INFRA S.A.

RELATÓRIO DE AVALIAÇÃO Nº 1566877
AUDITORIA INTERNA

Tema: Nível de Implementação dos Planos de Ação

Unidade examinada: DIRETORIA EXECUTIVA/SUINT

Exercício: 2024

Missão da INFRA S.A

Planejar, projetar e executar de forma eficiente, sustentável e inovadora a infraestrutura de transporte e logística do Brasil buscando a melhoria de vida das pessoas.

Visão da INFRA S.A

Ser referência no Brasil em planejamento e projetos de infraestrutura e logística.

Valores da INFRA S.A

Excelência; Respeito à Vida; Eficiência Logística; Sustentabilidade; Integridade; Inovação; e Valorização das pessoas.

Auditoria Interna Governamental

Atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização; deve buscar auxiliar a Infra S.A a realizar seus objetivos, a partir 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.

QUAL FOI O TRABALHO REALIZADO PELA INFRA S.A?

Em cumprimento ao Plano Anual de Auditoria Interna – PAINT/2024 e com base nas Normas Internacionais de Auditoria Interna emitidas pelo *The Institute of Internal Auditors (The IIA)* e normas internas de auditoria, avaliou-se o nível de implementação dos Planos de Ação, visando reduzir/mitigar os riscos estratégicos

POR QUE A INFRA S.A REALIZOU ESSE TRABALHO?

A razão para que a auditoria incluísse no PAINT/2024 este trabalho foi garantir que as medidas definidas para mitigar esses riscos estejam sendo aplicadas de maneira eficaz e dentro do prazo.

Uma auditoria nessa área é essencial para garantir que a organização está preparada para enfrentar e mitigar riscos estratégicos, alinhando a execução dos planos de ação aos objetivos de longo prazo da empresa.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA INFRA S.A?

A Auditoria Interna concluiu que o nível de implementação dos Planos de Ação para mitigação de riscos estratégicos apresenta avanços significativos em diversas áreas, mas ainda requer melhorias em pontos críticos. A análise demonstrou que o processo de gerenciamento de riscos adota práticas relevantes, com base em normativos internos e internacionais, mas enfrenta lacunas que podem comprometer a eficácia plena do sistema.

QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

Recomenda-se a documentação completa das etapas de identificação dos riscos, conforme normativos internos.

Sugere-se a implantação de um plano abrangente de contingência e continuidade de negócios que possa suportar eventos inesperados.

Recomenda-se a implementação de trilhas de capacitação abrangentes em gerenciamento de risco e controles internos para toda a organização.

As melhorias sugeridas visam fortalecer a governança, reduzir lacunas nos processos de gestão de riscos e aumentar a resiliência organizacional. Espera-se que a adoção das recomendações possibilite decisões mais informadas, maior eficiência operacional e melhor alinhamento estratégico.

LISTA DE QUADROS

SUMÁRIO

1. INTRODUÇÃO

1.1. Apresentação

O presente trabalho, foi realizado em cumprimento ao Plano Anual de Auditoria Interna – PAINT/2024, tendo como objeto o Nível de Implementação dos Planos de Ação visando reduzir/mitigar os riscos estratégicos**,** em observância às normas aplicáveis ao desempenho da atividade de auditoria interna emitidas pela Controladoria-Geral da União e pelo *The Institute of Internal Auditors (IIA)*.

O trabalho foi realizado junto à Superintendência de Integridade e Riscos – SUINT, responsável pela Segunda Linha do controle interno da Infra S.A. e que atua no apoio, supervisão e monitoramento das atividades desenvolvidas pela Primeira Linha, onde foram envolvidas as cinco diretorias da Empresa.

Nesta auditoria, o foco se deu em avaliar as ações e controles implementados para gerenciamento dos riscos estratégicos e acompanhamento dos Planos de Ação.

