Relatório de Auditoria – Gerir Riscos

2019

RELATÓRIO DE AUDITORIA Nº 03/2019: avaliação de conformidade.

Relatório de Auditoria como atividade de avaliação da conformidade do processo nuclear Gerir Riscos

JOÃO PESSOA

2019

UNIDADE DE AUDITORIA INTERNA GOVERNAMENTAL DO IFPB

Missão

Desempenhar uma atividade independente e objetiva de avaliação e consultoria desenhada para adicionar valor e melhorar as operações do Instituto Federal da Paraíba, buscando auxiliá-lo a realizar seus objetivos, através da aplicação de uma abordagem sistemática e disciplinada, para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos.

Visão

Ser reconhecida, em longo prazo, no Brasil, como órgão de excelência competente pela avaliação e consultoria dos controles internos, da governança e da gestão de risco contribuindo para o fortalecimento da gestão e para o desenvolvimento institucional.

Valores

I) Comportamento ético;
II) Cautela e zelo profissional;
III) Independência;
IV) Imparcialidade;
V) Objetividade;
VI) Conhecimento técnico e capacidade profissional;
VII) Atualização dos conhecimentos técnicos;
VIII) Cortesia;
IX) Intransferibilidade de Funções;
X) Sigilo e Discrição;
XI) Responsabilidade;
XII) Interesse Público;
XIII) Comunicação eficaz;
XIV) Alinhamento com as estratégias, objetivos e riscos da organização;
XV) Atuação respaldada na eficiência, eficácia, efetividade e economicidade;
XVI) Controle de qualidade; e
XVII) Transparência dos resultados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

Relatório de Auditoria – Macroprocesso Gerir Riscos

Natureza da Auditoria

Conformidade

Período de abrangência

2018

Unidade

Diretoria de Planejamento Institucional

Responsáveis

Cícero Nicácio do Nascimento Lopes – Reitor

Elaine Pereira de Brito – Diretora de Planejamento Institucional

Relatório nº

03/2019

Equipe de Trabalho

Kléber Cordeiro Costa – Auditor Interno

Bruno Rodrigues Cabral – Auditor Geral

JOÃO PESSOA

2019

SUMÁRIO

1. INTRODUÇÃO

O gerenciamento de riscos é o processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização.

Em seu planejamento decenal – PLANEDE – o IFPB mapeou seus macroprocessos nucleares, entre eles o processo nuclear de suporte Gerir Riscos, cuja gerência fica a cargo da Diretoria de Planejamento Institucional.

As atividades de uma organização pública, por sua própria natureza, envolvem riscos diversos quando se busca alcançar seus objetivos. Advindo, esses riscos, da própria dinâmica da administração pública. Assim, as organizações públicas necessitam gerenciar riscos, identificando-os, analisando-os e, em seguida, avaliando se eles devem ser modificados por algum tratamento, de maneira a propiciar segurança razoável para que os objetivos sejam alcançados. A Instrução Normativa Conjunta CGU/MP nº 01/2016 que foi elaborada a partir de um levantamento feito pelo TCU para avaliação da governança, identificou a falta de uma gestão de riscos efetiva como principal problema para se alcançar seus objetivos.

No contexto da Administração Pública Federal, 80% das organizações estariam no estágio inicial, 13% no estágio intermediário e apenas 7% têm a capacidade de estruturar a gestão de riscos de forma aprimorada. Tais resultados indicam que há uma séria ineficácia na gestão de riscos dessas organizações. A gestão de riscos busca efetivamente, suprir as deficiências que podem vir a causar a ineficiência dessas organizações. Assim, essa gestão de riscos gera benefícios que impactam diretamente cidadãos e outras partes interessadas da organização ao viabilizar o adequado suporte às decisões de alocação e uso apropriado dos recursos públicos, o aumento do grau de eficiência e eficácia no processo de criação, proteção e entrega de valor público, otimizando o desempenho e os resultados entregues à sociedade.

2. OBJETIVO

Avaliar o grau de maturidade da gestão de riscos no IFPB.

3. ESCOPO

A avaliação procurou abranger atos vinculados ao processo nuclear Gerir Riscos, seus princípios, estrutura e demais elementos do processo de gerenciamento de riscos colocados em prática pela organização para identificar, analisar, avaliar, tratar e comunicar riscos que possam impactar o alcance dos seus objetivos, com enfoque nas dimensões: ambiente, processo, parcerias e

resultados.

Considerando a relevância quanto aos objetivos estratégicos da instituição e no contexto de gestão de riscos, os exames recaíram sobre a Diretoria de Planejamento Institucional.

4. QUESTÕES DE AUDITORIA

1.1. Em que medida os responsáveis pela governança e a alta administração exercem suas responsabilidades de governança de riscos e cultura?

1.1.1. 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-chaves para o reforço da accountability?

1.1.2. 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?

1.1.3. Os responsáveis pela governança e a alta administração supervisionam a estratégia e exercem suas responsabilidades de governança de riscos?

1.2. Em que medida a organização dispõe de políticas e estratégias de gestão de riscos definidas, comunicadas e postas em prática?

1.2.1. A alta administração, com a supervisão dos responsáveis pela governança, estabelece de modo explícito o direcionamento estratégico?

1.2.2. A alta administração, com a supervisão e a concordância dos responsáveis pela governança, define, comunica, monitora e revisa o apetite a risco?

1.2.3. A gestão de riscos é integrada ao processo de planejamento estratégico implementado na organização e aos seus desdobramentos?

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

1.2.5. A organização dispõe de uma política de gestão de riscos estabelecida e aprovada pela alta administração, apropriadamente comunicada, abordando todos os aspectos relevantes?

1.2.6. Toda a gestão da organização é comprometida com a gestão de riscos?

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

1.3. Em que medida as pessoas na organização entendem seus papéis e responsabilidades relacionados à gestão de riscos e estão preparadas exercê-los?

1.3.1. 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?

1.3.2. Os grupos de pessoas que integram as três linhas de defesa na estrutura de

gerenciamento de riscos e controles por toda a organização 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?

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

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

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

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

2.1.4. No registro de riscos (sistema, planilhas ou matrizes de avaliação de riscos), a documentação da identificação e análise dos riscos contém elementos suficientes para apoiar um adequado gerenciamento dos riscos?

2.2 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. Os critérios estabelecidos para priorização de riscos são adequados para orientar decisões seguras por toda a organização?

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

2.2.3. 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?

2.2.4. Os elementos críticos da atuação da organização estão identificados e têm definidos planos e medidas de contingência?

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

2.3. Em que medida as atividades de monitoramento e comunicação estão estabelecidas e são aplicadas de forma consistente na organização?

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

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

2.3.3. Em todos os níveis da organização, os gestores que têm propriedade sobre riscos (primeira linha de defesa) monitoram o alcance de objetivos, riscos e controles chaves em suas respectivas áreas de responsabilidade?

2.3.4. As funções que supervisionam riscos ou que coordenam as atividades de gestão de riscos (comitê de governança, riscos e controles; comitê de auditoria ou grupos equivalentes da segunda linha de defesa) exercem suas atribuições de modo efetivo?

2.3.5. Há planos e medidas de contingência definidos para os elementos críticos da atuação da organização e estes são periodicamente testados e revisados?

2.3.7. A organização monitora as mudanças que podem aumentar sua exposição a riscos ter impacto nos seus objetivos?

2.3.8. 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?

3.1 Em que medida a organização 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. A capacidade das potenciais organizações parceiras para gerenciar os riscos das políticas de gestão compartilhadas é avaliada antes da realização das parcerias?

3.1.2. Existe clara e adequada designação de responsáveis pelo gerenciamento de riscos nas parcerias e de protocolos de informação e comunicação entre eles?

3.1.3. O processo de gestão de riscos é aplicado no âmbito das parcerias?

3.1.4. A identificação e avaliação de riscos em parcerias envolve as pessoas apropriadas das organizações parceiras e outras partes interessadas?

3.1.5. A gestão de riscos nas parcerias é apoiada por um registro de riscos único ou sistema de informação efetivo e atualizado?

3.1.6. Os riscos e o desempenho das parecerias são monitorados mediante troca regular de informação confiável?

3.2 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. São definidos planos e medidas de contingência no âmbito das parcerias, periodicamente testados e revisados?

4.1 Em que medida a gestão de riscos tem sido eficaz para a melhoria dos processos de governança e gestão?

4.1.1. Os responsáveis pela governança e a alta administração têm consciência do estágio

atual da gestão de riscos na organização?

4.1.2. 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?

