaliar se o FNDE definiu parâmetros para o registro de probabilidade e impacto dos riscos eventualmente identificados e analisados, incluindo os níveis de risco inerente resultantes da combinação dessas variáveis (além de outros fatores que a entidade possa considerar para determinar seus níveis de risco).

A ISO 31000:2018 recomenda que a análise de riscos considere fatores como a probabilidade de eventos e suas consequências, bem como a natureza e a magnitude das consequências (impacto).

Assim, tendo em vista que no âmbito dos tópicos 1.2.7.1 e 2.1.3.2 verificou a inexistência de registro de riscos em planilhas/sistemas e que o tópico 2.1.3.6 identificou a não existência de escalas padronizadas para análise de probabilidade e impacto, concluiu-se pela não existência de documentação acerca desse objeto (como a utilização de matrizes de probabilidade e impacto ou outros mecanismos de registro).

Destaca-se que, embora tenha sido informado pela organização auditada que são identificados riscos no âmbito do Termo de Abertura dos projetos estratégicos, identificando-se a probabilidade e o impacto de sua ocorrência, esta listagem se mostrou pontual e esparsa, novamente prejudicada pela ausência de diretrizes da organização (como uma política ou documento equivalente que oriente a gestão de riscos).

Adicionalmente, no âmbito da consultoria realizada entre 2017 e 2018, conforme já destacado no tópico 2.1.3.6 foram identificados alguns eventos de riscos e foi feito o seu enquadramento a partir de escalas de probabilidade e impacto. Destaca-se, porém, que os resultados desse trabalho não foram incorporados às práticas institucionais, de modo que não se identificou a utilização dos mecanismos apresentados pela consultoria na organização.

Trata-se, portanto, de prática informal e esporádica, aplicada a algumas unidades relevantes, mas sem a adoção formal de escalas padronizadas em todo o FNDE que atendam aos requisitos da documentação das etapas de identificação e análise de riscos.

Assim, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, a forma de documentar o registro de probabilidade e impacto dos riscos identificados e analisados, considerando também as boas práticas já abordadas no tópico 2.1.3.6.

2.1.4.6. Registro do risco inerente

Esta análise buscou avaliar se o FNDE possui documentação da etapa de identificação e análise dos riscos que contenha os níveis de risco inerente resultantes da combinação de probabilidade e impacto, além de outros fatores que eventualmente considerados para determinar o nível de risco da entidade.

Conforme explica o COSO-GRC (2007), a administração deve levar em conta tanto o risco inerente quanto o risco residual no processo de gestão de riscos. Nesse contexto:

> *Risco inerente é o risco que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. Risco residual é aquele que ainda permanece após a resposta da administração. A avaliação de riscos é aplicada primeiramente aos riscos inerentes. Após o desenvolvimento das respostas aos riscos, a administração passará a considerar os riscos residuais.*

Assim, entende-se que o risco inerente é o risco considerado antes da implementação de qualquer controle.

Tendo em vista que no âmbito dos tópicos 1.2.7.1 e 2.1.3.2 concluiu-se pela inexistência de registro de riscos em planilhas/sistemas, também não foi identificada documentação contendo o cálculo do risco inerente. Trata-se, portanto, de prática não implementada.

Com isso, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever a forma de calcular e documentar o risco inerente nos processos, nas atividades e nos projetos priorizados para terem seus riscos gerenciados.

2.1.4.7. Registro de controles

Esta análise buscou avaliar se o FNDE possui documentação da etapa de identificação e análise dos riscos que contenha a descrição dos controles existentes e as considerações quanto a sua eficácia e confiabilidade.

Conforme destacado pela ISO 31000:2018, a análise de riscos precisa considerar a eficácia dos controles existentes. O COSO-CI (2013) traz como princípio a seleção e o desenvolvimento de atividades de controle que contribuam para a redução, a níveis aceitáveis, dos riscos à realização dos objetivos. Assim, é de suma importância que os controles existentes sejam avaliados quanto a sua eficácia e quanto ao seu potencial de dar segurança razoável para a realização dos objetivos pré-estabelecidos.

Considerando que no âmbito dos tópicos 1.2.7.1 e 2.1.3.2 concluiu-se pela inexistência de registro de riscos em planilhas/sistemas, também não foi identificada documentação contendo a descrição dos controles existentes, tampouco as análises sobre a sua eficácia/confiabilidade.

Trata-se, portanto, de prática não implementada no FNDE a ser considerada quando da implementação de políticas e procedimentos de gestão de riscos, especialmente no tocante à etapa de análise de riscos.

2.1.4.8. Registro do risco residual

Esta análise buscou avaliar se o FNDE possui documentação da etapa de identificação e análise dos riscos que contenha o registro do risco residual.

Conforme já descrito no tópico 2.1.4.5, o processo de gestão de riscos leva em consideração tanto o cálculo do risco inerente, quanto o cálculo do risco residual. Este é conceituado como o risco remanescente após a implementação de controles internos. Ainda de acordo com o COSO-GRC (2007), o risco residual auxilia a administração a obter uma visão de portfólio de riscos, pois permite "determinar se o seu perfil de risco residual é compatível ao seu apetite a riscos relativo aos objetivos".

Tendo em vista que no âmbito dos tópicos 1.2.7.1 e 2.1.3.2 concluiu-se pela inexistência de registro de riscos em planilhas/sistemas, também não foi identificada documentação contendo o cálculo do risco residual. Trata-se, portanto, de prática não implementada.

Desse modo, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever também a forma de calcular e documentar o risco residual nos processos, nas atividades e nos projetos priorizados para terem seus riscos gerenciados.

2.2. Avaliação e resposta a riscos

Nesse componente, apurou-se a seguinte questão: em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente aos riscos identificados e analisados como significativos?

Buscou-se, para tanto, avaliar se as atividades de avaliação e resposta a riscos permitem que sejam tomadas decisões conscientes, razoáveis e efetivas para o tratamento dos riscos identificados como prioritários, bem como para reforçar a responsabilidade das pessoas designadas para implementar e reportar as ações de tratamento. A avaliação foi realizada a partir de quatro aspectos: 2.2.1. Critérios para priorização de riscos; 2.2.2. Processos de avaliação e seleção das respostas a riscos; 2.2.3. Pessoas envolvidas nos processos de avaliação e seleção das respostas a riscos; 2.2.4. Planos e medidas de contingência; e 2.2.5 Documentação da avaliação e seleção das respostas a riscos.

Inicialmente, destaca-se que, no processo de gestão de riscos preconizado pela ISO 31000:2018, após as etapas de identificação e análise, ocorre a etapa de *avaliação* de riscos. Com base nessas três etapas é que é possível partir para a etapa de *tratamento*, que contempla a definição de respostas a riscos. Assim, o presente capítulo tratará dos resultados das análises em

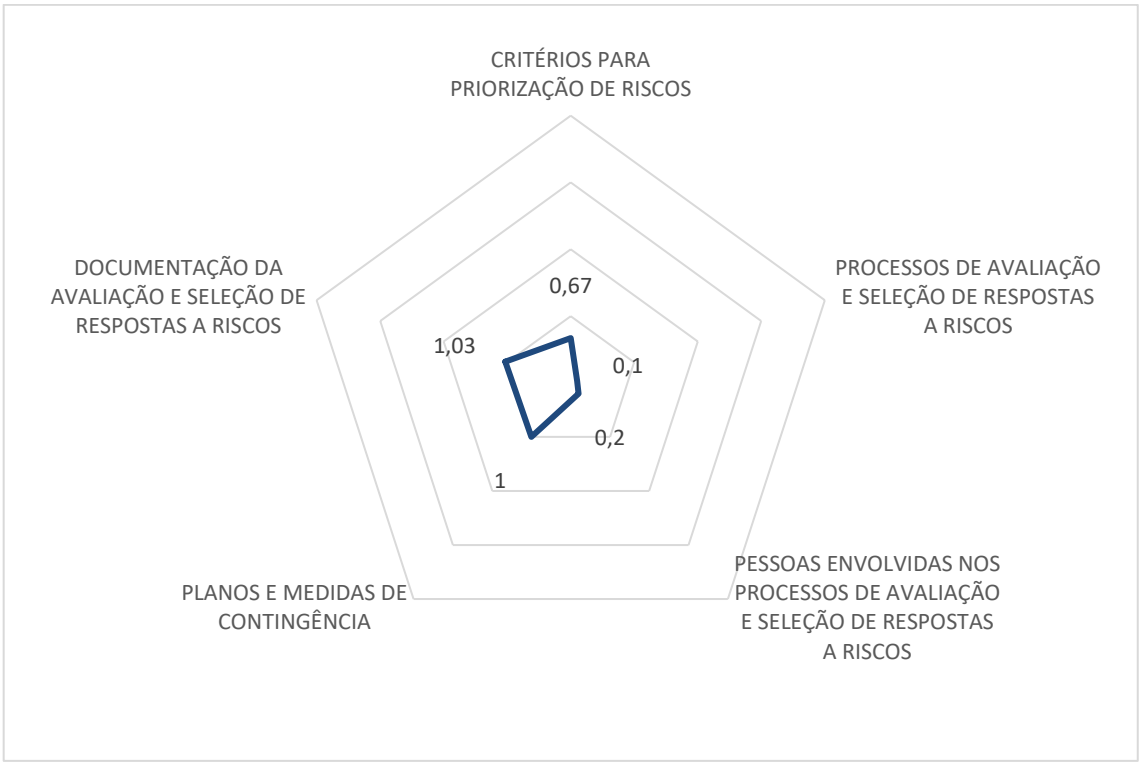
relação ao processo de avaliação de riscos juntamente com a definição de respostas de tratamento, no âmbito do FNDE.

Conforme a norma ISO acima referida, a análise de riscos fornece uma entrada para a avaliação de riscos. Esta etapa, por sua vez, consiste na comparação dos resultados da análise de riscos com os critérios definidos, apoiando as decisões e permitindo determinar onde é necessário algum tipo de tratamento. Assim, isso pode levar a uma decisão de: "fazer mais nada; considerar as opções de tratamento; realizar análises adicionais para melhor compreender o risco; manter os controles existentes; reconsiderar os objetivos". Ademais, a norma destaca que é preciso levar em consideração "o contexto mais amplo e as consequências reais e percebidas para as partes interessadas externas e internas".

Com base nessa decisão, parte-se para o tratamento de riscos, cujo propósito é "selecionar e implementar ações para abordar riscos". Esse processo considera uma análise de custo-benefício entre implementar ações de tratamento e o alcance de objetivos. Conforme o COSO-GRC (2007), as *respostas a riscos* incluem: *evitar*, descontinuando as atividades que geram os riscos; *reduzir*, adotando medidas que diminuam a probabilidade ou o impacto do risco (ou ambos, quando necessário); *compartilhar*, transferindo ou compartilhando uma porção do risco (como nos casos de aquisição de seguros ou terceirização de atividades); ou *aceitar*, quando nenhuma medida é adotada para afetar a probabilidade ou o impacto do risco.

No FNDE, o resultado do componente "Avaliação e resposta a riscos", a partir da avaliação dos seus aspectos, demonstra uma maturidade INICIAL, apurada em **8,00%**. O gráfico a seguir apresenta o resultado consolidado do componente:

Gráfico 39: Resultado da avaliação dos objetos – Componente Avaliação e resposta a riscos (resultado por aspecto)



Fonte: elaboração própria.

Já o próximo gráfico, apresenta os resultados de cada objeto analisado nos cinco aspectos que integram o componente “Avaliação e resposta a riscos”:

Gráfico 40: Resultado da avaliação dos objetos – Componente Avaliação e resposta a riscos (resultado por objeto)

Fonte: elaboração própria.

Dos gráficos 39 e 40, percebe-se que o grau de maturidade dos processos de avaliação e resposta a riscos no FNDE, ainda que inicial é maior do que a maturidade observada nos processos de identificação e análise de riscos (retratada no Gráfico 32). Tal situação se deu pois, mesmo sem a adequada formalização do processo de gestão de riscos (com o cumprimento de todas as etapas necessárias), a organização trata pontualmente alguns riscos significativos. No entanto, conforme será destacado nos próximos tópicos, esse tratamento decorre, em grande medida, mais da atuação de órgãos de controle e da necessidade de responder a eventos já concretizados, do que de um planejamento formalizado.

A seguir apresentam-se os aspectos avaliados no componente Avaliação e resposta a riscos, bem como os objetos relacionados a cada aspecto.

2.2.1. Critérios para priorização de riscos

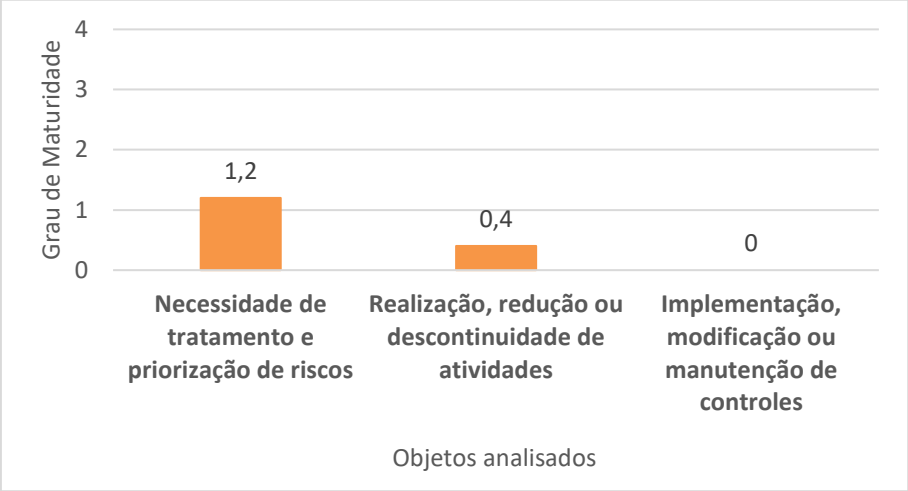
Os critérios estabelecidos para priorização de riscos são adequados para orientar decisões seguras por todo o FNDE?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à existência e à adequação dos critérios de priorização de riscos utilizados para orientar as decisões por toda a organização. A análise foi conduzida pela avaliação de três objetos de análise, a saber: 2.2.1.1.

Necessidade de tratamento e priorização de riscos; 2.2.1.2. Realização, redução ou descontinuidade de atividades; e 2.2.1.3. Implementação, modificação ou manutenção de controles.

A avaliação realizada mostrou que não há critérios de priorização formalmente estabelecidos para definir quais riscos serão tratados em âmbito institucional. Verificou-se, entretanto, que foram estabelecidos alguns critérios para projetos específicos (como no caso do Malha Fina), porém, sem que haja sua vinculação a uma diretriz superior da organização (p. ex., uma Política de Gestão de Riscos).

Gráfico 41: Resultado da avaliação – Aspecto Estabelecimento do contexto



Fonte: elaboração própria.

Dessa forma, os tópicos a seguir trazem informações sobre os objetos analisados e, ainda, boas práticas relacionadas ao conteúdo mínimo a ser observado na definição de critérios relacionados às etapas de avaliação e seleção de respostas a riscos.

2.2.1.1. Necessidade de tratamento e priorização de riscos

Os testes previstos buscaram avaliar se há critérios estabelecidos para priorização de riscos, levando em conta, por exemplo, a significância ou os níveis e tipos de risco, os limites de apetite a risco, as tolerâncias a risco ou variações aceitáveis no desempenho, os níveis recomendados de atenção, os critérios de comunicação a instâncias competentes, o tempo de resposta requerido, bem como se esses critérios revelam-se adequados para orientar decisões seguras quanto à necessidade de tratamento e priorização de um determinado risco. Nesse contexto, também foi coletada a percepção dos servidores e da Alta Administração sobre o tema.

A IN nº 01/2016, dispõe que precisam ser priorizados os temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão. Assim, após a identificação e a análise, tem-se uma base para definir quais riscos serão priorizados.

Acerca da definição de critérios de riscos, a norma ISO 31000:2018 indica que a organização especifique a quantidade e o tipo de risco que pode assumir em relação aos seus objetivos, bem como que estabeleça os critérios para avaliar a significância do risco e para apoiar a tomada de decisões.

Nesse sentido, o RMAF (UK, 2009) ressalta alguns critérios que podem ser definidos para avaliar riscos, como:

- questões financeiras ou relação custo-benefício;
- entrega de serviços ou qualidade dos serviços;
- preocupação pública / confiança pública;
- grau e natureza dos riscos para a sociedade;
- reversibilidade ou não da realização do risco;
- qualidade ou confiabilidade das evidências em torno do risco;
- impacto do risco na organização (incluindo questões relacionadas à sua reputação), nas partes interessadas (incluindo na sociedade), nas suas parcerias, dentre outros; e
- defensibilidade da realização do risco.

O guia estabelece, ainda, que os critérios selecionados precisam ser aplicados de forma consistente e metódica na lista de riscos identificados e priorizados para tratamento.

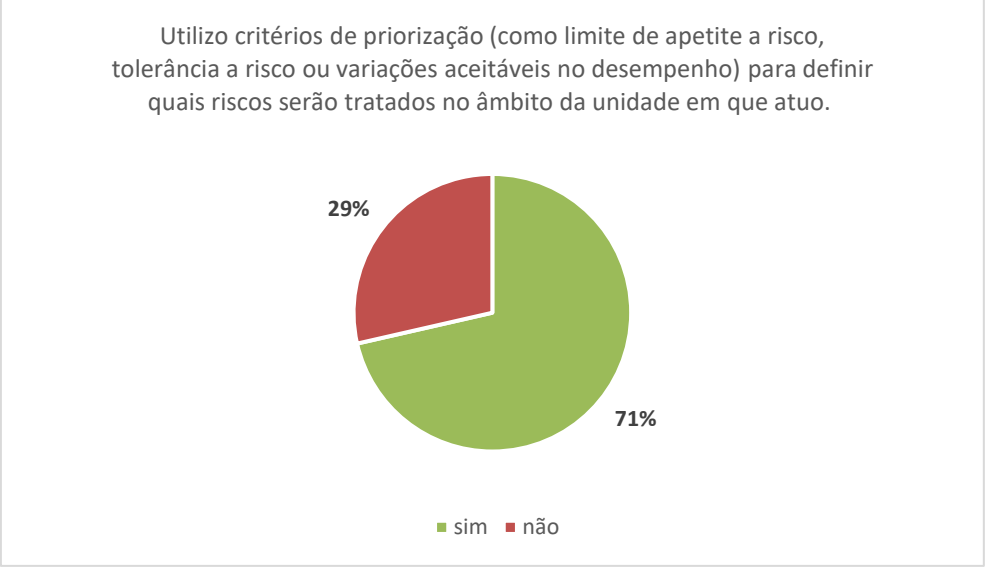
A avaliação realizada mostrou que o FNDE não definiu formalmente critérios para orientar a priorização de riscos e dar garantia razoável de que decisões seguras quanto a se um determinado risco precisa de tratamento (e a prioridade para isso) estão sendo tomadas por toda a organização. A ausência de uma Política de Gestão de Riscos (ou de outro documento equivalente) prejudica esse aspecto, dado que não há diretrizes que tratem da etapa de avaliação e resposta a riscos.

No entanto, observou-se o funcionamento da prática no âmbito de alguns projetos específicos, como é o caso do Malha Fina. Esse modelo é amparado por critérios de priorização para análise das prestações de contas, a partir de faixas de riscos pré-estabelecidas e de aspectos relacionados a materialidade, risco e sustentabilidade. Assim, especificamente em relação ao Malha Fina, entende-se que os critérios estabelecidos se encontram respaldados em uma análise prévia do nível de exposição a riscos.

Porém, cabe destacar que, tendo em vista a ausência diretrizes institucionais de gestão de riscos, não há vinculação entre o nível de exposição a riscos que respalda os critérios definidos para o Malha Fina com limites de apetite a risco, tolerâncias, variações aceitáveis no desempenho e níveis recomendáveis de atenção previamente definidos para toda a Autarquia.

Adicionalmente, destaca-se que, da coleta de percepção da Alta Administração acerca do tema, 71% dos respondentes afirmaram utilizar critérios de priorização (como limite de apetite a risco, tolerância a risco ou variações aceitáveis no desempenho) para definir quais riscos serão tratados no âmbito da unidade em que atuam, conforme gráfico a seguir:

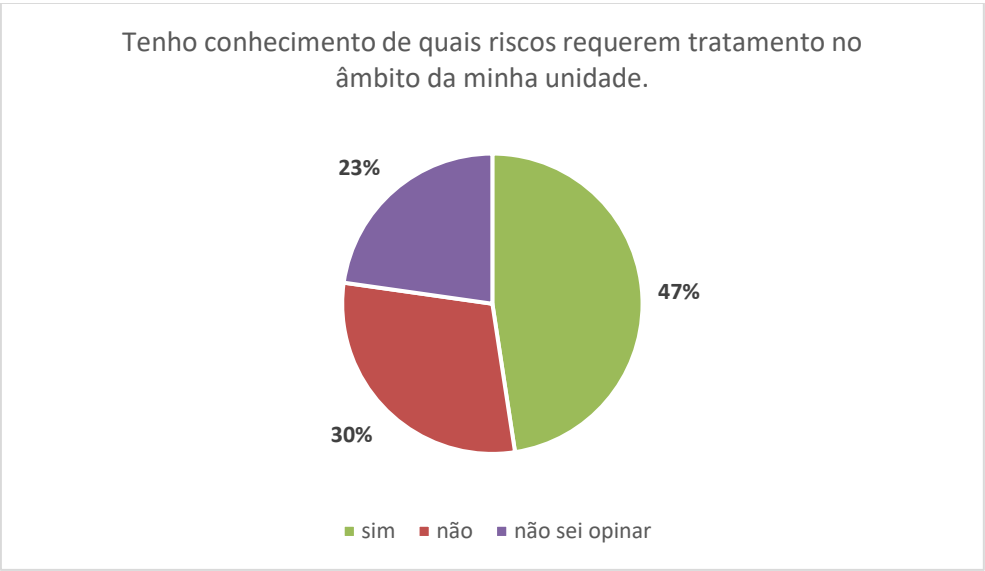
Gráfico 42: Percepção da Alta Administração – Necessidade de tratamento e priorização de riscos



Fonte: elaboração própria.

Já em relação à percepção dos servidores, 53% afirmaram não ter conhecimento de quais riscos requerem tratamento no âmbito de suas unidades ou não saber opinar sobre o tema.

Gráfico 43: Percepção dos servidores – Necessidade de tratamento e priorização de riscos



Fonte: elaboração própria.

A conclusão é que se trata de uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização, mas cujo funcionamento é observado e percebido em algumas áreas/processos relevantes.

Assim, eventuais política e procedimentos de gestão de riscos a serem implementados precisam considerar que a resposta a riscos precisa ser respaldada em critérios expressamente definidos e que a escolha da estratégia de tratamento depende do nível de exposição de riscos

previamente estabelecido pela organização, em confronto com a avaliação que se fez do risco, conforme preconizado pela IN nº 01/2016.

2.2.1.2. Realização, redução ou descontinuidade de atividades

Os testes previstos buscaram avaliar se os critérios estabelecidos para priorização de riscos revelam-se adequados para orientar decisões seguras quanto à realização, à redução ou à descontinuidade de uma atividade. Ainda, coletou-se a percepção da Alta Administração sobre o objeto.

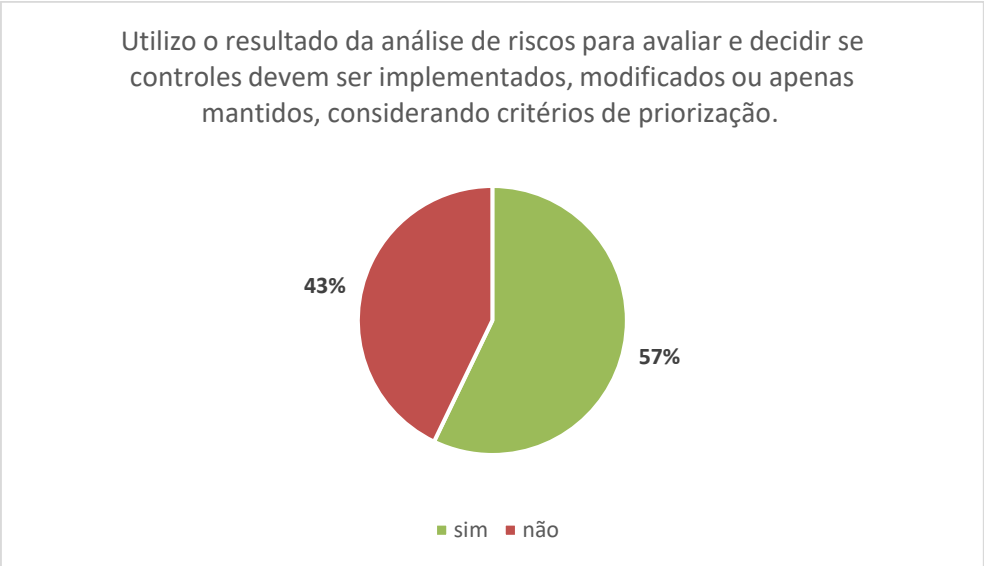
Conforme dispõe a IN nº 01/2016, ao implementar um modelo de gestão de riscos, a Alta Administração, bem como seus servidores ou funcionários, deverá definir as respostas a riscos, identificando qual estratégia seguir (evitar, transferir, aceitar ou tratar) em relação aos riscos mapeados e avaliados, a partir do nível de exposição a riscos previamente estabelecido.

A ISO 31000:2018 orienta ainda que, após a avaliação de riscos, os resultados dessa etapa sejam comparados com os critérios de risco estabelecidos, de modo a determinar as ações necessárias. Dessa forma, isso pode "levar a uma decisão de: fazer mais nada; considerar as opções de tratamento de riscos; realizar análises adicionais para melhor compreender o risco; manter os controles existentes, reconsiderar os objetivos". Assim, há uma base para refletir também sobre a realização, a redução ou a descontinuidade das atividades objeto da gestão de riscos.

A análise realizada demonstrou que o FNDE não definiu formalmente critérios para orientar a priorização de riscos e para dar garantia razoável de que decisões seguras quanto a se uma atividade deve ser realizada, reduzida ou descontinuada estão sendo tomadas.

Todavia, no que se refere à percepção da Alta Administração, 57% dos gestores que responderam ao questionário enviado afirmaram utilizar o resultado da etapa de análise de riscos para avaliar e decidir se uma atividade deve ser realizada, reduzida ou descontinuada no âmbito das unidades em que atuam, conforme gráfico a seguir:

Gráfico 44: Percepção da Alta Administração – Realização, redução ou descontinuidade de atividades



Fonte: elaboração própria.

Assim, considerando a ausência de mecanismos de suporte, verificou-se que se trata de uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização, mas cujo funcionamento é percebido por alguns gestores.

2.2.1.3. Implementação, modificação ou manutenção de controles

Os testes previstos buscaram avaliar se os critérios estabelecidos para priorização de riscos revelam-se adequados para orientar decisões seguras quanto à implementação, à modificação ou à manutenção de controles. Ainda, coletou-se a percepção da Alta Administração sobre o objeto.

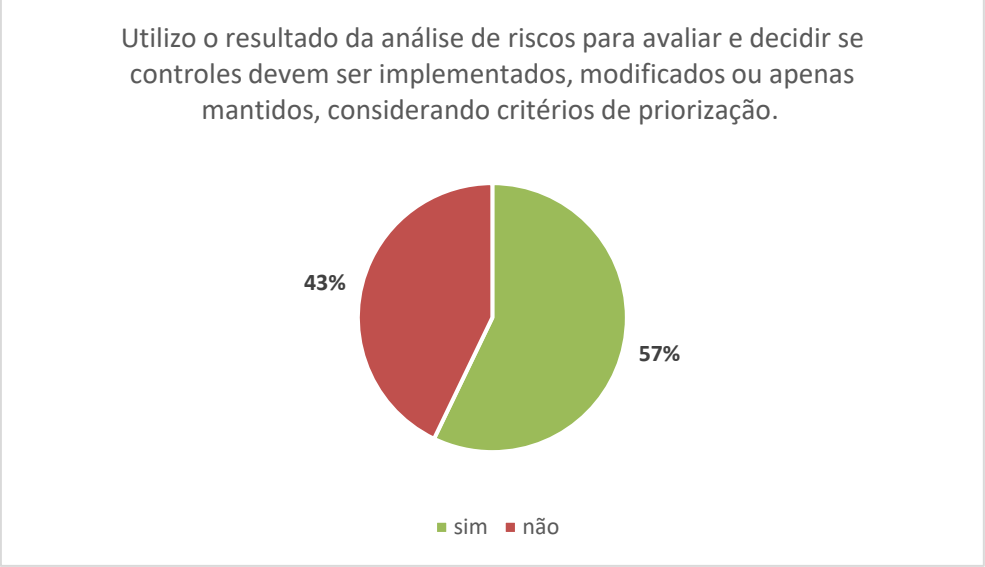
Dispõe a IN nº 01/2016, que os órgãos e entidades do Poder Executivo federal devem "implementar, manter, monitorar e revisar os controles internos da gestão, tendo por base a identificação, a avaliação e o gerenciamento de riscos que possam impactar a consecução dos objetivos estabelecidos pelo Poder Público". Assim, os controles internos da gestão devem basear-se no gerenciamento de riscos.

Segundo o COSO-CI (2013), a organização, para assegurar que as respostas a risco sejam executadas de forma adequada e oportuna, precisa identificar também as atividades de controle necessárias. Esclarece, ainda, que, "da mesma forma que a seleção de respostas a riscos considera a adequação e os riscos remanescentes ou residuais, a seleção ou a revisão das atividades de controle deve avaliar a pertinência e a adequação aos objetivos correspondentes".

Assim, verificou-se que o FNDE não definiu formalmente critérios para orientar a priorização de riscos e dar garantia razoável quanto a se controles devem ser implementados, modificados ou apenas mantidos. Por isso, não é possível afirmar que a organização atrelou o processo de revisão dos seus controles a um processo de gestão de riscos, especialmente por intermédio de atividades de avaliação e seleção de opções de tratamento.

Todavia, considerando a percepção da Alta Gestão, 57% dos dirigentes acreditam que os controles internos existentes são avaliados em relação aos riscos identificados. O mesmo percentual de respondentes afirmou que utiliza o resultado de análises de risco para avaliar e decidir sobre controles, conforme gráfico a seguir:

Gráfico 45: Percepção da Alta Administração – Implementação, modificação ou manutenção de controles



Fonte: elaboração própria.

Assim, conclui-se que se trata de uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização. No entanto, seu funcionamento é percebido por alguns gestores.

2.2.2. Processos de avaliação e seleção das respostas a riscos

A seleção de respostas para tratar riscos considera todas as opções de tratamento e o seu custo-benefício?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à existência e à adequação dos processos de seleção de respostas para tratar riscos. A análise foi conduzida pela avaliação do objeto de análise 2.2.2.1. Relação custo-benefício.

Considerando que não houve a definição formal de processos de avaliação e seleção de respostas a riscos pela organização (conforme concluído no aspecto 2.2.1), a avaliação realizada mostrou que também não há um processo disseminado pela organização considerando a avaliação de custo-benefício na decisão de implementar atividades de controle ou outras ações e medidas para tratar riscos.

Dessa forma, os tópicos a seguir trazem informações sobre o objeto analisado e, ainda, boas práticas relacionadas ao conteúdo mínimo a ser observado na definição de critérios relacionados às etapas de avaliação e seleção de respostas a riscos.

2.2.2.1. Relação custo-benefício

Os testes previstos buscaram verificar se as etapas de avaliação e seleção das respostas – adotadas para reduzir a exposição aos riscos identificados – consideram uma relação de custo-

benefício na decisão de implementar atividades de controle ou outras ações e medidas, bem como se consideram os controles internos em funcionamento.

Após as etapas de identificação, análise e avaliação de riscos, são definidas as respectivas medidas de tratamento para os riscos priorizados, por intermédio da seleção de respostas adequadas. Segundo a norma ISO 31000:2018, existe a necessidade de se balancearem os benefícios potenciais das respostas em relação ao alcance dos objetivos frente ao custo, ao esforço ou às desvantagens da implementação das medidas de tratamento selecionadas.

Apurou-se que o FNDE não definiu formalmente processos de avaliação e seleção de respostas a riscos (conforme já especificado nos objetos que integram o aspecto 2.2.1), de modo que a definição de respostas a serem adotadas para reduzir a exposição aos riscos identificados não perpassa um processo disseminado pela organização e que considere uma análise de custo-benefício. A ausência de uma Política de Gestão de Riscos ou de outro documento equivalente prejudica esse aspecto, dado que não há diretrizes sobre o tema.

Nesse contexto, eventuais política e procedimentos a serem instituídos na Autarquia devem prever a forma de avaliar essa relação de custo-benefício entre controles e objetivos alcançados. Ainda, cabe destacar que a avaliação sobre riscos que precisam ser priorizados para tratamento e para implementação de controles não pode ignorar eventuais ações que já existam, de modo a evitar a duplicação de esforços ou o sombreamento de atividades.

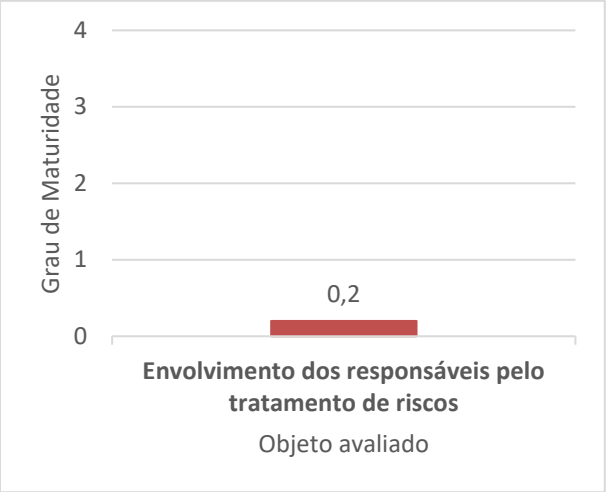
2.2.3. Pessoas envolvidas nos processos de avaliação e seleção das respostas a riscos

Os responsáveis pelo tratamento de riscos são envolvidos no processo de avaliação e seleção das respostas e são formalmente comunicados das ações de tratamento decididas?

Com vistas a avaliar este aspecto, foram previstos testes relacionados ao envolvimento de pessoas adequadas nos processos de seleção de respostas para tratar riscos. A análise foi conduzida pela avaliação do objeto de análise 2.2.3.1. Envolvimento dos responsáveis pelo tratamento de riscos.

Considerando que não houve a definição formal de processos de avaliação e seleção de respostas a riscos pela organização, a avaliação realizada mostrou que também não foram formalmente definidos os responsáveis pelo tratamento dos riscos. No entanto, existe um certo grau de percepção entre os servidores acerca de quem são os responsáveis por esse tratamento e sobre as formas de comunicá-los.

Gráfico 46: Resultado da avaliação – Aspecto Pessoas envolvidas nos processos de avaliação e seleção das respostas a riscos



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

2.2.3.1. Envolvimento dos responsáveis pelo tratamento de riscos

Os testes previstos buscaram avaliar se todos os responsáveis pelo tratamento de riscos são envolvidos no processo de seleção das opções de resposta e na elaboração dos planos de tratamento. Avaliou-se, ainda, se estes responsáveis são formalmente comunicados das ações de tratamento decididas, para garantir que sejam adequadamente compreendidas, se comprometam e sejam responsabilizados por elas. Por fim, coletou-se a percepção dos servidores quanto ao objeto.