1.2. Objeto

O objeto da presente auditoria foi selecionado no Plano Anual de Auditoria Interna (PAINT) para o exercício 2024 visando avaliar o processo de gerenciamento de riscos institucionais, em específico, a efetividade dos Planos de Ação para mitigação/redução de Riscos Estratégicos, examinando se o gerenciamento dos riscos estratégicos se mostra adequado ao alcance dos objetivos da organização, se estão sendo cumpridos conforme previsto e analisar se as ações implementadas estão alcançando o efeito esperado na mitigação do risco reduzindo o grau de exposição da empresa.

1.3. Objetivos

1.3.1. Objetivo geral

O objetivo geral desta auditoria consiste na avaliação do nível de implementação dos Planos de Ação para o atingimento dos objetivos estratégicos da Empresa. O trabalho também contribui para que a Auditoria Interna possa expressar opinião geral, sobre a adequação dos processos de governança, gestão de riscos e controles internos instituídos pela empresa, no que se refere à conformidade legal dos atos administrativos, bem como ao atingimento dos objetivos operacionais, nos termos exigidos pelo mencionado artigo 16 da IN/SFC/CGU nº 05/2021.

1.3.2. Objetivos específicos

A partir do objetivo geral deste trabalho de auditoria e considerando os critérios estabelecidos, as questões de auditoria foram formuladas de acordo com a natureza do assunto.

- O processo de gestão de riscos contempla prévia etapa de estabelecimento dos contextos interno e externo onde a Unidade opera de forma a atingir seus objetivos?

- A etapa de identificação dos riscos fornece informações sobre os riscos relevantes do objeto, incluindo suas causas, eventos e consequências que possam impactar o atingimento dos objetivos?

- Os riscos identificados são adequadamente analisados em termos de probabilidade de ocorrência, de impacto nos objetivos e do risco dos controles?

- O tratamento dos riscos está sendo realizado de forma tempestiva, eficiente, eficaz e suficiente?

- As unidades possuem pessoas capacitadas e em quantitativo suficiente para monitoramento dos planos de tratamento?

- Existe adequado acompanhamento e monitoramento dos riscos e controles-chave pelas áreas responsáveis e alta direção?

- A Empresa possui plano de continuidade de negócios adequadamente estruturado?

1.4. Escopo

A equipe de auditoria definiu como escopo a avaliação dos Riscos Estratégico e dos respectivos planos de ação. Para análise dos pontos, a equipe de auditoria, em conjunto com representantes de cada área, identificou os riscos mais prováveis de se materializarem entre os 14 riscos elencados, considerando o desenvolvimento dos projetos em cada setor.

- Risco 1 - Redução do ritmo de obras em função de impeditivos e não liberação de frentes pela Infra S.A.
- Risco 2 - Riscos de licitações estratégicas
- Risco 3 - Riscos de gestão contratual
- Risco 4 - Descumprimento ou atraso para atendimento de demandas de projetos e custos de engenharia
- Risco 5 - Não ingresso de benefícios financeiros oriundos de subconcessões e outras atividades econômicas da empresa
- Risco 6 - Saída da participação na TLSA com possível impacto financeiro à Infra S.A.
- Risco 7 - Riscos de integridade
- Risco 8 - Falhas no controle e governança das obrigações definidas no Anexo 9 no âmbito do Investimento Cruzado da FICO
- Risco 9 - Falta de dados e informações no processo de elaboração e conclusão do PNL 2055
- Risco 10 - Carteira priorizada de projetos não entregue pelos planos setoriais
- Risco 11 - Paralisação na elaboração/acompanhamento de estruturação de projetos de concessão em andamento
- Risco 12 - Formalização e implementação pela Infra S.A. da plataforma de informação DT-e
- Risco 13 - Ausência de instrumentos para fortalecimento da utilidade estratégica do Observatório Nacional de Transporte e Logística (ONTL)
- Risco 14 - Não execução do empreendimento subtrecho Salgueiro/PE e Porto SUAPE/PE pela Infra S.A.