4.1.3. Os objetivos estratégicos e de negócios estão estabelecidos juntamente com as respectivas medidas de desempenho?

4.1.4. Os principais riscos relacionados a cada objetivo, meta ou resultado chave pretendido estão identificados e incorporados ao processo de gerenciamento de riscos?

4.2 Em que medida os resultados da gestão de riscos têm contribuído para o alcance dos objetivos da organização?

4.2.1. Uma consciência sobre riscos, objetivos, resultados, papéis e responsabilidades está disseminada por todos os níveis da organização?

4.2.2. Os responsáveis pela governança e a administração têm uma garantia razoável, proporcionada pela gestão de riscos, do cumprimento dos objetivos da organização?

4.2.3. Os riscos da organização estão dentro dos seus critérios de risco?

5 ACHADOS DE AUDITORIA

Como resultado da comparação entre os critérios preestabelecidos e a condição real encontrada durante a realização dos exames, comprovadas por meio de evidências, apresentamos os achados de auditoria.

5.1 Achados do Tipo Informação

5.1.1 Descrição Sumária: Reconhecimento pela alta administração e os responsáveis pela governança da importância da cultura, da integridade, dos valores éticos e da consciência de riscos como aspectos chaves para o reforço da accountability

5.1.1.1 Critério

IN-MP/CGU Nº 1/2016, Art. 8º, I e II; Art. 11, I; Art. 16, I e Art. 21; COSO GRC 2004, 2; COSO GRC Public Exposure (PE) 2016, Princípios 3, 4 e 5; ISO 31000:2009, 3, “h” e 4.2; OCDE, 2011.

5.1.1.2 Condição encontrada

De averiguações junto à Diretoria de Planejamento, por meio de formulário de autoavaliação e solicitação de evidências, a gestão indicou medidas e normativos que atestariam a implementação de importantes instrumentos de controles internos, entre os quais a indicação das Resoluções que aprovam o Estatuto e Regimento da Instituição, bem como o sistema decorrente do Planejamento Estratégico Decenal (Planede), contemplando a mensuração de indicadores e a

Política de Gestão de Riscos (documento SGE004 - Governança, Risco e Compliance - GRC). A Portaria 2025/2017-Reitoria, de 24 de agosto de 2017 formaliza o planejamento decenal.

5.1.2 Descrição Sumária: Estabelecimento do direcionamento estratégico, alinhado com as finalidades e competências legais da entidade.

5.1.2.1 Critério

IN-MP/CGU Nº 1/2016, Art. 2º, II; Art. 14, II; Art. 16, II; e Art. 19; COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 1, 3 e 7. ISO 31000:2009, 5.3.3.

5.1.2.2 Condição encontrada

Em consulta ao sistema PLANEDE, ficou constada a definição dos elementos do direcionamento estratégico da organização, quais sejam objetivos-chave, missão, visão e valores fundamentais da organização.

5.1.3 Descrição Sumária: Estabelecimento formal dos níveis de exposição a risco.

5.1.3.1 Critério

IN-MP/CGU Nº 1/2016, Art. 2º, II, e Art. 14, II; Art. 16, II, e V; COSO GRC 2004, 1, 2 e 3; COSO GRC PE 2016, Princípios 1, 7 e 8; ISO 31000:2009, 3, “g” e 5.3.3.

5.1.3.2 Condição encontrada

Mediante levantamento das documentações da gestão de riscos no sistema do PLANEDE, especificamente a matriz de riscos, constatou-se a definição formal do apetite a riscos assim transcrito: Para fins de aplicação ao PLANEDE 2025, adota-se um apetite ao risco único, aqui declarado formalmente como "nulo apetite ao risco" para toda a instituição, consubstanciado nos parâmetros de forte exposição do IFPB a riscos relacionados a requisitos legais (e.g., leis, políticas, regulamentações, contratos) e dependência umbilical de orçamento público federal para o funcionamento (e.g., despesa com pessoal, expansão de oferta de vagas), fazendo com que se internalize o uso de controles que sejam rígidos em busca de prevenir perdas e assim fomentar um estilo de gestão institucional em "estado de alerta" em cada tomada de decisão para o alcance dos objetivos estratégicos.

5.1.4 Descrição Sumária: Estabelecimento formal dos objetivos estratégicos de alto nível e objetivos de negócios específicos.

5.1.4.1 Critério

IN-MP/CGU Nº 1/2016, Art. 8º, VI; Art. 14, IV; Art. 16, II. COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 9, 10 e 11;

5.1.4.2 Condição encontrada

Em consultas a Diretoria de Planejamento por meio de formulário, bem como através de acesso ao sistema de planejamento (PLANEDE), constatou-se a delimitação dos objetivos

estratégicos de alto nível, com respectiva correlação de riscos e indicadores de desempenho. Quanto aos objetivos de negócios, constatou-se que estes são tratados em termos de metas e indicadores-chave de desempenho, devidamente alinhados aos objetivos estratégicos em cada processo nuclear.

5.1.5 Descrição Sumária: Definição formal dos objetivos e suas respectivas medidas de desempenho em termos específicos e mensuráveis.

5.1.5.1 Critério

IN-MP/CGU Nº 1/2016, Art. 16, II. COSO GRC 2004, 3; COSO GRC PE 2016, Princípios 10 e 11; COSO 2013, Princípio 6, atributos "a" e "b"; INTOSAI GOV 9130,

5.1.5.2 Condição encontrada

Em consultas a Diretoria de Planejamento por meio de formulário, bem como através de acesso ao sistema de planejamento (PLANEDE), constatou-se a explicitação de objetivos e suas respectivas medidas de desempenho.

5.1.6 Descrição Sumária: Instituição formal de política de gestão de riscos

5.1.6.1 Critério

IN-MP/CGU Nº 1/2016, Art. 17; ISO 31000:2009, 4.3.2.

5.1.6.2 Condição encontrada

Do levantamento de informações junto à Diretoria de Planejamento, ao sistema do PLANEDE e consultando os boletins de serviço no site da instituição ficou evidenciada a existência da estrutura básica de uma política de gestão de riscos, quais sejam: a) os princípios e objetivos; b) as diretrizes para a integração da gestão de riscos a todos os processos organizacionais; c) a definição de responsabilidades; d) diretrizes sobre como e com qual periodicidade riscos devem ser identificados, avaliados, tratados, monitorados e comunicados; e) diretrizes sobre a aferição da efetividade da gestão de riscos.

5.1.7 Descrição Sumária: Comprometimento formal dos gestores com a gestão de riscos.

5.1.7.1 Critério

IN-MP/CGU Nº 1/2016, Art. 12 e 16, § único; Art. 17, II, "e" e "f"; Art. 19 e 20; ISO 31000:2009, 4.2 e 4.3.3.

5.1.7.2 Condição encontrada

Em consulta a Diretoria de Planejamento por meio de formulário e analisando os processos de capacitação em gestão de riscos e mapeamento dos riscos (em desenvolvimento) constatou-se a adoção da seguinte prática: a Diretoria de Planejamento está encabeçando a disseminação da gestão de riscos entre os gestores dos processos nucleares. Neste momento, além das atividades de capacitação, os gestores realizam o primeiro mapeamento dos riscos inerentes aos seus processos nucleares, além de firmarem termo de ciência e declaração formal de apoio à política de governança

institucional e gestão de riscos.

5.1.8 Descrição Sumária: Alocação de recursos suficiente e apropriada para a gestão de riscos.

5.1.8.1 Critério

IN-MP/CGU Nº 1/2016, Art. 17, II, "f"; Art. 23, II, III e IX. ISO 31000:2009, 4.3.5. COSO GRC PE 2016, Princípio 2.

5.1.8.2 Condição encontrada

Em consulta a Diretoria de Planejamento por meio de formulário e analisando os processos de capacitação em gestão de riscos e mapeamento dos riscos (em desenvolvimento) verificou-se a declaração de adequação de recursos para a gestão de riscos.

Por meio dos processos de capacitação e mapeamento de riscos, constatou-se a disponibilização de materiais e orientações que embasam o funcionamento da gestão de riscos na instituição.

5.1.9 Descrição Sumária: Estabelecimento de contexto previamente à identificação dos riscos.

5.1.9.1 Critério

ISO 31000:2009, 5.3. COSO GRC 2004, 4; COSO GRC PE 2016, Princípio 7.

5.1.9.2 Condição encontrada

Em consulta a Diretoria de Planejamento por meio de formulário, da análise dos processos de capacitação em gestão de riscos e mapeamento dos riscos (em desenvolvimento), bem como ao sistema PLANEDE verificou-se o que o sistema PLANEDE elenca as metas e objetivos-chave da gestão, correlacionando ainda seus respectivos processos nucleares e indicadores. Há, portanto, clareza quanto aos objetivos e identificação das partes interessadas.