A IN nº 01/2016, em seu art. 20, determina que "cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente identificado". Nesse contexto, o agente responsável deve ser o "gestor com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco". Suas responsabilidades envolvem:

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

Conforme já abordado na descrição do objeto de análise 1.1.2.1, as instâncias e os mecanismos definidos para apoiar as responsabilidades de governança de riscos e assegurar que a gestão de riscos seja integrada aos processos de gestão encontram-se em nível inicial de existência, carecendo de funcionamento direcionado e coordenado.

Adicionalmente, no objeto de análise relatado no tópico 1.2.5.3, verificou-se que a organização não dispõe de uma Política de Gestão de Riscos estabelecida e aprovada pela Alta Administração (ou de outro documento equivalente), o que prejudica o adequado estabelecimento de responsabilidades, competências e autoridades para as etapas do processo de gestão de riscos.

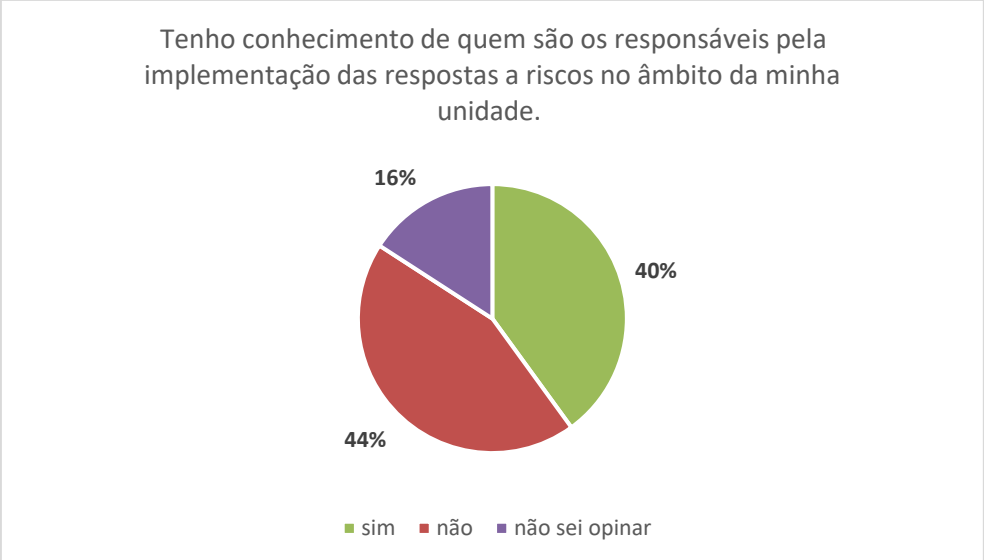
Ainda, no que se refere ao objeto de análise 1.2.6.1, que tratou do comprometimento da gestão para o estabelecimento e a revisão da estrutura e do processo de gestão de riscos e controles internos, concluiu-se que o comprometimento da Alta Gestão se encontra em nível inicial de maturidade, o que indica uma prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chave da organização (prejudicada pela ausência de diretrizes formalizadas).

Por fim, da avaliação do objetivo de análise 1.2.7.1, acerca da alocação de recursos para a gestão de riscos, concluiu-se que não existem pessoas, recursos, ferramentas e metodologias especificamente alocados para a gestão de riscos, em que pese a identificação de algumas iniciativas pontuais e mesmo alguma percepção sobre o tema.

Ademais, conforme já relatado nos objetos que compõem o aspecto 2.2.1, o FNDE não definiu formalmente processos de avaliação e seleção de respostas a riscos. Consequentemente, também não foram definidos os responsáveis pelos riscos e por seu tratamento. Assim, trata-se de uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização.

Da percepção dos servidores coletada, observou-se que apenas 21% dos respondentes já participaram de atividades de avaliação de riscos em suas unidades de atuação. Desses 21%, 90% disseram ter conhecimento dos riscos relacionados a atividades, projetos e processos em suas unidades de atuação. Complementarmente, destaca-se que 43% afirmaram ter conhecimento das respostas a riscos (evitar, reduzir, compartilhar ou aceitar) a serem adotadas para cada risco da sua unidade priorizado para tratamento e 40% manifestaram ter conhecimento acerca de quem são os responsáveis pela implementação dessas respostas:

Gráfico 47: Percepção dos servidores – Envolvimento dos responsáveis pelo tratamento de riscos



Fonte: elaboração própria.

Destaca-se também que 19% disseram ter conhecimento do cronograma a ser seguido para tratar os riscos identificados e priorizados; 26% informaram ter conhecimento das medidas de desempenho e dos requisitos para o reporte de informações relacionadas ao tratamento dos riscos; e 26% declararam ter conhecimento das formas de monitorar a implementação de medidas de tratamento de riscos.

Da análise realizada, observa-se, portanto, que, mesmo diante da falta de procedimentos formalizados e padronizados na organização no que se refere aos processos de avaliação e seleção de respostas a riscos, existe uma parcela de servidores que atua no FNDE e que reconhece a existência de responsáveis e de mecanismos associados à etapa de tratamento de risco. Cabe, assim, a formalização das instâncias e dos mecanismos bem como a indicação dos responsáveis pela gestão de riscos, para que possa ocorrer seu envolvimento no processo de tratamento de riscos.

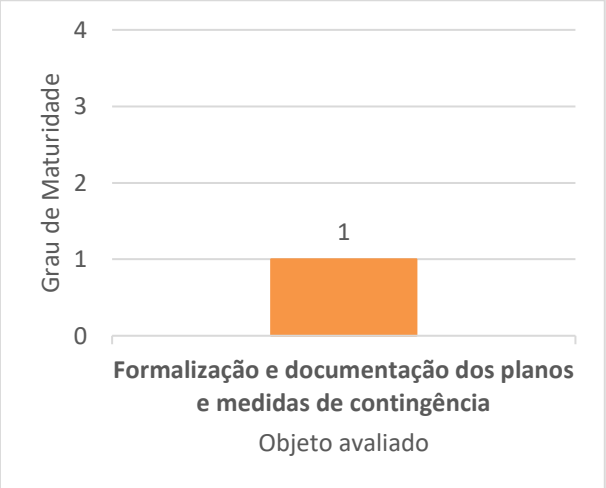
2.2.4. Planos e medidas de contingência

Os elementos críticos da atuação do FNDE estão identificados e têm definidos planos e medidas de contingência?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à existência e à adequação de planos e medidas de contingência formalizados e documentados para todas as áreas, funções e atividades relevantes do FNDE. A análise foi conduzida pela avaliação do objeto de análise 2.2.4.1. Formalização e documentação de planos e medidas de contingência.

Considerando que não houve a definição formal de processos de avaliação e seleção de respostas a riscos pela organização, a avaliação realizada mostrou que também não foram formalmente definidos planos e medidas de contingência para todas as áreas, funções e atividades relevantes da organização. No entanto, foram identificadas iniciativas no âmbito de unidades específicas e relativas a atividades cuja própria natureza demanda medidas dessa ordem. Também foram definidos Planos de Tratamento de Riscos para o Programa Nacional de Alimentação Escolar – PNAE e o Programa Dinheiro Direto na Escola – PDDE, com vistas ao enfretamento da pandemia do Covid-19.

Gráfico 48: Resultado da avaliação – Aspecto Planos e medidas de contingência



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado:

2.2.4.1. Formalização e documentação dos planos e medidas de contingência

Os testes previstos buscaram avaliar se todas as áreas, funções e atividades relevantes (unidades, processos, projetos) para a realização dos objetivos-chave da organização identificaram os elementos críticos de sua atuação e definiram planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos seus serviços em casos de desastres. Também foi coletada a percepção da Alta Administração e dos servidores sobre o tema.

Acerca do tema, a IN nº 01/2016 dispõe que, ao implementar o modelo de gestão de riscos, a Alta Administração, bem como seus servidores ou funcionários, deverá definir atividades de controles internos, preventivos e detectivos, bem como "a preparação prévia de planos de contingência e resposta à materialização dos riscos".

De acordo com a ISO 31000:2018, o proposito desses planos é "especificar como as opções de tratamento escolhidas serão implementadas, de maneira que os arranjos sejam compreendidos pelos envolvidos e o progresso em relação ao plano possa ser monitorado".

Tendo em vista que o FNDE não definiu formalmente processos de avaliação e seleção de respostas a riscos, não é possível obter segurança razoável de que, na definição de planos e medidas de contingência, sejam adequadamente considerados os elementos críticos da atuação da organização e vinculados os seus objetivos-chave. Adicionalmente, destaca-se que não foram identificados planos de contingência para todas as áreas funções e atividades relevantes do FNDE.

Verificou-se, no entanto, que há iniciativas em áreas específicas, tais como um Plano de Segurança Institucional, em elaboração na CGLOG/DIRAD e com previsão de publicação em novembro/2022, que, entre outros assuntos, irá prever medidas de contingência para gerenciamento de crises; e, ainda, eventuais planos adotados pela DIRTI para os principais sistemas e serviços de tecnologia do FNDE, como os referentes: à política de *backup* operacional; e à adoção de *Disaster Recovery* para os bancos de dados SGBD Oracle, que respondem pela maioria das bases de dados consideradas críticas pela DIRTI.

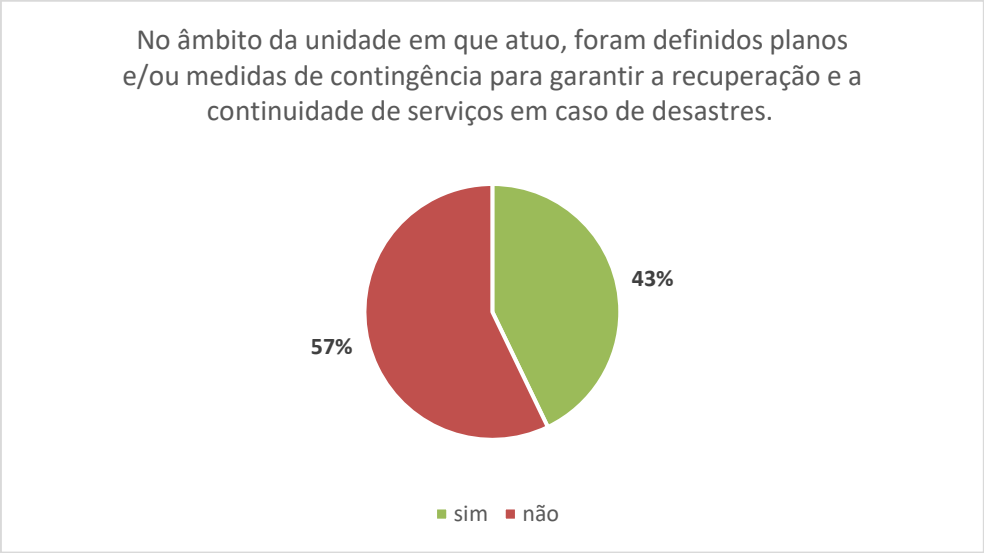
Vale ressaltar que os planos acima mencionados atendem a necessidades pontuais dos macroprocessos das unidades relacionadas, em decorrência, especialmente, da natureza das atividades executadas, que demandam o planejamento desse tipo de medida.

Adicionalmente, existem planos de tratamento de riscos para o Programa Nacional de Alimentação Escolar – PNAE e para o Programa Dinheiro Direto na Escola – PDDE, criados no contexto do Coopera (Programa especial de atuação no enfrentamento à crise da Covid-19) e instituídos por recomendação do TCU. Além de planos de tratamento, entende-se também seu papel enquanto planos de contingência, dado que foram criados para enfrentamento à situação emergencial enfrentada em decorrência da pandemia.

Assim, trata-se de uma prática esporádica, com funcionamento identificado em algumas áreas relevantes, mas não vinculada a diretrizes formais da organização. Novamente, a ausência de instâncias e mecanismos próprios de gestão de riscos prejudica a integração das iniciativas identificadas a um contexto mais amplo e integrado da gestão de riscos.

Por fim, coletada a percepção da Alta Administração, observou-se que 43% dos gestores afirmaram que no âmbito da unidade em que atuam foram definidos planos e/ou medidas de contingência para garantir a recuperação e a continuidade de serviços em caso de desastres. Dos 43% que responderam "sim", 100% afirmaram que esses planos foram formalizados em documentos que contêm as medidas e os controles de atenuação e recuperação a serem executados após a ocorrência do risco, com o intuito de diminuir o impacto de suas consequências.

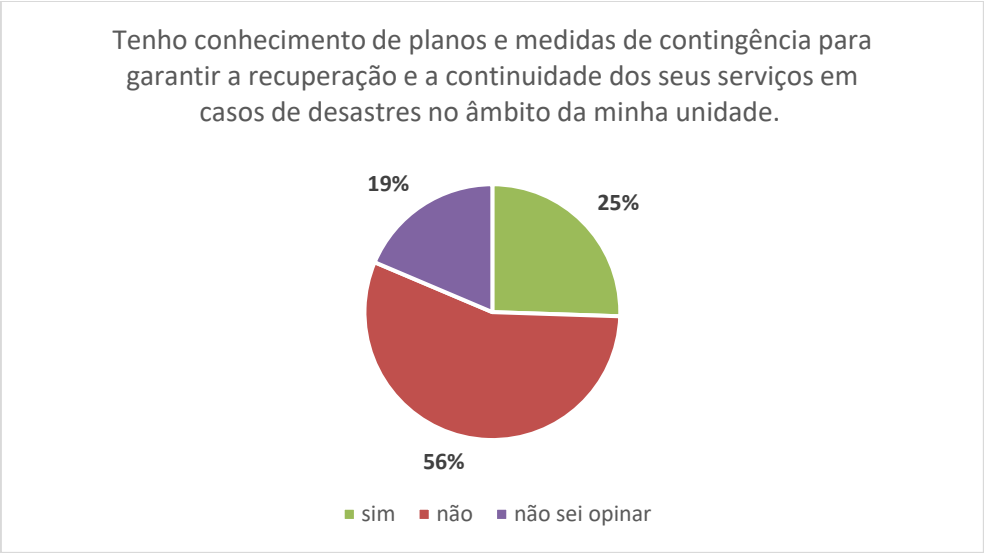
Gráfico 49: Percepção da Alta Administração – Formalização e documentação de planos e medidas de contingência



Fonte: elaboração própria.

Já no que se refere à percepção dos servidores, 56% afirmaram não ter conhecimento da existência de planos e medidas de contingência para garantir a recuperação e a continuidade dos seus serviços em casos de desastres no âmbito da sua unidade; ainda, 19% não souberam opinar sobre o tema, conforme abordado no próximo gráfico:

Gráfico 50: Percepção dos servidores – Formalização e documentação dos planos e medidas de contingência



Fonte: elaboração própria.

Pelo exposto, observa-se que a prática não foi implementada e instituída formalmente, de forma integrada e padronizada pela organização, mas cujo funcionamento é identificado em alguns processos críticos da Autarquia, sendo moderadamente percebido pela Alta Gestão e pouco percebido pelos servidores.

2.2.5. Documentação da avaliação e seleção de respostas a riscos

A documentação da avaliação e seleção de respostas a riscos inclui elementos suficientes para permitir o gerenciamento adequado da implementação das respostas?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à documentação dos processos de avaliação e seleção de respostas de riscos instituídos (ou seja, à documentação dos objetos avaliados nos aspectos 2.1.1 a 2.2.3), a partir de seis objetos de análise: 2.2.5.1. Plano de tratamento de risco; 2.2.5.2. Priorização de tratamento; 2.2.5.3. Razões para a seleção das opções de tratamento; 2.2.5.4. Recursos, cronograma e benefícios esperados; 2.2.5.5. Medidas de desempenho e reporte; e 2.2.5.6. Responsáveis pela aprovação e pela implementação.

De acordo com a ISO 31000:2018, é de suma importância que o processo de gestão de riscos e seus resultados sejam documentados e relatados por meio de mecanismos adequados. Esses registros objetivam comunicar atividades e resultados de gestão de riscos por toda a organização, fornecer informações para a tomada de decisão, aprimorar as atividades de gestão de riscos e auxiliar no relacionamento com as partes interessadas. Além disso, o relato serve para dar suporte à Alta Administração e para o cumprimento das responsabilidades pelo órgão de supervisão.

Ainda, a norma estabelece que o resultado da avaliação de riscos seja registrado, comunicado e então validado nos níveis apropriados da organização. Nesse sentido, a documentação da avaliação e seleção de respostas a riscos deve conter, no mínimo, informações sobre:

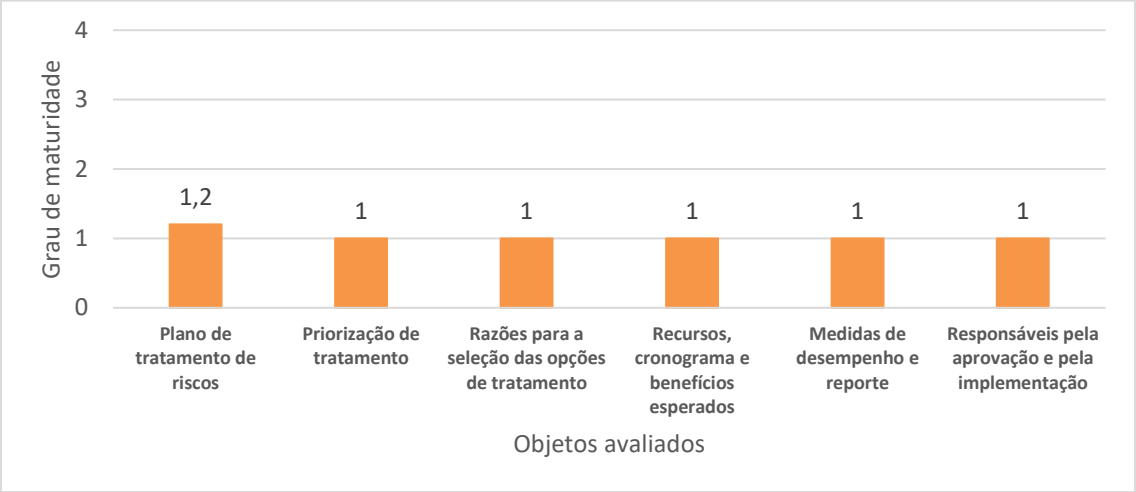
- a justificativa para a seleção das opções de tratamento, incluindo os benefícios esperados;
- aqueles que serão responsáveis por aprovar e implementar o plano;
- as ações propostas;
- os recursos requeridos, incluindo contingências;
- as medidas de desempenho;
- as restrições;
- os relatos e monitoramento requeridos; e
- quando se espera que as ações sejam tomadas e concluídas.

Em que pese a inexistência de processos e atividades relacionadas ao estabelecimento das etapas de avaliação e tratamento para a gestão de riscos, citada no aspecto 2.2.1, algumas iniciativas relacionadas à documentação das etapas de avaliação e seleção de respostas a riscos específicos foram encontradas nesse aspecto, especialmente a partir de planos de tratamento de riscos, o que acabou elevando a pontuação apurada para os objetos analisados.

No entanto, com exceção das práticas pontuais documentadas nesse aspecto (especialmente no âmbito da atuação de enfrentamento à pandemia do Covid-19, envolvendo PNAE

e PDDE), avaliou-se que não há adequada documentação das etapas no âmbito de um processo mais amplo de gestão de riscos da organização.

Gráfico 51: Resultado da avaliação – Aspecto Documentação da avaliação e seleção de respostas a riscos



Fonte: elaboração própria.

Dessa forma, os tópicos a seguir trazem informações sobre as análises realizadas e, ainda, boas práticas para a adequada documentação dessa etapa.

2.2.5.1. Plano de tratamento de riscos

Os testes previstos buscaram avaliar se a documentação das etapas de avaliação e seleção de respostas aos riscos inclui o plano de tratamento de riscos, preferencialmente integrado ao registro de riscos da organização, identificando claramente os riscos que requerem tratamento e suas respectivas classificações (de probabilidade, impacto, níveis de risco etc.). Ainda, coletou-se a percepção da Alta Administração sobre o tema.

Acerca da preparação e implementação de Planos de Tratamento de Riscos, a norma ISO 31000:2018 dita que seu propósito é "especificar como as opções de tratamento selecionadas serão implementadas", de forma compreensível aos envolvidos e possibilitando o monitoramento do seu progresso. Os planos de tratamento devem, ainda, ser integrados aos planos e processos da gestão, em consulta com suas partes interessadas.

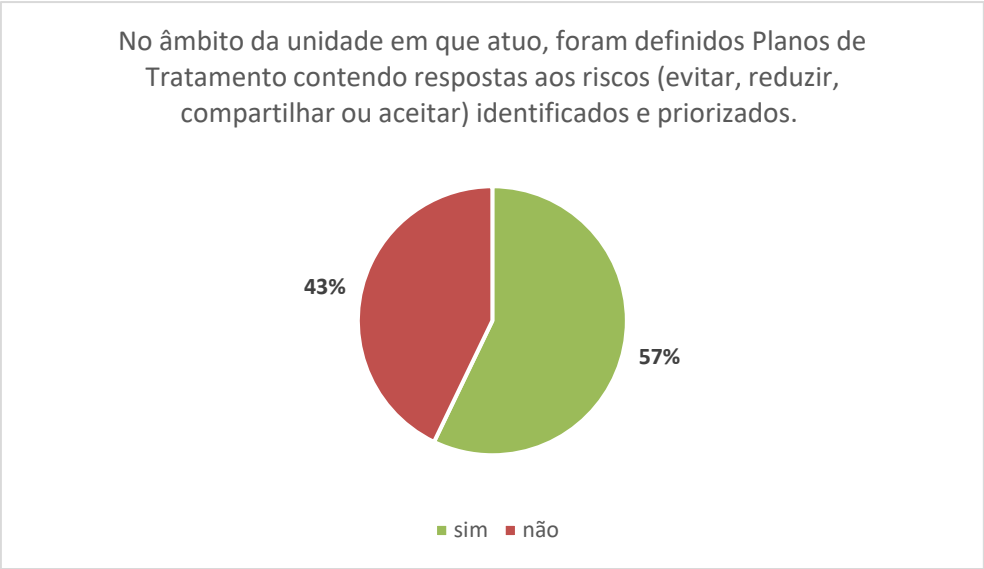
Da análise do objeto, apurou-se que o FNDE não definiu formalmente processos de avaliação e seleção de respostas a riscos, de modo que não há diretrizes para orientar a elaboração de planos de tratamento no contexto de um processo estruturado de gestão de riscos. Adicionalmente, a organização auditada corroborou essa informação, afirmando que não foram estabelecidos planos de tratamento de riscos ou outros documentos identificando os riscos que requerem tratamento e as respectivas respostas a serem adotadas.

Embora tenham sido elaborados Planos de Tratamento de Riscos para o PNAE e o PDDE durante a pandemia do Covid-19 (conforme já abordado no tópico 2.2.4.1), não há integração desses planos com um registro de riscos da organização. Ademais, a elaboração desses planos não

partiu de um processo instituído pelo FNDE para priorização, identificação, análise e avaliação dos riscos, mas sim de uma situação emergencial e de recomendação do TCU.

Coletada a percepção da Alta Administração, apurou-se que 43% dos gestores declararam que, no âmbito da unidade em que atuam, foram definidos Planos de Tratamento contendo respostas aos riscos identificados e priorizados. Destes 43%, todos afirmaram que os Planos definidos em suas unidades foram formalizados em documentos contendo as iniciativas definidas para tratamento, bem como informações sobre como se dará a implementação das respostas aos riscos.

Gráfico 52: Percepção da Alta Administração – Plano de tratamento de riscos



Fonte: elaboração própria.

Trata-se, portanto, de uma prática não instituída de forma padronizada na organização, mas com funcionamento identificado em algumas áreas relevantes, especialmente por necessidade de atendimento de uma situação emergencial, no âmbito de recomendação de órgão de controle, e com certo grau de percepção entre os gestores.

Assim, eventuais política e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, a forma de documentar as ações previstas para tratamento dos riscos, considerando também as boas práticas já abordadas nos demais tópicos desse componente.

2.2.5.2. Priorização de tratamento

Os testes previstos buscaram avaliar se a documentação das etapas de avaliação e seleção de respostas aos riscos inclui a ordem de prioridade para cada tratamento.

Uma informação importante a ser incluída nos Planos de Tratamento de Riscos é a priorização estabelecida para cada tratamento. Tendo em vista que a seleção das respostas a riscos envolve o balanceamento de benefícios frente aos custos, “as opções de tratamento não são necessariamente mutuamente exclusivas ou apropriadas em todas as circunstâncias”. Por isso, com base nos riscos identificados, analisados e avaliados, é feita a priorização.

Conforme já relatado no objeto de análise 2.2.5.1, verificou-se que a prática de estabelecimento de Planos de Tratamentos de Riscos não está instituída e integrada na organização.

Ressalta-se que, tendo em vista o contexto da pandemia de Covid-19 e a atuação do TCU por intermédio do Programa Coopera, foram estabelecidos pelo FNDE planos de tratamento de riscos para o PNAE e o PDDE. Nesses planos, os gestores classificaram os riscos em ordem de prioridade de atenção, desde o mais significativo ao menos relevante, conforme desdobramentos do Acórdão nº 1955/2020-TCU-Plenário. No entanto, ressalta-se novamente que não há integração desses planos com um registro de riscos da organização.

Assim, eventuais política e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, a forma de documentar a ordem de priorização de tratamento, considerando também as boas práticas já abordadas nos demais tópicos desse componente, bem como a experiência obtida no âmbito do Coopera.

2.2.5.3. Razões para a seleção das opções de tratamento

Os testes previstos buscaram avaliar se a documentação das etapas de avaliação e seleção de respostas inclui as razões para a escolha das opções de tratamento.

A ISO 31000:2018 exemplifica algumas opções para tratar riscos, que podem ser utilizadas de forma individual ou combinada:

- evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco;
- assumir ou aumentar o risco de maneira a perseguir uma oportunidade;
- remover a fonte de risco;
- mudar a probabilidade;
- mudar as consequências;
- compartilhar o risco; e
- reter o risco por decisão fundamentada.

Assim, é importante que os planos de tratamento contenham também a justificativa para as opções selecionadas, inclusive no que se refere à análise de custo-benefício realizada para se chegar naquele tratamento. Conforme a ISO 31000:2018, a justificativa é mais ampla do que apenas considerações econômicas, envolvendo também os objetivos da organização e outros fatores, como: obrigações assumidas, pontos de vista das partes interessadas e critérios de risco definidos. Por fim, vale ressaltar que o tratamento de riscos pode introduzir novos riscos, que também precisarão ser gerenciados.

Conforme já relatado no objeto de análise 2.2.5.1, verificou-se que a prática de estabelecimento de Planos de Tratamentos de Riscos não está instituída e integrada na organização, mas que há iniciativas pontuais (como no caso do PNAE e do PDDE) sendo executadas.

Assim, eventuais política e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, a forma de documentar as razões para a seleção das opções de tratamento, considerando também as boas práticas já abordadas nos demais tópicos desse componente.

2.2.5.4. Recursos, cronograma e benefícios esperados

Os testes previstos buscaram avaliar se a documentação das etapas de avaliação e seleção de respostas aos riscos inclui para as ações de tratamento definidas: recursos, cronograma e benefícios esperados.

Outras informações importantes a serem incluídas nos Planos de Tratamento de Riscos são: a previsão de recursos (financeiros, tecnológicos, humanos etc.) a serem utilizados na etapa de tratamento de riscos, o cronograma para as ações a serem desenvolvidas e os benefícios esperados com a adoção das opções selecionadas.

Conforme já relatado no objeto de análise 2.2.5.1, verificou-se que a prática de estabelecimento de Planos de Tratamentos de Riscos não está instituída e integrada na organização, mas que há iniciativas pontuais (como no caso do PNAE e do PDDE) sendo executadas.

Assim, eventuais política e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, a forma de documentar previsão de recursos, cronograma e benefícios esperados, considerando também as boas práticas já abordadas nos demais tópicos desse componente.

2.2.5.5. Medidas de desempenho e reporte

Os testes previstos buscaram avaliar se a documentação das etapas de avaliação e seleção de respostas aos riscos inclui as medidas de desempenho e os requisitos para o reporte de informações relacionadas ao tratamento dos riscos, bem como as formas de monitoramento da sua implementação.

A ISO 31000:2018 recomenda que o processo de gestão de riscos e seus resultados sejam documentados e relatados por meio de mecanismos apropriados. Nesse contexto, é necessário que os planos de tratamento documentem as medidas de desempenho, bem como os relatos e o monitoramento requeridos. Isso permite acompanhar as atividades de tratamento em implementação, auxilia na tomada de decisão e favorece a revisão e o ajuste de atividades, contribuindo com a melhoria das atividades de gerenciamento de riscos.

Conforme já relatado no objeto de análise 2.2.5.1, verificou-se que a prática de estabelecimento de Planos de Tratamentos de Riscos não está instituída e integrada na organização. Assim, apesar de ações pontuais relativas à monitoramento e tratamento de riscos, como relatado, ressalta-se que não há integração desses planos com um registro de riscos da organização.

Assim, eventuais política e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, a forma de documentar as medidas de desempenho e reporte, considerando também as boas práticas já abordadas nos demais tópicos desse componente, bem como a experiência obtida no âmbito do Coopera.

2.2.5.6. Responsáveis pela aprovação e pela implementação

Os testes previstos buscaram avaliar se a documentação das etapas de avaliação e seleção de respostas aos riscos inclui os responsáveis pela aprovação e pela implementação do plano de tratamento de riscos, com autoridade suficiente para gerenciá-lo.

Ainda de acordo com a ISO 31000:2018, é necessário que os Planos de Tratamento de Riscos especifiquem “aqueles que serão responsabilizáveis e responsáveis por aprovar e implementar o plano”.

Conforme já relatado no objeto de análise 2.2.5.1, verificou-se que a prática de estabelecimento de Planos de Tratamentos de Riscos não está instituída e integrada na organização, mas que há iniciativas pontuais (como no caso do PNAE e do PDDE) sendo executadas.

Assim, considerando que não foram institucionalizados mecanismos de gestão e tratamento de riscos, eventuais políticas e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, a forma de documentar previsão de recursos, cronograma e benefícios esperados, considerando também as boas práticas já abordadas nos demais tópicos desse componente.

2.3. Monitoramento e comunicação

Nesse componente, apurou-se a seguinte questão: em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente no FNDE?

Buscou-se, dessa forma, avaliar se as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente na organização, de modo a garantir que a gestão de riscos e os controles sejam eficazes e eficientes quanto a seu desenho e sua operação. A avaliação do componente foi feita a partir de oito aspectos: 2.3.1. Informação e comunicação; 2.3.2. Sistema de informação; 2.3.3. Monitoramento contínuo e autoavaliações – Primeira linha; 2.3.4. Monitoramento contínuo e autoavaliações – Segunda linha; 2.3.5. Monitoramento periódico e avaliações independentes – Terceira linha; 2.3.6. Monitoramento periódico e avaliações independentes – Planos e medidas de contingência; 2.3.7. Monitoramento de mudanças significativas; e 2.3.8. Correção de deficiências e melhoria contínua.

Cabe ressaltar que a informação e comunicação, bem como o monitoramento, são componentes essenciais da estrutura de gestão de riscos, conforme preconizado pela IN nº 01/2016. Enquanto este componente tem por objetivo avaliar a qualidade da gestão de riscos e dos controles internos; aquele busca garantir que informações relevantes sejam identificadas, coletadas e comunicadas, permitindo, por conseguinte, que as pessoas cumpram suas responsabilidades de gerenciamento de riscos, bem como garantir que as informações produzidas fluam por todos os níveis e em todos os sentidos da organização.

Segundo o COSO-GRC (2007), o monitoramento pode ser realizado através de atividades gerenciais contínuas, de avaliações independentes ou da combinação de ambas as formas. Ainda, o *framework* destaca:

> *O gerenciamento de riscos corporativos de uma organização modifica-se com o passar do tempo. As respostas a risco que se mostravam eficazes anteriormente podem tornar-se inócuas; as atividades de controle podem perder a eficácia ou deixar de ser executadas; ou os objetivos podem mudar. Essas modificações podem ser causadas pela chegada de novos profissionais, pelas mudanças na estrutura ou no direcionamento da organização ou, ainda, pela introdução de novos processos. Diante dessas mudanças, a administração necessita determinar se o funcionamento do gerenciamento de riscos corporativos permanece eficaz.*

Acerca da comunicação, o COSO-GRC destaca a importância tanto da comunicação interna, que precisa fluir em todos os níveis da organização, quanto da comunicação externa (envolvendo,

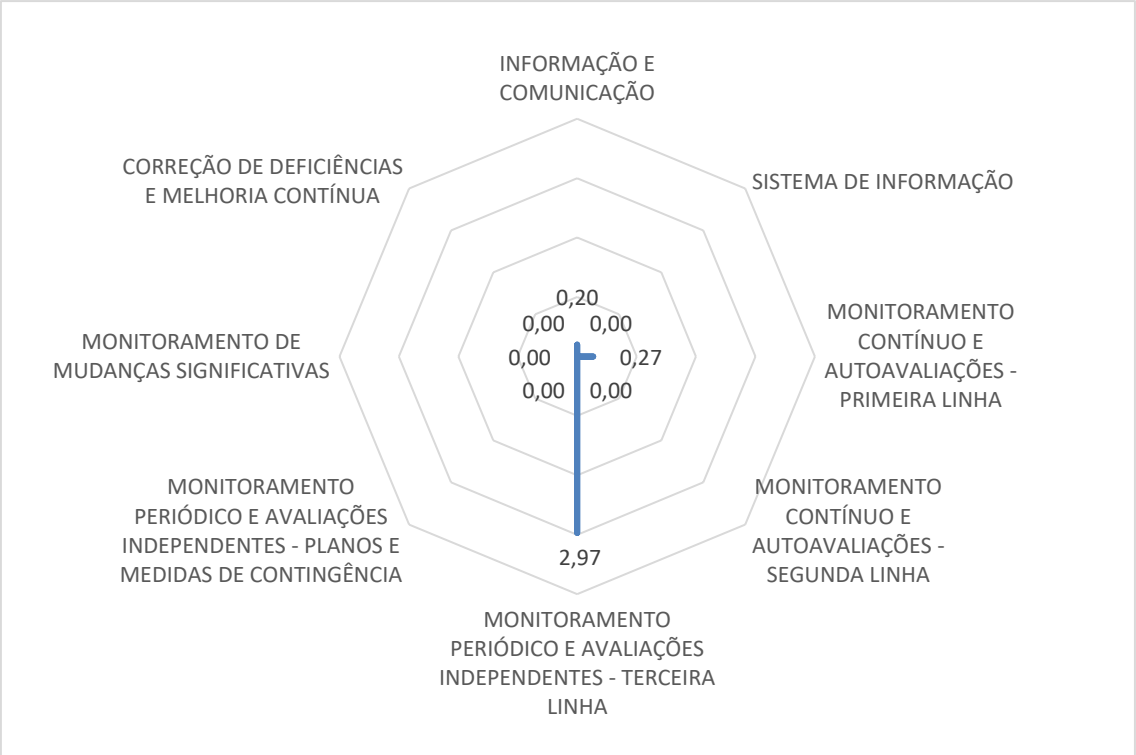
p. ex., fornecedores, órgãos reguladores, outras organizações parceiras, usuários de serviços públicos etc.). Destaca, ainda, relevantes informações que precisam ser transmitidas com eficácia, especialmente no âmbito interno:

- a importância e a pertinência do gerenciamento de riscos corporativos eficaz;
- os objetivos da organização;
- o apetite a riscos e a respectiva tolerância;
- uma linguagem comum de riscos; e
- as funções e as responsabilidades do pessoal ao conduzir e apoiar os componentes do gerenciamento de riscos corporativos.