Os riscos foram subdivididos conforme os processos de cada diretoria. Após esse

levantamento, a equipe de auditoria aplicou os testes substantivos cujos resultados e análises serão apresentadas no item 2 – *"Resultado de Exames"*.

Quadro 1 - Relação de diretorias, processos e riscos gerenciados

Diretoria	Processo administrativo	Riscos estratégicos
DIMEI	50050.003314/2023-41	2, 3, 7, 12 e 13
DIRAF	50050.003311/2023-16	2, 3, 5 e 7
DIREM	50050.003312/2023-52	1, 2, 3, 4, 5, 6, 7, 8 e 14
DIPLAN	50050.003313/2023-05	2, 3, 7, 9, 10 e 11
PRESI	50050.003292/2023-10	7

Fonte: AUDIN.

No que pese este trabalho ter sido realizado sobre os 14 riscos estratégicos, no decorrer do processo, o CONSAD realizou uma revisão e reavaliação desses riscos, resultando na consolidação e redução para 8 riscos estratégicos. Essa alteração foi baseada em critérios técnicos e estratégicos, buscando aprimorar a gestão e o monitoramento dos principais riscos da empresa:

Quadro 2 – Processo de Gestão de Riscos Estratégicos 2024

Unidade	Risco Estratégico
DIREM	Risco 1 - Redução do ritmo de obras em função de impeditivos e não liberação de frentes por outros órgãos envolvidos
DIRAF	Risco 2 - Ausência de definição formal das receitas da INFRA junto à ANTT, com o consequente não ingresso de benefícios financeiros oriundos de subconcessões e de outros serviços prestados pela empresa
DIREM	Risco 3 - Falhas no controle e governança das obrigações definidas no Anexo 9 no âmbito do Investimento Cruzado da FICO
DIREM	Risco 4 - Não execução de obras na EF-232 do subtrecho Salgueiro/PE e Porto SUAPE/PE pela Infra S.A.
DIREM	RISCO 5 - Saída da participação na TLSA com possível impacto financeiro à Infra S.A.
DIMEI	Risco 6 - Descumprimento ou atraso na elaboração dos Planos Integrantes do PIT
DIPLAN	Risco 7 - Paralisação na elaboração/acompanhamento de estruturação de projetos de concessão em andamento
DIMEI	Risco 8 - Base de dados do Observatório Nacional de Transporte e Logística (ONTL) não integrada às informações oficiais dos processos de estudos e do planejamento de transportes desenvolvidos pela INFRA S.A

Fonte: AUDIN.

1.5. Montante fiscalizado

A avaliação da conformidade não se mostrou aplicável à definição de valores sob fiscalização nesta auditoria, a qual se refere ao aspecto qualitativo e processual.

1.6. Metodologia

Os procedimentos e técnicas usados na execução do presente trabalho de avaliação estão registrados na Matriz de Planejamento, considerando as Normas Internacionais de Auditoria Interna emitidas pelo *The IIA* e normativos internos. As principais técnicas utilizadas nos testes foram a realização de reuniões com redução a termo e a análise documental.

1.7. Critérios de auditoria

Os principais normativos aplicáveis ao objeto da auditoria são:

a) Resolução CGPAR nº 48, de 6 de setembro de 2023;

b) Política de Gestão de Riscos e Controle Interno;

c) Manual e Tutorial de Gestão de Riscos;

d) Norma ABNT NBR ISO/IEC 31.000/2018; e

e) Norma ABNT NBR ISO/IEC 31.010/2021.

1.8. Avaliação de riscos e controles

Com o objetivo de orientar a extensão dos testes realizados durante a execução da auditoria, a equipe de auditoria realizou a avalição dos riscos e a estrutura básica dos controles internos por meio da metodologia disponibilizada pela CGU, a qual foi estabelecida para dar suporte as Unidades de Auditorias Internas Governamentais em seus processos de auditorias, conforme dispõe o papel de trabalho da Matriz de Riscos e Controles (MRC).