Nos processos de mapeamento dos riscos, em fase disseminação na gestão, são apresentados aos gestores os normativos aplicáveis a gestão de riscos bem como a sistemática para identificação destes, sendo realizado, neste primeiro momento, a primeira identificação dos riscos.

5.1.10 Descrição Sumária: Documentação contempla elementos essenciais para viabilização do processo de avaliação de riscos.

5.1.10.1 Critério

ISO 31000:2009, 5.4.2 e A.3.2.

5.1.10.2 Condição encontrada

Em consulta a Diretoria de Planejamento e ao sistema PLANEDE, constatou-se a documentação e adequação dos principais elementos necessários para estabelecimento do contexto, a exemplo da descrição dos objetivos-chave, dos fatores críticos para o sucesso, análise dos fatores dos ambientes internos e externos (por meio de análise SWOT), análise de stakeholders, bem como a clara definição dos critérios com base nos quais os riscos serão analisados, avaliados e

priorizados.

5.1.11 **Descrição Sumária**: Envolvimento dos responsáveis pelas respostas aos riscos no processo de avaliação e seleção das respostas.

5.1.11.1 Critério

IN-MP/CGU Nº 1/2016, Art. 20; ISO 31000:2009, 5.5.2 e A.3.2;

5.1.11.2 Condição encontrada

Em consulta a Diretoria de Planejamento e ao sistema PLANEDE quanto ao processo de identificação e análise de riscos, constatou-se a adoção da seguinte prática: a Diretoria elaborou cronograma para capacitação dos gestores dos processos nucleares. Nesta oportunidade, é apresentado o conjunto normativo e teórico sobre a gestão de riscos. Em sequência, por meio de brainstorming, os gestores listam os riscos relevantes para seus processos nucleares e indicam os responsáveis e as medidas de resposta.

Para cada processo nuclear foi instaurado um processo para gerenciamento dos riscos, sendo encaminhados para a Unidade de Auditoria os processos referentes aos seguintes processos nucleares: Gerir Ensino, Gerir Extensão, Planejamento, Conformidade, Gerir Financeiro, Gerir Infraestrutura, Gerir Segurança, Gerir Frota, Gerir Orçamento, Gerir Almoxarifado, Gerir Patrimônio, Gerir Contrato Terceirizado, Gerir Fornecedores, Normas Acadêmicas e Administrativas e Gerir Licitação.

Analisando a metodologia adotada, especificamente quanto a realização da capacitação e do "Brainstorming" para identificação dos riscos e repostas, há participação dos gestores dos processos nucleares e ainda demais gestores táticos.

5.1.12 **Descrição Sumária**: Elaborados planos de contingências relativos aos elementos críticos do IFPB.

5.1.12.1 Critério

IN-MP/CGU Nº 1/2016, Art. 16, VI; ISO 31000:2009, 5.5.3.

5.1.12.2 Condição encontrada

Em consulta a Diretoria de Planejamento e ao sistema PLANEDE quanto a existência de planos de contingência vinculados aos elementos críticos da atuação do IFPB constatou-se a seguinte situação: há a definição de objetivos e metas estratégicos da instituição, para cada um dos objetivos e metas foi identificado um ou mais riscos que possam afetá-los. Para estes riscos identificados, foi previsto um plano de contingência identificando a consequência, o gatilho, a resposta necessária, o gestor responsável e seu status.

5.1.13 **Descrição Sumária**: Estabelecimento das diretrizes e protocolos de informação e comunicação inerentes ao monitoramento dos riscos.

5.1.13.1 Critério

IN-MP/CGU Nº 1/2016, Art. 16, VII; ISO 31000:2009, 5.2 e A.3.4; COSO GRC 2004, 8; COSO GRC PE 2016, Princípio 20.

5.1.13.2 Condição encontrada

Em consulta a Diretoria de Planejamento e ao sistema PLANEDE quanto a definição de diretrizes e protocolos para monitoramento e comunicação dos riscos constatou-se a seguinte situação: a política de gestão de ricos, materializada pelo documento SGE004 - Governança, Risco e Compliance (GRC) - Sistema Planede - descreve o modo de operação para gerenciamento dos riscos, especificando os atores envolvidos e suas competências no âmbito das linhas de defesa.

Muito embora o gerenciamento dos riscos esteja em fase de implantação nos setores táticos da instituição, pela análise dos processos de identificação dos riscos nos processos nucleares há a participação dos gestores na identificação de riscos e seleção das respostas.

5.1.14 Descrição Sumária: Definição de 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 da organização

5.1.14.1 Critério

COSO GRC 2004, 9; COSO GRC PE 2016, Princípio 22.

5.1.14.2 Condição encontrada

Em consulta à Diretoria de Planejamento e ao sistema Planede, especificamente ao módulo GRC, verificou-se a previsão de protocolos para relatório e monitoramento.

As Camadas do GRI-IFPB possuem o seguinte modo de operação para antever problemas em potencial que comprometam o cumprimento da Missão, Visão e Sistema de Valores, Estratégia e Objetivos Institucionais e Evolução de Desempenho Institucional: (...) O quê - Camada 4: Informações sobre os Riscos Institucionais (Comunicação Ostensiva e Relatórios); Como - Utilização padronizada na Instituição da Matriz GUT (Mapeamento dos Riscos) e 6M (Resposta aos Riscos), visando a internalização do tema junto aos líderes da instituição e equipes no IFPB.

A Diretoria de Planejamento conduz eventos de capacitação e disseminação da gestão de riscos junto aos gestores dos macroprocessos, momento em que se firma Termo de Ciência de Risco de Macroprocesso que elenca entre as atividades de controle ações preventivas e de detecção contemplando verificações de relatórios.

5.1.15 Descrição Sumária: Identificação adequada dos objetivos chaves da organização.

5.1.15.1 Critério

IN-MP/CGU Nº 1/2016, Art. 22; ISO 31000:2009, 3 “a” e 5.3.1; COSO GRC 2004, Premissa; COSO GRC PE 2016, Premissa.

5.1.15.2 Condição encontrada

Em consulta à Diretoria de Planejamento e ao sistema PLANEDE, quanto a identificação dos objetivos-chave da organização, constatou-se o que no sistema PLANEDE está disponível o mapa estratégico seguindo o modelo Balance Scorecard (BSC), com a clara representação dos objetivos e suas dimensões (perspectivas).

Cada objetivo tem seu detalhamento e indicação de seus indicadores.

5.1.16 Descrição Sumária: Definição adequada de medidas de desempenho para os objetivos estratégicos.

5.1.16.1 Critério

IN-MP/CGU Nº 1/2016, Art. 16, II; ISO 31000:2009, 4.2, itens 3 e 4; COSO GRC 2004, 3. COSO GRC PE 2016, Dimensão 2.

5.1.16.2 Condição encontrada

Em consulta à Diretoria de Planejamento e ao sistema PLANEDE, quanto a identificação dos objetivos-chave da organização, constatou-se o que no sistema PLANEDE está disponível o mapa estratégico seguindo o modelo Balance Scorecard (BSC), com a clara representação dos objetivos e suas dimensões (perspectivas).

Cada objetivo tem seu detalhamento e indicação de seus indicadores.

5.1.17 Descrição Sumária: Identificação e gerenciamento dos principais riscos relacionados aos objetivos, metas e resultados chaves.

5.1.17.1 Critério

IN-MP/CGU Nº 1/2016, Art. 20; ISO 31000:2009, A.2 e A.3.2. COSO GRC 2004, 4; COSO GRC PE 2016, Princípios 12 a 16.

5.1.17.2 Condição encontrada

Em consulta a Diretoria de Planejamento e ao sistema PLANEDE quanto a existência de plano de contingência vinculados aos elementos críticos da atuação do IFPB constatou-se a seguinte situação: há a definição de objetivos e metas estratégicos da instituição. Para cada um dos objetivos e metas foi identificado um ou mais riscos que possam afetá-los. Para estes riscos identificados, foi previsto um plano de contingência identificando a consequência, o gatilho, a resposta necessária, o gestor responsável e seu status.

5.1.18 Descrição Sumária: Predominância da percepção, entre os gestores, de entendimento atual, correto e abrangente dos objetivos sob a sua gestão, de seus papéis e responsabilidades, e sabem em que medida os resultados de cada área ou pessoa para atingir os objetivos-chave envolvem riscos.