Ressalta-se também que esses dois componentes não devem ser abordados como etapas estanques e sequenciais, mas sim como atividades que devem ocorrer ao longo de todo o processo de gestão de riscos, visto que são fundamentais para garantir a qualidade do que está sendo feito.

No FNDE, o resultado do componente "Monitoramento e comunicação", a partir da avaliação dos seus aspectos, demonstra uma maturidade INICIAL, apurada em **8,33%**. O gráfico a seguir apresenta o resultado consolidado do componente:

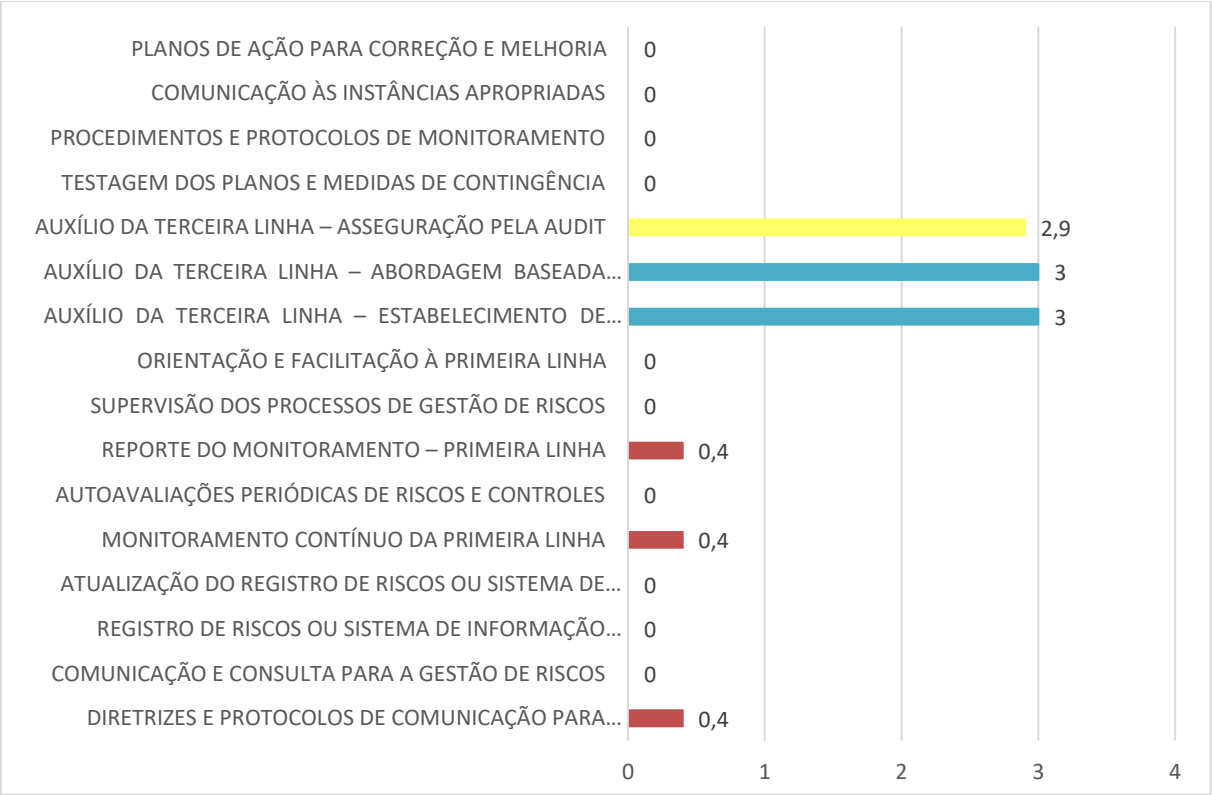
Gráfico 53: Resultado da avaliação dos objetos – Monitoramento e comunicação (resultado por aspecto)



Fonte: elaboração própria.

Já o próximo gráfico, apresenta os resultados de cada objeto analisado nos oito aspectos que integram o componente "Monitoramento e comunicação":

Gráfico 54: Resultado da avaliação dos objetos – Monitoramento e comunicação (resultado por objeto)



Fonte: elaboração própria.

Dos gráficos 53 e 54, percebe-se a baixa maturidade dos processos de monitoramento na primeira e na segunda linhas. Isso é reflexo também dos apontamentos já feitos na dimensão Ambiente, que concluiu que a primeira e a segunda linhas preconizadas pelo Modelo de 3 Linhas (IIA, 2020) não estão plenamente desenvolvidas para exercerem seus papéis no gerenciamento de riscos. Já em relação à terceira linha, percebe-se maior maturidade, o que decorre também das conclusões destacadas na primeira dimensão deste Relatório, cujas avaliações apontaram para uma maior estruturação e funcionamento das atividades de auditoria interna.

De todo modo, é preciso destacar que a ausência de diretrizes para a gestão de riscos (como uma Política de Gestão de Riscos) afeta também o presente componente.

A seguir apresentam-se os aspectos avaliados no componente Avaliação e resposta a riscos, bem como os objetos relacionados a cada aspecto.

2.3.1. Informação e comunicação

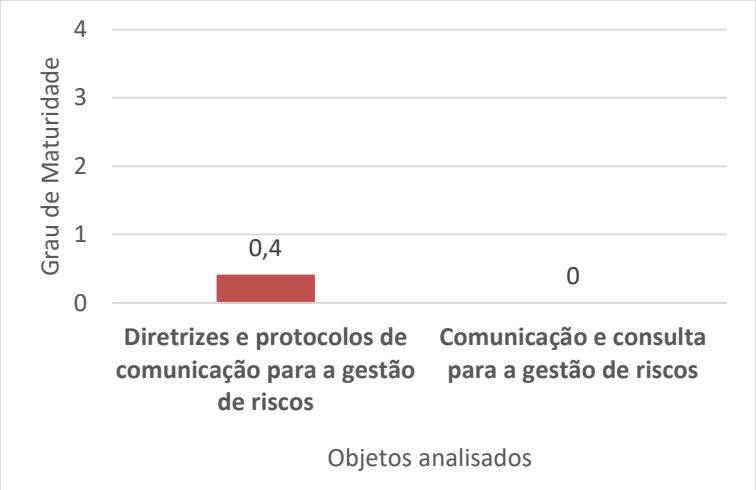
Diretrizes e protocolos de informação e comunicação estão estabelecidos e são efetivamente aplicados em todas as fases do processo de gestão de riscos?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à existência de atividades de informação e comunicação, estabelecidas em diretrizes e protocolos efetivamente

aplicados durante o processo de gerenciamento de riscos. A análise foi conduzida pela avaliação de dois objetos de análise, a saber: 2.3.1.1. Diretrizes e protocolos de comunicação para a gestão de riscos; e 2.3.1.2. Comunicação e consulta para a gestão de riscos.

A avaliação realizada mostrou que, dada a ausência de uma Política de Gestão de Riscos (ou de outro documento equivalente), não foram estabelecidos diretrizes ou protocolos de informação e comunicação para todas as fases do processo de gestão de riscos.

Gráfico 55: Resultado da avaliação – Aspecto Informação e comunicação



Fonte: elaboração própria.

Dessa forma, os tópicos a seguir trazem informações sobre os objetos analisados e, ainda, boas práticas relacionadas ao conteúdo mínimo a ser observado para a informação e a comunicação sobre os processos de gestão de riscos.

2.3.1.1. Diretrizes e protocolos de comunicação para gestão de riscos

Foram previstos testes com o objetivo de avaliar a existência e o funcionamento de diretrizes e protocolos para viabilizar o compartilhamento de informações sobre riscos e a comunicação clara, transparente, tempestiva, relevante e recíproca entre pessoas e grupos de profissionais no âmbito do FNDE, para que se mantenham informados e habilitados para exercer suas responsabilidades no gerenciamento de riscos. Também foi prevista a coleta de percepção da Alta Administração e dos servidores sobre este objeto.

O gerenciamento de riscos deve contar com atividades de informação e comunicação estabelecidas em diretrizes e protocolos e aplicados de forma efetiva no processo de gestão de riscos. O COSO-GRC (2007) orienta que é necessário fornecer informações ao pessoal apropriado para que as responsabilidades operacionais, de comunicação e de conformidade possam ser exercidas.

Nesse contexto, a IN nº 01/2016 dispõe que a estrutura da gestão de riscos deverá prover condições para que as informações externas e internas possam fluir dentro da organização de forma a permitir a gestão dos riscos e a tomada de decisão.

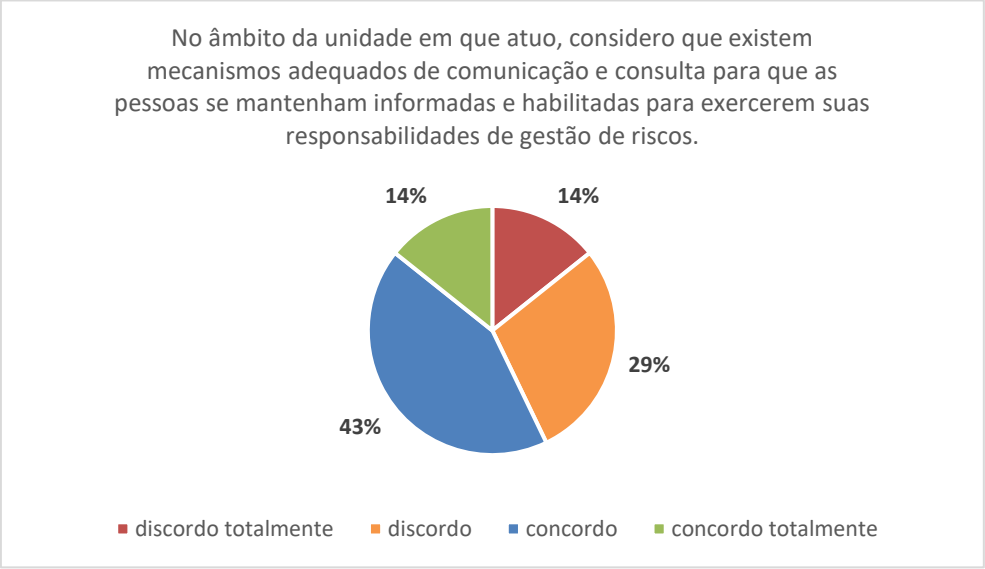
Em complemento, destaca-se orientação do *Orange Book* acerca do tema: a Alta Administração e os órgãos de governança devem especificar a natureza, a fonte, o formato e a frequência das informações que necessitam. Ademais, devem assegurar que alguns fatores sejam levados em consideração nos protocolos de comunicação, como:

- diferentes partes interessadas e suas necessidades e requisitos específicos de informação;
- custo, frequência e pontualidade dos relatórios;
- método de relatório; e
- relevância da informação para os objetivos organizacionais e a tomada de decisão.

Sobre o assunto, a organização auditada afirmou que não foram estabelecidos diretrizes e protocolos para informações relevantes e não foram definidas as formas de compartilhamento dessas informações e de comunicação entre pessoas e grupos de profissionais no âmbito do FNDE.

Contudo, 57%, entre aqueles que responderam ao questionário enviado para a Alta Administração "concordaram" ou "concordaram totalmente" que, no âmbito de suas unidades, existem mecanismos adequados de comunicação e consulta para que as pessoas se mantenham informadas e habilitadas para exercerem suas responsabilidades de gestão de riscos:

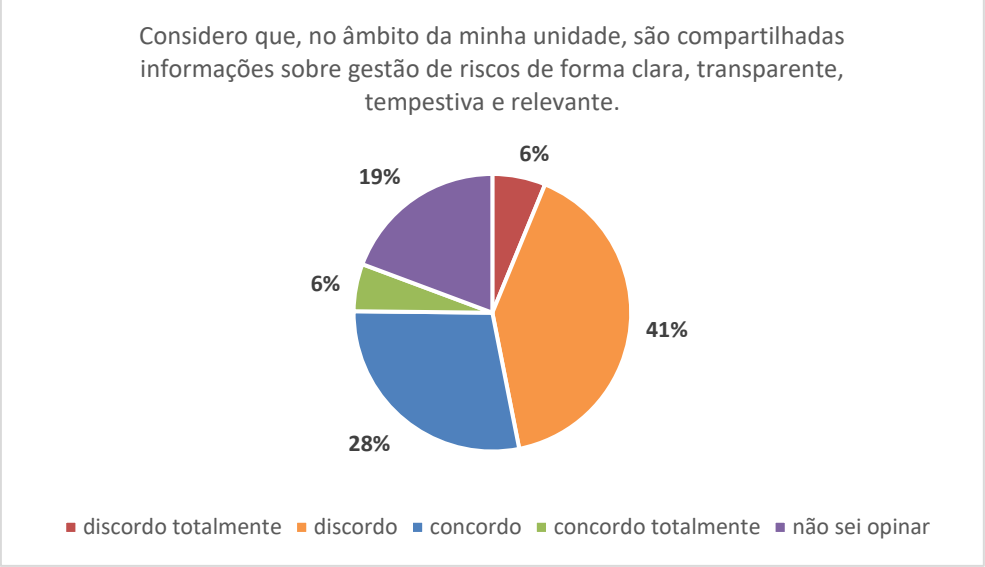
Gráfico 56: Percepção da Alta Administração – Diretrizes e protocolos de comunicação e consulta



Fonte: elaboração própria.

Por outro lado, quando questionados acerca do compartilhamento de informações sobre gestão de riscos em suas unidades, apenas 34% dos servidores respondentes "concordaram" ou "concordaram totalmente" com a existência da prática, de acordo com o gráfico a seguir:

Gráfico 57: Percepção dos servidores – Diretrizes e protocolos de comunicação e consulta



Fonte: elaboração própria.

Considerando que o FNDE não estabeleceu diretrizes e protocolos de informação e comunicação para as fases do processo de gestão de riscos entende-se que não há mecanismos estabelecidos para permitir o compartilhamento de informações de forma que os profissionais no âmbito da organização possam exercer suas responsabilidades no gerenciamento de riscos. No entanto, existe certa percepção entre gestores e servidores sobre o princípio na organização.

Para melhor atendimento das boas práticas sobre o tema, eventual Política de Gestão de Riscos deve incluir diretrizes e recomendar o estabelecimento de protocolos de comunicação para gestão de riscos, orientando as pessoas quanto ao fluxo de informações, de forma a permitir que as partes interessadas possam assumir suas reponsabilidades no processo.

2.3.1.2. Comunicação e consulta para a gestão de riscos

Foram previstos testes com o objetivo de avaliar se há efetiva comunicação e consulta às partes interessadas internas e externas durante todas as fases do processo de gestão de riscos.

Ainda sobre as atividades de comunicação, é importante não só o estabelecimento das diretrizes e protocolos, conforme abordado acima, mas também que a comunicação e consulta entre as partes interessadas internas e externas sejam efetivas durante todas as fases do processo de gestão de riscos. De acordo com o ISO 31000:2018 o propósito da comunicação e consulta é auxiliar as partes interessadas na compreensão do risco, tendo em vista que ele deve ser a base na qual as decisões são tomadas e pela qual ações específicas são requeridas.

A norma diferencia comunicação e consulta: enquanto a primeira busca promover a conscientização e o entendimento do risco, a segunda envolve obter retorno e informação para auxiliar a tomada de decisão. Nesse contexto, as duas atividades precisam ser coordenadas, de modo a facilitar a troca de informações factuais, oportunas, pertinentes, precisas e compreensíveis (em todas as etapas e ao longo de todo o processo de gestão de riscos).

Dado que o FNDE, conforme demonstrado na análise do tópico 2.3.1.1, não estabeleceu diretrizes e protocolos de informação e comunicação para as fases do processo de gestão de riscos, não há previsão formalizada e disseminada pela organização de comunicação e consulta com partes interessadas (externas e internas) para o processo de gestão de riscos. Dessa forma, considera-se que a prática não está implementada.

Assim, eventuais política e procedimentos de gestão de riscos a serem implementados precisam considerar diretrizes para coordenar e integrar por toda a Autarquia as atividades de comunicação e consulta sobre gestão de riscos, conforme preconizado pela IN nº 01/2016.

2.3.2. Sistema de informação

A gestão de riscos é apoiada por um registro de riscos ou sistema de informação efetivo e atualizado?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à existência de um sistema de informação (ou de outros mecanismos para registro) com o intuito de apoiar a gestão de riscos no FNDE. A análise foi conduzida pela avaliação de dois objetos de análise, a saber: 2.3.2.1. Registro de riscos ou sistema de informação utilizado; e 2.3.2.2. Atualização do registro de riscos ou sistema de informação utilizado.

A avaliação realizada mostrou que não foi estabelecido um sistema específico para gestão de riscos no FNDE. Assim, não há o apoio de um mecanismo que facilite a comunicação e permita uma visão integrada da gestão de riscos.

Nesse contexto, entende-se que eventual disponibilização de um sistema (ou de outro mecanismo priorizado para adoção na Autarquia) auxilia na documentação das atividades integrantes do processo de gestão de riscos, o que afeta também os objetos abordados nos itens 2.1.4 e 2.2.5.

Dessa forma, os tópicos a seguir trazem informações sobre os objetos analisados e, ainda, boas práticas relacionadas ao conteúdo mínimo a ser observado para a informação e a comunicação sobre os processos de gestão de riscos.

2.3.2.1. Registro de riscos ou sistema de informação utilizado

Foram previstos testes com o objetivo de avaliar a existência e o funcionamento de um registro de riscos ou um sistema de informação que apoiasse a gestão de riscos da organização e facilitasse a comunicação entre pessoas e grupos de profissionais com responsabilidades sobre o processo de gestão de riscos, permitindo uma visão integrada das atividades de identificação, análise, avaliação, tratamento e monitoramento de riscos, incluindo a sua documentação.

De acordo com o COSO-GRC-EP (2017), a organização deve maximizar a utilização dos sistemas de informação e tecnologias existentes, de maneira que o gerenciamento de riscos corporativos possa seja impulsionado. Ademais, o COSO-GRC (2007) explica que os sistemas de informática geralmente empregam dados gerados internamente e informações de fontes externas,

possibilitando, dessa forma, esclarecimentos para o gerenciamento de riscos e a tomada de decisão baseadas em dados relacionados aos objetivos.

Além das duas versões do COSO, cabe mencionar a ABNT IEC 31010:2021, que sugere que o registro de riscos inclua, por exemplo:

- uma breve descrição do risco (por exemplo, um nome para o risco identificado, as suas consequências e a sequência de eventos que levam a essas consequências etc.);
- uma declaração sobre a probabilidade de ocorrência de consequências;
- fontes ou causas do risco; e
- o que está sendo feito atualmente para controlar o risco.

Conforme disposto nos tópicos 1.2.7.1 e 2.1.3.2, que trataram, respectivamente, da alocação de recursos para a gestão de riscos e das técnicas e ferramentas utilizadas para a identificação e análise de riscos, não há um sistema específico para gestão de riscos implementado no FNDE.

Desse modo, a gestão de riscos não é apoiada por um registro de riscos ou sistema de informação que facilite a comunicação, permita uma visão integrada e documente as atividades do processo de gestão de riscos.

Destaca-se, por fim, que a equipe de auditoria identificou sistemas e modelos de registro de riscos em utilização por outros órgãos e entidades da administração pública, incluindo uma plataforma gerenciada pelo Ministério da Educação que contempla a disponibilização de *software* de gerenciamento de riscos[28]. Tais modelos podem ser estudados pela organização, visando trazer maior celeridade e economia quando da implementação dos mecanismos citados.

2.3.2.2. Atualização do registro de riscos ou sistema de informação utilizado

Foram previstos testes com o objetivo de avaliar se eventual registro de riscos ou sistema de informação é mantido atualizado pelas diversas pessoas e funções que têm responsabilidades pela gestão de riscos em todas as áreas da organização, tanto em função das decisões e ações implementadas em todas as etapas do processo de gestão de riscos, quanto pelas atividades de monitoramento e correção de deficiências (tratadas no próximo aspecto), pelo menos quanto aos seus resultados e com referências para a documentação original completa.

Conforme disposto nos tópicos 1.2.7.1 e 2.1.3.2, que trataram, respectivamente, da alocação de recursos para a gestão de riscos e das técnicas e ferramentas utilizadas para a identificação e análise de riscos, e relatado no tópico anterior (2.3.2.1) não há um sistema específico para gestão de riscos implementado no FNDE. Dessa forma, não foi possível avaliar a sua atualização.

[28] A Plataforma For é uma ferramenta tecnológica para auxiliar na criação do Plano de Desenvolvimento Institucional e no Gerenciamento de Riscos das instituições da Rede Federal de Educação. Contempla um conjunto de soluções, incluindo o ForRisco, *software* destinado à gestão de riscos.

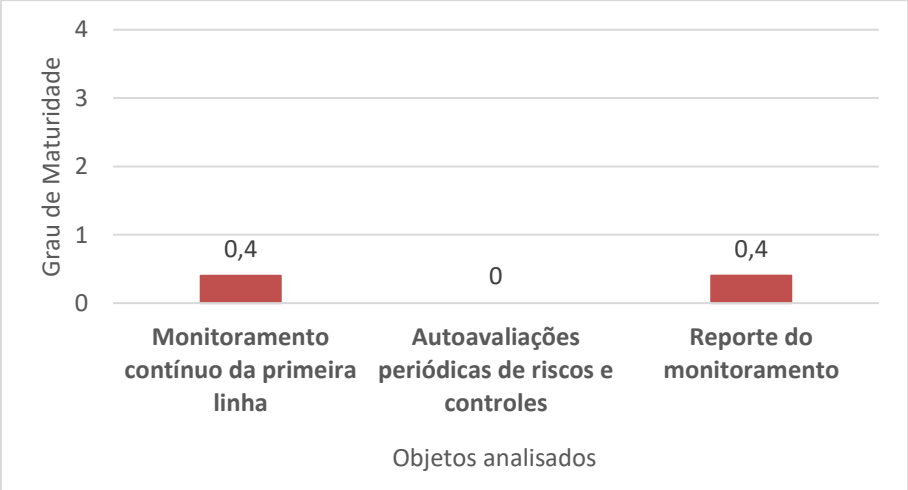
2.3.3. Monitoramento contínuo e autoavaliações – Primeira linha

Em todos os níveis do FNDE, os gestores que têm propriedade sobre riscos (primeira linha) monitoram o alcance de objetivos, riscos e controles chave em suas respectivas áreas de responsabilidade?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à existência e ao funcionamento de atividades de monitoramento contínuo, no âmbito da primeira linha, ou seja, pelos gestores que têm propriedade sobre riscos e monitoram o alcance de objetivos, riscos e controles-chave em suas respectivas áreas de responsabilidade. A análise foi conduzida pela avaliação de três objetos de análise, a saber: 2.3.3.1. Monitoramento contínuo da primeira linha; 2.3.3.2. Autoavaliações periódicas de riscos e controles; e 2.3.3.3. Reporte do monitoramento.

A avaliação realizada mostrou que o FNDE não definiu diretrizes e protocolos para monitoramento contínuo e autoavaliações da gestão de riscos. A ausência de uma Política de Gestão de Riscos (ou de outro documento equivalente) prejudica esse aspecto, dado que não há diretrizes que tratem da etapa de monitoramento e comunicação.

Gráfico 58: Resultado da avaliação – Aspecto Monitoramento contínuo e autoavaliações – Primeira linha



Fonte: elaboração própria.

Dessa forma, os tópicos a seguir trazem informações sobre os objetos analisados e, ainda, boas práticas relacionadas ao conteúdo mínimo a ser observado para o monitoramento contínuo dos processos de gestão de riscos.

2.3.3.1. Monitoramento contínuo da primeira linha

Os testes previstos buscaram avaliar se, em todos os níveis da organização, os proprietários de riscos (primeira linha) monitoram o alcance de objetivos, riscos e controles-chave, de modo contínuo (ou pelo menos frequente), por meio de indicadores-chave de risco, indicadores-chave de desempenho e verificações rotineira, para manter riscos e resultados dentro das tolerâncias a riscos

definidas ou variações aceitáveis no desempenho. Além disso, foi coletada a percepção da Alta Administração sobre o tema.

Para a ISO 31000:2018, o monitoramento, assim como a análise crítica, deve ser instituído em todas as etapas da gestão de riscos de forma "assegurar e melhorar a qualidade e eficácia da concepção, implementação e resultados do processo". Para tanto precisa ser uma atividade planejada com responsabilidades definidas.

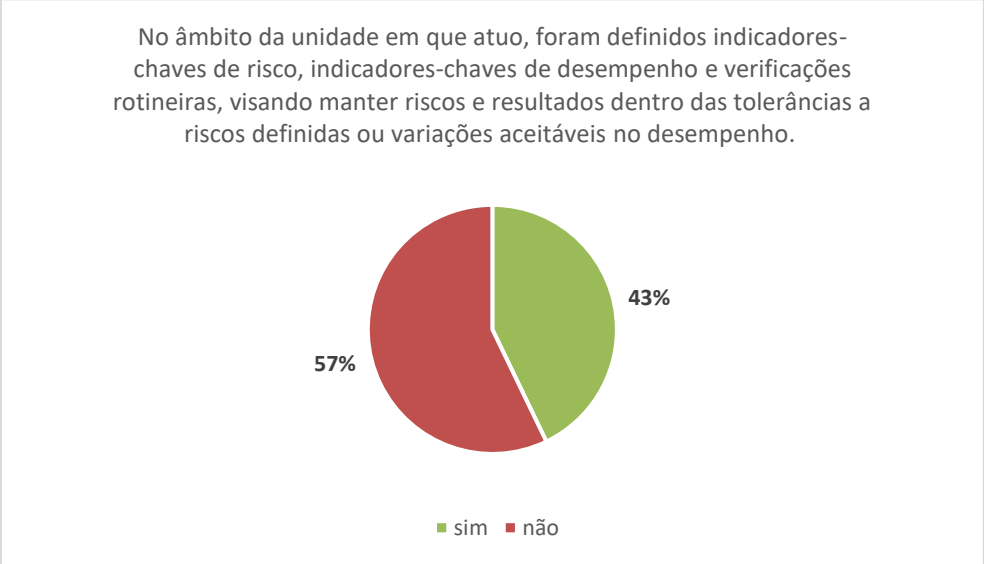
De acordo com o COSO-GRC (2007), o monitoramento permite avaliar a presença e o funcionamento dos componentes da gestão de riscos ao longo do tempo. Ainda, conforme o *framework*:

> *Essa tarefa é realizada mediante atividades contínuas de monitoramento, avaliações independentes ou uma combinação de ambas. O monitoramento contínuo ocorre no decurso normal das atividades de administração. O alcance e a frequência das avaliações independentes dependerá (sic) basicamente de uma avaliação dos riscos e da eficácia dos procedimentos contínuos de monitoramento. As deficiências no gerenciamento de riscos corporativos são relatadas aos superiores, sendo as questões mais graves relatadas ao Conselho de administração e à diretoria executiva.*

Sobre o monitoramento contínuo da primeira linha, a organização auditada afirmou que não foram estabelecidas iniciativas voltadas ao monitoramento contínuo da gestão de riscos, nem ao acompanhamento da evolução dos níveis de risco e da efetividade de controles implementados em processos que serão objeto da gestão de riscos. Aliado a isso, ressalta-se mais uma vez a ausência de uma Política de Gestão de Riscos (ou de outro documento equivalente), impactando a definição de diretrizes que tratem da etapa de monitoramento e comunicação.

Sobre a percepção da Alta Administração, 57% dos dirigentes que responderam ao questionário afirmam que, no âmbito de suas unidades, não foram definidos indicadores-chave de risco e de desempenho, nem verificações rotineiras, conforme gráfico a seguir:

Gráfico 59: Percepção da Alta Administração – Monitoramento contínuo da primeira linha



Fonte: elaboração própria.

Do exposto, verifica-se que é uma prática não implementada na organização, mas percebida por alguns gestores. Ademais, cabe ressaltar que, conforme demonstrado nos tópicos 1.2.2.1 e 1.2.3.2, respectivamente, não foram definidos o apetite a risco do FNDE e as tolerâncias a riscos. A ausência de objetivos de negócio claramente definidos (também apontada no tópico 1.2.3.2), também prejudica o acompanhamento de variações aceitáveis no desempenho para os objetivos operacionais, de conformidade e de divulgação.

Assim, eventuais políticas e procedimentos de gestão de riscos a serem implementados precisam considerar diretrizes para coordenar e integrar por toda a Autarquia as atividades de monitoramento pela primeira linha.

2.3.3.2. Autoavaliações periódicas de riscos e controles

Os testes previstos buscaram avaliar se, em todos os níveis da organização, os proprietários de riscos (primeira linha) monitoram o alcance de objetivos, riscos e controles-chave, de modo contínuo (ou pelo menos frequente), por meio de autoavaliações periódicas de riscos e controles (*Control and Risk Self Assessment* – CRSA), que constam de um ciclo de revisão periódica estabelecido.

Esta autoavaliação consiste num processo no qual os próprios gestores avaliam seus controles e riscos, conforme explica o TCU[29]. Tipicamente, ocorre por meio de questionários ou oficinas de autoavaliação das práticas existentes para lidar com os riscos. Dentre os benefícios da prática, tem-se a identificação precoce de fragilidades na implantação de controles internos, com a possibilidade de corrigi-las e o aumento da probabilidade de alcance dos objetivos da organização.

Não foram identificados elementos que comprovem haver autoavaliações periódicas de riscos e controles pelo FNDE. Adicionalmente, a Autarquia não estabeleceu diretrizes e protocolos para monitoramento contínuo e autoavaliações da gestão de riscos (conforme abordado no tópico 2.3.3.1). Assim, trata-se de prática não implementada na organização.

Por isso, eventuais políticas e procedimentos de gestão de riscos a serem implementados precisam considerar os benefícios da implementação de autoavaliações contínuas que apoiem a gestão de riscos na organização.

2.3.3.3. Reporte do monitoramento – Primeira linha

Os testes previstos buscaram avaliar se, em todos os níveis da organização, a execução e os resultados do monitoramento do alcance de objetivos, riscos e controles-chave são documentados e reportados às instâncias apropriados da administração e da governança.

De acordo com o documento "Alavancar o COSO nas três linhas de defesa", do IIA (2015), cabe à primeira linha comunicar as informações sobre as deficiências às partes responsáveis pelas medidas corretivas, bem como à Alta Administração e ao Conselho de Administração, conforme apropriado". Nesse contexto, os resultados do monitoramento contínuo e das autoavaliações auxiliam na avaliação da qualidade da gestão de riscos e controle, assegurando o seu funcionamento

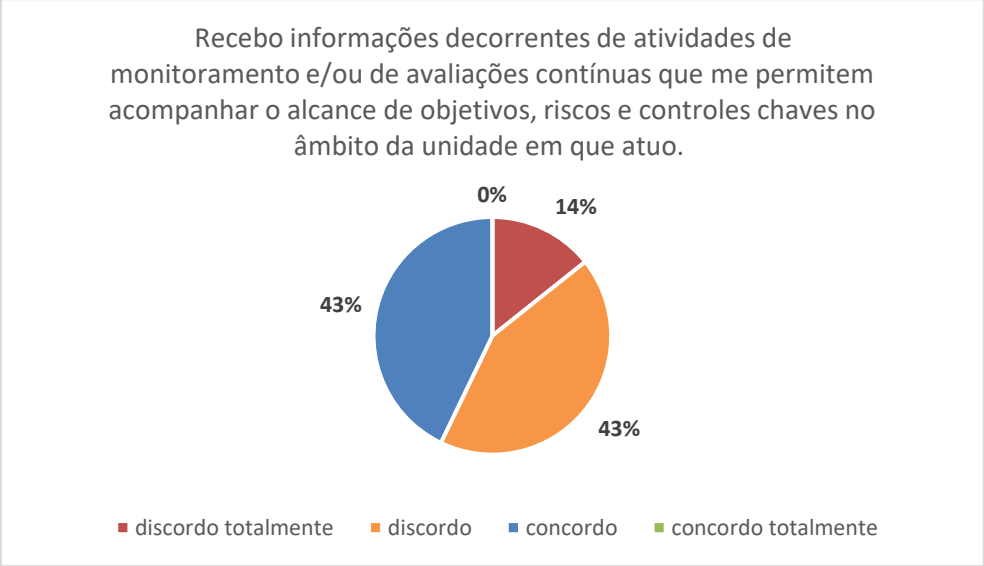
[29] Em: https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/autoavaliacao-de-controles/.

e garantindo que as modificações necessárias sejam feitas, “de acordo com mudanças nas condições que alterem o nível de exposição a riscos”, conforme preconizado pela IN nº 01/2016.

Da análise dos objetos relatados nos tópicos 2.3.3.1 e 2.3.3.2, foi possível concluir que o FNDE não estabeleceu diretrizes e protocolos para monitoramento contínuo e autoavaliações da gestão de riscos. A organização auditada corrobora essa informação, informando que não foram estabelecidas iniciativas voltadas ao reporte do monitoramento por intermédio de encaminhamento de seus resultados às instâncias apropriadas da administração e da governança.

Em relação à percepção da Alta Administração, destaca-se que 57% dos dirigentes “discordaram” ou “discordaram totalmente” quanto ao recebimento de informações relacionadas ao seu papel de monitoramento, conforme gráfico a seguir:

Gráfico 60: Percepção da Alta Administração – Reporte do monitoramento – Primeira linha



Fonte: elaboração própria.

Nesse contexto, além da definição de diretrizes para a realização de atividades de monitoramento contínuo e de autoavaliações periódicas, eventuais políticas e procedimentos de gestão de riscos a serem implementados precisam estabelecer também os mecanismos de reporte dos resultados desse monitoramento da primeira linha.

2.3.4. Monitoramento contínuo e autoavaliações – Segunda linha

As funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos (como: comitê de governança, riscos e controles; comitê de auditoria ou grupos equivalentes da segunda linha) exercem suas atribuições de modo efetivo?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à existência e ao funcionamento de atividades de monitoramento contínuo, no âmbito da segunda linha, ou seja, pelas funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos (como: comitê de governança, riscos e controles; comitê de auditoria ou grupos equivalentes da segunda

linha). A análise foi conduzida pela avaliação de dois objetos de análise, a saber: 2.3.4.1. Supervisão dos processos de gestão de riscos; e 2.3.4.2. Orientação e facilitação à primeira linha.

A avaliação realizada mostrou que o FNDE não definiu diretrizes e protocolos para monitoramento contínuo e autoavaliações da gestão de riscos. A ausência de uma Política de Gestão de Riscos (ou de outro documento equivalente) prejudica esse aspecto, dado que não há diretrizes que tratem da etapa de monitoramento e comunicação.

Dessa forma, os tópicos a seguir trazem informações sobre os objetos analisados e, ainda, boas práticas relacionadas ao conteúdo mínimo a ser observado para o monitoramento contínuo dos processos de gestão de riscos.

2.3.4.1. Supervisão dos processos de gestão de riscos

Os testes previstos buscaram avaliar se as funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos exercem uma supervisão efetiva dos processos de gerenciamento de riscos, inclusive das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa.