1.9. Contextualização

O gerenciamento de riscos, conforme definição em norma, é um processo estruturado com vistas à identificação, análise, avaliação e tratamento dos eventos de riscos, de forma a fornecer razoável certeza quanto ao alcance dos objetivos da organização.

Na Infra S.A., a matéria está regulamentada por meio da Política de Gestão de Riscos e Controles Internos, aprovada por meio da Resolução nº 11/2023 do Conselho de Administração (CONSAD), do Conselho de Administração, o Manual de Gestão de Riscos e o Tutorial de Gestão de Riscos, aprovados pela Resolução CONSAD nº 12/2022.

O Manual apresenta os conceitos, as responsabilidades e atribuições das três linhas que compõe a estrutura de gestão de riscos e controles internos no âmbito da Infra S.A., as etapas do processo de gestão de riscos conforme ABNT NBR ISO 31000:2018 e, para fins de caracterização, os níveis e categorias dos riscos. Por sua vez, o Tutorial de Gestão de Riscos apresenta a abordagem das diversas referências normativas utilizadas como base no desenvolvimento da metodologia e as etapas a serem perseguidas pelos gestores para o completo processo de gerenciamento dos riscos.

Para desenvolvimento das responsabilidades e atribuições das três linhas, foram utilizados: o Modelo das Três Linhas do Instituto de Auditores Internos (traduzido de *The Institute of Internal Auditors-IIA,* 2020); Estatuto Social; Instrução Normativa Conjunta CGU/MP (Controladoria-Geral da União e Ministério do Planejamento, Orçamento e Gestão) nº 01, de 10 de maio de 2016; e o Regimento Interno da Auditoria Interna, Resolução CONSAD nº 7/2020.

Destaca-se que a Superintendência de Integridade e Riscos (SUINT) é a responsável pelo apoio e suporte metodológico para a gestão de riscos e controles internos nas unidades organizacionais, sendo operacionalizado pela sua Gerência de Riscos e Controles (GRCOI). Por conseguinte, na condução do processo de gestão de riscos, a GRCOI/SUINT realiza oficinas de instrução e oficinas de campo com as diretorias e superintendências, com a aplicação dos normativos relacionados.

2. RESULTADOS DOS EXAMES

Para verificar a efetividade dos planos de tratamento aos riscos estratégicos, o trabalho foi estruturado de forma segmentada, pela ordenação natural do processo de gerenciamento de riscos, seguindo suas etapas desde a contextualização e identificação dos riscos até seus efetivos tratamentos. Sendo assim, o gerenciamento e mitigação dos riscos estratégicos só poderia ser considerado efetivo se todos o processo estiver alinhado às normas e boas práticas, não somente com a execução dos planos de tratamento já aprovados.

Passa-se então a apresentar os resultados das análises para cada etapa.

2.1. Estabelecimento de contexto

Para o estabelecimento de contexto levou-se em consideração a análise das respostas apresentadas pela área oriundas da S.A. nº 1 onde busca responder se o processo de gestão de riscos contempla prévia etapa de estabelecimento dos contextos interno e externo onde a Unidade opera de forma a atingir seus objetivos.

Para tal, foram aplicados os seguintes testes:

- Identificar se houve análise de contextos interno e externo no processo de identificação dos riscos estratégicos.
- Verificar a abrangência da análise de contexto da organização (ambientes internos e fatores positivos e negativos).

Ao se avaliar o processo de gestão de risco, observou-se que a área se preocupou com a uma análise prévia do estabelecimento dos contextos interno externo vislumbrando o atingimento dos objetivos.

Para isso a área utilizou como base os instrumentos de estratégia da Infra que são: Planejamento Estratégico, Plano de Negócios, Mapa Estratégico e relatórios trimestrais relacionados com a Reunião de Avaliação Estratégica (ERA); os planos que envolvem planejamento orçamentário, tais como: Plano Plurianual-PPA, Lei Orçamentária Anual e Plano de Contratação Anual - PCA da empresa, os processos e relatórios de auditoria do Tribunal de Contas da União – TCU que envolvem empreendimento Infra S.A bem como, as notícias da mídia relacionadas com os empreendimentos que a Infra S.A. tem participação.