5.1.18.1 Critério

ISO 31000:2009, A.2.; COSO GRC 2004, 1, Anexo 1.1.

5.1.18.2 Condição encontrada

Em consulta realizada a servidores do IFPB por meio de formulário eletrônico, especificamente se estes julgavam-se ter um entendimento atual, correto e abrangente dos objetivos sob a sua gestão, de seus papéis e responsabilidades, e sabem em que medida os resultados de cada área ou pessoa para atingir os objetivos-chave envolvem riscos, obtivemos o seguinte resultado: 10% concordaram totalmente e 45,6% concordaram em parte, totalizando 55,6% de concordância neste quesito.

O formulário foi encaminhado para a lista de e-mails tas@ifpb.edu.br, obtendo um total de 90 respostas.

5.2 Achados do Tipo Constatação

5.2.1 Descrição Sumária: Ausência de atuação do Comitê de Gestão de Riscos.

5.2.1.1 Critério

IN-MP/CGU Nº 1/2016, Art. 23, II, Art. 17, II, “a” e “d”; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 1, e 2; ISO 31000:2009, 3, “b”, “c”, “e” e 4.1.

5.2.1.2 Condição encontrada

Em avaliações junto à Diretoria de Planejamento, por meio de formulário de autoavaliação e solicitação de evidências, a gestão indicou que a composição das instâncias internas de apoio à gestão de riscos estavam previstas no Programa de Governança, Riscos e Compliance (GRC). Contudo, não ficou comprovado que o Comitê de Gestão de Riscos, previsto no referido programa, esteja em plena atividade.

5.2.1.3 Causa

Falha de governança quanto a formalização das instruções e designação dos membros.

5.2.1.4 Manifestação do auditado

A unidade auditada, em resposta à Solicitação de Auditoria n. 01/2019, informou:

> Existe a previsão do Comitê de Gestão de Riscos conforme a Portaria n° 2025/2017 e Portaria n° 1770/2018, todavia esta última estabelece o prazo da implantação até o dia 31 de dezembro de 2019.

5.2.1.5 Consequência

Sem a instituição e efetiva atuação de comitê de gestão de riscos, as atribuições inerentes a segunda linha de defesa ficam prejudicadas, entre as quais a supervisão e monitoramento dos controles internos.

5.2.1.6 Análise da Auditoria Interna

A manifestação da unidade auditada evidencia que atuação do Comitê de Riscos ainda está

pendente de efetiva implementação.

5.2.1.7 Recomendação

Atuação efetiva de comitê responsável pela supervisão e monitoramento dos controles internos com vistas a aprimorar a gestão de riscos no âmbito do IFPB.

5.2.2 Descrição Sumária: Ausência de revisão sistemática da visão de portfólio de riscos e notificação regular e oportuna sobre as exposições da organização a riscos.

5.2.2.1 Critério

IN-MP/CGU Nº 1/2016, Art. 16, parágrafo único; Art. 19, 20 e 23, IX; COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 1, 2 e 5; ISO 31000:2009, 4.2.

5.2.2.2 Condição encontrada

A unidade apresentou a previsão e gerenciamento de indicadores de risco e indicadores chave de desempenho por meio do sistema Planede. Através do mesmo sistema também é possível constatar a identificação dos principais riscos para os objetivos estratégicos. Contudo, a revisão do gerenciamento de riscos e notificação regular e oportuna sobre as exposições a riscos estão pendentes ações de capacitação junto aos gestores dos macroprocessos.

5.2.2.3 Causa

Falta de capacitação de pessoal.

5.2.2.4 Manifestação do auditado

A unidade auditada, em resposta à Solicitação de Auditoria n. 01/2019, informou:

> No tocante ao item " Ausência de revisão sistemática da visão de portfólio de ricos" é importante esclarecer que na gestão de Riscos do IFPB integrada ao Planejamento Estratégico do IFPB, disponível em https://planejamento.ifpb.edu.br, menu "Riscos" contém a periodicidade de revisões: semestral e Anual dos macroprocessos finalísticos, conforme prevê o art. 3 da IN-MP/CGU Nº 1/2016

5.2.2.5 Consequência

Sem a supervisão da governança e da alta administração, as atividades de gerenciamento de riscos podem ficar desalinhadas com as expectativas da organização quanto ao apetite ao risco e os caminhos que a gestão deve tomar.

5.2.2.6 Análise da Auditoria Interna

Muita embora haja definição da periodicidade de revisão do portfólio de riscos, não ficou evidenciado o efetivo acompanhamento pela gestão.

5.2.2.7 Recomendação

Instituir rotinas de revisão do portfólio de riscos pela alta administração e de notificação

regular e oportuna sobre as exposições da organização a riscos

5.2.3 Descrição Sumária: Baixo entendimento entre as pessoas da organização sobre suas responsabilidades no gerenciamento de riscos

5.2.3.1 Critério

IN-MP/CGU Nº 1/2016, Art. 11, IV e II; e Art. 16, III a VI; INTOSAI GOV 9130/2007, 2.7.3. ISO 31000:2009, 5.2. COSO GRC 2004, 2, 8 e 10; COSO GRC PE 2016, Princípios 3, 5, 20.

5.2.3.2 Condição encontrada

Em consulta realizada a servidores do IFPB por meio de formulário eletrônico, especificamente se estes teriam recebido uma mensagem clara da gestão quanto à importância de cumprir suas responsabilidades de gerenciamento de riscos, bem como se seriam orientados e saberiam como proceder para encaminhar assuntos relacionados a risco às instâncias pertinentes, obtivemos o seguinte resultado: 40% discordou totalmente e 33,3% discordou em parte, totalizando 73,3% de discordância neste quesito.

Restringindo o resultado aos que informaram não ocupar cargo de direção ou função gratificada, obteve-se o seguinte resultado: 49% discordaram totalmente, 28,6% discordaram em parte, totalizando 77,6% de discordância nesse quesito.

O formulário foi encaminhado para a lista de e-mails tas@ifpb.edu.br, obtendo 90 respostas.

5.2.3.3 Causa

Falta de capacitação de pessoal.

5.2.3.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.3.5 Consequência

O sucesso de qualquer política de gestão de riscos não pode ser alcançado sem o claro entendimento de todos os agentes sobre seus papéis. Todas as pessoas da organização devem ser informadas sobre suas responsabilidades e a quem encaminhar assuntos relacionados a riscos.

5.2.3.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.3.7 Recomendação

Difundir as responsabilidades sobre a gestão de riscos entre todos os atores da organização.

5.2.4 Descrição Sumária: Necessidade de capacitação aos gestores da primeira linha de defesa

5.2.4.1 Critério

IN-MP/CGU Nº 1/2016, Art. 2º, III; e 3º e 6º; ISO 31000:2009, 4.3.3. COSO GRC 2004, 10; COSO GRC PE 2016, Princípios 2, 5 e Apêndice B.

5.2.4.2 Condição encontrada

Em consulta realizada a servidores do IFPB por meio de formulário eletrônico, especificamente se estes julgavam-se regularmente capacitado para conduzir o processo de gestão de riscos em suas áreas de responsabilidade e para orientar as suas equipes sobre esse tema, obtivemos o seguinte resultado: 48,2% discordou totalmente e 27,1% discordou em parte, totalizando 75,3% de discordância neste quesito.

O resultado foi restrito aos servidores que informaram não ocupar cargo de direção para afastar aqueles que não integravam a primeira linha de defesa.

O formulário foi encaminhado para a lista de e-mails tas@ifpb.edu.br, obtendo um total de 90 respostas. Destas, 85 preencheram os requisitos para esta questão.

5.2.4.3 Causa

Falta de capacitação de pessoal.

5.2.4.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.4.5 Consequência

Sem a regular capacitação os gestores da primeira linha de defesa não estarão aptos para conduzir o processo de gestão de riscos em suas áreas de responsabilidade e para orientar as suas equipes sobre esse tema.

5.2.4.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.4.7 Recomendação

Capacitar os gestores da primeira linha de defesa para a condução do processo de gestão de riscos.

5.2.5 Descrição Sumária: Utilização de formulário para identificação de riscos sem a verificação

da probabilidade e causa dos eventos.

5.2.5.1 Critério

ISO 31000:2009, 5.4.2, 5.4.3 e 5.7. ISO 31000:2009, 5.5.1

5.2.5.2 Condição encontrada

Em consulta a Diretoria de Planejamento e ao sistema PLANEDE quanto ao processo de identificação e análise de riscos, constatou-se a adoção da seguinte prática. A Diretoria elaborou cronograma para capacitação dos gestores dos processos nucleares. Nesta oportunidade, é apresentado o conjunto normativo e teórico sobre a gestão de riscos. Na sequência, por meio de brainstorming, os gestores listam os riscos relevantes para seus processos nucleares e indicam os responsáveis e as medidas de resposta.