A supervisão dos processos de gestão de riscos é uma atividade a ser desenvolvida pela segunda linha da organização, que é essencialmente uma função de gerência e/ou de supervisão responsável por muitos aspectos da gestão de riscos, compilando as informações de toda a organização para utilizar nas atividades de monitoramento, conforme dispõe o IIA (2015). Uma importante função nesse sentido é o compilamento de informações de toda a organização para subsidiar as atividades de monitoramento.

Conforme relatado no objeto de análise descrito no tópico 1.3.2.2, verificou-se não foram formalmente atribuídos os papéis de segunda linha. Ademais, a ausência de uma diretriz (como, p. ex., uma Política de Gestão de Riscos) prejudica a supervisão dos processos de gestão de riscos do FNDE.

Assim, eventuais política e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, a forma de supervisionar os processos de gestão de riscos, considerando também as boas práticas já abordadas no tópico 1.3.2.3.

2.3.4.2. Orientação e facilitação à primeira linha

Os testes previstos buscaram avaliar se as funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos fornecem orientação e facilitação na condução das atividades de monitoramento contínuo e autoavaliações da primeira linha de defesa, mantém sua documentação e comunica os seus resultados às instâncias apropriados da administração e da governança.

Cabe destacar o que dispõe IIA (2015) sobre as responsabilidades da primeira e da segunda linha:

> *A primeira linha de defesa tem a responsabilidade principal pelos riscos e métodos utilizados para gerenciá-los. A segunda linha fornece conhecimento especializado em riscos, ajuda a definir a estratégia da implementação e auxilia na implementação de*

> *políticas e procedimentos. Embora essas duas linhas tenham responsabilidades diferentes perante os riscos e controles, é fundamental que elas trabalhem em parceria utilizando a mesma terminologia, entendam a avaliação de cada uma com relação aos riscos da organização e, sempre que possível, alavanquem um conjunto comum de ferramentas e processos.*

Dessa forma, cabe à segunda linha orientar e facilitar a atuação da primeira linha. Quando a estruturação dessas linhas está bem estabelecida, elas tendem a funcionar de forma efetiva, a partir do entendimento de seus papéis no contexto geral da gestão de riscos, de modo que não haja lacunas ou duplicação desnecessária de esforços (Orange Book, 2020).

Conforme relatado no objeto de análise descrito no tópico 1.3.2.2, verificou-se não foram formalmente atribuídos os papéis de segunda linha. Ademais, a ausência de uma diretriz (como, p. ex., uma Política de Gestão de Riscos) prejudica os papéis de orientação e facilitação à primeira linha.

Assim, eventuais política e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, a forma de a segunda linha orientar e auxiliar a primeira linha, considerando também as boas práticas já abordadas no tópico 1.3.2.3.

2.3.5. Monitoramento periódico e avaliações independentes – Terceira linha

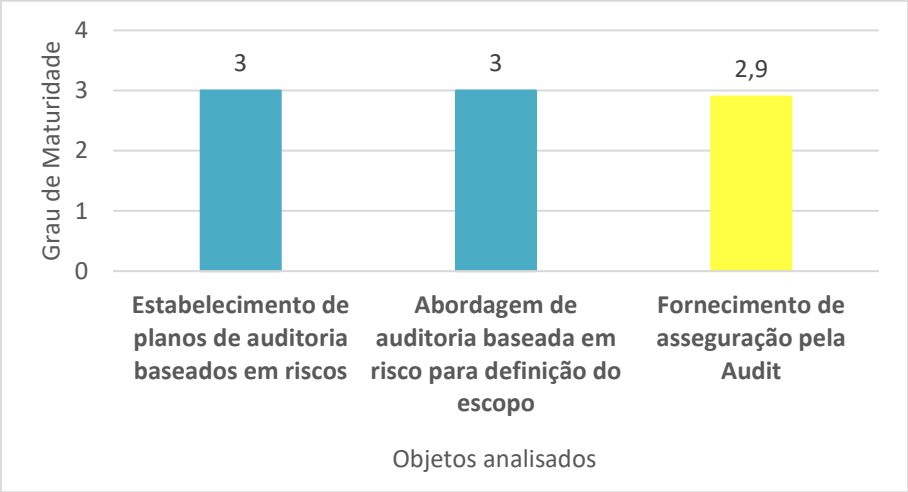
A função de auditoria interna auxilia o FNDE a realizar seus objetivos aplicando abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à existência e ao funcionamento da função de auditoria interna, no âmbito da terceira linha[30], bem como a sua atuação no papel de auxílio à realização dos objetivos da organização, por intermédio da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança. A análise foi conduzida pela avaliação de três objetos de análise, a saber: 2.3.5.1. Estabelecimento de planos de auditoria baseados em riscos; 2.3.5.2. Abordagem de auditoria baseada em risco para definição do escopo; e 2.3.5.3. Fornecimento de asseguração pela Audit.

A avaliação realizada mostrou que a Auditoria Interna do FNDE, atuando enquanto terceira linha, tem auxiliado a Autarquia com avalições e consultorias, aplicando abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controles internos e governança. Observou-se, também, atendimento das principais normas que regulamentam a atividade de auditoria interna governamental e definição dos trabalhos com base em fatores de riscos.

[30] Em que pese a Controladoria-Geral da União (CGU) também ser considerada instância de terceira linha no âmbito do Poder Executivo federal, destaca-se que os testes da presente avaliação tiveram como foco a atuação da Auditoria Interna do FNDE. Ressalta-se, porém, que os serviços entregues pela CGU também auxiliam a organização na realização de seus objetivos, agregando valor aos processos de governança, gestão de riscos e controles internos.

Gráfico 61: Resultado da avaliação – Aspecto Monitoramento periódico e avaliações independentes – Terceira linha



Fonte: elaboração própria.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir dos objetos de análise selecionados:

2.3.5.1. Estabelecimento de planos de auditoria baseados em riscos

Os testes previstos buscaram avaliar se a função de auditoria interna estabelece planos anuais ou plurianuais baseados em riscos, de modo a alinhar as atividades da auditoria interna com as prioridades da organização e garantir que os seus recursos são alocados em áreas de maior risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança.

De acordo com a IN SFC nº 3/2017, o planejamento da Unidade de Auditoria Interna Governamental (UAIG) deve considerar as estratégias, os objetivos, as prioridades, as metas da Unidade Auditada e os riscos a que seus processos estão sujeitos. O resultado é um plano de auditoria interna baseado em riscos com a identificação dos trabalhos prioritários a serem realizados em certo período. Adicionalmente, o planejamento, deve considerar a identificação prévia do universo auditável, as expectativas da administração e demais partes interessadas, bem como a análise de riscos da unidade auditada com base em processo de gerenciamento de riscos.

Na ausência de um processo formal de gerenciamento de riscos instituído pela Unidade Auditada, a UAIG deve coletar as expectativas da unidade auditada e entender os principais processos e os riscos associados. Dessa forma, é importante que a UAIG elabore seu Plano de Auditoria Interna, priorizando os processos ou unidades organizacionais de maior risco.

Para desempenho de suas atividades, a auditoria interna baseia-se nos princípios, nos padrões e nas normas nacionais e internacionais relativos à conduta e à prática profissional de auditoria interna, compatíveis com as Normas para a Prática Profissional de Auditoria Interna (IPPF) e com o Código de Ética do *Institute of Internal Auditors* – IIA, e, ainda, com as normas editadas pela Controladoria-Geral da União.

No tocante às normas que tratam do estabelecimento de planos de auditoria baseados em riscos, destacam-se as seguintes orientações do IPPF:

> ***2010**: O chefe executivo de auditoria deve estabelecer um plano baseado em riscos para determinar as prioridades da atividade de auditoria interna, de forma consistente com as metas da organização.*
>
> ***2100**: A atividade de auditoria interna deve avaliar e contribuir para a melhoria dos processos de governança, gerenciamento de riscos e controle da organização, usando uma abordagem sistemática, disciplinada e baseada em riscos. A credibilidade e o valor da auditoria interna são aperfeiçoados quando os auditores são proativos, e suas avaliações oferecem novos pontos de vista e consideram o impacto futuro.*
>
> ***2110**: A atividade de auditoria interna deve avaliar e propor recomendações apropriadas para melhorar os processos de governança da organização [...].*

Da análise realizada, verificou-se que a Auditoria Interna do FNDE, enquanto instância posicionada na terceira linha, estabelece planos anuais baseados em riscos, de modo a alinhar as suas atividades com as prioridades da organização e garantir que os seus recursos são alocados em áreas de maior risco, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança. A análise documental efetuada evidenciou que:

- existe Plano Anual de Auditoria Interna (Paint), aprovado pelo CD/FNDE e publicado a cada exercício;
- a elaboração do Paint parte do mapa estratégico do FNDE e a definição dos temas a serem trabalhados a cada exercício baseia-se em mapeamento do universo auditável[31], anualmente atualizado, a partir de fatores de risco pré-definidos e de critérios de qualificação (relevância, vulnerabilidade e oportunidade). Ainda, é agregada a percepção da Alta Administração quanto aos temas prioritários para a gestão; e
- existem diretrizes e sistemas para monitorar as recomendações de auditoria emitidas, a saber: a Política e Procedimentos para Monitoramento das Recomendação e a utilização do Sistema e-Aud (da CGU). Ainda, é feita a contabilização de benefícios (financeiros e não financeiros).

No entanto, destaca-se que, tendo em vista a ausência de processo de gerenciamento de riscos implementado no FNDE (com a identificação dos principais riscos pela própria unidade auditada), atualmente, a seleção e a priorização de trabalhos de auditoria pela Audit é feita com base na associação indireta entre os trabalhos e os riscos da organização, por intermédio de "fatores de riscos", os quais são empregados para identificar a importância relativa das condições e eventos que podem afetar adversamente a organização.

Por isso, entende-se que a atuação da Audit pode ser aprimorada a partir do alcance de um nível maior de maturidade do processo de gestão de riscos do FNDE e, consequentemente, da indicação de que o cadastro de riscos da organização é confiável. Com isso, a atuação da auditoria interna também poderá se tornar mais madura, de modo a englobar os riscos identificados e mensurados pela própria organização na elaboração de seu planejamento.

Dessa forma, conclui-se que a auditoria interna atende aos requisitos necessários no tocante ao planejamento baseado em riscos, em que pese ainda existir a possibilidade de melhoria, especialmente considerando que a estratégia de auditoria depende em grande parte do grau de maturidade da gestão de riscos da unidade auditada, conforme destacado no tópico 1.3.2.3.

[31] Conforme Política e Procedimentos – Mapeamento do Universo Auditável, publicada pela Audit/FNDE

2.3.5.2. Abordagem de auditoria baseada em risco para definição do escopo

Os testes previstos buscaram avaliar se a função de auditoria interna utiliza abordagem baseada em risco ao definir o escopo e planejar a natureza, época e extensão dos procedimentos de auditoria em seus trabalhos individuais, incluindo a identificação e análise dos riscos e o exame de como eles são gerenciados pela gestão da área responsável.

Para a função da auditoria interna, o IPPF estabelece parâmetros que servem de base para cada trabalho, conforme detalhado a seguir:

> ***2200:*** *Os auditores internos devem desenvolver e documentar um plano para cada trabalho de auditoria, incluindo os objetivos, o escopo, o período e a alocação de recursos do trabalho de auditoria. O plano deve considerar as estratégias, objetivos e riscos da organização que sejam relevantes para o trabalho de auditoria.*
>
> ***2201:*** *No planejamento de trabalhos de auditoria, os auditores internos devem considerar:*
>
> • *As estratégias e os objetivos da atividade que está sendo revisada e os meios pelos quais a atividade controla seu desempenho.*
>
> • *Os riscos significantes aos objetivos, recursos e operações da atividade e os meios pelos quais o impacto potencial do risco é mantido em um nível aceitável.*
>
> • *A adequação e a eficácia dos processos de governança, de gerenciamento de riscos e de controle da atividade, em comparação com um framework ou modelo relevante.*
>
> • *As oportunidades de melhorias significantes nos processos de governança, gerenciamento de riscos e controle da atividade.*
>
> ***2210:*** *Os objetivos devem ser estabelecidos para cada trabalho de auditoria.*

Da análise dos papéis de trabalhos das avaliações realizadas no último exercício, concluiu-se que a Audit/FNDE se utiliza de abordagem baseada em risco no planejamento de seus trabalhos individuais. A análise documental mostrou que:

- os projetos a serem executados passam por análise preliminar, em cujo contexto é elaborado entendimento da(s) unidade(s) e do(s) objeto(s) auditado(s), para que sejam estabelecidos os objetivos, o escopo e os exames a serem realizados. Esse entendimento parte também da análise do plano de auditoria baseado em riscos e do alinhamento aos objetivos e estratégias das unidades auditadas, dos riscos significativos e das medidas de controle relacionadas;
- também é elaborada proposta de projeto contemplando, dentre outras informações: justificativa para execução do trabalho; principais requisitos; metodologia a ser utilizada; benefícios e resultados esperados; custo estimado; partes interessadas; fases e marcos do trabalho;
- ainda na fase de análise preliminar é elaborada Matriz de Riscos e Controles, por meio da qual é efetuada a avaliação dos riscos inerentes, da probabilidade e do impacto de cada um dos riscos-chave identificados, bem como é feita a identificação e a avaliação dos controles existentes, além do cálculo do risco residual; e
- a atuação da unidade baseia-se especialmente em suas políticas e procedimentos e em conformidade com os princípios, os padrões e as normas nacionais e internacionais

relativos à conduta e à prática profissional de auditoria interna, compatíveis com as Normas para a Prática Profissional de Auditoria Interna e com o Código de Ética do *Institute of Internal Auditors* – IIA, e, ainda, com as normas editadas pela Controladoria-Geral da União, conforme disposto no art. 12 do Estatuto da Audit/FNDE.

Dessa forma, entende-se que a auditoria interna atende aos requisitos necessários e, portanto, aplicando abordagem baseada em risco ao definir o escopo e planejar a natureza, a época e a extensão dos procedimentos de auditoria em seus trabalhos individuais, incluindo a identificação e a análise dos riscos, bem como o exame de como eles são gerenciados pela área responsável.

2.3.5.3. Fornecimento de asseguração pela Audit

Os testes previstos buscaram avaliar se a função de auditoria interna fornece asseguração aos órgãos de governança e à alta administração, bem como aos órgãos de controle e regulamentação, de que os processos de gestão de riscos e controle operam de maneira eficaz e que os riscos significativos são gerenciados adequadamente em todos os níveis da organização. Além disso, foi coletada a percepção da Alta Administração sobre a atuação da auditoria interna.

Um trabalho de asseguração, conforme a NBC TA - Estrutura conceitual, é aquele "no qual o auditor independente visa obter evidências apropriadas e suficientes para expressar sua conclusão, de forma a aumentar o grau de confiança dos usuários previstos sobre o resultado da mensuração ou avaliação do objeto, de acordo com os critérios que sejam aplicáveis".

Ainda, o IIA (2009) define o papel da Auditoria Interna no gerenciamento de riscos corporativo como uma atividade independente, de avaliação (*assurance*) e de consultoria. Seu papel fundamental em relação à gestão de riscos é fornecer avaliação objetiva (*objective assurance)* quanto à eficácia do gerenciamento de riscos.

Nesse contexto, destaca-se que a Audit tem incluído como objetivo de seus trabalhos a avaliação de processos de gerenciamento de riscos e controles internos, com base nas normas editadas pela CGU e nos padrões de auditoria disseminados pelo IIA. No exercício de 2021, foram realizadas três avaliações em áreas e processos relevantes da organização, dos quais dois tiveram como foco a avaliação de controles internos e um teve como foco avaliação preventiva, com base em riscos.

Adicionalmente, destaca-se que os temas de atuação da Audit decorrem de metodologia baseada em fatores de risco (exposta no documento "Políticas e Procedimentos para Mapeamento do Universo Auditável"), conforme já exposto no tópico 2.3.5.1. Dessa forma, são identificados macroprocessos da cadeia de valor e os temas relacionados para atuação e execução de trabalhos de auditoria, com qualificação segundo critérios de relevância, vulnerabilidade e oportunidade. Trata-se de boa prática, mas com oportunidades de melhoria identificadas, como a inclusão de percepção dos órgãos de controle e das unidades técnicas do FNDE e, especialmente, o estímulo à rotação de ênfase no Planejamento Operacional da Audit, proporcionando a atuação em temas diversificados.

Ressalta-se também que a Audit ainda não desenvolveu plenamente algumas competências técnicas que permitam a atuação em todos os temas relevantes do FNDE. É o caso, por exemplo, dos temas "Desenvolvimento de Sistemas de TI" e "Infraestrutura de TI", mapeados no universo

auditável e apontados como de grande relevância a partir de levantamento coletado junto à Alta Administração, mas que ainda não foram objeto de avaliação ou consultoria nos últimos exercícios.

Em sintonia com as evidências coletadas e a análise realizada, a percepção da Alta Administração quanto à atuação da Audit/FNDE demonstra que:

- 86% dos dirigentes "concordaram" ou "concordaram totalmente" que a Audit tem atuado em processos relevantes para a organização;
- 71% dos dirigentes "concordaram" ou "concordaram totalmente" totalmente que a Audit tem realizado avaliações com a finalidade de melhorar a eficiência e a eficácia dos processos de gestão de riscos;
- 86% dos dirigentes "concordaram" ou "concordaram totalmente" totalmente que a Audit tem proposto melhorias ou a implementação de novos controles considerando riscos identificados;
- 100% dos dirigentes "concordaram" ou "concordaram totalmente" totalmente que a Audit, no decorrer de seus trabalhos, considera mudanças que poderiam afetar de maneira significativa o sistema de controles internos.

Assim, ao se averiguar a existência e o funcionamento de asseguração pela Auditoria Interna do FNDE, enquanto instância posicionada na terceira linha, evidenciou-se que há fornecimento de asseguração aos órgãos de governança e à Alta Administração, bem como aos órgãos de controle e de regulamentação. Evidenciou-se, ainda, que a unidade fornece asseguração sobre os processos de gestão de riscos e de controle por intermédio da realização de trabalhos de auditoria, apesar da carência de atuação em alguns temas relevantes.

2.3.6. Monitoramento periódico e avaliações independentes – Planos e medidas de contingência

Há planos e medidas de contingência definidos para os elementos críticos da atuação do FNDE e estes são periodicamente testados e revisados?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à testagem periódica de planos e medidas de contingência para os elementos críticos da atuação da entidade. A análise foi conduzida pela avaliação do seguinte objeto de análise, a saber: 2.3.6.1. Testagem dos planos e medidas de contingência.

Conforme verificado, a organização não dispõe de processos formais de avaliação e seleção de respostas a riscos, culminando na não formalização de planos e medidas de contingência para todas as áreas, funções e atividades relevantes da organização, apesar da existência de iniciativas pontuais.

Assim, a avaliação realizada no presente aspecto mostrou que não há diretrizes para a elaboração de planos e medidas de contingência para os elementos críticos da organização, por isso não houve análise acerca do funcionamento dos processos de testagem e revisão desses planos.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado, bem como boas práticas para institucionalização desse aspecto.

2.3.6.1. Testagem dos planos e medidas de contingência

Os testes previstos buscaram avaliar se há planos e medidas de contingência definidos para os elementos críticos da atuação do FNDE, em todos as áreas, funções e atividades relevantes para o alcance dos objetivos-chave da organização e se estes são periodicamente testados e revisados.

Os planos e as medidas de contingência de riscos conforme a ISO 31000:2018 têm por objetivo "especificar como as opções de tratamento escolhidas serão implementadas de maneira que os arranjos sejam compreendidos pelos envolvidos, e o progresso em relação ao plano possa ser monitorado". A ISO também orienta quanto aos requisitos e medidas a serem seguidos no estabelecimento de tais planos.

Da análise realizada no tópico 2.2.4, concluiu-se que o FNDE não definiu formalmente processos de avaliação e seleção de respostas a riscos. Eventuais planos e medidas de contingência existentes em algumas áreas e funções relevantes da organização decorreram mais da própria natureza do trabalho que os demanda (ex.: recursos logísticos e serviços de TIC) do que de uma diretriz disseminada pela Autarquia para sua elaboração. Ainda, foram observadas inciativas pontuais no contexto da pandemia de Covid-19, no âmbito do Coopera-TCU.

Assim, considerando a ausência de práticas, entende-se que eventuais política e procedimentos a serem instituídos na Autarquia devem prever, adicionalmente, diretrizes para a testagem e a revisão de eventuais planos e medidas de contingência elaborados, considerando também as boas práticas já abordadas no aspecto 2.2.4, bem como as ações pontuais existentes.

2.3.7. Monitoramento de mudanças significativas

O FNDE monitora as mudanças que podem aumentar sua exposição a riscos e ter impacto nos seus objetivos?

Com vistas a avaliar este aspecto, foram previstos testes relacionados ao estabelecimento e ao funcionamento de procedimentos e protocolos para monitoramento de mudanças significativas. A análise foi conduzida pela avaliação do seguinte objeto de análise, a saber: 2.3.7.1. Procedimentos e protocolos de monitoramento.

A avaliação realizada mostrou que não dispõe de mecanismos formais e padronizados para monitorar as mudanças significativas que podem aumentar sua exposição a riscos e ter impacto nos seus objetivos. Por isso, concluiu-se pela ausência de procedimentos e protocolos de monitoramento no âmbito de um processo estruturado de gestão de riscos.

Assim, a seguir, descrevem-se os resultados encontrados neste aspecto, a partir do objeto de análise selecionado, bem como boas práticas para institucionalização desse aspecto.

2.3.7.1. Procedimentos e protocolos de monitoramento

Os testes previstos buscaram avaliar se estão estabelecidos e em funcionamento procedimentos e protocolos para monitorar e comunicar mudanças significativas nas condições que

possam alterar o nível de exposição a riscos e ter impactos significativos na estratégia e nos objetivos do FNDE.

Os procedimentos e protocolos do monitoramento são importantes na medida em que, conforme dispõe o COSO-CI (2013), "cada entidade precisa de um processo para identificar e avaliar fatores internos e externos que podem afetar significativamente a capacidade de realizar seus objetivos". Por isso, O COSO-GRC (2007) recomenda que o monitoramento de eventuais modificações (causadas, p. ex., pela chegada de novos atores, por mudanças na estrutura ou no direcionamento da organização, pela introdução de novos processos) precisa ser monitorado, de modo a determinar se o gerenciamento de riscos permanece eficaz.

Da análise realizada, concluiu-se que o FNDE não dispõe de mecanismos formais e padronizados para monitorar as mudanças significativas. Ademais, a unidade informou que não foram estabelecidas iniciativas voltadas ao monitoramento contínuo (ou ao menos frequente) no âmbito de um processo de gestão de riscos.

Assim, entende-se que eventuais política e procedimentos a serem instituídos na Autarquia devem prever diretrizes para o monitoramento de mudanças significativas, direcionando também a formalização de procedimentos e protocolos de monitoramento.

2.3.8. Correção de deficiências e melhoria contínua

São tomadas as medidas necessárias para a correção de deficiências e a melhoria contínua do desempenho da gestão de riscos em função dos resultados das atividades de monitoramento?

Com vistas a avaliar este aspecto, foram previstos testes relacionados à comunicação dos resultados resultantes das atividades de monitoramento. A análise foi conduzida pela avaliação de dois objetos de análise, a saber: 2.3.8.1. Comunicação às instâncias apropriadas; e 2.3.8.2. Planos de ação para correção e melhorias.

A avaliação realizada mostrou que não foram instituídos mecanismos para comunicação dos resultados da etapa de monitoramento às instâncias apropriadas.

A seguir, descrevem-se os resultados encontrados neste aspecto, a partir dos objetos de análise selecionados:

2.3.8.1. Comunicação às instâncias apropriadas

Os testes previstos buscaram avaliar se os resultados das atividades de monitoramento são utilizados para as tomadas de medidas necessárias à correção de deficiências e à melhoria contínua do desempenho da gestão de riscos, a partir da comunicação às instâncias apropriadas da administração e da governança com autoridade e responsabilidade para adotar as medidas necessárias.

Os relatos da avaliação dos controles internos dependerão, conforme dispõe o COSO-CI (2013), "dos critérios estabelecidos por órgãos reguladores, autoridades normativas e pela administração e pela estrutura de governança, conforme apropriado". O resultado das avaliações

contínuas e independentes de monitoramento permite determinar a quem e o que relatar de forma que os responsáveis possam tomar ações corretivas quando necessário. Dentro dessa perspectiva, é necessário comunicar eventuais deficiências às instâncias corretas, para que as ações corretivas necessárias sejam tomadas.

Pela análise realizada, concluiu-se que o FNDE não dispõe de mecanismos formais e padronizados para correção de deficiências e melhoria contínua dos seus processos de gestão de riscos. Ainda, a unidade apresentou que não há comunicação dos resultados do monitoramento de riscos às instâncias apropriadas. Ademais, conforme apurado no tópico 2.3.7, não há procedimentos/protocolos estabelecidos para monitoramento da gestão de riscos.

Assim, entende-se que eventuais política e procedimentos a serem instituídos na Autarquia devem prever também diretrizes para a comunicação dos resultados do monitoramento às instâncias apropriadas.

2.3.8.2. Planos de ação para correção e melhoria

Os testes previstos buscaram avaliar se os resultados das atividades de monitoramento são utilizados para as tomadas de medidas necessárias à correção de deficiências e à melhoria contínua do desempenho da gestão de riscos, a partir da elaboração e do devido acompanhamento de planos de ação para corrigir as deficiências identificadas e melhorar o desempenho da gestão de riscos.

É importante que a organização, na busca pela melhoria contínua de seus processos – e notadamente na busca pela adequação, suficiência, integração e eficácia da estrutura de gestão de riscos – identifique lacunas ou oportunidades de melhoria. Nesse contexto, a ISO 31000:2018 recomenda que sejam desenvolvidos, bem como atribuídos aos responsáveis pela implementação, planos e tarefas que permitam o planejamento de atividades de correção e melhoria.

A análise realizada mostrou que o FNDE não dispõe de planos de ação para corrigir as deficiências eventualmente identificadas e para melhoria do desempenho da gestão de riscos. Destaca-se, ainda, que o não estabelecimento de processos de monitoramento de mudanças significativas para a gestão de riscos, conforme demonstrado no tópico 2.3.7, também prejudica o presente objeto analisado.

Assim, entende-se que eventuais política e procedimentos a serem instituídos na Autarquia devem prever também diretrizes para a elaboração de planos de ação com vistas à melhoria contínua do processo de gestão de riscos.

3. DIMENSÃO PARCERIAS

Conforme exposto no *Orange Book*, o processo de gestão de riscos deve ser conduzido sistematicamente, iterativamente e colaborativamente, com base no conhecimento e nos pontos de vista de especialistas e das partes interessadas.

Em relação às partes interessadas, destaca-se que a efetividade da gestão de riscos em uma organização depende também da efetividade dos arranjos para gerenciar riscos em parcerias, ou seja, em políticas, programas ou projetos de gestão compartilhada.

Nesse contexto, parcerias podem ser definidas como os "arranjos estabelecidos para possibilitar relacionamento colaborativo entre as partes para alcançar objetivos de interesse comum", seja um objetivo estratégico ou a entrega de um produto ou serviço, envolvendo riscos e benefícios compartilhados (TCU, 2018a).

Ainda nesse tema, o TCU[32] destaca a importância de serem estabelecidos mecanismos de atuação conjunta entre órgãos e entidades com vistas à formulação, à implementação, ao monitoramento e à avaliação de políticas transversais e descentralizadas.

Já a ISO 31000:2018 ressalta, acerca da compreensão da organização e de seu contexto para o processo de gestão de riscos, a necessidade de incluir na concepção da estrutura para gerenciar riscos relacionamentos, percepções, valores, necessidades/expectativas das partes interessadas externas e a complexidade das redes de relacionamento e as dependências.

O Guia de Orientação para o Gerenciamento de Riscos (MP, 2013) traz o conceito de "organização estendida" para se referir às interdependências inerentes a qualquer tipo de organização e que impactam a sua gestão de riscos, dando origem a riscos adicionais que precisam ser gerenciados. Nesse contexto, o documento destaca os relacionamentos dentro da estrutura do Estado (entre órgãos e entidades da administração pública, nas diferentes esferas) e fora dela (como no caso de contratações de serviços terceirizados com empresas privadas, de interdependências com fornecedores e financiadores de projeto, ou de terceiros, de maneira geral). Assim:

> *[...] é essencial o alinhamento entre estas organizações com o objetivo de facilitar uma abordagem de gerenciamento de riscos que permita às partes atingir e/ou ajustarem os seus objetivos.*
>
> *[...] Qualquer que seja a natureza das relações de riscos entre as organizações participantes desta cadeia de valor de serviços governamentais, há necessidade de se assegurar que o risco está sendo gerenciado em todos os níveis (integração vertical) e em toda a cadeia de valor (integração horizontal).*

Assim, destaca-se a necessidade de que o processo de gestão de riscos do FNDE consiga identificar e avaliar riscos relacionados a cada um desses elementos (dentre outros elementos que possam ser relevantes no contexto da organização). Ainda, que envolva o estabelecimento de arranjos claros, que ajudem a assegurar um entendimento comum sobre riscos no âmbito de parcerias, definindo quais riscos serão gerenciados e por quem, bem como definindo canais para trocas de informações e comunicações sobre o assunto.

A avaliação realizada na presente dimensão focou nos aspectos relacionados à gestão de riscos no âmbito de políticas de gestão compartilhada, procurando avaliar em que medida o FNDE estabelece arranjos com clareza sobre quais riscos serão gerenciados e por quem, e como se darão as trocas de informações sobre o assunto, de modo a assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento.

Concluiu-se que o FNDE não estabeleceu diretrizes nem arranjos claros para assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento no âmbito de parcerias. Tal constatação decorre em grande parte da ausência de um processo estabelecido para a gestão de riscos em parcerias.

Consequentemente, há possíveis impactos no atingimento dos objetivos, metas e resultados esperados para as políticas compartilhadas; as entidades parceiras podem desconhecer os riscos

[32] Referencial básico de governança aplicável a órgãos e entidades da administração pública (TCU, 2014).

envolvidos na execução das políticas compartilhadas, prejudicando a adoção de medidas de tratamento de riscos, e, da mesma forma, os Conselhos podem ter maior dificuldade de fiscalizar a execução das políticas. Ainda, há prejuízo na comunicação entre o FNDE e as entidades parceiras, limitando o tratamento de falhas e conflitos.

Por fim, não há garantia razoável de recuperação e continuidade de serviços em caso de ocorrência de eventos de risco, devido à ausência de estabelecimento de planos e medidas de contingência para garantir a recuperação e a continuidade dos serviços no âmbito das parecerias realizadas.

O índice de maturidade obtido na dimensão Parcerias foi inexpressivo, o que significa uma maturidade **INICIAL** do seu modelo de gestão de riscos aplicado a parcerias. Quanto a cada um dos componentes relacionados à dimensão (3.1. Gestão de riscos em parcerias e 3.2. Planos e medidas de contingência em parcerias), não foram observadas práticas associadas.

Nos parágrafos a seguir, estão descritos os achados relativos aos dois componentes avaliados na dimensão Parcerias.

3.1. Gestão de riscos em parcerias

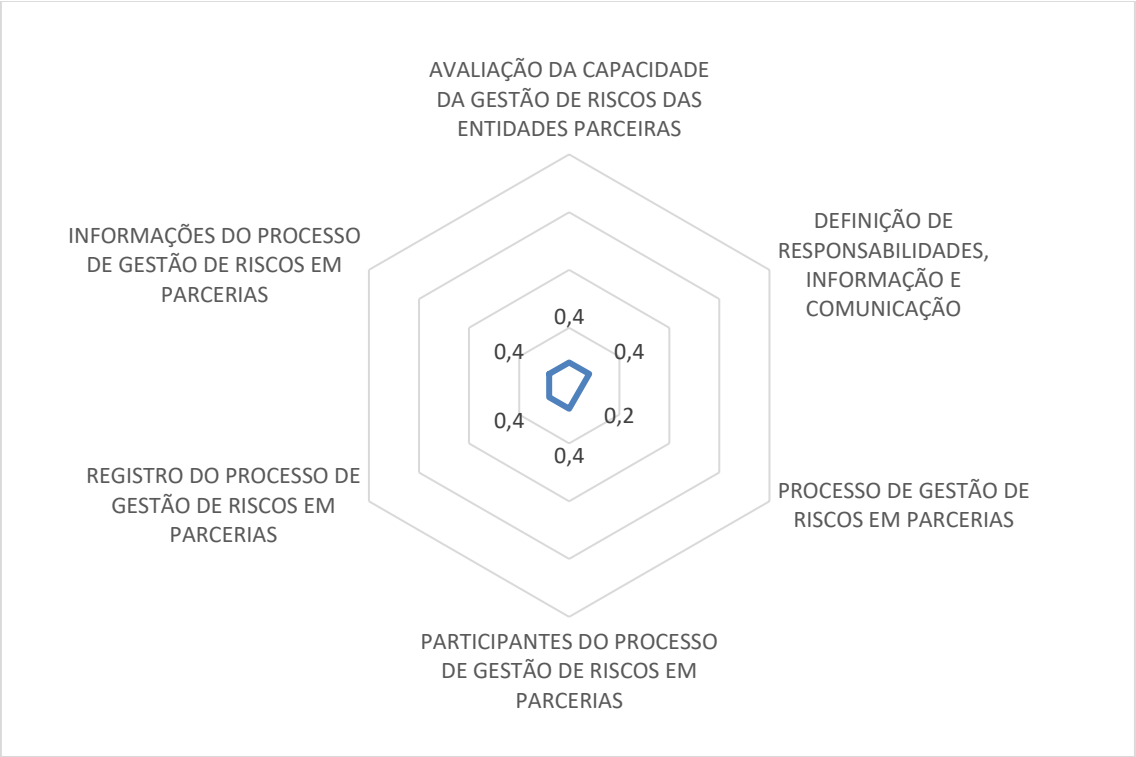
Nesse componente, apurou-se a seguinte questão: em que medida o FNDE estabelece arranjos com clareza para assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento no âmbito das parcerias?

Buscou-se, para tanto, avaliar em que medida a organização adota um conjunto de práticas essenciais de gestão de riscos para ter segurança razoável de que os riscos no âmbito das parcerias serão adequadamente gerenciados e os objetivos alcançados. A avaliação do componente foi feita a partir de seis aspectos: 3.1.1. Avaliação da capacidade da gestão de riscos das entidades parceiras; 3.1.2. Definição de responsabilidades, informação e comunicação; 3.1.3. Processos de gestão de riscos em parcerias; 3.1.4. Participantes do processo de gestão de riscos em parcerias; 3.1.5. Registro do processo de gestão de riscos em parcerias; e 3.1.6. Informações sobre o processo de gestão de riscos em parcerias.

No FNDE, o resultado do componente “Gestão de riscos em parcerias”, a partir da avaliação dos seus aspectos, demonstrou uma maturidade **INICIAL**.

O gráfico a seguir apresenta o resultado consolidado do componente, a partir dos resultados apurados em cada aspecto analisado:

Gráfico 62: Resultado da avaliação dos aspectos – Gestão de riscos em parcerias



Fonte: elaboração própria.

A partir do gráfico 62, verifica-se o baixo grau de maturidade dos processos de gestão de riscos em parcerias no FNDE, de modo que a maior parte dos elementos mínimos necessários para o desenvolvimento dessa dimensão ainda não foi instituída pela organização auditada.