Diante do exposto, a AUDIN entende que a elaboração dos riscos contempla fatores relevantes, onde quanto mais precisa for a análise, menos surpresas e imprevistos a Infra deverá enfrentar no decorrer do projeto, além do fato que esta análise permite o desenvolvimento de estratégias adequadas para o gerenciamento dos riscos. Contudo, os elementos utilizados para a análise e para a construção dos riscos não estão registrados, não deixando claro os parâmetros que descrevem especificamente como o ambiente interno e externo foram analisados e considerados.

Já considerando a abrangência da análise do contexto dentro da organização ela utiliza fontes variadas permitindo uma compreensão holística dos riscos e oportunidades que afetam a organização o que facilita a identificação e gestão de riscos de maneira informada e proativa.

2.2. Identificação dos riscos

Para avaliar a etapa de identificação dos riscos foram aplicadas as seguintes verificações:

- Verificar relatórios de risco e processos relacionados para identificar se houve identificação completa dos riscos conforme critérios.
- Verificar relatórios de risco e processos relacionados para identificar se houve identificação completa dos riscos relacionados aos objetivos estratégicos estabelecidos e se estão abarcados por seus respectivos planos de tratamento.

As verificações visaram aferir se a etapa de identificação dos riscos fornece informações sobre os riscos relevantes do objeto, incluindo suas causas, eventos e consequências que possam impactar o atingimento dos objetivos. Portanto, em face ao achado que se apresenta na sequência, responde-se que há lacunas de informação que podem impactar o atingimento dos objetivos.

2.2.1. Achado de auditoria: Registros da identificação de riscos estão incompletos.

Critério

Tutorial de Gestão de Riscos, item 5.2 – Resolução CONSAD nº 12/2022.

NBR ISO 31.000/2018, item 6.4.2.

Análise e evidência

No processo administrativo estão registrados os relatórios de riscos, porém o registro da "*Tabela 1 - Identificação de riscos*" (item 5.2 do Tutorial de Gestão de Riscos) não está instruído nos autos. Deste modo, o tipo e a categoria dos eventos de riscos não estão sendo contemplados no processo da gestão de riscos, estando assim em desconformidade com os normativos.

Nos registros das oficinas instruídos nos autos, restam identificados somente os riscos a serem gerenciados, ou seja, aqueles para os quais a Instituição estabelece medidas mitigatórias por meio de planos de tratamento, além dos controles internos já existentes. Deste modo, o processo de identificação de riscos não se demonstra exaustivo, identificando e documentando a completude dos riscos relacionados às funções, objetos, projetos e objetivos institucionais.

A exemplo, relacionando os 14 riscos estratégicos gerenciados aos objetivos estratégicos, constata-se que certos objetivos estratégicos não possuem riscos gerenciados em nível estratégico. São os seguintes objetivos: *"1.3 Implementar e valorizar as iniciativas ambientais e sociais"*, relacionado à responsabilidade ambiental; e *"3.2 Desenvolver, valorizar, atrair e reter talentos"*, relacionado à governança e gestão de pessoas.

A identificação dos riscos estratégicos traz confusão pois dos 14 riscos gerenciados, 11 são identificados como eventos de risco específicos, enquanto os outros 3 são identificados por categorias (RE02 Risco de contratação, RE03 Risco de gestão contratual e RE07 Risco de Integridade), sem, no entanto, explicitar o rol de eventos de risco associados.

Ainda, não foram identificados registros das consequências atribuídas aos riscos

identificados. Em que pese as causas e as consequências serem tratadas nas oficinas de instrução, conforme prevê a norma, a unidade responsável somente registra no mapa de riscos as causas.