Para cada processo nuclear foi instaurado um processo para gerenciamento dos riscos. Foram encaminhados para a Unidade de Auditoria os processos referentes aos seguintes processos nucleares: Gerir Ensino, Gerir Extensão, Planejamento, Conformidade, Gerir Financeiro, Gerir Infraestrutura, Gerir Segurança, Gerir Frota, Gerir Orçamento, Gerir Almoxarifado, Gerir Patrimônio, Gerir Contrato Terceirizado, Gerir Fornecedores, Normas Acadêmicas e Administrativas e Gerir Licitação.

Analisando a metodologia adotada, especificamente quanto ao formulário "Brainstorm: Gestão de Riscos Operacionais no IFPB", constatou-se a ausência de avaliação da probabilidade dos riscos e suas causas para os processos nucleares Gerir Ensino, Gerir Extensão, Gerir Planejamento, Gerir Normas Acadêmicas e Administrativas.

5.2.5.3 Causa

Falha na concepção do processo de identificação de riscos.

5.2.5.4 Manifestação do auditado

A unidade auditada, em resposta à Solicitação de Auditoria n. 01/2019, informou:

> A gestão de Riscos do IFPB integrada ao Planejamento Estratégico do IFPB, disponível em https://planejamento.ifpb.edu.br, menu "Riscos" contém identificação e análise de riscos envolvem pessoas e utilizam técnicas e ferramentas que asseguram a identificação abrangente e a avaliação. Ex. Descrição, Categoria, Tipo, Consequência, Probabilidade, Impacto, Severidade, Ação Gatilho, Resposta ao Risco, Responsável e Status

5.2.5.5 Consequência

A adoção de técnicas inadequadas na gestão de riscos pode dificultar a hierarquização dos

eventos em função de sua probabilidade e impacto, dificultando a implementação de ações de controle efetivas.

5.2.5.6 Análise da Auditoria Interna

Das análises ao sistema Planede bem como os processos mencionados no campo "condição encontrada" evidenciou-se a duplicidade de um registro de riscos. Efetivamente, no menu "Riscos" do sistema Planede, há a previsão da probabilidade para os riscos identificados. Todavia, tal matriz contempla apenas um risco para cada um dos objetivos ou metas estratégicos. Os demais riscos identificados nos processos mencionados não tiveram a probabilidade e causa identificadas bem como não foram transcritos para a uma matriz única no sistema Planede.

5.2.5.7 Recomendação

Adotar ferramenta padronizada de identificação de riscos que contemple a análise da probabilidade de ocorrência dos eventos bem como suas possíveis causas.

5.2.6 Descrição Sumária: Ausência de elementos que apoiariam o adequado gerenciamento dos riscos.

5.2.6.1 Critério

ISO 31000:2009, 5.4.2, 5.4.3 e 5.7.

5.2.6.2 Condição encontrada

Da análise dos registros de riscos adotados pelo IFPB constantes no sistema Planede e nos processos de mapeamentos de riscos dos processos nucleares, encaminhados através de memorando pela Diretoria de Planejamento Institucional, constatou-se a limitação destes registros quanto a elementos que permitiriam o adequado gerenciamento dos riscos, a exemplo de suas causas, a probabilidade de ocorrência, os níveis de risco inerente resultantes da combinação de probabilidade e impacto, a descrição dos controles existentes, as considerações quanto à sua eficácia e confiabilidade e o risco residual.

5.2.6.3 Causa

Falha na concepção do processo de identificação de riscos.

5.2.6.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.6.5 Consequência

Avaliar riscos sem aferir suas causas, a probabilidade, os controles já existentes bem como o risco inerente e residual, pode dificultar a adoção de medidas efetivas como resposta.

5.2.6.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a

análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.6.7 Recomendação

Fazer constar, no registro de riscos, pelo menos os seguintes elementos: i) o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise; ii) os participantes das atividades de identificação e análise de riscos; iii) a abordagem ou o método de identificação e análise utilizado, as especificações utilizadas para as classificações de probabilidade e impacto e as fontes de informação consultadas; v) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e a sua descrição, bem como considerações quanto à análise desses elementos; v) os níveis de risco inerente resultantes da combinação de probabilidade e impacto, além de outros fatores que a entidade considera para determinar o nível de risco; vi) a descrição dos controles existentes, as considerações quanto à sua eficácia e confiabilidade; e vii) o risco residual

5.2.7 Descrição Sumária: Ausência de definição de critérios para priorização de riscos.

5.2.7.1 Critério

IN-MP/CGU Nº 1/2016, Art. 16, V; ISO 31000:2009, 5.4.4; COSO GRC 2004, 6; COSO GRC PE 2016, Princípio 14.

5.2.7.2 Condição encontrada

Realizando análise do sistema Planede quanto à Gestão de Riscos, não ficou evidenciada a existência de critérios adequados para priorização dos riscos mapeados em relação a todas as operações, funções e atividades relevantes da organização.

Não há especificação de critérios que orientem qual estratégia seguir (evitar, transferir, aceitar ou tratar) em relação aos riscos mapeados e avaliados. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco.

5.2.7.3 Causa

Falha na concepção do processo de identificação de riscos.

5.2.7.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.7.5 Consequência

A ausência de definição de critérios objetivos que permitam orientar as decisões sobre os riscos mapeados podem prejudicar as decisões sobre as medidas de controles a serem

implementadas de forma prioritária; se determinada atividade deve ser realizada, reduziada ou descontinuada; bem como se os controles devem ser implementados, modificados ou apenas mantidos.

5.2.7.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.7.7 Recomendação

Estabelecer critérios para orientar as decisões sobre riscos em relação a todas as operações, funções e atividades relevantes da organização e que os critérios levem em conta fatores como 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, critérios de comunicação a instâncias competentes, o tempo de resposta requerido e que possibilitem orientar decisões quanto a se: i) um determinado risco precisa de tratamento e a prioridade para isso; ii) uma atividade deve ser realizada, reduzida ou descontinuada; iii) controles devem ser implementados, modificados ou apenas mantidos.

5.2.8 Descrição Sumária: Ausência de avaliação do custo-benefício quanto as medidas de respostas aos riscos.

5.2.8.1 Critério

IN-MP/CGU Nº 1/2016, Art. 14, III; ISO 31000:2009, 5.5.2; COSO GRC PE 2016, Princípio 15.

5.2.8.2 Condição encontrada

Dentre os processos nucleares que concluíram a primeira etapa de mapeamento de riscos, quais sejam: Gerir Ensino, Gerir Extensão, Planejamento, Conformidade, Gerir Financeiro, Gerir Infraestrutura, Gerir Segurança, Gerir Frota, Gerir Orçamento, Gerir Almoxarifado, Gerir Patrimônio, Gerir Contrato Terceirizado, Gerir Fornecedores, Normas Acadêmicas e Administrativas e Gerir Licitação; quanto as ações identificadas para resposta aos riscos identificados, nenhuma das ações mapeadas trazia a informação quanto ao seu custo de implementação.

5.2.8.3 Causa

Falha na concepção do processo de identificação de riscos.

5.2.8.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.8.5 Consequência

A ausência de avaliação do fator custo, quanto a implementação de controles internos, pode permitir a implementação de um controle desproporcional ao risco quanto ao custo-benefício.

5.2.8.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.8.7 Recomendação

Avaliar o custo-benefício de todas as opções de tratamento dos riscos.

5.2.9 Descrição Sumária: Insuficiência na documentação da avaliação e seleção das respostas a riscos

5.2.9.1 Critério

ISO 31000:2009, 5.5.3 e 5.7.

5.2.9.2 Condição encontrada

Em análise aos processos de identificação de riscos dos processos nucleares já concluídos e encaminhados pela Diretoria de Planejamento, bem com o Plano de Contingência dos riscos inerentes aos objetivos e metas estratégicos, constata-se a previsão de ações de resposta para os riscos identificados, todavia, não há robustez quanto a avaliação e seleção das respostas por meio de documentos que contemplem, pelo menos: i) o plano de tratamento de riscos identificando claramente os riscos que requerem tratamento e a ordem de prioridade para cada tratamento; ii) as respostas a riscos selecionadas e as razões para a seleção, incluindo justificativa de custo-benefício; as ações propostas, os recursos requeridos, o cronograma e os benefícios esperados; iii) as medidas de desempenho e os requisitos para o reporte de informações relacionadas ao tratamento dos riscos, e as formas de monitoramento da sua implementação; iv) a identificação dos responsáveis pela aprovação e pela implementação de cada ação do plano de tratamento, com autoridade suficiente para gerenciá-las.