Reforça-se que um grau maior de maturidade relacionado a essa etapa depende também de uma maior maturidade da dimensão processos, especialmente no que se refere ao estabelecimento de uma Política de Gestão de Riscos, que contemple também diretrizes para o gerenciamento de riscos em programas e projetos compartilhados.

3.1.1. Avaliação da capacidade da gestão de riscos das entidades parceiras

A capacidade de potenciais organizações parceiras para gerenciar os riscos das políticas de gestão compartilhadas é avaliada antes da realização das parcerias?

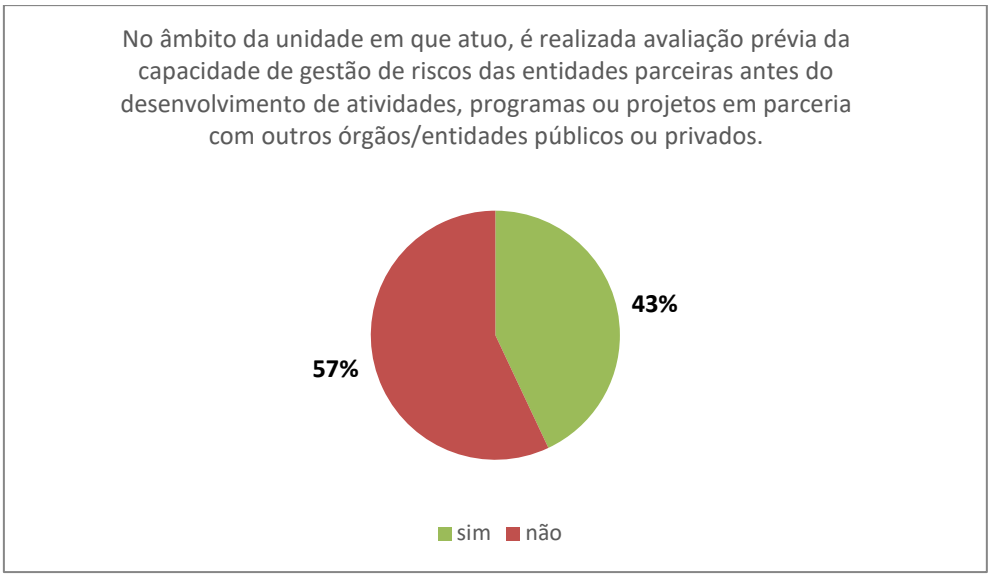
Com vistas a avaliar este aspecto, foram realizados testes para um objeto relacionado à existência de avaliação prévia ao compartilhamento de riscos, de maneira fundamentada e documentada, para concluir acerca da capacidade de potenciais organizações parceiras para gerenciar os principais riscos relacionados a cada objetivo, meta ou resultado. Além disso, coletou-se a percepção da Alta Administração acerca da gestão de riscos das entidades parceiras.

A análise realizada apontou para a ausência de documentos que evidenciassem que o compartilhamento dos principais riscos relacionados aos programas e projetos do FNDE tenha sido precedido de avaliação fundamentada e documentada da capacidade de potenciais organizações parceiras. Adicionalmente, não foi apresentada pela organização auditada documentação que

indicasse a existência de políticas, procedimentos ou protocolos específicos para gestão de riscos no âmbito de políticas e programas compartilhados.

Na pesquisa de percepção junto à Alta Administração verificou-se que 100% dos respondentes afirmaram que no âmbito da unidade em que atuam existem atividades, programas ou projetos em parceria com outros órgãos/entidades públicos ou privados. Ainda, 43% afirmaram que no âmbito da unidade em que atuam, existem ações e/ou atividades específicas de gestão de riscos direcionadas para parcerias e, por fim, 43% afirmaram que realizam avaliação prévia da capacidade de gestão de riscos das entidades parceiras antes do desenvolvimento de atividades, programas ou projetos em parceria com outros órgãos/entidades públicos ou privados.

Gráfico 63: Percepção da Alta Administração – Gestão de Riscos das entidades parceiras



Fonte: elaboração própria.

Conclui-se, portanto, que é uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização, mas percebida por alguns gestores, apontando para um grau de maturidade inicial (resultado apurado de 0,4).

Assim, entende-se que eventuais política e procedimentos de gestão de riscos a serem implementados precisam considerar diretrizes para coordenar e integrar as entidades parceiras e seus próprios processos de gestão de riscos, conforme preconizado pelo TCU (2014).

3.1.2. Definição de responsabilidades, informação e comunicação

Existe clara e adequada designação de responsáveis pelo gerenciamento de riscos nas parcerias e de protocolos de informação e comunicação entre eles?

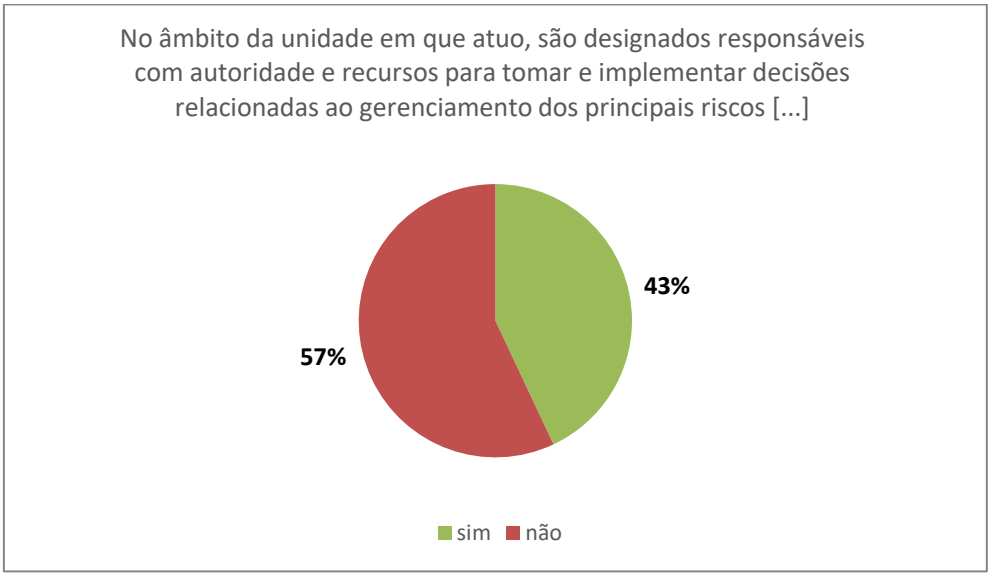
Com vistas a avaliar este aspecto, foram previstos testes para um objeto visando avaliar se são designados responsáveis com autoridade e recursos para tomar e implementar decisões relacionadas ao gerenciamento dos principais riscos relacionados a cada objetivo, meta ou

resultado esperado das políticas de gestão compartilhadas por meio de parcerias, bem como para avaliar em quais condições e para quem cada responsável deve fornecer informações. Além disso, coletou-se a percepção da Alta Administração acerca dessas definições.

Conforme já abordado nos tópicos 2.1.2.2 e 2.1.1.3, o FNDE não definiu uma Política de Gestão de Riscos (ou documento equivalente) e não mapeou as partes interessadas e nem mesmo definiu os responsáveis que internamente se responsabilizariam por cada aspecto da gestão de riscos. Adicionalmente, não foram apresentados pela unidade auditada documentos que evidenciassem a definição de responsáveis pelo gerenciamento de riscos nas parcerias nem de protocolos de informação e comunicação entre eles.

Em complemento, a partir da análise de percepção da Alta Administração, perguntados se tinham conhecimento dos processos de gestão de riscos aplicados nas entidades parceiras, no âmbito de políticas, programas e projetos compartilhados, 57% dos respondentes afirmaram que nas suas unidades de atuação não foram designados responsáveis com autoridade e recursos para tomar e implementar decisões relacionadas ao gerenciamento dos principais riscos relacionados a cada objetivo, meta ou resultado esperado das políticas de gestão compartilhadas por meio de parcerias, conforme gráfico a seguir:

Gráfico 64: Percepção da Alta Administração – Designação de responsáveis pela gestão de riscos em parcerias



Fonte: elaboração própria.

Conclui-se, portanto, que é uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização, mas percebida por alguns gestores, apontando para um grau de maturidade inicial (resultado apurado de 0,4).

Assim, entende-se que eventuais política e procedimentos de gestão de riscos a serem implementados precisam orientar a definição expressa de responsáveis pelo gerenciamento de riscos nas parcerias, bem como a formalização de protocolos de informação e comunicação entre eles.

3.1.3. Processo de gestão de riscos em parcerias

O processo de gestão de riscos é aplicado no âmbito das parcerias?

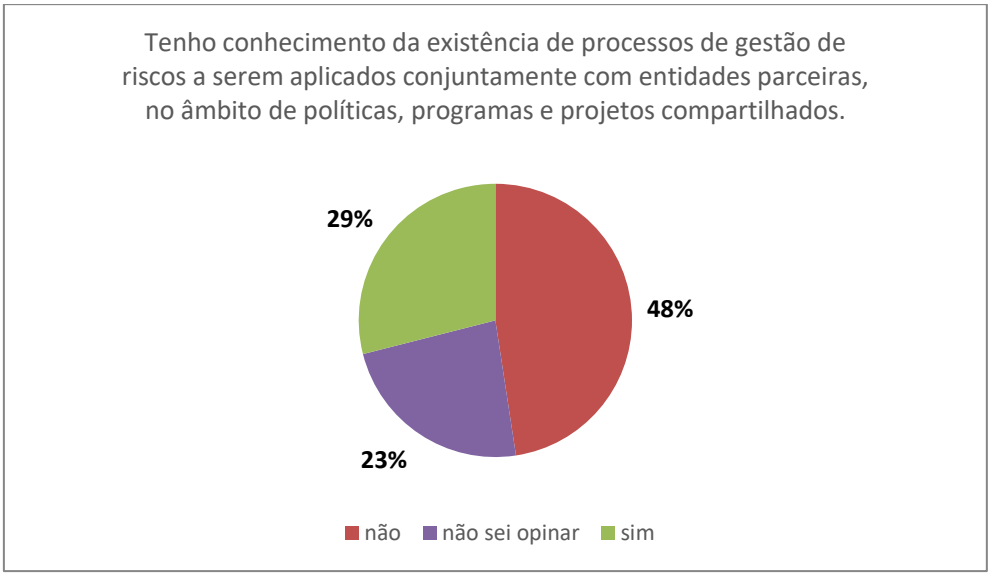
Com vistas a avaliar este aspecto, foram previstos testes para um objeto relacionado à aplicação do processo de gestão de riscos em parcerias, com vistas a identificar, avaliar, gerenciar e comunicar riscos relacionados a cada objetivo, meta ou resultado pretendido das políticas de gestão compartilhadas. Além disso, coletou-se a percepção dos servidores acerca da aplicação do processo de gestão de riscos em parceiras.

A ISO 31000:2018 afirma que o processo da gestão de riscos envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto, avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos. Entende-se que essas mesmas etapas devem ser aplicadas no gerenciamento de riscos em relação às parcerias.

Considerando que não há Política de Gestão de Riscos (ou outro documento equivalente), conforme já destacado no tópico 1.2.5, verificou-se que não há diretrizes para a integração de um processo gestão de riscos no âmbito de parcerias. Considerando ainda a avaliação realizada nos tópicos abordados na dimensão Processos, que concluiu que o FNDE não dispõe de um processo de gestão de riscos estruturado e formalmente instituído, entende-se que também não existe um processo de gestão de riscos sendo aplicado no âmbito das parcerias.

Em complemento, a análise de percepção dos servidores mostrou que 71% dos respondentes não têm conhecimento ou não soube opinar sobre processos de gestão de riscos aplicados nas entidades parceiras, no âmbito de políticas, programas e projetos compartilhados:

Gráfico 65: Percepção dos servidores – Aplicação do processo de gestão de riscos em parcerias



Fonte: elaboração própria.

Conclui-se, portanto, que é uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização, mas percebida por alguns servidores, demonstrando, assim, para um grau de maturidade inicial (resultado apurado de 0,2).

Assim, entende-se que eventuais política e procedimentos de gestão de riscos a serem implementados no FNDE precisam considerar também diretrizes específicas para as etapas do processo de gestão de riscos no âmbito de parcerias.

3.1.4. Participantes do processo de gestão de riscos em parcerias

A identificação e avaliação de riscos em parcerias envolve as pessoas apropriadas das organizações parceiras e outras partes interessadas?

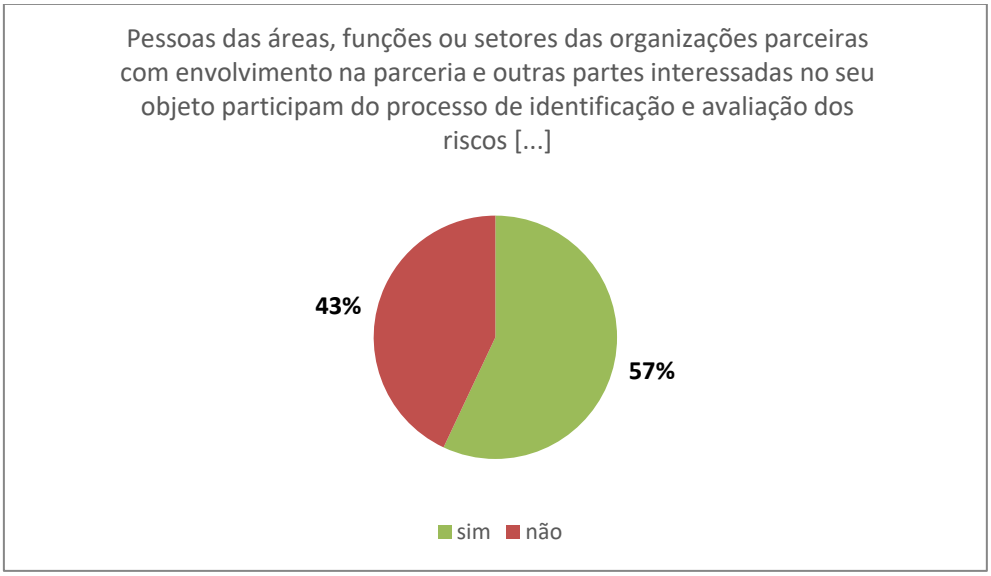
Com vistas a avaliar este aspecto, foram previstos testes para um objeto relacionado à participação de pessoas de todas as áreas, funções ou setores das organizações parceiras com envolvimento na parceria (bem como outras partes interessadas) nas etapas de identificação e avaliação de riscos, para cada objetivo, meta ou resultado esperado dos programas ou projetos compartilhados. Além disso, coletou-se a percepção da Alta Administração acerca dessas etapas.

Cumpre mencionar que não restou demonstrada a alocação de pessoas especificamente para a realização de atividades de gestão de riscos, como descrito nos objetos 1.1.2.2 e 1.2.7.1. Ademais, não há uma política institucional de gestão de riscos, nos termos da análise do tópico 1.2.5.

Ademais, não foi identificada a aplicação de um processo de gestão de riscos em parcerias, conforme relatado no tópico 3.1.3. Assim, não há diretrizes formalizadas na organização que tratem do envolvimento de pessoas apropriadas das organizações parceiras e de outras partes interessadas para a identificação e avaliação de riscos.

Quanto à percepção da Alta Administração, verificou-se que 57% dos respondentes afirmaram que pessoas, funções ou setores das organizações parceiras participam do processo de identificação e avaliação dos riscos, conforme gráfico a seguir:

Gráfico 66: Percepção da Alta Administração – Pessoas selecionadas para a gestão de riscos em parcerias



Fonte: elaboração própria.

Conclui-se, portanto, que é uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização, mas percebida por alguns gestores apontando para um grau de maturidade inicial (resultado apurado de 0,4).

Assim, entende-se que eventuais política e procedimentos de gestão de riscos a serem implementados precisam considerar diretrizes específicas para as etapas do processo de gestão de riscos em parcerias, incluindo a previsão de participação de pessoas específicas das entidades parceiras nas etapas de identificação e avaliação de riscos.

3.1.5. Registro do processo de gestão de riscos em parcerias

A gestão de riscos nas parcerias é apoiada por um registro de riscos único ou sistema de informação efetivo e atualizado?

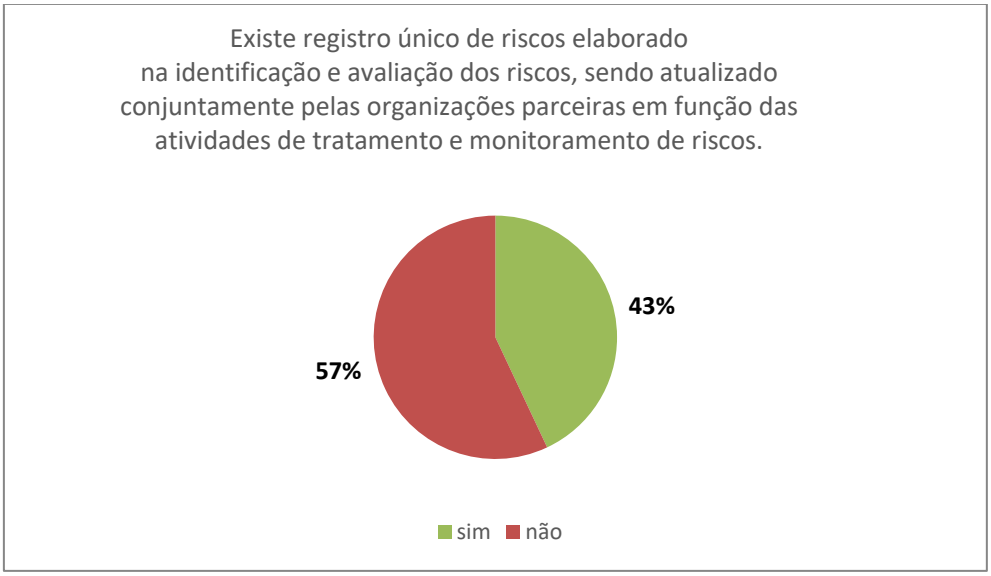
Com vistas a avaliar este aspecto, foram previstos testes para um objeto relacionado à existência e à atualização conjunta, pelas organizações parceiras, de registro do processo de gestão de riscos em função das atividades de tratamento e monitoramento de riscos. Além disso, coletou-se a percepção da Alta Administração acerca desse registro.

Conforme já destacado no tópico 2.1.4.1, o FNDE não dispõe de técnicas e ferramentas para a gestão de riscos, de modo que não é feito o registro dos riscos em sistemas ou planilhas.

No âmbito das parcerias, observou-se que a Autarquia não possui processo comum de gestão de riscos envolvendo organizações parceiras (conforme tópico 3.1.3), não existindo também um registro de riscos único ou sistema de informação efetivo e atualizado que permita a troca de informações regulares e confiáveis.

No mesmo sentido, a percepção da Alta Administração mostrou que 57% dos dirigentes respondentes afirmaram não existir esse registro único, conforme demonstrado no gráfico a seguir:

Gráfico 67: Percepção da Alta Administração – Registro de riscos único nas parcerias



Fonte: elaboração própria.

Conclui-se, portanto, que é uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização, mas percebida por alguns gestores. Assim, a unidade demonstra um grau de maturidade inicial (resultado apurado de 0,4).

Assim, entende-se que eventuais política e procedimentos de gestão de riscos a serem implementados precisam considerar diretrizes específicas para as etapas do processo de gestão de riscos em parcerias, incluindo os mecanismos conjuntos a serem utilizados para registro de riscos.

3.1.6. Informações sobre o processo de gestão de riscos em parcerias

Os riscos e o desempenho das parcerias são monitorados mediante troca regular de informação confiável?

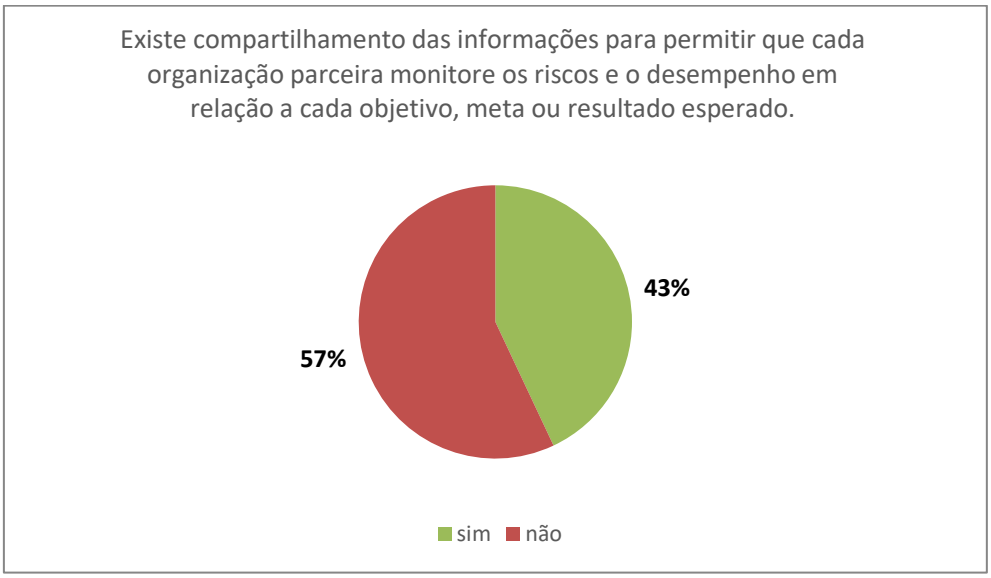
Com vistas a avaliar este aspecto, foram previstos testes para um objeto relacionado aos mecanismos de informação e comunicação para o processo de gestão de riscos no âmbito de parcerias, com vistas a concluir sobre a existência de informação regular e confiável para permitir que cada organização parceira monitore os riscos e o desempenho em relação a cada objetivo, meta ou resultado esperado. Além disso, coletou-se a percepção da Alta Administração acerca desse registro.

Conforme já destacado no tópico 2.3.1.1, o FNDE não dispõe de diretrizes ou protocolos de informação e comunicação para todas as fases do processo de gestão de riscos. No âmbito das parcerias, observou-se que a Autarquia não possui processo comum de gestão de riscos envolvendo organizações parceiras (conforme tópico 3.1.3), inexistindo também diretrizes ou protocolos de informação e comunicação para a gestão de riscos em parcerias. Ademais, a ausência de um registro

de riscos único ou de um sistema de informação efetivo e atualizado, conforme demonstrado no tópico 3.1.5, prejudica o monitoramento dos riscos e do desempenho[33].

No mesmo sentido, a percepção da Alta Administração mostrou que 57% dos dirigentes entenderam não existir compartilhamento de informações que permita que cada organização parceira monitore riscos e desempenho, conforme demonstrado no gráfico a seguir:

Gráfico 68: Percepção da Alta Administração – Informação regular e confiável no processo de gestão de riscos em parcerias



Fonte: elaboração própria.

Conclui-se, portanto, que é uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização, mas percebida por alguns gestores, apontando para um grau de maturidade inicial (resultado apurado de 0,4).

Assim, entende-se que eventuais política e procedimentos de gestão de riscos a serem implementados precisam considerar diretrizes específicas para as etapas do processo de gestão de riscos em parcerias, incluindo os mecanismos de informação e comunicação.

3.2. Planos e medidas de contingência em parcerias

Nesse componente, apurou-se a seguinte questão: em que medida são estabelecidos planos ou medidas de contingência para garantir a recuperação e a continuidade dos serviços no âmbito das parecerias realizadas?

Buscou-se, para tanto, avaliar se as organizações parceiras definem planos e medidas de contingência para garantir a recuperação e a continuidade dos serviços ou para minimizar efeitos

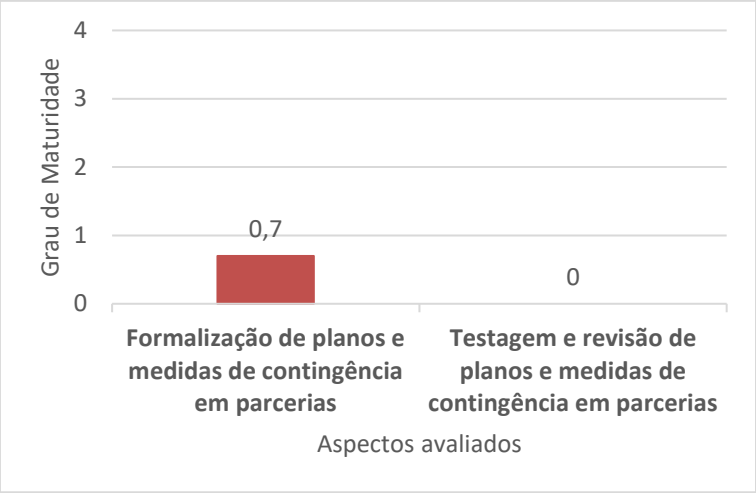
[33] Cumpre destacar que o enfoque dos testes não foi relacionado a atividades usuais de gestão dos programas e projetos desenvolvidos no âmbito do FNDE, mas sim a eventuais atividades específicas para o contexto de um processo regular e estruturado de gestão de riscos em parcerias. Dessa forma, em que pese não ser possível descartar que exista troca de informações entre o FNDE e seus parceiros, o ponto a ser ressaltado nesse aspecto refere-se à estruturação e à formalização de diretrizes de comunicação e consulta para fins de monitoramento compartilhado.

adversos sobre o fornecimento de serviços ao público quando uma ou outra parte falhar, bem como se esses planos são periodicamente testados e revisados. A avaliação do componente foi feita a partir de dois aspectos: 3.2.1. Formalização de planos e medidas de contingência em parcerias e 3.2.2. Testagem e revisão de planos e medidas de contingência.

No FNDE, o resultado do componente "Planos e medidas de contingência em parcerias", a partir da avaliação dos seus aspectos, demonstrou uma maturidade **INICIAL**.

O gráfico a seguir apresenta o resultado consolidado do componente, a partir dos resultados apurados em cada aspecto analisado:

Gráfico 69: Resultados da avaliação dos aspectos – Planos e medidas de contingência em parcerias



Fonte: elaboração própria.

A seguir apresentam-se os aspectos avaliados no componente Planos e Medidas de Contingência, bem como os objetos relacionados a cada aspecto.

3.2.1. Formalização de planos e medidas de contingência em parcerias

São definidos planos e medidas de contingência no âmbito das parcerias?

Com vistas a avaliar este aspecto, foram previstos testes para um objeto relacionado à existência de planos e medidas de contingência formais e documentados para garantir a recuperação e a continuidade dos serviços em casos de desastres ou para minimizar efeitos adversos sobre o fornecimento de serviços ao público quando uma ou outra parte falhar. Além disso, coletou-se a percepção dos servidores acerca de eventuais planos existentes.

Conforme já abordado no tópico 2.2.4.1, a IN nº 01/2016 dispõe sobre a necessidade de serem estabelecidos planos de contingência e resposta à materialização dos riscos como parte das atividades de controles internos implementadas pela organização.

Ainda, segundo o COSO-ERM-2007, é importante a Administração manter uma comunicação aberta com outras organizações associadas, levando em conta "o modo pelo qual o seu apetite a

riscos e a tolerância a riscos estão alinhados com o dos parceiros [...], assegurando que a organização não aceitará, por falta de controle, um excesso de riscos de seus parceiros".

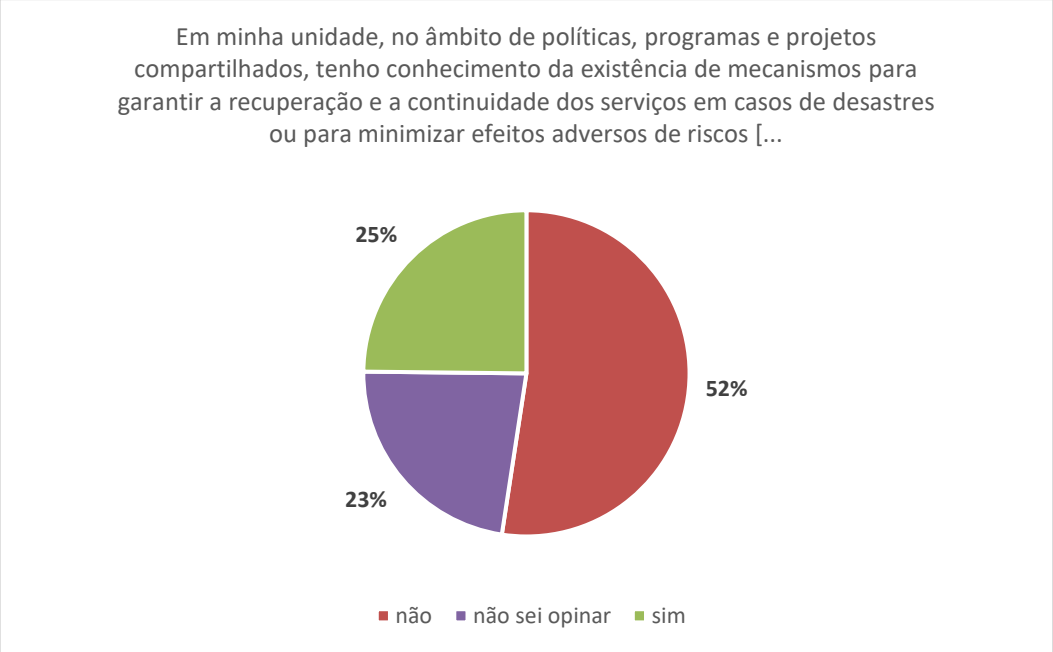
Incialmente, cumpre considerar que a própria definição de tais planos de contingência pressupõe que os riscos à continuidade ou ao fornecimento de serviços tenham sido identificados, bem como definidos o apetite e a tolerância a riscos. Como já descrito no componente 3.1, não há um processo de gestão de riscos aplicado no âmbito das parcerias, o que reflete na incapacidade de se preverem situações internas e externas que possam impactar o atingimento dos objetivos relacionados a programas e projetos compartilhados.

Tendo em vista que o FNDE atua também por meio de repasse a Entidades e Unidades Executoras, dentre outras, entende-se que estas podem ser consideradas como parceiras na realização da sua missão organizacional. Desse modo, os planos de contingência elaborados para o PNAE e para o PDDE com vistas ao enfrentamento à pandemia, tratados no tópico 2.2.4, contemplariam também estas parcerias. Vale destacar, porém, que esses planos decorrem de um contexto específico e da recomendação de um órgão de controle, de modo que sua elaboração não partiu de um processo prévio de avaliação e seleção de respostas a riscos.

Diante do exposto, não foi demonstrada a existência de um processo estruturado para a elaboração de planos e medidas de contingência no âmbito de parcerias, que garantam orientação, organização e respostas necessárias para a intervenção, controle e combate às consequências e aos impactos de determinados eventos adversos sobre o fornecimento de serviços ao público quando uma ou outra parte falhar.

No mesmo sentido, a percepção dos servidores indicou que apenas 25% afirmaram ter conhecimento da existência de mecanismos para garantir a recuperação e a continuidade dos serviços em casos de desastres ou para minimizar efeitos adversos de riscos relacionados a esses desastres:

Gráfico 70: Percepção dos servidores – Formalização de planos e medidas de contingência em parcerias



Fonte: elaboração própria.

Conclui-se, portanto, que é uma prática não expressiva e não instituída formalmente, de forma integrada e padronizada pela organização, com algumas iniciativas pontuais e específicas em desenvolvimento, e percebida por alguns gestores. Assim, a unidade apresenta um grau de maturidade inicial (resultado apurado de 0,7).

Assim, entende-se que eventuais política e procedimentos de gestão de riscos a serem implementados precisam considerar diretrizes específicas para a formalização de planos e medidas de contingência, direcionando também para a participação das organizações parceiras nesse processo.

3.2.2. Testagem e revisão de planos e medidas de contingência em parcerias

Os planos e as medidas de contingência no âmbito das parcerias são periodicamente testados e revisados?

Com vistas a avaliar este aspecto, foram previstos testes para um objeto relacionado à testagem e à revisão periódica de eventuais planos e medidas de contingência existentes no âmbito de parcerias.

Conforme descrito no aspecto 3.2.1, não foram identificados planos ou medidas de contingência especificamente formulados no âmbito de parcerias. Desse modo, não foi possível avaliar a existência de processos de testagem e revisão periódica desses planos.

Em que pese a existência de planos de contingência elaborados para o PNAE e o PDDE (no contexto da pandemia de Covid-19 e no âmbito da atuação do Programa Coopera/TCU) e o eventual envolvimento de entidades parceiras decorrente da natureza desses programas, destaca-se que esses planos não decorrem de uma política institucional de gestão de riscos, buscando abranger todas as áreas, funções e atividades relevantes (conforme abordado no tópico 2.2.5.1), não havendo, portanto, integração desses planos com um registro de riscos da organização ou com um processo aplicado para gestão de riscos em parcerias.

Ademais, não foram evidenciadas ações empreendidas pelas áreas visando a testagem e a revisão periódica dos planos elaborados, mesmo que de forma isolada.

Trata-se, assim, de uma prática não implementada e não instituída formalmente, de forma integrada e padronizada pela organização, apresentando um grau de maturidade inicial.

4. DIMENSÃO RESULTADOS

Após os princípios, as estruturas e os processos de gestão de riscos terem sido colocados em prática, espera-se que o gerenciamento de riscos flua por toda a organização, de forma integrada aos processos de gestão, desde o planejamento estratégico até os projetos e processos de todas as áreas, funções e atividades relevantes para o alcance dos objetivos-chave da organização.

Com isso, esperam-se resultados na melhoria do desempenho e no alcance de objetivos, a partir do aumento do grau de eficiência e eficácia no processo de criação, proteção e entrega de valor público. Assim,

> *Esta dimensão trata de aspectos relacionados aos efeitos das práticas de gestão de riscos, procurando avaliar em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão e os resultados da gestão de riscos têm contribuído para os objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.*

Conforme exposto pelo TCU (2018a), os resultados da gestão de riscos em uma organização se dão de maneira *imediata*, a partir dos efeitos das práticas de gestão de riscos na qualidade do processo decisório, na coordenação entre unidades organizacionais, no gerenciamento de riscos com parceiros, no aperfeiçoamento de planos e políticas organizacionais, na comunicação sobre riscos com partes interessadas e no envolvimento do pessoal com a avaliação e o controle dos riscos; e de maneira *mediata*, com efeitos que surgem a partir dos efeitos imediatos, com a melhoria de resultados e a otimização do desempenho da organização na sua capacidade de gerar, preservar e entregar valor público.