A ausência das informações indica uma lacuna na documentação e no monitoramento do plano de tratamento de riscos. Sem os registros não se pode afirmar que as ações do plano de tratamento também tragam olhar às consequências (efeitos) da materialização dos riscos ou à dimensão "impacto" dos eventos, o que pode comprometer também eventuais ações de contingenciamento.

Causa

São possíveis causas para o risco-chave materializado e identificado: a baixa proficiência, a inadequação dos fluxos de trabalho do processo e a ausência de estratégia e objetivos para o processo de gestão de riscos e controles.

Efeito

Tem como efeitos ao presente achado: a existência de riscos descobertos pelo processo de gestão ou riscos não relacionados aos objetivos da empresa, com consequente comprometimento de todo o processo de gerenciamento de riscos institucionais.

Manifestação das Unidades examinadas

As oficinas de gestão de riscos são realizadas trimestralmente, seguindo a Metodologia do Manual e Tutorial de Riscos, em conformidade com a ISO 31.000/2018.
O resultado dos dados, atualizações e informações geradas ficam registradas em e-mails encaminhados às unidades organizacionais. Os temas discutidos, novos riscos e monitoramento das ações também ficam registrados nestes e-mails.
A partir destas informações são gerados o Mapa de Gestão de Risco anexados aos respectivos processos abertos por diretoria.
Portanto, os registros e documentação gerada são os e-mails e Mapas acostados aos processos.
A partir dos Mapas de Gestão de Riscos, a SUINT elabora o relatório semestral para Diretoria Executiva e Conselho de Administração.
Em análise ao relatório, a SUINT concorda com a auditoria no sentido de adicionar mais informações ao Mapa de Gestão de Riscos, em destaque: Objetivo Estratégico Relacionado, tipo e categoria. No que concerne às consequências algumas informações podem ser sensíveis para ampla divulgação, pois envolvem diretamente as políticas públicas da empresa, nesse sentido sugerimos a anexação em repositório e banco de dados da SUINT.
Outro ponto que a SUINT pode adotar como ação para melhoria do gerenciamento de riscos e registros, é acostar todos os e-mails encaminhados aos processos.

Manifestação da Auditoria Interna

A manifestação acatada.

Recomendações

1) A etapa de identificação dos riscos no processo de gerenciamento, por meio das oficinas, deve estar documentada de modo a garantir completa rastreabilidade da informação, realizando as atividades previstas no normativo interno e instruindo os artefatos necessários ao processo administrativo, tal como a Tabela de Identificação dos Riscos, de modo a demonstrar o

exaurimento da identificação de todos os eventos possíveis relacionados aos empreendimentos, programas, negócios, objetivos, dentre outros, assim como as consequências relacionadas.

Benefícios esperados

Com isso, espera-se obter um processo de gerenciamento de riscos mais completo e coeso, mitigando eventuais lacunas de informação e de cobertura do monitoramento.

2.3. Análise e avaliação dos riscos

A seguinte etapa diz respeito à análise e avaliação dos riscos, que compreende o cálculo do grau de exposição da empresa aos eventos de risco identificado, sendo o grau de exposição (nível de risco) calculado a partir de critérios de probabilidade e impacto.

Para esta etapa de análise dos riscos, foram aplicados os seguintes testes com o fito de aferir se os riscos identificados são adequadamente analisados em termos de probabilidade de ocorrência, de impacto nos objetivos e do risco dos controles:

- Verificar relatórios de risco e processos relacionados para identificar se as métricas para mensuração de impacto e probabilidade são adequadas à realidade dos processos.
- Verificar se foram identificados todos os controles existentes/relevantes para o processo.
- Verificar a suficiência e a compatibilidade dos controles existentes com o risco de controle para redução do risco inerente.

Conforme a norma vigente, para o cálculo do grau de exposição de cada evento de risco são atribuídos valores a partir de uma escala de probabilidade e impacto. Estes valores são definidos de acordo com informações e a percepção dos gestores acerca do evento de risco. Registra-se que tanto a escala de probabilidade quanto a de impacto se dão por método semiquantitativo, atribuindo uma classificação numérica logarítmica para cada nível de significância dos fatores do produto "Nível de Risco".