5.2.9.3 Causa

Falha na concepção do processo de identificação de riscos.

5.2.9.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.9.5 Consequência

A ausência de definição de critérios objetivos que permitam orientar as decisões sobre os riscos mapeados podem prejudicar as decisões sobre as medidas de controles a serem

implementadas de forma prioritária.

5.2.9.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.9.7 Recomendação

Documentar os atos de avaliação e seleção das respostas a riscos com pelo menos os seguintes elementos: i) o plano de tratamento de riscos, preferencialmente integrado ao registro de riscos, identificando claramente os riscos que requerem tratamento, suas respectivas classificações (probabilidade, impacto, níveis de risco etc.), a ordem de prioridade para cada tratamento; ii) as respostas a riscos selecionadas e as razões para a seleção, incluindo justificativa de custo-benefício; as ações propostas, os recursos requeridos, o cronograma e os benefícios esperados; iii) as medidas de desempenho e os requisitos para o reporte de informações relacionadas ao tratamento dos riscos, e as formas de monitoramento da sua implementação; iv) a identificação dos responsáveis pela aprovação e pela implementação de cada ação do plano de tratamento, com autoridade suficiente para gerenciá-las.

5.2.10 Descrição Sumária: Ausência de sistema de tecnologia da informação próprio para gestão de riscos.

5.2.10.1 Critério

ISO 31000:2009, 5.7.

5.2.10.2 Condição encontrada

Em análise aos processos de identificação de riscos dos processos nucleares já concluídos e encaminhados pela Diretoria de Planejamento, constata-se a ausência de sistema de tecnologia da informação próprio para gerenciamento de riscos. As matrizes de riscos geradas nestes processos eram processadas em planilhas eletrônicas ou documentos elaborados pelos próprios gestores dos processos nucleares. Mesmo os processos que adoraram a ferramenta de Brainstorm proposta pela Diretoria de Planejamento, não ficou evidenciado que tal ferramenta faz parte de um sistema de tecnologia da informação, capaz de consolidar as informações em bancos de dados próprios.

Não ficou comprovado que os riscos identificados nestes processos passou a integrar algum sistema (a exemplo do Planede ou algum módulo específico).

O registro do plano de contingência dos riscos inerentes aos objetivos e metas estratégicos, disponível no sistema Planede, recebeu a última atualização em 18 de Fevereiro de 2017.

5.2.10.3 Causa

Falta de investimento em Tecnologia da Informação.

5.2.10.4 Manifestação do auditado

A unidade auditada, em resposta à Solicitação de Auditoria n. 01/2019, informou:

> A gestão de Riscos do IFPB integrada ao Planejameno Estratégico do IFPB, disponível em https://planejamento.ifpb.edu.br, menu "Riscos" onde consta o Mapeamento dos Macroprocessos Finalísticos.

5.2.10.5 Consequência

A ausência de sistema informatizado ou registro adequado para a gestão de riscos dificulta que as atividades de gestão de riscos sejam rastreáveis. No processo de gestão de riscos, os registros fornecem os fundamentos para a melhoria dos métodos e ferramentas, bem como de todo o processo.

5.2.10.6 Análise da Auditoria Interna

A rotina apontada pela gestão direciona para uma página web com uma matriz de riscos para os objetivos e metas estratégicos. Contudo, não representa efetivamente a existência de um sistema de informação que permita, pelo menos, a inclusão, alteração ou consulta de dados por usuários cadastrados.

5.2.10.7 Recomendação

Implementar sistema de tecnologia da informação próprio para a gestão de riscos.

5.2.11 Descrição Sumária: Monitoramento incipiente dos riscos.

5.2.11.1 Critério

IN-MP/CGU Nº 1/2016, Art. 11, V; Art. 16, VIII; ISO 31000:2009, 5.6; COSO 2013, Princípios 16 e 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 21/23.

5.2.11.2 Condição encontrada

Em consulta realizada a servidores do IFPB por meio de formulário eletrônico, especificamente se estes monitoram o alcance de objetivos, riscos e controles chaves em suas respectivas áreas de responsabilidade, obteve-se o resultado a seguir.

a) Se monitoram de modo contínuo, ou, pelo menos, frequente, por meio de indicadores chaves de risco, indicadores chaves de desempenho e verificações rotineiras, para manter riscos e resultados dentro das tolerâncias a riscos definidas ou variações aceitáveis no desempenho, obteve-se o seguinte resultado: 28,24% discordaram totalmente; 40% discordaram em parte, 27,06% concordaram em parte e 4,7% concordaram totalmente. 68,24% com viés de discordância.

b) Se há monitoramento por meio de autoavaliações periódicas de riscos e controles, que constam de um ciclo de revisão periódica estabelecido, obteve-se o que segue: 37,6% discordaram totalmente; 40% discordaram em parte; 18,8% concordaram em parte e 3,5% concordaram totalmente. 77,6% com viés de discordância.

c) Se a execução e os resultados desses monitoramentos são documentados e reportados às instâncias apropriados da administração e da governança. obteve-se: 38,82% discordaram totalmente, 36,47% discordaram em parte, 18,82% concordou em parte e 5,88% concordou totalmente. 75,29% das respostas tiveram viés de discordância.

O resultado foi restrito aos servidores que informaram não ocupar cargo de direção para afastar aqueles que não integravam a primeira linha de defesa.

O formulário foi encaminhado para a lista de e-mails tas@ifpb.edu.br, obtendo um total de 90 respostas. Destas, 85 preencheram os requisitos para esta questão.

5.2.11.3 Causa

Falha na concepção dos processos de monitoramento dos riscos.

5.2.11.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.11.5 Consequência

As atividades de monitoramento e comunicação na gestão de riscos possibilitam o amadurecimento e o aumento da efetividade da gestão de riscos na organização.

5.2.11.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.11.7 Recomendação

Instituir e difundir rotinas de monitoramento dos indicadores chaves de riscos e de desempenho; Instituir autoavaliações periódicas de riscos e controles; Documentar e comunicar às instâncias apropriadas os resultados destes monitoramentos.

5.2.12 Descrição Sumária: Ausência de atuação do Comitê de Gestão de Riscos do IFPB

5.2.12.1 Critério

IN-MP/CGU Nº 1/2016, Art. 11, V; Art. 16, VIII; ISO 31000:2009, 5.6; COSO 2013,

Princípios 16 e 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípios 21/23.

5.2.12.2 Condição encontrada

A Política de Gestão de Riscos do IFPB prevê a existência do Comitê de Gestão de Riscos. Sua composição e atribuições estão materializadas no Plano de Contingências disponível no sistema Planede.

Não ficou comprovada a nomeação dos membros do referido Comitê bem como a realização das atividades de sua competência.

5.2.12.3 Causa

Falha de governança quanto a formalização das instruções – designação dos membros.

5.2.12.4 Manifestação do auditado

A unidade auditada, em resposta à Solicitação de Auditoria n. 01/2019, informou:

> Existe a previsão do Comitê de Gestão de Riscos conforme a Portaria n° 2025/2017 e Portaria n° 1770/2018, todavia esta última estabelece o prazo da implantação até o dia 31 de dezembro de 2019.

5.2.12.5 Consequência

A falta de atuação efetiva de importantes órgãos da segunda linha de defesa na gestão de riscos pode comprometer a eficácia da gestão de riscos, especialmente quanto ao seu monitoramento objetivando avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos

5.2.12.6 Análise da Auditoria Interna

A manifestação da unidade auditada evidencia que atuação do Comitê de Riscos ainda está pendente de efetiva implementação.

5.2.12.7 Recomendação

Nomear os membros do Comitê de Gestão de Riscos para que estes atuem efetivamente desempenhando as atribuições previstas para o Comitê.

5.2.13 Descrição Sumária: Ausência de testes e revisões periódicas dos planos de contingência.

5.2.13.1 Critério

ISO 31000:2009, 5.6.

5.2.13.2 Condição encontrada

Em consulta ao sistema Planede, constatou-se a existência de plano de contingência para os objetivos e metas estratégicos intitulado Plano de Gerenciamento de Riscos (PGR). No documento

registra-se sua última atualização em 18 de fevereiro de 2017. Portanto, há, pelo menos, mais de 21 meses sem registro de atualizações.