A partir de levantamento de políticas e metodologias utilizadas por outros órgãos e entidades públicas, foram observadas boas práticas e a presença comum de elementos que subsidiam uma cultura de gestão baseada em riscos, dentre os quais se destacam:

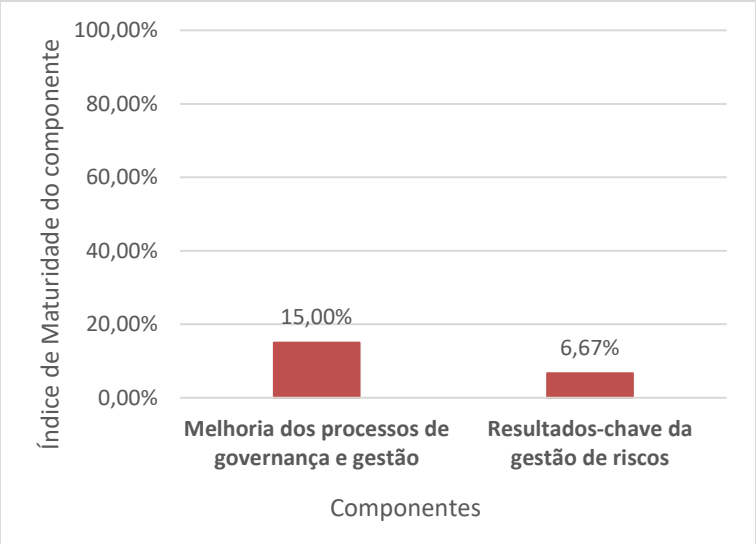
- A implementação da gestão de riscos se beneficia da existência de processos mapeados e de metodologias de gestão de processos, bem como do patrocínio da Alta Administração, da publicação de normativos (especialmente no que se refere a uma Política de Gestão de Riscos), da avaliação do grau de maturidade da gestão de riscos e do fomento a uma cultura favorável à gestão de riscos;
- Todos as organizações analisadas definiram uma estrutura organizacional para implementação de sua gestão de riscos, atribuindo responsabilidades formais a unidades e agentes. Ainda, as organizações se beneficiam da adoção de sistemas para gerenciamento de riscos;
- A estrutura organizacional definida envolve a participação da Alta Gestão, como elemento impulsionador, porém, envolve também os níveis tático e operacional, de modo a favorecer a integração;
- Os processos priorizados para a gestão de riscos costumam estar alinhados ao Planejamento Estratégico das organizações, especialmente no que se refere à Cadeia de Valor; e
- Os processos e procedimentos relacionados à identificação, à priorização, à avaliação e ao tratamento de riscos, ainda que elaborados pelas unidades responsáveis pelos programa/projetos/atividades, devem envolver também participação de pessoas que têm conhecimento sobre gestão de riscos, como gestores de segunda linha, que atuam na facilitação e na orientação.

A avaliação realizada na presente dimensão examinou os efeitos das práticas de gestão de riscos e a sua eficácia para a melhoria dos processos de governança e gestão. Ademais, avaliou-se em que medida os resultados da gestão de riscos têm contribuído para os objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos.

Como resultado, observou-se que FNDE ainda não possui um ambiente favorável e processos estruturados que permitam que a gestão de risos prospere e seja eficaz para a melhoria dos processos de governança e gestão. Tal constatação está associada aos achados relacionados nas dimensões Ambiente, Processos e Parcerias.

O índice de maturidade obtido na dimensão Resultados foi de **11,43%**, o que significa uma maturidade **INICIAL** do seu modelo de gestão de riscos aplicado a parcerias. O gráfico a seguir apresenta o Índice de Maturidade para cada um dos componentes relacionados à dimensão:

Gráfico 71: Índice de Maturidade por Componente – Dimensão Resultados



Fonte: elaboração própria.

Nos parágrafos a seguir, estão descritos os achados relativos a cada um dos componentes avaliados na dimensão Resultados (Melhoria dos processos de governança e gestão e Resultados-chave da gestão de riscos).

4.1. Melhoria dos processos de governança e gestão

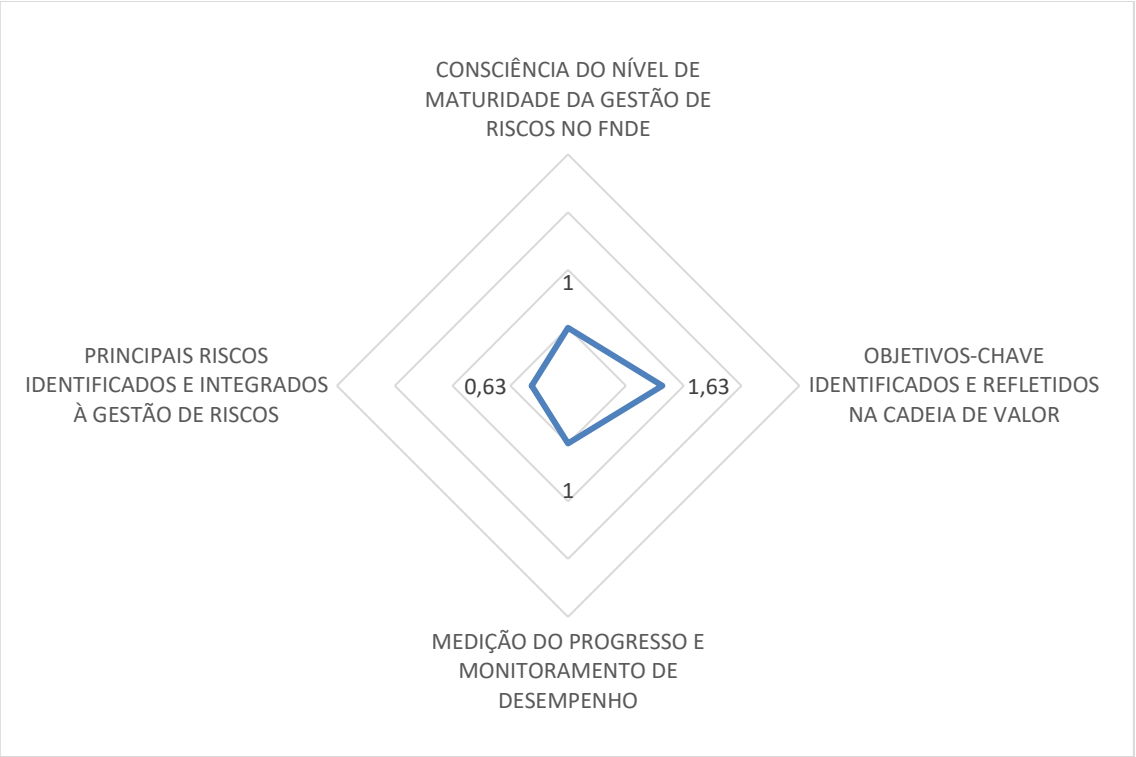
Nesse componente, apurou-se a seguinte questão: em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão?

Buscou-se, para tanto, avaliar em que medida os principais riscos relacionados a cada objetivo, meta ou resultado-chave pretendido estão identificados e incorporados ao processo de gerenciamento de riscos. A avaliação do componente foi feita a partir de quatro aspectos: 4.1.1. Consciência do Nível de Maturidade da gestão de riscos no FNDE; 4.1.2. Objetivos-chave identificados e refletidos na Cadeia de Valor; 4.1.3. Medição do progresso e monitoramento do desempenho; e 4.1.4. Principais riscos identificados e integrados à gestão de riscos.

No FNDE, o resultado do componente “Melhoria dos processos de governança e gestão”, a partir da avaliação dos seus aspectos, demonstrou uma maturidade **INICIAL**, apurada em **15,00%**.

O gráfico a seguir apresenta o resultado consolidado do componente, a partir dos resultados apurados em cada aspecto analisado:

Gráfico 72: Resultado da avaliação dos aspectos – Melhoria dos processos de governança e gestão



Fonte: elaboração própria.

A partir do gráfico 72, verifica-se a presença, em um nível inicial de elementos que auxiliam a gestão de riscos, como é caso da consciência do nível de maturidade, da identificação dos objetivos-chave, da medição do progresso e do monitoramento do desempenho. No entanto, há que se ressaltar que, em que pese a percepção das pessoas que atuam na organização acerca da existência de resultados da gestão de riscos em alguma medida, o FNDE ainda não conseguiu integrá-la ao seu planejamento estratégico e às suas atividades operacionais, o que impede a organização de atingir maior segurança em relação à melhoria de seus processos de governança e gestão (refletido na ausência de ações implementadas associadas ao aspecto "Principais riscos identificados e integrados à gestão de riscos).

4.1.1. Consciência do Nível de Maturidade da gestão de riscos no FNDE

Os responsáveis pela governança e a alta administração têm consciência do estágio atual da gestão de riscos na organização?

Com vistas a avaliar este aspecto, foram realizados testes para um objeto relacionado à consciência do nível de maturidade da gestão de riscos e do progresso de eventuais ações em curso para atingir ao nível almejado. Além disso, coletou-se a percepção dos servidores e da Alta Administração acerca desse nível.

Conforme destacado no tópico 1.1.3.5, a Autarquia vem se utilizando dos resultados do Levantamento de Governança e Gestão Públicas (iGG/TCU) como parâmetro para avaliar o tema, tendo sido a gestão de riscos identificada como uma das fragilidades da organização. Nesse sentido,

o relatório individual da autoavaliação do FNDE apontou em relação ao indicador 2110 (Capacidade em gerir riscos), um nível "inexpressivo" para a organização, distante da média de outras Autarquias (inicial) e distante também da média da administração indireta (intermediária) e da média do Poder Executivo (intermediária). Ainda, em relação aos indicadores 2111 (A estrutura da gestão de riscos está definida), 2113 (O processo de gestão de riscos da organização está implantado), 2114 (Os riscos considerados críticos para a organização são geridos) e 2115 (A organização executa processo de gestão de continuidade do negócio), os resultados também indicaram um grau "inexpressivo". Já em relação ao índice 2112 (Atividades típicas de segunda linha estão estabelecidas), a classificação apurada foi "inicial".

Ademais, a presente avaliação identificou que ainda não foi definido um nível de maturidade almejado para a gestão de riscos da organização, de modo que não há um parâmetro e um indicador definidos e que possam auxiliar no monitoramento e na medição do progresso. Adicionalmente, alguns pontos avaliados na dimensão Ambiente evidenciam o baixo grau de consciência da organização no tocante à gestão de riscos, como:

- A unidade definiu algumas instâncias para atuar na gestão de riscos como os Comitês de Gestão Estratégica e Governança (CGEG) e de Gestão de Riscos, Controles Internos e Integridade (CGRCI), porém não houve atuação dessas instâncias durante os exercícios de 2020 e 2021 (conforme demonstrado no tópico 1.1.2.1);
- Não foram definidos Política e procedimentos para gestão de riscos (conforme demonstrado no tópico 1.1.5); e
- O comprometimento da Alta Administração e do corpo executivo da gestão resta prejudicado em relação ao estabelecimento e à revisão da estrutura e do processo de gestão de riscos e controles internos, dado que não foram estabelecidas estruturas e processos adequados (conforme demonstrado no tópico 1.2.6.1).

Quando questionados acerca do nível de maturidade em que consideram que a gestão de riscos do FNDE se encontra, 40% dos servidores entenderam que a Autarquia está no nível Básico, com práticas de gestão de riscos realizadas de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chave da organização.

Quando questionados sobre o mesmo tema, 43% dos respondentes da Alta Administração também entenderam que o FNDE está no nível Básico, com práticas de gestão de riscos realizadas de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chave da organização.

A análise realizada apontou que os responsáveis pela governança e a Alta Administração têm apenas uma consciência superficial do estágio atual da gestão de riscos do FNDE, dado que ainda não foram feitas avaliações sobre a maturidade da gestão de riscos na organização. Nesse contexto, entende-se que é necessário compreender melhor o nível de maturidade da organização, de modo a possibilitar a priorização de ações para atingir o nível desejado e compatível com as atividades e o porte da organização. Assim, trata-se de prática percebida em alguma medida na organização, mas ainda sem indicadores internos que possam medi-la.

4.1.2. Objetivos-chave identificados e refletidos na Cadeia de Valor

Os objetivos-chaves da organização estão identificados e refletidos na sua cadeia de valor e nos seus demais instrumentos de direcionamento e comunicação da estratégia?

Com vistas a avaliar este aspecto, foram realizados testes para um objeto relacionado à identificação de objetivos-chave na cadeia de valor, na missão, na visão da organização e nos seus valores fundamentais, de modo a se formar uma base para a definição da estratégia e a fixação de objetivos estratégicos e de negócios.

Inicialmente cumpre destacar que o FNDE revisou sua Cadeia de Valor, tendo sido validada em julho de 2022. O novo modelo de Cadeia de Valor Integrada foi construído no âmbito das ações do TransformaGov – Programa de Apoio à Gestão estratégica e Transformação do Estado. A construção foi feita em parceria com o Ministério da Economia e tomou como premissa a metodologia de Gestão de Processos de Negócio – *Business Process Management* (BPM).

Dentre os propósitos apresentados para a nova Cadeia de Valor Integrada estão:

- Descrever a estrutura hierárquica da criação de valor;
- Declarar o valor público que é entregue à sociedade;
- Representar o modelo de negócio por meio dos macroprocessos e processos;
- Priorizar serviços e processos para a inovação e transformação; e
- Iniciar como um dos referenciais do planejamento estratégico.

A nova Cadeia é dividida em *arquitetura de negócio* (o que é feito) – a partir de macroprocessos e processos que geram valor para a sociedade – e *arquitetura de processos* (como é feito) – com o detalhamento dos serviços/processos de trabalho e suas respectivas atividades e tarefas associadas, descrevendo assim o fluxo do serviço/processo de trabalho.

Assim, a Cadeia de Valor servirá de base, dentre outros, para a estrutura organizacional, a elaboração de indicadores de desempenho, a definição de perfil de competências e o estabelecimento de controles.

Da versão validada observa-se o macroprocesso finalístico definido para o FNDE (Gestão do financiamento para o desenvolvimento da educação), seus respectivos macroprocessos gerenciais e finalísticos, bem como os macroprocessos de suporte, com base nas definições do Órgão Central do Siorg.

Como resultado, foram também estabelecidos os valores públicos entregues pelo FNDE, que podem ser entendidos como os objetivos-chave da organização: bem-estar na educação, acesso à educação superior privada, acesso ao material didático e segurança alimentar e nutricional no ensino básico.

Dessa forma, entende-se que os objetivos-chaves, que traduzem o conjunto de valores a serem gerados, preservados e/ou entregues à sociedade estão identificados e refletidos na cadeia de valor, de modo que, em alguma medida, o funcionamento desse aspecto é percebido na organização.

Destaca-se, porém, que o próximo passo para avançar em um maior grau de maturidade é a revisão do Planejamento Estratégico do FNDE, de modo a fazer com que essa nova Cadeia de Valor esteja refletida no direcionamento estratégico, formando a base para a definição a fixação de objetivos estratégicos e de negócios. Ademais, entende-se relevante dar continuidade à

estruturação e à revisão dos processos de trabalho, tarefas e atividades a partir da nova cadeia. Também será necessário disseminar essas novas definições por toda a organização.

4.1.3. Medição do progresso e monitoramento de desempenho

Os objetivos estratégicos e de negócios estão estabelecidos juntamente com as respectivas medidas de desempenho?

Com vistas a avaliar este aspecto, foram realizados testes para um objeto relacionado à identificação de objetivos-chave na cadeia de valor, na missão, na visão da organização e nos seus valores fundamentais, de modo a se formar uma base para a definição da estratégia e a fixação de objetivos estratégicos e de negócios.

Conforme destacado no tópico 1.2.4.1, foram definidos os objetivos estratégicos do FNDE e as respectivas medidas de desempenho. No entanto, observaram-se fragilidades relacionadas ao objeto analisado, especialmente no tocante à articulação do nível estratégico com os níveis tático e operacional. Ademais, dado que não foram estabelecidos objetivos de negócio, não houve o estabelecimento de medidas de desempenho no que se refere às categorias operacional, de conformidade e de divulgação.

Adicionalmente alguns pontos avaliados na dimensão Ambiente evidenciam o baixo grau de consciência da organização no tocante à gestão de riscos e à sua medição de desempenho, como:

- não foram definidos indicadores-chave de riscos, que possibilitem monitorar variações aceitáveis no desempenho em relação às metas estabelecidas. Também não houve definição do apetite a risco e da tolerância a risco (tópico 1.1.3.1);
- não foi definido apetite a risco da organização (tópico 1.2.2.1);
- não existem fluxos ou canais exclusivos para a comunicação de riscos (tópicos 1.1.2.1 e 1.1.3.2); e
- não foi evidenciada uma visão de portfólio de riscos no FNDE, conforme destacado no tópico 1.1.3.3.

Por isso, entende-se que as fragilidades apresentadas limitam a adequada medição do progresso e o monitoramento do desempenho de todas as áreas, funções e atividades relevantes da organização para a realização dos seus objetivos-chave, demonstrando um nível inicial. Para que essa medição seja possível, é necessário tratar as deficiências identificadas – especialmente no que se refere à articulação entre os níveis estratégico, tático e operacional – e fazer com que os objetivos estratégicos estejam adequadamente desdobrados em dimensões operacionais, de conformidade e de divulgação, conforme recomendam as boas práticas de gestão de riscos, possibilitando também a construção de indicadores para monitoramento dessas dimensões e dos objetivos relacionados.

Considerando a nova versão da Cadeia de Valor do FNDE, entende-se que há uma base para que esse aprimoramento seja feito, de modo que a evolução do nível de maturidade neste aspecto depende em grande parte das ações que serão desdobradas a partir dessa nova cadeia.

Ademais, caberá, quando da elaboração do novo Plano Estratégico do FNDE, considerar a integração da gestão de riscos aos processos de gestão, além de avançar no sentido de definir indicadores de risco que possam medir as variações em relação ao apetite a risco a ser definido.

4.1.4. Principais riscos identificados e integrados à gestão de riscos

Os principais riscos relacionados a cada objetivo, meta ou resultado-chave pretendido estão identificados e incorporados ao processo de gerenciamento de riscos?

Com vistas a avaliar este aspecto, foram realizados testes para um objeto relacionado à existência de identificação, avaliação, tratamento, comunicação e monitoramento dos principais riscos da organização.

A avaliação realizada nas dimensões Ambiente e Processos mostrou que o FNDE não instituiu um processo de gestão de riscos, de modo que não foram identificadas diretrizes para a realização de atividades integrantes desse processo. Tampouco foi identificado o adequado funcionamento dessas atividades.

Corroboram essa conclusão as seguintes condições encontradas:

- Ausência de Política de Gestão de Riscos ou de outro documento equivalente (conforme tópico 1.2.5);
- Não alocação de recursos para gestão de riscos – não existem pessoas, recursos, ferramentas e metodologias específicas para a gestão de riscos –, também não foram formalmente definidos gestores de risco (conforme tópicos 1.1.2.1 e 1.2.7.1);
- A realização esporádica da etapa de estabelecimento do contexto, em algumas unidades relevantes, mas sem a presença de diretrizes ou de uma metodologia que possam orientar e padronizar a identificação dos objetivos-chave da atividade, do processo ou do projeto a ser objeto da gestão de riscos e sem considerar o contexto dos objetivos-chave da organização como um todo, de modo a assegurar que os riscos significativos de cada objeto possam ser apropriadamente identificados (conforme tópico 2.1.1);
- A inexistência de uma lista abrangente de riscos, incluindo causas, fontes e eventos que possam ter um impacto na consecução dos objetivos da organização (conforme tópico 2.1.3.4);
- A não definição de critérios para orientar a priorização de riscos e dar garantia razoável de que decisões seguras estão sendo tomadas por toda a organização quanto a se um determinado risco precisa de tratamento e a prioridade para isso (conforme tópico 2.2.1.1); e
- A ausência de diretrizes e protocolos de informação e comunicação para as fases do processo de gestão de riscos, tendo em vista que não há previsão formalizada e disseminada pela organização de comunicação e consulta com partes interessadas (externas e internas) para o processo de gestão de riscos (conforme tópico 2.3.1.1).

Destaca-se também que, conforme relatado na dimensão Processos, o FNDE não definiu formalmente um processo de identificação de riscos, mas observam-se iniciativas pontuais no tema (como: na consultoria realizada entre 2017 e 2018, que identificou e categorizou alguns eventos de riscos; no âmbito do Malha Fina; no PNAE e no PDDE no contexto do Coopera-TCU). Porém, dada a ausência de diretrizes instituídas a incorporação dessas iniciativas às práticas institucionais restou prejudicada.

Pelo exposto, não foi evidenciado que estão avaliados e sob tratamento e monitoramento os principais riscos relacionados a cada objetivo, meta ou resultado-chave pretendido de todas as áreas, funções e atividades relevantes para a realização dos objetivos-chave da organização, com o

desempenho sendo comunicado aos níveis apropriados da administração e da governança. Também não foi evidenciado que há indicadores adequados para medir como os resultados de cada área ou pessoa contribuem com o atingimento dos objetivos-chave que envolvem riscos, especialmente dada a ausência de indicadores de riscos (já citada no tópico 1.1.3.1).

4.2. Resultados-chave da gestão de riscos

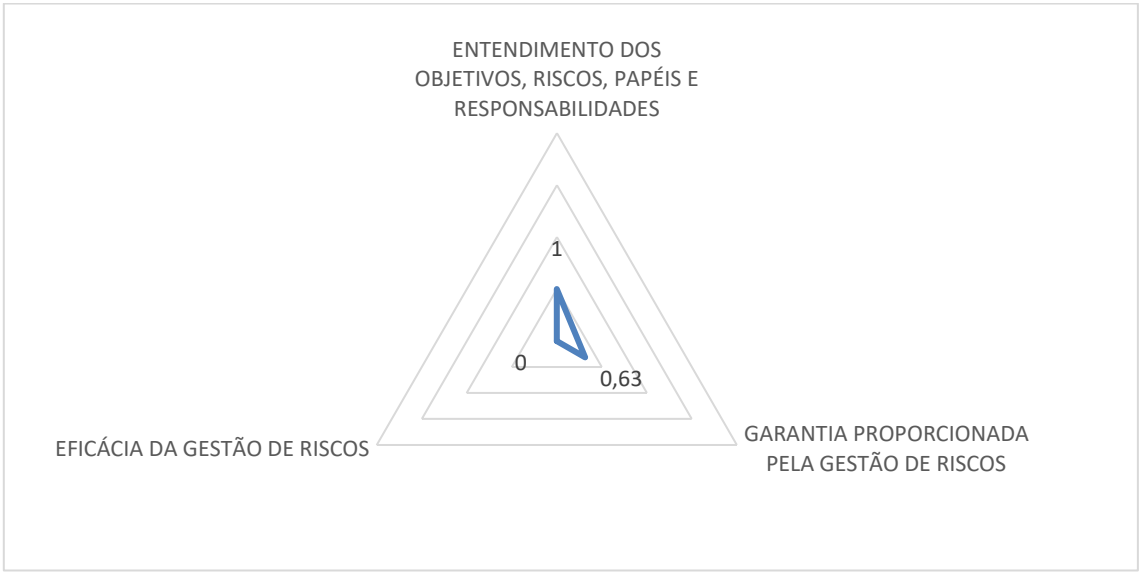
Nesse componente, apurou-se a seguinte questão: em que medida os resultados da gestão de riscos têm contribuído para os alcances dos objetivos do FNDE?

Buscou-se, para tanto, avaliar se os resultados da gestão de riscos têm contribuído para o alcance dos objetivos relacionados à eficiência das operações, à qualidade de bens e serviços, à transparência e à prestação de contas e ao cumprimento de leis e regulamentos. A avaliação do componente foi feita a partir de três aspectos: 4.2.1. Entendimento dos objetivos, riscos, papéis e responsabilidades; 4.2.2. Garantia proporcionada pela gestão de riscos; e 4.2.3. Eficácia da gestão de riscos.

No FNDE, o resultado do componente "Resultados-chave da gestão de riscos", a partir da avaliação dos seus aspectos, demonstrou uma maturidade **INICIAL**, apurada em **6,67%**.

O gráfico a seguir apresenta o resultado consolidado do componente, a partir dos resultados apurados em cada aspecto analisado:

Gráfico 73: Resultado da avaliação dos aspectos – Resultados-chave da gestão de riscos



Fonte: elaboração própria.

A partir do gráfico 73, verifica-se que a baixa maturidade do ambiente e dos processos tende a impactar diretamente a eficácia da gestão de riscos da organização, de modo que não é possível garantir que os riscos do FNDE estão dentro de critérios de risco compatíveis com seus objetivos e com o seu porte. Assim, restaram não evidenciados os resultados-chave da gestão de riscos no âmbito do FNDE, de modo que não há adequado entendimento acerca de aspectos relacionados à gestão de riscos, tampouco há garantia por ela proporcionada, o que impacta sua eficácia.

4.2.1. Entendimento dos objetivos, riscos, papéis e responsabilidades

Uma consciência sobre riscos, objetivos, resultados, papéis e responsabilidades está disseminada por todos os níveis da organização?

Com vistas a avaliar este aspecto, foram realizados testes para um objeto relacionado à consciência sobre objetivos, riscos, resultados, papéis e responsabilidades para atingimento de objetivos-chave que envolvem riscos.

Conforme abordado no tópico 1.2.1.1, o FNDE possui consciência básica sobre os seus objetivos, o que pode ser demonstrado por intermédio de seu direcionamento estratégico, traduzido a partir da definição da missão, da visão e dos valores fundamentais da organização, bem como da definição de objetivos estratégicos, formalizados em seu PEI 2018-2022, em seu Mapa Estratégico e em sua Cadeia de Valor.

No entanto, não foram identificadas iniciativas que demonstrem a consideração do risco no estabelecimento da estratégia, especialmente em decorrência da ausência de diretrizes formalmente estabelecidas para a gestão de riscos na organização. Assim, não é possível afirmar que há integração da gestão de riscos à estratégia da Autarquia.

Adicionalmente, foram encontradas fragilidades relacionadas à definição de papéis e responsabilidades que impactam no presente aspecto. Nesse sentido, cabe destacar:

- não foram definidos Políticas e Procedimentos para gestão de riscos (conforme destacado nos tópicos relacionados ao aspecto 1.2.5);
- os mecanismos existentes na organização não fornecem suporte para o correto funcionamento da primeira linha e não foram formalmente definidas as correspondentes responsabilidades dessa linha, p. ex. não há “gestores de riscos” nas unidades e nos processos mais relevantes (conforme destacado no tópico 1.3.2.1);
- também não foram formalmente atribuídos os papéis de segunda linha, de modo que não há pessoas formalmente designadas para atuar no âmbito de um processo coordenado e integrado de supervisão da gestão de riscos (conforme destacado no tópico 1.3.2.2);
- em que pese a existência de uma unidade de auditoria interna, atuando no papel de terceira linha, com clareza acerca de seu papel e com conhecimento dos papéis fundamentais que deve assumir, a inexistência de uma Política de Gestão de Riscos e a não definição de um cadastro de riscos da organização impede sua atuação em um nível avançado, dado que a definição da estratégia de auditoria depende em grande parte do grau de maturidade da gestão de riscos da unidade auditada (conforme destacado no tópico 1.3.2.3); e
- complementarmente, concluiu-se que, no âmbito de um modelo de governança do FNDE, não estão claramente identificadas as instâncias internas e de apoio à governança, o que tem potencial para prejudicar a gestão de riscos (conforme destacado no tópico 1.1.2.1).

Nesse contexto, conclui-se que a organização precisa avançar no sentido de integrar à gestão de riscos ao seu direcionamento estratégico, fazendo também com que essa integração seja refletida nos níveis tático e operacional e em todas as áreas, funções e atividades relevantes, de maneira a favorecer a eficiência e a eficácia de suas operações.

Os resultados obtidos nos questionários das dimensões Ambiente e Processos demonstram que há uma percepção acerca do tema, com reconhecimento de riscos, objetivos, resultados, papéis e responsabilidades. No entanto, a análise documental evidencia que a organização ainda não conseguiu avançar em relação à institucionalização de mecanismos que permitam gerenciar adequadamente seus riscos, com vistas ao atingimento de objetivos, tampouco em relação à adequada definição de papéis e responsabilidades que possam subsidiar seus processos de gestão de riscos.

4.2.2. Garantia proporcionada pela gestão de riscos

Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, do cumprimento dos objetivos da organização?

Com vistas a avaliar este aspecto, foram realizados testes para um objeto relacionado à garantia proporcionada pela gestão de riscos, com vistas a entender até que ponto: os objetivos estratégicos e operacionais estão sendo alcançados; a comunicação de informações é realizada de forma confiável; e as leis e regulamentos aplicáveis estão sendo cumpridos.

A análise realizada nas dimensões anteriores mostrou que o FNDE definiu seus objetivos estratégicos alinhados ao direcionamento estratégico (conforme o tópico 1.2.3.1) e, ainda, que ocorre o monitoramento desses objetivos por intermédio de medidas de desempenho (conforme o tópico 1.2.4.1). No entanto, mostrou-se também que não há 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. Desse modo, há prejuízo para a garantia de alcance dos objetivos estratégicos definidos.

Adicionalmente, no que se refere à definição de objetivos correlatos, mostrou-se que a organização não desdobrou formalmente os objetivos estratégicos em objetivos de negócios, nas categorias operacional, de divulgação (transparência e prestação de contas) e de conformidade, o que foi relatado nos tópicos 1.2.3.1 e PA 1.2.3.2. Assim, não há garantia proporcionada pela gestão de riscos no que se refere ao alcance dos objetivos de negócio.

Importante ressaltar também que não foram estabelecidos diretrizes e protocolos de informação e comunicação para as fases do processo de gestão de riscos (tópico 2.3.1.1). Por isso, não há garantia de que as informações necessárias são coletadas e produzidas (bem como comunicadas) a todos os níveis da organização, para desempenho das responsabilidades de gestão de riscos.

Por fim, as fragilidades relacionadas ao direcionamento estratégico e ao aspecto “Informação e Comunicação” prejudicam a gestão de riscos, fragilizando também a garantia de que as leis e os regulamentos aplicáveis estão sendo cumpridos.

Destaca-se também que a avaliação realizada na dimensão Parcerias concluiu que não foram estabelecidas diretrizes nem arranjos claros para assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento no âmbito de programas, projetos e atividades compartilhadas. Desse modo, considerando o baixo grau de maturidade, há prejuízo da garantia proporcionada pela gestão de riscos às parcerias do FNDE.

Dessa forma, os resultados obtidos nos questionários das dimensões Ambiente e Processos demonstram que há uma percepção acerca do tema, com reconhecimento de iniciativas pontuais relacionadas com as etapas do processo de gestão de riscos. Porém, o baixo grau de maturidade dos processos de gestão de riscos evidencia que os responsáveis pela governança e a administração ainda não podem contar com uma garantia razoável, proporcionada pela gestão de riscos, do cumprimento dos objetivos da organização.

4.2.3. Eficácia da gestão de riscos

Os riscos da organização estão dentro dos seus critérios de risco?

Com vistas a avaliar este aspecto, foram realizados testes para um objeto relacionado à adequação dos riscos aos critérios e ao apetite a risco definidos, com vistas a entender se os riscos da organização estão dentro do apetite a risco definido e das variações aceitáveis no desempenho ou tolerâncias a risco estabelecidas.

Tendo em vista que não foi identificado um processo estruturado e integrado de gestão de riscos na organização (conforme condições evidenciadas na dimensão Processos, a partir das análises dos componentes 2.1, 2.2. e 2.3) e que não foram estabelecidos critérios de risco (conforme observado no aspecto 2.2.1), não havendo, portanto, apetite a risco, tolerâncias a risco ou variações aceitáveis no desempenho formalmente definidos (conforme tópico 1.2.2.1), não é possível obter garantia razoável de que os riscos da organização estão dentro de critérios adequados de risco.

Também é importante destacar que não há uma visão de portfólio de riscos (conforme relatado no tópico 1.1.3.3), de modo que não há alinhamento do gerenciamento de riscos com os objetivos estratégicos, levando em conta os riscos combinados em uma visão de carteira. Ou seja, não há uma visão clara da Alta Administração sobre os riscos selecionados e priorizados, de forma global e integrada.

Ademais, a avaliação realizada na dimensão Parcerias concluiu que o FNDE não estabeleceu diretrizes nem arranjos claros para assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento no âmbito de parcerias. Assim, verifica-se o baixo grau de maturidade dos processos de gestão de riscos em parcerias na organização, de modo que a maior parte dos elementos mínimos necessários ainda não foi instituída.

Por todo o exposto, conclui-se que não há evidência do adequado funcionamento dos princípios, estruturas e processos da gestão de riscos com vistas a contribuir com o alcance dos objetivos da organização. Assim, observa-se que há prejuízo para a eficácia da gestão de riscos, dado que os riscos da organização não estão sendo gerenciados dentro de critérios de risco previamente definidos, no âmbito de um processo estruturado e integrado.

RECOMENDAÇÕES

Diante das dimensões avaliadas ao longo do presente trabalho (e de seus respectivos componentes, aspectos e objetos), apresentam-se as seguintes recomendações:

Achados relacionados ao Componente 1.1. Liderança.

Recomendação 1: Mapear os níveis de competência necessários para ocupação dos postos de trabalho com vistas a fortalecer o desenvolvimento de pessoas em temas relevantes para o alcance dos objetivos da organização, utilizando-se, para tanto, do Projeto de Dimensionamento da Força de Trabalho já em andamento ou de outro mecanismo que permita construir o adequado alinhamento entre conhecimentos/habilidades necessários e os postos de trabalho das unidades.

Achados relacionados ao Componente 1.1. Liderança.

Recomendação 2: Estabelecer Política de Desenvolvimento da Alta Administração com vistas ao desenvolvimento gerencial dos ocupantes de cargo em comissão e funções comissionadas e à habilitação de servidores para ocupação desses postos, em conformidade com o que dispõe a Lei nº 14.204/2021 e a legislação correlata.

Achados relacionados aos Componentes 1.1. Liderança; 1.2. Políticas e Estratégias; 1.3. Pessoas.

Recomendação 3: Incluir no Plano de Desenvolvimento de Pessoas da Autarquia capacitações de servidores e colaboradores relacionadas às temáticas integridade, ética e gestão de riscos, com vistas ao fortalecimento da cultura de gestão baseada em riscos.

Achados relacionados ao Componente 1.1. Liderança.

Recomendação 4: Atualizar a página de Acesso à Informação do Portal do FNDE e adequá-la às diretrizes de transparência ativa preconizadas pelo Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011, considerando, ao menos, a divulgação das principais metas, indicadores e principais resultados no item “Ações e Programas”, e as informações sobre audiências públicas, conselhos, órgãos colegiados e conferências no item “Participação Social”.

Achados relacionados ao Componente 1.1. Liderança.

Recomendação 5: Divulgar a Carta de Serviços ao Usuário, informando os usuários sobre os serviços prestados pelo FNDE, as formas de acesso a esses serviços e seus compromissos e padrões de qualidade de atendimento ao público, em conformidade com a Lei nº 13.460/2017.

Achados relacionados ao Componente 1.1. Liderança.

Recomendação 6: Revisar e adequar o Plano de Integridade do FNDE, de modo a:

I - Contemplar o levantamento de riscos para a integridade;

II - Estabelecer expressamente as formas e as periodicidades de atualização e de monitoramento do Plano; e

III - Estabelecer um plano de divulgação, contemplando ações periódicas para reforço da integridade na organização.

Achados relacionados ao Componente 1.1. Liderança.

Recomendação 7: Fortalecer a gestão da ética, a partir da adoção, ao menos, das seguintes medidas:

I - Publicar plano de trabalho específico para a Comissão de Ética do FNDE;

II - Instituir modelo de monitoramento do cumprimento do Código de Ética; e

III - Estabelecer um plano de divulgação, contemplando ações periódicas para fomento às práticas éticas na organização.

Achados relacionados aos Componentes 1.1. Liderança; e 1.3. Pessoas.

Recomendação 8: Instituir formalmente o modelo de governança do FNDE, identificando expressamente as instâncias internas de apoio à governança e as instâncias de gestão, as linhas de atuação no âmbito da organização, bem como suas respectivas responsabilidades nos processos de gestão de riscos.

Achados relacionados ao Componente 1.1. Liderança.