Segundo preconiza a ABNT NBR ISO/IEC 31010, quando a análise é qualitativa, convém que exista uma explicação clara de todos os termos empregados e que a base para todos os critérios seja registrada. Portanto, se faz oportuna a melhoria em se registrar no documento *"Mapa de Risco"* o critério utilizado para escolha dos níveis de significância dos fatores probabilidade e impacto.

É também uma oportunidade de melhoria ao processo de gerenciamento de riscos, em específico nesta etapa de análise e avaliação dos riscos, conforme o nível de maturidade em gestão de riscos da organização aumenta, aprimorar as escalas de modo a evitar a subjetividade da análise qualitativa ou semiquantitativa, passando a considerar também escalas quantitativas para os atributos "probabilidade", a medida em que se dispõe de registro de séries históricas para determinado objeto em análise, e "impacto", conferindo faixas de valores financeiros adequados à realidade do objeto e da empresa, quando possível.

Conforme demonstram os relatórios de risco (mapas de risco), a maior parcela dos riscos estratégicos (8 em 14) foi identificada e analisada sem considerar qualquer controle interno existente. O fato reforça a necessidade de execução dos planos de tratamento e implementação de controles para retroalimentação do processo de identificação e análise.

Pode-se afirmar que as Unidades examinadas foram conservadoras na análise e avaliação dos riscos. Contatou-se que, com exceção ao risco estratégico 9, foram aplicados riscos de controles elevados, que potencializaram os níveis dos riscos residuais, e na maior parte das ocorrências em razão da inexistência de controles. Contudo, a Administração optou ainda por considerar o tratamento dos riscos mesmo para aqueles que tiveram um resultado residual dentro do apetite a riscos da empresa, conforme depreende-se do Relatório de Riscos, Controles e Integridade 3° Tri/2023 (7648408):

> De acordo com a Tabela 1 - Processo de Gestão de Riscos Estratégicos, constata-se que 7 dos 13 eventos de riscos estratégicos, estão avaliados com o nível de risco residual além do apetite a riscos da companhia. Portanto, destaca-se a necessidade de implementação das ações e controles internos dos planos de tratamento pela primeira linha de defesa, principalmente no que tange aos riscos estratégicos. Todos os riscos estratégicos são objeto de ações em planos de tratamento. (Original sem grifo)

Destarte, é possível afirmar que os riscos identificados são adequadamente analisados em termos de probabilidade de ocorrência, de impacto nos objetivos e do risco dos controles.

2.4. Tratamento dos riscos

Nesta etapa de análise do tratamento de risco, foram aplicados os seguintes testes:

- Verificar relatórios de risco e processos relacionados para identificar se houve completa cobertura dos riscos estratégicos por planos de tratamento.
- Verificar a relação custo x benefício dos planos de tratamento. Se houve análise para definição das ações.
- Verificar se a execução dos planos de tratamento retroalimentou o processo de gestão de riscos e a suficiência das ações para redução dos riscos inerentes.
- Verificar se as ações do plano de tratamento tratam também as consequências dos riscos.
- Verificar a existência de plano de contingência ou de continuidade dos negócios e sua adequabilidade ao processo relacionado.

Como já trazido no item 2.2.1 deste Relatório, não são todos os objetivos estratégicos que têm seus riscos gerenciados em nível estratégico. Contudo, foi possível identificar que para todos os riscos monitorados existem planos de tratamento relacionados, abrangendo uma ou mais ações de melhoria dos controles internos existentes.

Não obstante existam planos de tratamento para todos os riscos estratégicos que foram identificados, não há registros que demonstrem a utilização de análise de custo dos controles *versus* benefícios implementados (redução dos níveis de probabilidade e/ou impacto ou redução do risco de controle) para definição das ações de tratamento. A Unidade informou que em razão de não existir centro de custos, não se faz possível dimensionar o custo das ações internas às unidades organizacionais e que, para as ações que envolvam execução de contratos, o custo fica associado ao montante necessário para a efetiva contratação.