5.2.13.3 Causa

Falha na definição e disseminação de instruções do processo de gerenciamento de riscos.

5.2.13.4 Manifestação do auditado

A unidade auditada, em resposta à Solicitação de Auditoria n. 01/2019, informou:

> A gestão de Riscos do IFPB integrada ao Planejamento Estratégico do IFPB, disponível em https://planejamento.ifpb.edu.br, menu "Riscos" contém a periodicidade de revisões: semestral e Anual dos macroprocessos finalísticos.

5.2.13.5 Consequência

A ausência de revisão periódica do plano de contingência pode trazer fragilidade as seguintes finalidades da boa gestão de riscos: a) garantia que os controles sejam eficazes e eficientes no projeto e na operação; b) obter informações adicionais para melhorar o processo de avaliação dos riscos; c) analisar os eventos (incluindo os "quase incidentes"), mudanças, tendências, sucessos e fracassos e aprender com eles; d) detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, as quais podem requerer revisão dos tratamentos dos riscos e suas prioridades; e e) identificar os riscos emergentes.

5.2.13.6 Análise da Auditoria Interna

A manifestação da unidade avaliada oportunamente registra a necessidade de revisões na gestão de riscos. Contudo, não evidencia que tais revisões efetivamente têm ocorrido.

5.2.13.7 Recomendação

Realizar revisão periódica do plano de contingência, de forma que os resultados do monitoramento e da análise crítica sejam registrados e reportados conforme apropriado, e também que sejam utilizados como entrada para a análise crítica da estrutura de gestão de riscos.

5.2.14 Descrição Sumária: Ausência de atividades efetivas de monitoramento da gestão de riscos e dos controles.

5.2.14.1 Critério

IN-MP/CGU Nº 1/2016, Art. 8º, XV; ISO 31000:2009, 4.5, 4.6 e A.3.1; COSO 2013, Princípio 17; COSO GRC 2004, 9; COSO GRC PE 2016, Princípio 23.

5.2.14.2 Condição encontrada

Em consulta a Diretoria de Planejamento sobre a ao sistema Planede, quanto à comunicação e implementação das medidas de correção das fragilidades encontradas nas atividades de monitoramento, não se evidenciou a realização de tal prática.

O sistema Planede prevê a aplicação de giro PDCA (planejar, fazer, verificar e ajustar)

para constante melhoria dos processos. Dentre os detalhamentos das etapas necessárias, estão previstas, entre outras medidas, a realização de planos de ações, mapeamentos e resoluções de problemas prioritários (matriz GUT e diagrama causa-efeito), além de reuniões de acompanhamentos de dados.

Contudo, a execução de tais medidas e a comprovação de sua atualização não ficou comprovada.

5.2.14.3 Causa

Falha na definição e disseminação de instruções do processo de gerenciamento de riscos.

5.2.14.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.14.5 Consequência

A ausência de atividades efetivas de monitoramento, em que os resultados são devidamente comunicados às instâncias apropriados da administração e da governança com autoridade e responsabilidade para adotar as medidas necessárias, assim como a ausência de elaboração de planos de ação para correção das deficiências encontradas fragilizam a busca contínua de melhoria dos processos da gestão.

5.2.14.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.14.7 Recomendação

Elaborar plano de ação para identificação de deficiências na gestão de riscos.

5.2.15 Descrição Sumária: Aplicação parcial do processo de gestão de riscos no âmbito das parcerias.

5.2.15.1 Critério

ISO 31000:2009, 4.3.3, A.3.2, 4.4.2, 5.4.2, a.3.2 e A.3.3; IN-MP/CGU Nº 1/2016, Art. 20 e 16, VII;

5.2.15.2 Condição encontrada

Em consulta a Diretoria de Planejamento quanto à gestão de riscos nas parcerias, foi informado que são consideradas apenas a gestão quanto aos fornecedores de bens e serviços selecionados por meio de processos licitatórios.

Em consulta ao site do IFPB, constata-se a formalização e vigência de outros tipos de

parcerias que não as decorrentes de processos de contratação de bens e serviços. A exemplo de convênios com entidades internacionais, disponível para consulta em http://www.ifpb.edu.br/relacoes-internacionais/parceiros/convenios-vigentes.

Mesmo no âmbito local, constatou-se a formalização de parceria com a Secretaria Municipal de Educação de João Pessoa visando o uso compartilhado das instalações da Escola Aruanda para funcionamento provisório do Campus Mangabeira, conforme notícia disponível em: www.ifpb.edu.br/noticias/2018/01/ifpb-celebra-parceria-com-prefeitura-de-joao-pessoa.

A Diretoria de Planejamento não indicou os controles inerentes à gestão de riscos nestas outras modalidades de parcerias.

5.2.15.3 Causa

Falha de governança quanto a definição de responsabilidades.

5.2.15.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.15.5 Consequência

A ausência de gerenciamento de riscos no âmbito das parcerias pode comprometer o alcance de seus objetivos, tendo em vista que não são identificados e tratados os riscos potenciais.

5.2.15.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.15.7 Recomendação

Aplicar o processo de gestão de riscos no âmbito de todas as parcerias.

5.2.16 Descrição Sumária: Ausência de registro único de riscos inerentes às parcerias.

5.2.16.1 Critério

ISO 31000:2009, 5.7 e 5.6 (final).

5.2.16.2 Condição encontrada

Em consulta a Diretoria de Planejamento quanto à gestão de riscos nas parcerias, foi informado que são consideradas apenas a gestão quanto aos fornecedores de bens e serviços selecionados por meio de processos licitatórios. Informou ainda que os riscos inerentes às parcerias são aqueles constantes do sistema PLANEDE, menu "Riscos".

No âmbito da Reitoria, o setor responsável pela formalização destas parcerias e o gerenciamento de seus riscos é o DCCL.

Solicitou-se, do DCCL, um processo de contratação sob a égide da IN 05/2017 (processo 23381.003160.2017-25, pregão 15/2017) para averiguação da formalização da gestão de riscos, nos termos da referida IN.

O mapa de riscos para a contratação estava devidamente formalizado. Entretanto, os riscos identificados no mapa autuado não estavam contemplados no módulo "Riscos" do Sistema PLANEDE, configurando controles paralelos.

5.2.16.3 Causa

Falha na concepção do processo de identificação de riscos.

5.2.16.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.16.5 Consequência

A ausência de sistema informatizado ou registro adequado para a gestão de riscos dificulta que as atividades de gestão de riscos sejam rastreáveis. No processo de gestão de riscos, os registros fornecem os fundamentos para a melhoria dos métodos e ferramentas, bem como de todo o processo.

5.2.16.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.16.7 Recomendação

Adotar registro único ou sistema de informação para a gestão de riscos, que contemple os riscos inerentes às parcerias.

5.2.17 Descrição Sumária: Ausência de planos e medidas de contingência no âmbito das parcerias.

5.2.17.1 Critério

"IN-MP/CGU Nº 1/2016, Art. 16, VI; ISO 31000:2009, 5.6."

5.2.17.2 Condição encontrada

Em consulta a Diretoria de Planejamento e ao sistema PLANEDE quanto a existência de plano de contingência no âmbito das parcerias constatou-se a seguinte situação.

A Diretoria de Planejamento indicou o menu Plano de Contingências e Riscos no sistema PLANEDE. O referido documento consubstancia a declaração formal da Política de Gestão Integrada de Riscos do IFPB e traz efetivamente plano e medidas de contingências. Entretanto, tal plano e medidas não são específicos com relação às parcerias. As duas únicas referências a parcerias constantes do plano são inerentes a riscos que dificultem a celebração de parcerias, não a manutenção ou continuidade das parcerias formalizadas.

Registra-se ainda que última atualização foi realizada em 18 de fevereiro de 2017.

5.2.17.3 Causa

Falha na concepção do processo de formalização de parcerias.

5.2.17.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.17.5 Consequência

A ausência de planos ou medidas de contingências no âmbito das parcerias pode comprometer a recuperação e a continuidade dos serviços decorrentes das parcerias realizadas.

5.2.17.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.17.7 Recomendação

Implementar planos de contingências no âmbitos das parcerias realizadas.

5.2.18 Descrição Sumária: Ausência de consciência sobre o nível atual de maturidade quanto à gestão de riscos.

5.2.18.1 Critério

IN-MP/CGU Nº 1/2016, Art. 8º, II; Arts. 19, 20, 21, parágrafo único, 22 e 23; ISO 31000:2009, 4.3.4 e A.3.5; COSO GRC 2004, 10. COSO GRC PE 2016, Princípio 1.