Recomendação 9: Qualificar a atuação do Comitê de Gestão Estratégica e Governança (CGEG) e do Comitê de Gestão de Riscos, Controles Internos e Integridade (CGRCI), enquanto instâncias de apoio à segunda linha, estabelecendo plano para sua efetiva atuação, definindo

medidas e prazos para o cumprimento e monitoramento das competências estabelecidas no §2º do art. 23 da IN MP/CGU nº 01/2016.

Achados relacionados aos Componentes 1.1. Liderança; 1.2. Políticas e Estratégias; 1.3. Pessoas; 2.1. Identificação e Análise de Riscos; 2.2. Avaliação e Resposta a Riscos; 2.3. Monitoramento e Comunicação; 3.1. Gestão de Riscos em Parcerias; e 3.2. Planos e Medidas de Contingência.

Recomendação 10: Estabelecer Política de Gestão de Riscos para o FNDE, em cumprimento ao art. 17 da IN MP/CGU nº 01/2016, especificando, 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) como serão integradas as entidades parceiras à gestão de riscos da organização, considerando políticas e programas compartilhados;

f) a utilização de metodologia e ferramentas para o apoio à gestão de riscos;

g) 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.

Achados relacionados aos Componentes 2.1. Identificação e Análise de Riscos; 2.2. Avaliação e Resposta a Riscos; 2.3. Monitoramento e Comunicação; 3.1. Gestão de Riscos em Parcerias; e 3.2. Planos e Medidas de Contingência.

Recomendação 11: Implementar processo de gestão de riscos compatível com a missão e os objetivos estratégicos do FNDE, em cumprimento aos arts. 13 e 16 da IN MP/CGU nº 01/2016, a partir das boas práticas referenciadas sobre o tema e definindo, ao menos, os seguintes componentes da estrutura de gestão de riscos:

I - Ambiente interno;

II- Fixação de objetivos;

III - Identificação de eventos;

IV - Avaliação de riscos;

V - Resposta a riscos;

VI - Atividades de controles internos;

VII - Informação e comunicação; e

VIII - Monitoramento.

Achados relacionados aos Componentes 1.1. Liderança; e 1.2. Políticas e Estratégias.

Recomendação 12: Adotar medidas quanto à integração da gestão de riscos ao planejamento estratégico e às operações da organização, estabelecendo, ao menos:

I - O desdobramento dos objetivos estratégicos em objetivos de negócio (nas categorias operacional, de comunicação e de conformidade);

II - Indicadores-chave de risco associados aos objetivos priorizados;

III - Os níveis de apetite a riscos e as respectivas tolerâncias a risco, ao menos para os objetivos estratégicos;

IV - Planos de ação e/ou outros mecanismos e estratégias para garantir atingimento dos objetivos estratégicos; e

V - Fluxos e canais formais e padronizados para comunicação de informações sobre riscos.

CONCLUSÃO

O presente Relatório de Auditoria apresenta os resultados da avaliação de maturidade da gestão de riscos do Fundo Nacional de Desenvolvimento da Educação (FNDE). A partir de quatro dimensões (Ambiente, Processos, Parcerias e Resultados), avaliou-se em que medida a organização conta com a existência de princípios, estruturas e processos em funcionamento e operando de forma integrada com vistas à adequada gestão de riscos.

A partir do referencial adotado, dos critérios selecionados e das boas práticas sobre o tema, foram calculados os níveis de maturidade, sendo o resultado global de 11,42% e os índices de maturidade das dimensões, a saber: 17,83% para Ambiente; 6,67% para Processos; 0,00% para Parcerias; e 11,43% para Resultados. Nesse contexto, foram identificadas fragilidades que impactam o adequado funcionamento da gestão de riscos e garantia razoável de atingimento dos objetivos da organização.

No tocante à dimensão Ambiente, foram avaliadas as capacidades existentes no FNDE, em termos de *liderança, políticas, estratégias e preparo das pessoas*. Os resultados obtidos demonstram que o FNDE ainda não assume um compromisso suficientemente forte e sustentado com a cultura e o desenvolvimento de estruturas para a gestão baseada em riscos. Dentre as causas identificadas, destaca-se a ausência de uma Política de Gestão de Riscos, o que fragiliza aspectos relacionados a liderança, políticas e estratégias e pessoas. Consequentemente, não existe uma consciência sobre riscos na organização, tampouco há asseguração acerca do funcionamento e da integração da gestão de riscos e não se garante o correto entendimento de papéis e responsabilidades para a gestão de riscos.

Em relação à dimensão Processos, foram avaliados os processos de gestão de riscos adotados pela Autarquia. Os resultados obtidos demonstraram que, dado que o FNDE não dispõe de um modelo de processo formal para a gestão de riscos, não foram estabelecidos padrões e critérios prejudicando a identificação, a análise e a avaliação de riscos; a seleção e a implementação de respostas aos riscos avaliados; o monitoramento de riscos e controles; e a comunicação sobre riscos com partes interessadas, internas e externas. Como consequência, os responsáveis pela governança, a Alta Administração e as pessoas que atuam em todos os níveis não têm uma compreensão adequada dos objetivos sob a sua gestão e de seus papéis e responsabilidades, tampouco sabem em que medida os resultados de cada área ou pessoa são significativos para atingir os objetivos-chave da organização.

Para a dimensão Parcerias, avaliaram-se os arranjos colocados em prática para a gestão de riscos no âmbito de políticas, programas e projetos compartilhados, concluindo-se que não foram estabelecidos arranjos adequados para a gestão de riscos. Tal situação decorre também da ausência de um modelo de processos formal para o tema, tendo como consequência o desconhecimento dos riscos envolvidos na execução de políticas e projetos compartilhados, com possíveis impactos no atingimento de objetivos e com a limitação do tratamento de falhas e conflitos.

Por fim, na dimensão Resultados, a partir da avaliação das contribuições da arquitetura de gestão de riscos disponível no FNDE para a melhoria dos processos de governança e gestão, bem como da avaliação dos resultados-chave da gestão de riscos, evidenciou-se que a organização ainda não pode se beneficiar da melhoria dos processos de governança e gestão e dos resultados proporcionados pela adequada gestão de riscos. A causa para isso decorre principalmente dos achados relacionados às dimensões anteriores.

Diante desse cenário, as recomendações tiveram como foco: os elementos mínimos necessários para o desenvolvimento de um ambiente que fomente a importância da gestão de riscos; as obrigações legais relacionadas ao tema, especialmente aquelas decorrentes da IN MP/CGU nº 01/2016; e algumas boas práticas aplicáveis para o presente nível de maturidade da organização. Como resultados advindos da implementação dessas recomendações, espera-se auxiliar na estruturação de mecanismos e práticas de gestão baseada em risco no FNDE.

Espera-se, ainda, que as medidas recomendadas auxiliem a Alta Administração no processo de implementação de mecanismos e práticas de gestão baseada em riscos no FNDE, agregando, portanto, valor aos processos de governança organizacional. Ainda, vislumbra-se que um maior grau de maturidade da gestão de riscos, compatível com o porte e com os objetivos-chave da Autarquia, permitirá que a organização se beneficie dos resultados proporcionados pela adequada gestão de riscos.

ANEXO I – Manifestação das Unidades Auditadas e Análise da Equipe de Auditoria

a) Manifestação da Unidade Auditada

A Presidência do FNDE se manifestou por intermédio da Nota Técnica nº 3184186/2022/AGEST/GABIN, SEI nº 3184186:

> *4. ANÁLISE*
>
> *4.1. Diante da elaboração do Relatório Preliminar de Auditoria, bem como das inferências resultantes da Reunião de Busca Conjunta de Soluções, em 18/10/2022, relativamente ao tema avaliação da maturidade da gestão baseada em risco no FNDE, registra-se as manifestações oriundas das constatações e das recomendações dos itens abaixo discriminados, quais sejam:*
>
> > *4.1.1) RECOMENDAÇÃO (liderança) - Mapear os níveis de competência necessários para ocupação dos postos de trabalho com vistas a fortalecer o desenvolvimento de pessoas em temas relevantes para o alcance dos objetivos da organização; utilizando-se, para tanto, do Projeto de Dimensionamento da Força de Trabalho já em andamento ou de outro mecanismo que permita construir o adequado alinhamento entre conhecimentos/habilidades necessários e os postos de trabalho das unidades;*
> >
> > *4.1.1) RECOMENDAÇÃO (liderança) - Mapear os níveis de competência necessários para ocupação dos postos de trabalho com vistas a fortalecer o desenvolvimento de pessoas em temas relevantes para o alcance dos objetivos da organização; uti lizando-se, para tanto, do Projeto de Dimensionamento da Força de Trabalho já em andamento ou de outro mecanismo que permita construir o adequado alinhamento entre conhecimentos/habilidades necessários e os postos de trabalho das unidades;*
> >
> > *4.1.2) RECOMENDAÇÃO (liderança) - Estabelecer Política de Desenvolvimento da Alta Administração com vistas ao desenvolvimento gerencial dos ocupantes de cargo em comissão e funções comissionadas e à habilitação de servidores para ocupação desses postos, em conformidade com o que dispõe a Lei nº 14.204/2021 e a legislação correlata;*
> >
> > *4.1.3) RECOMENDAÇÃO (liderança, políticas e estratégias e pessoas) - Incluir no Plano de Desenvolvimento de Pessoas da Autarquia capacitações de servidores e colaboradores relacionadas às temáticas integridade, ética e gestão de riscos, com vistas ao fortalecimento da cultura de gestão baseada em riscos;*
> >
> > *4.1.4) RECOMENDAÇÃO (liderança) - Atualizar a página de Acesso à Informação do Portal do FNDE e adequá-la às diretrizes de transparência ativa preconizadas pelo Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527/2011; considerando, ao menos, a divulgação das principais metas, indicadores e principais resultados no item "Ações e Programas", e as*

informações sobre audiências públicas, conselhos, órgãos colegiados e conferências no item "Participação Social";

4.1.5) RECOMENDAÇÃO (liderança) - Divulgar a Carta de Serviços ao Usuário, informando os usuários sobre os serviços prestados pelo FNDE, as formas de acesso a esses serviços e seus compromissos e padrões de qualidade de atendimento ao público, em conformidade com a Lei nº 13.460/2017;

4.1.6) RECOMENDAÇÃO (liderança) - Revisar e adequar o Plano de Integridade do FNDE, de modo a:

I - Contemplar o levantamento de riscos para a integridade;

II - Estabelecer expressamente as formas e as periodicidades de atualização e de monitoramento do Plano; e

III - Estabelecer um plano de divulgação, contemplando ações periódicas para reforço da integridade na organização;

4.1.7) RECOMENDAÇÃO (liderança) - Fortalecer a gestão da ética, a partir da adoção, ao menos, das seguintes medidas:

I - Publicar plano de trabalho específico para a Comissão de Ética do FNDE;

II - Instituir modelo de monitoramento do cumprimento do Código de Ética; e

III - Estabelecer um plano de divulgação, contemplando ações periódicas para fomento às práticas éticas na organização;

4.1.8) RECOMENDAÇÃO (liderança e pessoas) - Instituir formalmente o modelo de governança do FNDE, identificando expressamente as instâncias internas de apoio à governança e as instâncias de gestão, as linhas de atuação no âmbito da organização, bem como suas respectivas responsabilidades nos processos de gestão de riscos;

4.1.9) RECOMENDAÇÃO (liderança) - Qualificar a atuação do Comitê de Gestão Estratégica e Governança (CGEG) e do Comitê de Gestão de Riscos, Controles Internos e Integridade (CGRCI), enquanto instâncias de apoio à segunda linha, estabelecendo plano para sua efetiva atuação, definindo medidas e prazos para o cumprimento e monitoramento das competências estabelecidas no §2º do art. 23 da IN MP/CGU nº 01/2016;

4.1.10) RECOMENDAÇÃO (liderança, políticas e estratégias, pessoas, identificação e análise de riscos, avaliação e resposta a riscos, monitoramento e comunicação, gestão de riscos em parcerias e planos e medidas de contingência) – Estabelecer Política de Gestão de Riscos para o FNDE, em cumprimento ao art. 17 da IN MP/CGU nº 01/2016; especificando, 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) como serão integradas as entidades parceiras à gestão de riscos da organização, considerando políticas e programas compartilhados;

f) a utilização de metodologia e ferramentas para o apoio à gestão de riscos;

g) 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;

4.1.11) RECOMENDAÇÃO (identificação e análise de riscos, avaliação e resposta a riscos, monitoramento e comunicação, gestão de riscos em parcerias e planos e medidas de contingência) - Implementar processo de gestão de riscos compatível com a missão e os objetivos estratégicos do FNDE, em cumprimento aos arts. 13 e 16 da IN MP/CGU nº 01/2016, a partir das boas práticas referenciadas sobre o tema e definindo, ao menos, os seguintes componentes da estrutura de gestão de riscos:

I - Ambiente interno;

II - Fixação de objetivos;

III - Identificação de eventos;

IV - Avaliação de riscos;

V - Resposta a riscos;

VI - Atividades de controles internos;

VII - Informação e comunicação; e

VIII - Monitoramento;

4.1.12) RECOMENDAÇÃO (liderança e políticas e estratégias) - Adotar medidas quanto à integração da gestão de riscos ao planejamento estratégico e às operações da organização; estabelecendo, ao menos:

I - O desdobramento dos objetivos estratégicos em objetivos de negócio (nas categorias operacional, de comunicação e de conformidade);

II - Indicadores-chave de risco associados aos objetivos priorizados;

III - Os níveis de apetite a riscos e as respectivas tolerâncias a risco, ao menos para os objetivos estratégicos;

IV - Planos de ação e/ou outros mecanismos e estratégias para garantir atingimento dos objetivos estratégicos; e

V - Fluxos e canais formais e padronizados para comunicação de informações sobre riscos.

4.2. Mister destacar que, com supedâneo na Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016, a qual "estabeleceu a obrigatoriedade de os órgãos e entidades do Poder Executivo federal implementarem, manterem, monitorarem e revisarem o processo de gestão de riscos, de forma compatível com sua missão e seus objetivos estratégicos"; a entidade auditada já promove iniciativas estratégicas a respeito, conquanto as dificuldades enfrentadas na implementação de mecanismos e de práticas na gestão baseada em riscos, que vêm perpassando sucessivas

administrações; mormente, no que tange ao reduzido quadro de servidores, prejudicando o alcance das finalidades públicas com melhor relação custo-benefício.

4.3. Nesse diapasão, deve-se salientar, todavia, a incipiência da maturidade global do FNDE - de 11,42% - em gestão de riscos; a qual, embora inadequada, conta com instrumentos importantes para o seu avanço como: as instâncias em gestão de riscos, além do Plano de Integridade a ser lapidado e publicado no Portal da Autarquia, que passará a divulgar a Carta de Serviços do Usuário e a versão atualizada da página de Acesso à Informação ulteriormente, de acordo com o ora sugerido, a fim de certificar a transparência dos indicadores e das metas no site institucional.

4.4. Ademais, em pese à baixa realização de cursos relativos às temáticas: integridade, ética e gestão de riscos; observou-se, outrossim, a comparência e o funcionamento de ações relacionadas ao Plano de Desenvolvimento de Pessoas, a partir da estruturação de uma política de capacitação no âmbito do FNDE.

4.5. Dessarte, o estabelecimento da Política de Desenvolvimento da Alta Administração e do Projeto de Dimensionamento da Força de Trabalho alinhados ao processo de gestão de riscos, em consonância com a integração proposta pela Auditoria Interna ao planejamento estratégico e às operações da organização, auxiliarão na construção de um modelo que atravessa as unidades do FNDE em nível operacional, qualificando as atividades dos Comitês (CGEG e CGRCI), logo contribuindo para o futuro desdobramento positivo dessas diligências.

4.6. Sobremaneira relevante seria o aproveitamento das disposições pré-existentes acerca do assunto em relevo, visto que o aprimoramento dessas resoluções suscitaria a continuidade das determinações e evitaria a criação ineficaz de ferramentas inócuas no transcorrer do desenvolvimento da ideia de gestão de riscos na Casa. Nesse sentido, as ações do âmbito do Plano de Gestão Estratégica e Transformação Institucional (PGT) do FNDE e a elaboração de nova estrutura do FNDE, efetivada pelo Decreto nº 11.196, de 13 de setembro de 2022, são medidas basilares para a criação de condições sem as quais tornar-se-ia inverossímil propor a efetivação de uma política de gestão de riscos. Trata-se de medidas que convergiam para esse fim, realizadas em paralelo ao trabalho da Audit e que evidenciam consciência institucional, de forma por vezes não captada no Relatório, apesar de noticiadas múltiplas vezes ao longo do trabalho.

4.7. De todo modo, a consideração do parágrafo anterior traz impacto quanto às recomendações, razão pela qual entende-se que se justificam maiores esforços de pontuar excertos do relatório que trazem.

4.8. Por fim, como elemento a ser considerado nos próximos passos e no equilíbrio entre possibilidades e expectativas, cabe registrar que a Gestão de Riscos é tema incipiente na Administração Pública Federal, bem como que essa dimensão da gestão deve dialogar eminentemente com a finalidade institucional. Nesse sentido, enquanto há boas práticas consolidadas em campos como o mercado financeiro ou na gestão de emergências, a constituição de uma política de gestão de riscos no campo das políticas educacionais é tema sobremodo desafiador e que exige constituição de boas práticas. Nesse sentido, cumpre destacar a Nota Técnica nº 2971952/2022/DILEP/COLEP/CGPEO/DIRAD, em especial os itens 7 e 8, que evidencia institucionalmente que "fatores como gestão de riscos, integridade e efetividade se impõem à pauta"; e que pela relevância do FNDE, é necessário que a Autarquia conte com condições exemplares, em que se inclui a capacidade de efetivar a adequada gestão de riscos.

4.9. Cumpre registrar que expressiva gama dos pontos recomendados estão presentes também nos trabalhos para reelaboração do Plano Estratégico do FNDE para o próximo ciclo, expressando que a instituição reconhece suas necessidades de melhoria e está empreendendo esforços no sentido de fortalecimento da gestão de riscos, no entendimento de que esta é relevante mecanismo para o melhor alcance dos objetivos institucionais.

A organização auditada assim conclui:

5. CONCLUSÃO

5.1. Por conseguinte, vale enfatizar que o FNDE atua com o compromisso de resguardar o valor público ao qual se dedica e o cumprimento de sua missão, voltado a atuar de maneira eficiente e eficaz na gestão dos recursos públicos, atentando às disposições normativas, no sentido de aprimorar os mecanismos de gestão de riscos do Órgão, com o fito de potencializar os resultados almejados e fortalecer a gestão pública.

5.2. Em face ao exposto, esta Coordenação-Geral não tem reparos a propor quanto as recomendações dispostas no Relatório Preliminar de Auditoria – N° 01/2022, ficando no aguardo do recebimento da versão definitiva para contribuir com a implementação de medidas de aprimoramento.

b) Análise da Equipe de Auditoria

Em sua manifestação, a organização destacou o cenário de dificuldades enfrentadas na implementação de mecanismos e práticas de gestão de riscos, destacando o quadro reduzido de servidores. Nesse sentido, esta unidade de Auditoria Interna compreende as limitações apontadas e, por intermédio deste Relatório, buscou apresentar iniciativas que podem auxiliar no contexto de um tema tão complexo.

Assim, entende-se que há ações preliminares que podem ser iniciadas mesmo com limitações de recursos humanos (e que inclusive podem auxiliar a lidar com esse problema), especialmente no âmbito do estabelecimento de um ambiente adequado para a gestão de riscos.

A manifestação da unidade apontou ainda para a incipiência da maturidade global (de 11,42%). Desse modo, destacamos que a compreensão do nível de maturidade é apenas um primeiro passo, cuja importância é destacada na literatura de referência sobre o tema: conhecer o nível de maturidade da organização auxilia a projetar metas realistas para manter o nível ou alcançar níveis mais elevados. Portanto, mais do que uma pontuação a ser considerada, o foco a partir do nível de maturidade deve ser a priorização e a estruturação de ações que auxiliem o FNDE a chegar no nível que a organização pretende atingir.

A unidade elencou também instrumentos importantes que já foram desenvolvidos ou estão em desenvolvimento, como: o Plano de Integridade, as ações relacionadas ao Plano de Desenvolvimento de Pessoas e ao Projeto de Dimensionamento da Força de Trabalho. Entende-se, assim, que a Alta Administração tem consciência da ligação entre essas ações e a gestão de riscos, o que tende a auxiliar nas melhorias apontadas para esses objetos ao longo deste Relatório.

Ademais, a unidade auditada apresentou ações que estavam sendo realizadas em paralelo ao trabalho de avaliação ora apresentado, a saber: as ações definidas no âmbito do Plano de Gestão

Estratégica e Transformação Institucional (PGT) do FNDE e a elaboração da nova estrutura da Autarquia.

Dentre as ações do PGT, a equipe de auditoria cuidou de ressaltar sua importância, notadamente a partir do reconhecimento do papel da nova Cadeia de Valor[34], validada em julho de 2022, que poderá servir de base, por exemplo, para a elaboração de indicadores de desempenho, para a definição de competências e para o estabelecimento de controles internos.

Em relação à nova estrutura do FNDE, efetivada pelo Decreto nº 11.196, de 13 de setembro de 2022, – posterior, portanto, aos exames de auditoria executados e cujo conteúdo não foi diretamente abordado no escopo deste trabalho –, esta Audit reconhece também a sua relevância para o contexto de implementação da gestão baseada em riscos.

Ao final de sua manifestação, a organização destacou o trabalho de reelaboração do Plano Estratégico do FNDE para o ciclo 2023-2026 e o reconhecimento de necessidades de melhoria no que tange à estratégia da organização. Assim como a Cadeia de Valor, as ações desenvolvidas no âmbito do TransformaGov e a recente reestruturação regimental e do quadro demonstrativo de cargos em comissão e funções de confiança do FNDE, esta Audit entende a relevância da atualização do Plano Estratégico da Autarquia, o qual poderá servir como norte para a implementação da gestão baseada em riscos.

Destaca-se, por fim, que, no âmbito de uma organização do porte do FNDE, é compreensível que a implementação de uma arquitetura de gestão de riscos seja um grande desafio. Observa-se, porém, o esforço empreendido pela Autarquia em desenvolver ações importantes para o amadurecimento institucional. No entanto, mecanismos essenciais para o funcionamento de uma gestão baseada em riscos precisam ser implementados, para se obter maior grau de maturidade no tema. Nesse sentido, o presente relatório busca auxiliar detalhando os componentes essenciais, bem como os respectivos objetos a serem desenvolvidos, com base nos critérios de referência e nas boas práticas encontradas.

[34] Conforme exposto nos tópicos 1.2.1, 4.1.2 e 4.1.3.

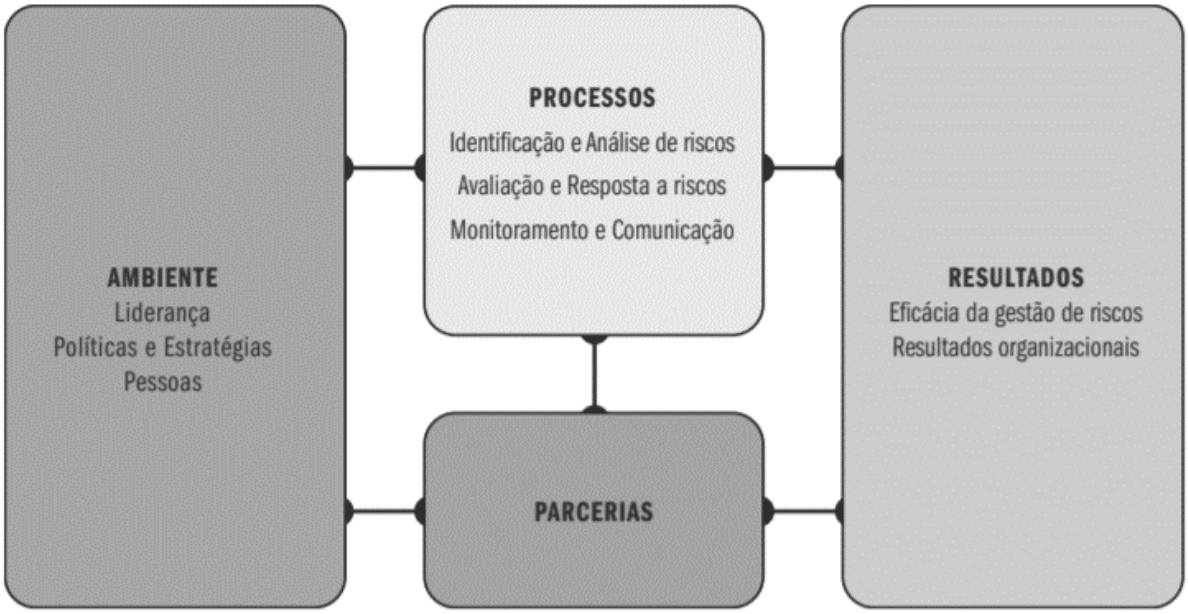
ANEXO II – Metodologia

Considerando a complexidade das operações desenvolvidas, bem como o grande volume de processos e atividades em curso no âmbito do FNDE, optou-se pela utilização de um modelo referencial para embasar a avaliação do grau de maturidade. Para tanto, foi utilizado como referência o material "Gestão de Riscos – Avaliação da Maturidade", elaborado pelo Tribunal de Contas da União – TCU.

Vislumbrou-se também que a utilização de um modelo padrão permitiria a comparabilidade da evolução do grau de maturidade da Autarquia ao longo do tempo. Assim, o procedimento utilizado poderá ser reaplicado futuramente, possibilitando o monitoramento da evolução da gestão de riscos na organização a partir das recomendações e proposições da Auditoria Interna decorrentes do presente trabalho.

A partir do modelo de avaliação desenvolvido pelo TCU e apresentado no guia "Gestão de Riscos – Avaliação da Maturidade" (TCU, 2018a), a maturidade em gestão de riscos do FNDE foi avaliada em relação a quatro dimensões: Ambiente, Processos, Parcerias e Resultados.

Figura 3: Modelo de avaliação da maturidade em gestão de riscos



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

Com base nas dimensões definidas (Ambiente, Processos, Resultados e Parcerias), foram elaboradas as questões de auditoria traduzidas no que se passou a denominar ***componentes*** de avaliação. As questões foram divididas em subquestões de auditoria, as quais foram traduzidas nos ***aspectos*** de análise. Por fim, no âmbito de cada aspecto, foram escolhidos os ***objetos*** de análise, que nortearam os procedimentos de auditoria a serem executados para fins de testagem e obtenção de evidências, com vistas a compor as pontuações de avaliação de maturidade.

Assim, partiu-se dos objetos de análise e dos critérios de auditoria definidos para cada objeto, para, com base nas evidências obtidas, ser feita a comparação entre o critério definido e a situação encontrada, de modo a se chegar nos achados de auditoria e, consequentemente, na

pontuação de cada objeto. Posteriormente, foi feito o cálculo do índice de maturidade de cada dimensão e do índice de maturidade global da gestão de riscos da organização avaliada.

Nesse contexto, a determinação do nível de maturidade do FNDE envolveu quatro etapas:

1) Testagem dos ***objetos*** de análise escolhidos e atribuição de pontuação – variando de 0 a 4 pontos, conforme escala apresentada no quadro 2, a seguir – para todos os ***aspectos*** formulados pela equipe de auditoria (subquestões de auditoria). Para as subquestões que se desdobraram em mais de um objeto de análise, a pontuação do aspecto foi calculada a partir da média das pontuações obtidas em cada objeto que compõe o aspecto, baseando-se da análise global;
2) Cálculo da ***maturidade de cada componente*** (questões de auditoria), a partir do somatório de pontos do conjunto de subquestões (aspectos testados) que a compõe e calculando-se a razão entre a pontuação alcançada e a pontuação máxima possível e expressando-se esse quociente com um número entre 0 e 100%;
3) Consolidação das maturidades dos componentes, para compor o índice de maturidade de cada uma das quatro dimensões (***índice de maturidade das dimensões – IMD***), a partir do somatório de pontos do conjunto de questões que a compõe e calculando-se a razão entre a pontuação alcançada e a pontuação máxima possível e expressando-se esse quociente com um número entre 0 e 100%; e
4) Cálculo do ***índice de maturidade global*** (IMG) da gestão de riscos do FNDE, a partir da média ponderada dos índices de maturidade das dimensões, de acordo com os pesos sugeridos pelo guia do TCU: 40 para Ambiente; 30 para Processos; 10 para Parcerias; e 20 para Resultados.

A avaliação realizada considerou a seguinte escala para avaliação de evidências:

Quadro 1: Escala para avaliação de evidências

PONTUAÇÃO	0 - INEXISTENTE	1- INICIAL	2 - BÁSICO	3 - APRIMORADO	4 - AVANÇADO
Dimensão 1	Prática inexistente, não implementada ou não funcional.	Prática realizada de maneira informal e esporádica em algumas áreas relevantes para os objetivos-chaves da organização.	Prática realizada de acordo com normas e padrões definidos em algumas áreas relevantes para os objetivos-chaves da organização.	Prática realizada de acordo com normas e padrões definidos na maior parte das áreas relevantes para os objetivos-chaves da organização.	Prática realizada de acordo com normas e padrões definidos em todas as áreas relevantes para os objetivos-chaves da organização.
Dimensão 2					
Dimensão 3					
Dimensão 4	Não há evidências de que o resultado descrito tenha sido obtido.	Existe a percepção entre os gestores e o pessoal de que o resultado descrito tenha sido obtido em alguma medida.	Existem indicadores definidos que mostram que o resultado descrito vem sendo obtido em grau baixo.	Existem indicadores consistentes, monitorados periodicamente, que mostram que o resultado descrito vem sendo obtido em grau moderado.	Existem indicadores consistentes, monitorados periodicamente, que mostram que o resultado descrito vem sendo obtido em grau elevado.

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

Complementarmente, efetuou-se o detalhamento da escala apresentada no guia do TCU, de forma que cada objeto, dentro de cada Aspecto, no âmbito de cada Dimensão, foi analisado conforme as escalas descritas abaixo:

Quadro 2: Perguntas e escalas de pontuação direcionadoras para a análise

Perguntas direcionadoras			Escalas direcionadoras				
			0 - Inexistente	**1 - Inicial**	**2 - Básico**	**3 - Aprimorado**	**4 - Avançado**
Conformidade	Existência do princípio, estrutura ou processo no âmbito do FNDE?	Dimensões 1, 2 e 3	não identificada ou inexpressiva	sim, informal ou esporádica	sim, formal ou padronizada, com atendimento dos principais critérios	sim, formal ou padronizada, com atendimento dos principais critérios e disseminada pela organização	sim, formal ou padronizada, com atendimento dos principais critérios, disseminada e monitorada pela organização
		Dimensão 4	não evidenciada	percebida em alguma medida	mensurada	mensurada	mensurada
Conformidade	Funcionamento do princípio, estrutura ou processo nas unidades relevantes[35] do FNDE	Dimensões 1, 2 e 3	em nenhuma unidade relevante	em algumas unidades relevantes	em algumas unidades relevantes	na maior parte das unidades relevantes	em todas as unidades relevantes
		Dimensão 4	não evidenciado	percebido em alguma medida	em grau baixo	em grau moderado	em grau elevado
Percepção	Percepção dos atores consultados sobre o princípio, estrutura ou processo?		alta discordância	discordância	concordância parcial	concordância	alta concordância

Fonte: elaboração própria.

Tendo em vista que os testes executados envolveram tanto a avaliação documental, com foco na conformidade, quanto a coleta de percepção por intermédio de questionários, essas duas análises precisaram ser agregadas para a composição da pontuação de cada objeto analisado. Por isso, foram estabelecidos pesos para ponderar: a *existência* do objeto avaliado (peso 5); seu *funcionamento* na organização (peso 3); e a *percepção* das pessoas que atuam no FNDE (peso 2).

[35] Entende-se como unidade relevante aquela que tem responsabilidade sobre a estrutura ou processo analisado. Por exemplo, aspectos relacionados à gestão de pessoas tendem a ter como unidade relevante a Diretoria de Administração, dadas as suas competências regimentais.

Já para cálculo do índice de maturidade, a partir dos índices apurados (em cada dimensão – IMD e na organização de forma global – IMG), foi utilizada a escala abaixo:

Quadro 3: Níveis de maturidade da gestão de riscos (via TCU, 2018a)

ÍNDICE DE MATURIDADE APURADO	NÍVEL DE MATURIDADE
De 0% a 20%	Inicial
De 20,1% a 40%	Básico
De 40,1% a 60%	Intermediário
De 60,1% a 40%	Aprimorado
De 80,1% a 100%	Avançado

Fonte: Gestão de Riscos – Avaliação da Maturidade" (TCU, 2018a).

Questionários de auditoria

Com vistas a coletar a percepção acerca das dimensões avaliadas foi utilizada a técnica de indagação escrita, por intermédio de questionários de auditoria, encaminhados a todos os indivíduos dos seguintes grupos: Alta Administração, servidores do FNDE, servidores que atuam na Auditoria Interna e servidores que compõem a Comissão de Ética. Os dados foram coletados no período entre janeiro e março de 2022, utilizando-se o *Microsoft Forms.*

Como resultados, foram obtidos os seguintes totais de respostas:

Quadro 4: Quantidade de respostas obtidas nos questionários aplicados

QUESTIONÁRIO	TOTAL DE RESPOSTAS
Alta Administração	7
Servidores do FNDE	145
Servidores que atuam no serviço de Auditoria Interna	6
Servidores da Comissão de Ética	4

Fonte: Elaboração própria, a partir da consolidação dos dados obtidos via *Microsoft Forms.*

Foram utilizadas majoritariamente questões fechadas e, em alguns casos, complementou-se a indagação com questões abertas, de modo a obter informações de caráter qualitativo que subsidiaram a resposta às questões de auditoria inseridas na Matriz de Planejamento elaborada.

Para as questões fechadas foram solicitadas, preponderantemente, respostas textuais, dicotômicas [sim/não] e de múltiplas alternativas, utilizando-se, neste caso, a escala Likert de avaliação com variáveis de concordância [discordo totalmente, discordo, concordo totalmente, não sei opinar].

No caso das respostas enquadradas na escala Likert, tomou-se como premissa a uniformidade entre a distância das categorias, de modo a transformar os dados em razão. Assim, os percentuais de resposta obtidos foram categorizados em faixas percentuais, enquadrando-se os dados na escala apresentada no Quadro 2 (referenciado anteriormente neste anexo) e possibilitando a avaliação da diferença entre as variáveis.

Para as respostas obtidas a partir dos questionários enviados aos servidores do FNDE, analisou-se a representatividade e a adequabilidade do tamanho da amostra.

Quanto ao tamanho da amostra, considerando que se trata de uma população finita (a amostra obtida representa mais de 5% do total de servidores em exercício no FNDE) e considerando a quantidade de respostas obtidas, calculou-se o erro máximo de estimativa. Para fins deste trabalho, foi estabelecido que o erro amostral não deveria ultrapassar o limite de 10%, sabendo-se que o ideal seria o limite de até 5%, para um nível de segurança de 95%. A partir dos dados coletados, obteve-se um erro amostral de 6,2%, considerado aceitável para o contexto.

Em relação à representatividade da amostra tratada, considerando o perfil da população (unidades diretivas no âmbito do FNDE), aplicou-se o teste Qui-quadrado, para identificação da significância e da homogeneidade das distribuições de classes. Como resultado, observou-se diferença residual significativa para duas das noves classes existentes. Assim, visando a adequação da representatividade da amostra, foram retirados de forma aleatória seis registros da classe 2 e nove da classe 3. Como resultado, não se observou diferença significativa entre o coletado e o esperado.

No caso do questionário aplicado à Alta Administração e à Auditoria Interna, considerando a obtenção de resposta de todos os indivíduos da população analisada, não houve necessidade de tratamento.

Por fim, quanto ao questionário aplicado aos servidores que atuam na Comissão de Ética, considerando o tamanho reduzido da população e a quantidade de respostas obtidas, chegou-se um erro amostral de 30% (considerando um grau de confiança de 95%). Desse modo, as respostas obtidas neste questionário não foram utilizadas para fim de composição das pontuações relacionadas às percepções do objeto relacionado, não fazendo parte, portanto, dos índices de maturidade calculados.

ANEXO III – Objetos de análise

Conforme descrito não tópico “Da metodologia utilizada”, as dimensões Ambiente, Processos, Resultados e Parcerias foram traduzidas em componentes a serem avaliados (questões de auditoria), divididos em aspectos de análise (subquestões de auditoria). Ainda, no âmbito de cada aspecto, foram escolhidos objetos de análise que nortearam os procedimentos de auditoria aplicados e ajudaram a compor as pontuações da avaliação de maturidade.

O quadro a seguir apresenta as questões e subquestões utilizadas no presente trabalho, bem como os objetos avaliados em cada dimensão e seus respectivos graus de maturidade obtidos após a avaliação, conforme legenda:

Índice de maturidade - Legenda				
0	**1**	**2**	**3**	**4**
INEXISTENTE	INICIAL	BÁSICO	APRIMORADO	AVANÇADO

DIMENSÃO AMBIENTE			
COMPONENTE	**ASPECTO**	**OBJETO DE ANÁLISE**	**RESULTADO**
1.1. LIDERANÇA: Em que medida os responsáveis pela governança e a Alta Administração do FNDE exercem suas responsabilidades de governança de riscos e cultura?	**1.1.1. CULTURA:** A Alta Administração e os responsáveis pela governança reconhecem a importância da cultura, da integridade, dos valores éticos e da consciência de riscos como aspectos-chave para o reforço da *accountability*?	1.1.1.1. DESENVOLVIMENTO DE PESSOAS	2,70
		1.1.1.2. COMPROMETIMENTO DAS LIDERANÇAS	1,20
		1.1.1.3. INTEGRIDADE E VALORES ÉTICOS	1,50
	1.1.2. GOVERNANÇA DE RISCOS: Existem estruturas e processos definidos para apoiar as responsabilidades de governança de riscos e assegurar que a gestão de riscos seja integrada aos processos de gestão?	1.1.2.1. INSTÂNCIAS E ESTRUTURAS PARA GESTÃO DE RISCOS	1,20
	1.1.3. SUPERVISÃO DA GOVERNANÇA E DA ALTA ADMINISTRAÇÃO: Os responsáveis pela governança e a Alta Administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos?	1.1.3.1. INDICADORES-CHAVE DE RISCOS E DE DESEMPENHO	2,00
		1.1.3.2. NOTIFICAÇÃO SOBRE EXPOSIÇÃO A RISCOS	0,90

		1.1.3.3. VISÃO DE PORTFÓLIO DE RISCOS	0,40
		1.1.3.4. INSTÂNCIAS DE ASSEGURAÇÃO	3,20
		1.1.3.5. NÍVEL DE MATURIDADE ALMEJADO PARA GESTÃO DE RISCOS	0,63
1.2. POLÍTICAS E ESTRATÉGIAS: Em que medida o FNDE dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática?	**1.2.1. DIRECIONAMENTO ESTRATÉGICO:** A Alta Administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico?	1.2.1.1. OBJETIVOS ESTRATÉGICOS, MISSÃO, VISÃO E VALORES FUNDAMENTAIS	2,70
	1.2.2. APETITE A RISCO: A Alta Administração, com a supervisão e a concordância dos responsáveis pela governança, define, comunica, monitora e revisa o apetite a risco?	1.2.2.1. DEFINIÇÃO, COMUNICAÇÃO E MONITORAMENTO DO APETITE A RISCO	0,00
	1.2.3. INTEGRAÇÃO DA GESTÃO DE RISCOS AO PROCESSO DE PLANEJAMENTO: A gestão de riscos é integrada ao processo de planejamento estratégico implementado no FNDE e aos seus desdobramentos?	1.2.3.1. DEFINIÇÃO DE OBJETIVOS ESTRATÉGICOS	2,40
		1.2.3.2. DEFINIÇÃO DE OBJETIVOS DE NEGÓCIO	1,30
	1.2.4. MEDIDAS DE DESEMPENHO: A administração define e comunica os objetivos e as respectivas medidas de desempenho em termos específicos e mensuráveis?	1.2.4.1. DEFINIÇÃO DE MEDIDAS DE DESEMPENHO	1,63
	1.2.5. POLÍTICA DE GESTÃO DE RISCOS: O FNDE dispõe de uma política de gestão de riscos estabelecida e aprovada pela Alta Administração, apropriadamente comunicada, abordando todos os aspectos relevantes?	1.2.5.1. ASPECTOS DA POLÍTICA DE GESTÃO DE RISCOS – PRINCÍPIOS E OBJETIVOS	0,00
		1.2.5.2. ASPECTOS DA POLÍTICA DE GESTÃO DE RISCOS – DIRETRIZES PARA A INTEGRAÇÃO	0,00
		1.2.5.3. ASPECTOS DA POLÍTICA DE GESTÃO DE RISCOS – RESPONSABILIDADES, COMPETÊNCIAS E AUTORIDADES	0,00
		1.2.5.4. ASPECTOS DA POLÍTICA DE GESTÃO DE RISCOS – PLANO DE IMPLEMENTAÇÃO	0,00
		1.2.5.5. ASPECTOS DA POLÍTICA DE GESTÃO DE RISCOS – REPORTE	0,00
		1.2.5.6. ASPECTOS DA POLÍTICA DE GESTÃO DE RISCOS – MONITORAMENTO	0,00

	1.2.6. COMPROMETIMENTO DA GESTÃO: Toda a gestão do FNDE é comprometida com a gestão de riscos?	1.2.6.1. COMPROMETIMENTO COM A ESTRUTURA E O PROCESSO DE GESTÃO DE RISCOS	0,63
	1.2.7. ALOCAÇÃO DE RECURSOS: A administração aloca recursos suficientes e apropriados para a gestão riscos?	1.2.7.1. ALOCAÇÃO DE RECURSOS PARA GESTÃO DE RISCOS	0,90
1.3. PESSOAS: Em que medida as pessoas que atuam no FNDE entendem seus papéis e responsabilidades relacionados à gestão de riscos e estão preparadas exercê-los?	**1.3.1. REFORÇO DA *ACCOUNTABILITY*:** A gestão transmite uma mensagem clara quanto à importância de se levar a sério as responsabilidades de gerenciamento riscos e o pessoal recebe orientação e capacitação suficiente para exercer essas responsabilidades?	1.3.1.1. MENSAGEM DA GESTÃO QUANTO À GESTÃO DE RISCOS	1,10
	1.3.2. ESTRUTURA DE GERECIAMENTO DE RISCOS E CONTROLES: Os grupos de pessoas que integram as três linhas na estrutura de gerenciamento de riscos e controles por todo o FNDE têm clareza quanto aos seus papéis, entendem os limites de suas responsabilidades e como seus cargos se encaixam na estrutura geral de gestão de riscos e controles da organização?	1.3.2.1. PRIMEIRA LINHA	1,40
		1.3.2.2. SEGUNDA LINHA	0,50
		1.3.2.3. TERCEIRA LINHA	3,20
DIMENSÃO PROCESSOS			
COMPONENTE	**ASPECTO**	**OBJETO DE ANÁLISE**	**RESULTADO**
2.1. IDENTIFICAÇÃO E ANÁLISE DE RISCOS: Em que medida as atividades de identificação e análise de riscos são aplicadas de forma consistente a todas as operações, funções e atividades relevantes do FNDE (unidades, processos e atividades que são críticos para a realização dos objetivos-chave da organização)?	**2.1.1. ESTABELECIMENTO DO CONTEXTO:** A identificação de riscos é precedida de uma etapa de estabelecimento do contexto?	2.1.1.1. ENTENDIMENTO DOS OBJETIVOS-CHAVE E DO AMBIENTE	1,20
		2.1.1.2. IDENTIFICAÇÃO DAS PARTES INTERESSADAS	0,00
		2.1.1.3. COMUNICAÇÃO E CONSULTA COM PARTES INTERESSADAS	0,00
	2.1.2. DOCUMENTAÇÃO DO CONTEXTO: A documentação da etapa de estabelecimento do contexto inclui elementos essenciais para viabilizar um processo de avaliação de riscos consistente?	2.1.2.1. OBJETIVOS-CHAVE E FATORES DO AMBIENTE	0,00
		2.1.2.2. ANÁLISE DAS PARTES INTERESSADAS	0,00
		2.1.2.3. CRITÉRIOS DE PRIORIZAÇÃO DE RISCOS	0,00
	2.1.3. PROCESSOS DE IDENTIFICAÇÃO E ANÁLISE DE RISCOS: Os processos de identificação e análise de riscos envolvem pessoas e utilizam técnicas e ferramentas que asseguram a	2.1.3.1. PESSOAS ENVOLVIDAS E SUAS QUALIFICAÇÕES	0,20
		2.1.3.2. TÉCNICAS E FERRAMENTAS UTILIZADAS	0,20
		2.1.3.3. RISCOS DE FRAUDES	0,00

	identificação abrangente e a avaliação consistente dos riscos?	2.1.3.4. LISTA DE RISCOS	0,00
		2.1.3.5. SELEÇÃO DE INICIATIVAS ESTRATÉGICAS E NOVOS PROJETOS	0,90
		2.1.3.6. ANÁLISE DE PROBABILIDADE E IMPACTO	0,90
	2.1.4. DOCUMENTAÇÃO DA IDENTIFICAÇÃO E ANÁLISE DOS RISCOS: No registro de riscos, a documentação da identificação e análise dos riscos contém elementos suficientes para apoiar um adequado gerenciamento dos riscos?	2.1.4.1. REGISTRO DOS RISCOS	0,00
		2.1.4.2. ESCOPO	0,00
		2.1.4.3. PARTICIPANTES	0,00
		2.1.4.4. MÉTODOS UTILIZADOS	0,00
		2.1.4.5. REGISTRO DE PROBABILIDADE E IMPACTO	0,00
		2.1.4.6. REGISTRO DO RISCO INERENTE	0,00
		2.1.4.7. REGISTRO DE CONTROLES	0,00
		2.1.4.8. REGISTRO DO RISCO RESIDUAL	0,00
2.2. AVALIAÇÃO E RESPOSTA A RISCOS: Em que medida as atividades de avaliação e resposta a riscos são aplicadas de forma consistente aos riscos identificados e analisados como significativos?	**2.2.1. CRITÉRIOS PARA PRIORIZAÇÃO DE RISCOS:** Os critérios estabelecidos para priorização de riscos são adequados para orientar decisões seguras por todo o FNDE?	2.2.1.1. NECESSIDADE DE TRATAMENTO E PRIORIZAÇÃO DE RISCOS	1,20
		2.2.1.2. REALIZAÇÃO, REDUÇÃO OU DESCONTINUIDADE DE ATIVIDADES	0,40
		2.2.1.3. IMPLEMENTAÇÃO, MODIFICAÇÃO OU MANUTENÇÃO DE CONTROLES	0,40
	2.2.2. PROCESSOS DE AVALIAÇÃO E SELEÇÃO DAS RESPOSTAS A RISCOS: A seleção de respostas para tratar riscos considera todas as opções de tratamento e o seu custo-benefício?	2.2.2.1. RELAÇÃO CUSTO-BENEFÍCIO	0,00
	2.2.3. PESSOAS ENVOLVIDAS NOS PROCESSOS DE AVALIAÇÃO E SELEÇÃO DAS RESPOSTAS A RISCOS: Os responsáveis pelo tratamento de riscos são envolvidos no processo de avaliação e seleção das respostas e são formalmente comunicados das ações de tratamento decididas?	2.2.3.1. ENVOLVIMENTO DOS RESPONSÁVEIS PELO TRATAMENTO DE RISCOS	0,20
	2.2.4. PLANOS E MEDIDAS DE CONTINGÊNCIA: Os elementos críticos da atuação do FNDE estão identificados e têm definidos planos e medidas de contingência?	2.2.4.1. FORMALIZAÇÃO E DOCUMENTAÇÃO DOS PLANOS E MEDIDAS DE CONTINGÊNCIA	1,00

	2.2.5. DOCUMENTAÇÃO DA AVALIAÇÃO E SELEÇÃO DE RESPOSTAS A RISCOS: A documentação da avaliação e seleção de respostas a riscos inclui elementos suficientes para permitir o gerenciamento adequado da implementação das respostas?	2.2.5.1. PLANO DE TRATAMENTO DE RISCOS	1,20
		2.2.5.2. PRIORIZAÇÃO DE TRATAMENTO	1,00
		2.2.5.3. RAZÕES PARA A SELEÇÃO DAS OPÇÕES DE TRATAMENTO	1,00
		2.2.5.4. RECURSOS, CRONOGRAMA E BENEFÍCIOS ESPERADOS	1,00
		2.2.5.5. MEDIDAS DE DESEMPENHO E REPORTE	1,00
		2.2.5.6. RESPONSÁVEIS PELA APROVAÇÃO E PELA IMPLEMENTAÇÃO	1,00
2.3. MONITORAMENTO E COMUNICAÇÃO: Em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente no FNDE?	**2.3.1. INFORMAÇÃO E COMUNICAÇÃO:** Diretrizes e protocolos de informação e comunicação estão estabelecidos e são efetivamente aplicados em todas as fases do processo de gestão de riscos?	2.3.1.1. DIRETRIZES E PROTOCOLOS DE COMUNICAÇÃO PARA GESTÃO DE RISCOS	0,40
		2.3.1.2. COMUNICAÇÃO E CONSULTA PARA A GESTÃO DE RISCOS	0,00
	2.3.2 SISTEMA DE INFORMAÇÃO: A gestão de riscos é apoiada por um registro de riscos ou sistema de informação efetivo e atualizado?	2.3.2.1. REGISTRO DE RISCOS OU SISTEMA DE INFORMAÇÃO UTILIZADO	0,00
		2.3.2.2. ATUALIZAÇÃO DO REGISTRO DE RISCOS OU SISTEMA DE INFORMAÇÃO UTILIZADO	0,00
	2.3.3. MONITORAMENTO CONTÍNUO E AUTOAVALIAÇÕES – PRIMEIRA LINHA: Em todos os níveis do FNDE, os gestores que têm propriedade sobre riscos (primeira linha) monitoram o alcance de objetivos, riscos e controles chave em suas respectivas áreas de responsabilidade?	2.3.3.1. MONITORAMENTO CONTÍNUO DA PRIMEIRA LINHA	0,40
		2.3.3.2. AUTOAVALIAÇÕES PERIÓDICAS DE RISCOS E CONTROLES	0,00
		2.3.3.3. REPORTE DO MONITORAMENTO – PRIMEIRA LINHA	0,40
	2.3.4. MONITORAMENTO CONTÍNUO E AUTOAVALIAÇÕES – SEGUNDA LINHA: As funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos (como: comitê de governança, riscos e controles; comitê de auditoria ou grupos equivalentes da segunda linha) exercem suas atribuições de modo efetivo?	2.3.4.1. SUPERVISÃO DOS PROCESSOS DE GESTÃO DE RISCOS	0,00
		2.3.4.2. ORIENTAÇÃO E FACILITAÇÃO À PRIMEIRA LINHA	0,00
	2.3.5. MONITORAMENTO PERIÓDICO E AVALIAÇÕES INDEPENDENTES – TERCEIRA LINHA: A função de auditoria interna auxilia o FNDE a realizar seus objetivos aplicando abordagem sistemática e disciplinada para avaliar e	2.3.5.1. ESTABELECIMENTO DE PLANOS DE AUDITORIA BASEADOS EM RISCOS	3,00
		2.3.5.2. ABORDAGEM DE AUDITORIA BASEADA EM RISCO PARA DEFINIÇÃO DO ESCOPO	3,00

	melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança?	2.3.5.3. FORNECIMENTO DE ASSEGURAÇÃO PELA AUDIT	2,90
	2.3.6. MONITORAMENTO PERIÓDICO E AVALIAÇÕES INDEPENDENTES – PLANOS E MEDIDAS DE CONTINGÊNCIA: Há planos e medidas de contingência definidos para os elementos críticos da atuação do FNDE e estes são periodicamente testados e revisados?	2.3.6.1. TESTAGEM DOS PLANOS E MEDIDAS DE CONTINGÊNCIA	0,00
	2.3.7. MONITORAMENTO DE MUDANÇAS SIGNIFICATIVAS: O FNDE monitora as mudanças que podem aumentar sua exposição a riscos e ter impacto nos seus objetivos?	2.3.7.1. PROCEDIMENTOS E PROTOCOLOS DE MONITORAMENTO	0,00
	2.3.8. CORREÇÃO DE DEFICIÊNCIAS E MELHORIA CONTÍNUA: São tomadas as medidas necessárias para a correção de deficiências e a melhoria contínua do desempenho da gestão de riscos em função dos resultados das atividades de monitoramento?	2.3.8.1. COMUNICAÇÃO ÀS INSTÂNCIAS APROPRIADAS	0,00
		2.3.8.2. PLANOS DE AÇÃO PARA CORREÇÃO E MELHORIA	0,00
DIMENSÃO PARCERIAS			
COMPONENTE	**ASPECTO**		**RESULTADO**
3.1. GESTÃO DE RISCOS EM PARCERIAS: Em que medida o FNDE estabelece arranjos com clareza para assegurar que haja um entendimento comum sobre os riscos e o seu gerenciamento no âmbito das parcerias?	**3.1.1. AVALIAÇÃO DA CAPACIDADE DA GESTÃO DE RISCOS DAS ENTIDADES PARCEIRAS:** A capacidade de potenciais organizações parceiras para gerenciar os riscos das políticas de gestão compartilhadas é avaliada antes da realização das parcerias?	AVALIAÇÃO DA CAPACIDADE DA GESTÃO DE RISCOS DAS ENTIDADES PARCEIRAS	0,40
	3.1.2. DEFINIÇÃO DE RESPONSABILIDADES, INFORMAÇÃO E COMUNICAÇÃO: Existe clara e adequada designação de responsáveis pelo gerenciamento de riscos nas parcerias e de protocolos de informação e comunicação entre eles?	DEFINIÇÃO DE RESPONSABILIDADES, INFORMAÇÃO E COMUNICAÇÃO	0,40
	3.1.3. PROCESSO DE GESTÃO DE RISCOS EM PARCERIAS: O processo de gestão de riscos é aplicado no âmbito das parcerias?	PROCESSO DE GESTÃO DE RISCOS EM PARCERIAS	0,20
	3.1.4. PARTICIPANTES DO PROCESSO DE GESTÃO DE RISCOS EM PARCERIAS: A identificação e avaliação de riscos em parcerias envolve as pessoas apropriadas das organizações parceiras e outras partes interessadas?	PARTICIPANTES DO PROCESSO DE GESTÃO DE RISCOS EM PARCERIAS	0,40

	3.1.5. REGISTRO DO PROCESSO DE GESTÃO DE RISCOS EM PARCERIAS: A gestão de riscos nas parcerias é apoiada por um registro de riscos único ou sistema de informação efetivo e atualizado?	REGISTRO DO PROCESSO DE GESTÃO DE RISCOS EM PARCERIAS	0,40
	3.1.6. INFORMAÇÕES SOBRE O PROCESSO DE GESTÃO DE RISCOS EM PARCERIAS: Os riscos e o desempenho das parcerias são monitorados mediante troca regular de informação confiável?	INFORMAÇÕES SOBRE O PROCESSO DE GESTÃO DE RISCOS EM PARCERIAS	0,40
3.2. PLANOS E MEDIDAS DE CONTINGÊNCIA EM PARCERIAS: Em que medida são estabelecidos planos ou medidas de contingência para garantir a recuperação e a continuidade dos serviços no âmbito das parecerias realizadas?	**3.2.1. FORMALIZAÇÃO DE PLANOS E MEDIDAS DE CONTINGÊNCIA EM PARCERIAS:** São definidos planos e medidas de contingência no âmbito das parcerias?	FORMALIZAÇÃO DE PLANOS E MEDIDAS DE CONTINGÊNCIA EM PARCERIAS	0,70
	3.2.2. TESTAGEM E REVISÃO DE PLANOS E MEDIDAS DE CONTINGÊNCIA EM PARCERIAS: Os planos e as medidas de contingência no âmbito das parcerias são periodicamente testados e revisados?	TESTAGEM E REVISÃO DE PLANOS E MEDIDAS DE CONTINGÊNCIA EM PARCERIAS	0,00
DIMENSÃO RESULTADOS			
COMPONENTE	**ASPECTO**	**OBJETO DE ANÁLISE**	**RESULTADO**
4.1. MELHORIA DOS PROCESSOS DE GOVERNANÇA: Em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão do FNDE?	**4.1.1. CONSCIÊNCIA DO NÍVEL DE MATURIDADE DA GESTÃO DE RISCOS NO FNDE:** Os responsáveis pela governança e a alta administração têm consciência do estágio atual da gestão de riscos na organização?	CONSCIÊNCIA DO NÍVEL DE MATURIDADE DA GESTÃO DE RISCOS NO FNDE	1,00
	4.1.2. OBJETIVOS-CHAVE IDENTIFICADOS E REFLETIDOS NA CADEIA DE VALOR: Os objetivos-chave da organização estão identificados e refletidos na sua cadeia de valor e nos seus demais instrumentos de direcionamento e comunicação da estratégia?	OBJETIVOS-CHAVE IDENTIFICADOS E REFLETIDOS NA CADEIA DE VALOR	1,63
	4.1.3. MEDIÇÃO DE PROGRESSO E MONITORMENTO DE DESEMPENHO: Os objetivos estratégicos e de negócios estão estabelecidos juntamente com as respectivas medidas de desempenho?	MEDIÇÃO DE PROGRESSO E MONITORMENTO DE DESEMPENHO	1,00
	4.1.4. PRINCIPAIS RISCOS IDENTIFICADOS E INTEGRADOS À GESTÃO DE RISCOS: Os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido estão	COMUNICAÇÃO AOS NÍVEIS APROPRIADOS	0,63

	identificados e incorporados ao processo de gerenciamento de riscos?		
4.2. RESULTADOS-CHAVE DA GESTÃO DE RISCOS: Em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos do FNDE?	**4.2.1. ENTENDIMENTO DOS OBJETIVOS, RISCOS, PAPÉIS E RESPONSABILIDADES:** Uma consciência sobre riscos, objetivos, resultados, papéis e responsabilidades está disseminada por todos os níveis da organização?	ENTENDIMENTO DOS OBJETIVOS, RISCOS, PAPÉIS E RESPONSABILIDADES	1,00
	4.2.2. GARANTIA PROPORCIONADA PELA GESTÃO DE RISCOS: Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, do cumprimento dos objetivos da organização?	GARANTIA PROPORCIONADA PELA GESTÃO DE RISCOS	0,63
	4.2.3. EFICÁCIA DA GESTÃO DE RISCOS: Os riscos da organização estão dentro dos seus critérios de risco?	EFICÁCIA DA GESTÃO DE RISCOS	0,00

BIBLIOGRAFIA POR TEMA

Auditoria Interna

BRASIL. Ministério da Transparência e Controladoria-Geral da União. **Manual de orientações técnicas da atividade de auditoria interna governamental do Poder Executivo federal**. Brasília: SFC/CGU, 2017a.

BRASIL. Ministério da Transparência, Fiscalização e Controladoria-Geral da União. **Instrução Normativa nº 03, de 09 de junho de 2017**. Aprova o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo federal. 2017b.

INSTITUTO DOS AUDITORES INTERNOS (IIA). **Declaração de posicionamento do IIA:** O papel da Auditoria Interna no gerenciamento de riscos. Flórida, 2009. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2009.

INSTITUTO DOS AUDITORES INTERNOS – THE INSTITUTE OF INTERNAL AUDITORS (IIA). **Normas Internacionais para a Prática Profissional de Auditoria Interna**. Tradução: Instituto dos Auditores Internos do Brasil – IIA Brasil. São Paulo, 2016. Disponível em: https://iiabrasil.org.br/ippf/normas-internacionais.

THE INTERNATIONALAUDITING AND ASSURANCE SATANDARDS BOARD (Iaasb). **ISA 240:** The auditor's responsibilities relating to fraud in an audit of financial statements. 2009.

Controles Internos

BRASIL. Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União. **Instrução Normativa Conjunta nº 01, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. 2016.

GAO. United States General Accounting Office. **Internal control management and evaluation tool,** 2001.

INSTITUTO DOS AUDITORES INTERNOS (IIA). **Declaração de posicionamento do IIA:** As três linhas de defesa no gerenciamento eficaz de riscos e controles. Flórida, 2013. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2013.

INSTITUTO DOS AUDITORES INTERNOS (IIA). **Declaração de posicionamento do IIA:** Modelo das três linhas do IIA 2020 – uma atualização das três linhas de defesa. Flórida, 2013. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2020.

INTOSAI. International Organization of Supreme Audit Institutions. **INTOSAI GOV 9100:** Guidelines for internal control standards for the public sector**,** 2004.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Controle interno:** Estrutura integrada – Sumário executivo. Tradução: PwC e IIA Brasil, São Paulo, 2013a.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Controle interno:** Estrutura integrada – Estrutura e anexos. Tradução: PwC e IIA Brasil, São Paulo, 2013b.

Desenvolvimento de Pessoas

BRASIL. **Lei nº 13.346, de 10 de outubro de 2016**. Dispõe sobre a extinção de cargos em comissão do Grupo-Direção e Assessoramento Superiores e a criação de funções de confiança denominadas Funções Comissionadas do Poder Executivo. 2016.

BRASIL. **Decreto nº 7.133, de 19 de março de 2010**. Regulamenta os critérios e procedimentos gerais a serem observados para a realização das avaliações de desempenho individual e institucional e o pagamento das gratificações de desempenho [...]. 2010.

BRASIL. **Decreto nº 9.991, de 28 de agosto de 2019**. Dispõe sobre a Política Nacional de Desenvolvimento de Pessoas da administração pública federal direta, autárquica e fundacional, e regulamenta dispositivos da Lei nº 8.112, de 11 de dezembro de 1990, quanto a licenças e afastamentos para ações de desenvolvimento. 2019.

BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. Secretaria de Gestão e Desempenho Pessoal. **Instrução Normativa SGP-ENAP/SEDGG/ME nº 21, de 1º de fevereiro de 2021**. Estabelece orientações aos órgãos do Sistema de Pessoal Civil da Administração Pública Federal - SIPEC, quanto aos prazos, condições, critérios e procedimentos para a implementação da Política Nacional de Desenvolvimento de Pessoas - PNDP de que trata o Decreto nº 9.991, de 28 de agosto de 2019. 2021.

Ética Pública

BRASIL. **Decreto nº 1.171, de 22 de junho de 1994**. Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo federal. 1994.

OCDE. Organização para a Cooperação e o Desenvolvimento Econômico. **Towards a sound integrity framework**: instruments, processes, structures and conditions for implementation. GO/PGC/GF(2009)1. Paris: OCDE, 2009.

BRASIL. **Decreto nº 6.029, de 1º de fevereiro de 2007**. Instituiu o Sistema de Gestão da Ética do Poder Executivo federal, 2007.

BRASIL. Tribunal de Contas da União. **Acórdão nº 851/2013 – TCU – Plenário**, de 29 de março de 2017. Relatório de levantamento de auditoria. Conhecimento sobre as práticas adotadas para a promoção da ética em organizações públicas nacionais e internacionais. Desenvolvimento de metodologia de avaliação da gestão da ética aplicável à administração pública federal. Oportunidades de melhorias. Autorização de auditoria piloto com o objetivo de validar e aperfeiçoar o modelo de avaliação da gestão da ética. 2017.

IBE. Institute of Business Ethics. **Corporate ethics policies and programmes**. 2016 UK and Continental Europe Survey, 2017.

Gestão de Riscos

ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000:2018. Gestão de riscos – Diretrizes**. 2. Ed. Rio de Janeiro, 2018.

ABNT. Associação Brasileira de Normas Técnicas. **ABNT NBR IEC 31010:2021. Gestão de riscos – Técnicas para o processo de avaliação de riscos**. 2. Ed. Rio de Janeiro, 2021.

BRASIL. Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União. **Instrução Normativa Conjunta nº 01, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. 2016.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Gestão Púbica. **Guia de orientação para o gerenciamento de riscos.** Brasília: Segep, 2013.

BRASIL. Tribunal de Contas da União. Acórdão n. 2467/2013-TCU-Plenário. Ata 35, Sessão de 11/09/2013. **Levantamento de auditoria para elaboração de indicador para medir o grau de maturidade de entidades públicas na gestão de riscos**. Brasília, 2013.

BRASIL. Tribunal de Contas da União. **10 passos para a boa gestão de riscos**. Brasília: SEMEC/TCU, 2017.

BRASIL. Tribunal de Contas da União. **Gestão de riscos:** avaliação da maturidade. [2018a]. Brasília: SEGECEX/ADGECEX/SEMEC/TCU, 2018.

BRASIL. Tribunal de Contas da União. **Referencial básico de gestão de riscos**. [2018b]. Brasília: SEGECEX/COGER, 2018.

BRASIL. Tribunal de Contas da União. **Referencial de combate a fraude e corrupção:** aplicável a órgãos e entidades da administração pública. [2018c]. Brasília: SEGECEX/SECCOR/SEMEC, 2018.

HILLSON, D. A. Towards a risk maturity model. **The International Journal of Project & Business Risk Management**, v.1, n. 1, p. 35-45, 1997.

INSTITUTO DOS AUDITORES INTERNOS (IIA). **Declaração de posicionamento do IIA:** O papel da Auditoria Interna no gerenciamento de riscos. Flórida, 2009. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2009.

INSTITUTO DOS AUDITORES INTERNOS (IIA). **Declaração de posicionamento do IIA:** As três linhas de defesa no gerenciamento eficaz de riscos e controles. Flórida, 2013. Tradução: Instituto dos Auditores Internos do Brasil. São Paulo, 2013.

INTOSAI. International Organization of Supreme Audit Institutions. **INTOSAI GOV 9130:** Further information on entity risk management**,** 2004.

REINO UNIDO (UK). HM Treasury. **Management of risk - Principles and concepts - The Orange Book.** HM Treasury do HM Government, 2020.

REINO UNIDO (UK). HM Treasury. **Risk management assessment framework:** a tool for departments. London, 2009.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Gerenciamento de riscos corporativos:** Estrutura integrada – Sumário executivo e estrutura. Tradução: PwC e IIA Brasil, São Paulo, 2007.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). **Gerenciamento de riscos corporativos:** integrado com estratégia e performance – Sumário executivo. Tradução: PwC, São Paulo, 2017.

VIEIRA, J. B.; BARRETO, R. T. S. **Governança, gestão de riscos e integridade**. Brasília: Enap, 2019.

Gestão Estratégica

BRASIL. **Decreto nº 10.382, de 28 de maio de 2020**. Institui o Programa de Gestão Estratégica e Transformação do Estado, no âmbito da administração pública federal direta, autárquica e fundacional [...]. 2020.

BRASIL. Ministério da Economia. **Instrução Normativa nº 24, de 18 de março de 2020**. Dispõe sobre a elaboração, avaliação e revisão do planejamento estratégico institucional dos órgãos e das entidades da administração pública federal integrantes do Sistema de Organização e Inovação Institucional do Governo Federal - SIORG, estruturado nos termos do art. 21 do Decreto nº 9.739, de 28 de março de 2019. 2020.

BRASIL. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. Secretaria de Gestão. **Guia técnico de gestão estratégica.** v. 1.0; Brasília: SEGES/ME, 2020.

IBGC. Instituto Brasileiro de Governança Corporativa. **O papel do Conselho de Administração na estratégia das organizações,** 2017.

Governança

ANAO. Australian National Audit Office. **Public sector governance:** better practice guide. Framework, processes and practices, 2003.

BRASIL. Casa Civil da Presidência da República. **Guia da Política de Governança Pública**, 2018.

BRASIL. Ministério do Planejamento, Orçamento e Gestão e Controladoria-Geral da União. **Instrução Normativa Conjunta nº 01, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. 2016.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança organizacional para organizações públicas e outros entes jurisdicionados ao TCU**. 2. ed. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão, 2014.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança organizacional para organizações públicas e outros entes jurisdicionados ao TCU**. 3. ed. Brasília: TCU, SecexAdministração, 2020.

BRASIL. Tribunal de Contas da União. **Referencial para avaliação de governança em políticas públicas**, 2014.

BRASIL. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional, 2017.

CIPFA. Chartered Institute of Public Finance and Accountancy. **The good governance standard for public services,** 2004.

INSTITUTO DOS AUDITORES INTERNOS (IIA). **Alavancar o COSO nas três linhas de defesa**. Carolina do Norte, 2015. Tradução: Fundação Latino-Americana de Auditores Internos.

IBGC. Instituto Brasileiro de Governança Corporativa. **Código das melhores práticas de governança corporativa.** 5. ed. Brasil, 2015.

IFAC. International Federation of Accountants. **Governance in the public sector:** a governing body perspective. International public sector study n. 13., 2001.

IFAC. International Federation of Accountants. CIPFA, The Chartered Institute of Public Finance & Accountancy. **International framework:** good governance in the public sector**,** 2014.

OCDE. Organização para a Cooperação e o Desenvolvimento Econômico. Avaliações da OCDE Sobre Governança Pública: **Avaliação da OCDE sobre o sistema de integridade da administração pública federal brasileira:** Gerenciando riscos por uma administração pública mais íntegra. OECD Publishing, 2011.

VIEIRA, J. B.; BARRETO, R. T. S. **Governança, gestão de riscos e integridade**. Brasília: Enap, 2019.

Integridade

BRASIL. Controladoria-Geral da União. **Guia prático de gestão de riscos para a integridade:** orientações para a administração pública federal, direta, autárquica e fundacional, 2018.

BRASIL. Controladoria-Geral da União. **Portaria nº 57, de 4 de janeiro de 2019**. Altera a Portaria CGU n. 1.089, de 25 de abril de 2018, que estabelece orientações para que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional adotem procedimentos para a estruturação, a execução e o monitoramento de seus programas de integridade e dá outras providências. 2019.

OCDE. Organização para a Cooperação e o Desenvolvimento Econômico. **Towards a sound integrity framework**: instruments, processes, structures and conditions for implementation. GO/PGC/GF(2009)1. Paris: OCDE, 2009.

VIEIRA, J. B.; BARRETO, R. T. S. **Governança, gestão de riscos e integridade**. Brasília: Enap, 2019.

Transparência Pública e Acesso à Informação

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**, Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. 2011.

BRASIL. **Lei nº 13.460, de 26 de junho de 2017**. Dispõe sobre a participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. 2017.

BRASIL. **Decreto nº 7.724, de 16 de maio de 2012**. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. 2012.

BRASIL. Controladoria-Geral da União. **Guia de transparência ativa (GTA) para os órgãos e entidades do Poder Executivo federal**, 6ª versão. Brasília: CGU, 2019.