5.2.18.2 Condição encontrada

Em consulta à Diretoria de Planejamento e ao sistema PLANEDE quanto ao grau de consciência sobre o estágio atual da gestão de riscos, constatou-se o que segue.

A Diretoria de Planejamento está coordenando ações de capacitação e disseminação da gestão de riscos. Estes eventos objetivam além da capacitação quanto a gestão de riscos, a

declaração de ciência e comprometimento dos gestores quanto ao seu papel no gerenciamento de riscos, bem como a identificação dos riscos inerentes aos seus processos nucleares. O programa ainda não foi concluído.

Dentre os documentos já elaborados quanto à gestão de riscos, especialmente os constantes no sistema PLANEDE, não ficou evidenciado o registro do grau de maturidade da gestão de riscos na organização (inicial, básico, intermediário, aprimorado ou avançado, conforme classificação sugerida pelo TCU).

5.2.18.3 Causa

Falta de capacitação de pessoal.

5.2.18.4 Manifestação do auditado

Solicitada a se manifestar a Unidade Auditada não apresentou esclarecimentos, avaliações ou informações adicionais.

5.2.18.5 Consequência

A ausência de conhecimento sobre o nível atual de maturidade de gestão de riscos prejudica a definição de um progresso eficaz de ações que levem ao nível satisfatório quanto à gestão de riscos.

5.2.18.6 Análise da Auditoria Interna

Diante da ausência de manifestação da unidade examinada após a apresentação dos fatos, a análise do Controle Interno sobre a constatação consta registrada acima, no campo "condição encontrada".

5.2.18.7 Recomendação

Determinar o nível de maturidade da gestão de riscos, considerando as dimensões Ambiente, Processos, Parcerias e Resultados.

5. RESUMO DAS CONSTATAÇÕES E RESPECTIVAS RECOMENDAÇÕES

Nr	Constatação	Recomendação
1	Ausência de atuação do Comitê de Gestão de Riscos.	Atuação efetiva de comitê responsável pela supervisão e monitoramento dos controles internos com vistas a aprimorar a gestão de riscos no âmbito do IFPB.
2	Ausência de revisão sistemática da visão de portfólio de ricos e notificação regular e oportuna sobre as exposições da organização a riscos.	Instituir rotinas de revisão do portfólio de riscos pela alta administração e de notificação regular e oportuna sobre as exposições da organização a riscos
3	Baixo entendimento entre as	Difundir as responsabilidades sobre a gestão de riscos

	pessoas da organização sobre suas responsabilidades no gerenciamento de riscos.	entre todos os atores da organização.
4	Necessidade de capacitação aos gestores da primeira linha de defesa.	Capacitar os gestores da primeira linha de defesa para a condução do processo de gestão de riscos.
5	Utilização de formulário para identificação de riscos sem a verificação da probabilidade e causa dos eventos.	Adotar ferramenta padronizada de identificação de riscos que contemple a análise da probabilidade de ocorrência dos eventos bem como suas possíveis causas.
6	Ausência de elementos que apoiariam o adequado gerenciamento dos riscos.	Fazer constar, no registro de riscos, pelo menos os seguintes elementos: i) o escopo do processo, da atividade, da iniciativa estratégica ou do projeto coberto pela identificação e análise; ii) os participantes das atividades de identificação e análise de riscos; iii) a abordagem ou o método de identificação e análise utilizado, as especificações utilizadas para as classificações de probabilidade e impacto e as fontes de informação consultadas; v) a probabilidade de ocorrência de cada evento, a severidade ou magnitude do impacto nos objetivos e a sua descrição, bem como considerações quanto à análise desses elementos; v) os níveis de risco inerente resultantes da combinação de probabilidade e impacto, além de outros fatores que a entidade considera para determinar o nível de risco; vi) a descrição dos controles existentes, as considerações quanto à sua eficácia e confiabilidade; e vii) o risco residual
7	Ausência de definição de critérios para priorização de riscos.	Estabelecer critérios para orientar as decisões sobre riscos em relação a todas as operações, funções e atividades relevantes da organização e que os critérios levem em conta fatores como 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, critérios de comunicação a instâncias competentes, o tempo de resposta requerido e que possibilitem orientar decisões quanto a se: i) um determinado risco precisa de tratamento e a prioridade para isso; ii) uma atividade deve ser realizada, reduzida ou descontinuada; iii) controles devem ser implementados, modificados ou apenas mantidos.
8	Ausência de avaliação do custo-benefício quanto as medidas de respostas aos riscos.	Avaliar o custo-benefício de todas as opções de tratamento dos riscos.
9	Insuficiência na documentação da avaliação e seleção das respostas a	Documentar os atos de avaliação e seleção das respostas a riscos com pelo menos os seguintes

	riscos	elementos: i) o plano de tratamento de riscos, preferencialmente integrado ao registro de riscos, identificando claramente os riscos que requerem tratamento, suas respectivas classificações (probabilidade, impacto, níveis de risco etc.), a ordem de prioridade para cada tratamento; ii) as respostas a riscos selecionadas e as razões para a seleção, incluindo justificativa de custo-benefício; as ações propostas, os recursos requeridos, o cronograma e os benefícios esperados; iii) as medidas de desempenho e os requisitos para o reporte de informações relacionadas ao tratamento dos riscos, e as formas de monitoramento da sua implementação; iv) a identificação dos responsáveis pela aprovação e pela implementação de cada ação do plano de tratamento, com autoridade suficiente para gerenciá-las.
10	Ausência de sistema de tecnologia da informação próprio para gestão de riscos.	Implementar sistema de tecnologia da informação próprio para a gestão de riscos.
11	Monitoramento incipiente dos riscos.	Instituir e difundir rotinas de monitoramento dos indicadores chaves de riscos e de desempenho; Instituir autoavaliações periódicas de riscos e controles; Documentar e comunicar às instâncias apropriadas os resultados destes monitoramentos.
12	Ausência de atuação do Comitê de Gestão de Riscos do IFPB	Nomear os membros do Comitê de Gestão de Riscos para que estes atuem efetivamente desempenhando as atribuições previstas para o Comitê.
13	Ausência de testes e revisões periódicas dos planos de contingência.	Realizar revisão periódica do plano de contingência, de forma que os resultados do monitoramento e da análise crítica sejam registrados e reportados conforme apropriado, e também que sejam utilizados como entrada para a análise crítica da estrutura de gestão de riscos.
14	Ausência de atividades efetivas de monitoramento da gestão de riscos e dos controles.	Elaborar plano de ação para identificação de deficiências na gestão de riscos
15	Aplicação parcial do processo de gestão de riscos no âmbito das parcerias.	Aplicar o processo de gestão de riscos no âmbito de todas as parcerias.
16	Ausência de registro único de riscos inerentes às parcerias.	Adotar registro único ou sistema de informação para a gestão de riscos, que contemple os riscos inerentes às parcerias.
17	Ausência de planos e medidas de contingência no âmbito das parcerias.	Implementar planos de contingências no âmbitos das parcerias realizadas.
18	Ausência de consciência sobre o	Determinar o nível de maturidade da gestão de riscos,

	nível atual de maturidade quanto à gestão de riscos.	considerando as dimensões Ambiente, Processos, Parcerias e Resultados.

6. CONCLUSÃO

De acordo com os fatores e informações que a equipe de auditoria teve acesso durante o trabalho, podemos concluir que a gestão de riscos no IFPB, em linhas gerais, possui uma boa base de ferramentas que permitiria sustentar uma gestão de riscos mais madura e efetiva, tendo em vista que na atual configuração a efetivação da gestão de riscos está incipiente.

Muitas dessas estruturas foram implementadas com o advento do planejamento decenal – PLANEDE, a exemplo das ferramentas de direcionamento estratégico e da instituição formal da política de gestão de riscos.

Em contrapartida, constatou-se oportunidades de melhora na efetiva implementação da gestão de riscos, na capacitação e disseminação da cultura de riscos em todos os níveis da organização bem como na adoção de processos e ferramentas mais avançados na operacionalização da gestão de riscos.

A realização da presente auditoria oportuniza um momento de adequação mais eficiente das ações na gestão de riscos, vez que identifica no estágio inicial da implementação da gestão de riscos pontos a serem refinados.

Diante do exposto, para implementar as ações visando aprimorar os controles, torna-se imprescindível a atuação conjunta dos diversos setores estratégicos com o dirigente máximo do IFPB.

João Pessoa, 11 de novembro de 2019.

Bruno Rodrigues Cabral
Auditor Interno Geral
Matrícula 1115863

Kléber Cordeiro Costa
Auditor Interno
Matrícula 2736382