Com relação ao ciclo da gestão de riscos, a Unidade responsável pela Segunda

Linha demonstrou por meio de fluxograma a forma pela qual as análises dos riscos e execução dos planos de tratamento retroalimentam o processo. Informou ainda que *"em eventual situação de materialização do risco, é realizada uma nova análise de contexto e as ações e controles são revisadas no mesmo Mapa de Gestão de Riscos. Portanto é elaborado um novo plano de tratamento no mesmo Mapa de Gestão de Riscos."*. Não identificamos, contudo, a forma como é registrada a materialização dos eventos de riscos.

Pode-se afirmar, portanto, que o tratamento dos riscos está sendo realizado de forma tempestiva, eficiente e eficaz. Entretanto, apresenta-se ressalva com relação às medidas de contingenciamento em caso de materialização dos eventos de riscos.

2.4.1. Achado de auditoria: Ausência do Plano de Contingência ou Continuidade do Negócio

Critério

Resolução CGPAR nº 48/2023, Art. 23º item IX:

> *IX- Fornecer apoio técnico e metodológico para que os gestores responsáveis pelos principais processos de trabalho da organização identifiquem seus respectivos riscos e estabeleçam planos de contingência ou de continuidade de negócios;*

Análise e Evidência

Durante a análise, constatou-se a ausência de um plano de contingência formalmente elaborado e implementado. Essa lacuna pode comprometer a capacidade de resposta da organização diante de situações inesperadas, como falhas operacionais, emergenciais ou incidentes que impactem a continuidade das atividades.

Embora a Unidade tenha destacado *"que para alguns riscos já estão previstas no plano as ações de contingências"*, as ações constantes nos planos de tratamento apresentados se caracterizam como ações de tratamento/controle. Ações de contingência são ações a serem tomadas na ocasião dos danos começarem a ocorrer com a materialização dos riscos previstos. Isto é, são medidas tomadas para lidar com emergências ou crises, visando minimizar os danos e garantir a continuidade das operações. Essas ações são planejadas antecipadamente e fazem parte do plano de contingência de uma empresa.

Constatou-se que a forma de trabalho utilizada pela SUINT é de, em caso de materialização de um evento de risco gerenciado, realizar nova análise de contexto e ajustar as ações do plano de tratamento, não dispondo de um plano de contingência propriamente dito. Deste modo, a Empresa acaba respondendo às eventuais materializações dos riscos de forma emergencial com nível reduzido de capacidade para gestão de crises.

Causa

A materialização do risco chave pode ser atribuída às seguintes causas: falta de conscientização sobre os riscos, recursos limitados, cultura organizacional, complexidade e desafios de implantação, confiança excessiva nos sistemas atuais e rejeição a mudanças.

Efeito

A materialização do risco pode resultar nos seguintes efeitos: perdas financeiras significativas, danos à reputação e consequências legais.

Manifestação das Unidades examinadas

A SUINT concorda com o achado de auditoria.

Em relação ao Plano de Contingência, este achado também foi identificado na auditoria realizada que teve como objeto verificar atendimento de obrigações da CGPAR (CGPAR) nº 30, 31, 35, 39, 42, 48 e 50.

Para o referido achado foi elaborado Plano de Ação com medidas e prazos em andamento.

Manifestação da Auditoria Interna

Manifestação acatada.

Recomendações

2) Recomenda-se a implantação de um plano de contingência abrangente, contemplando ações de mitigação e estratégias de recuperação a fim de assegurar a resiliência organizacional para os riscos gerenciados, em especial àqueles cujo impacto for considerado significativo para a Empresa, seus objetivos e suas operações.

Benefícios Esperados

Espera-se os seguintes benefícios: garantia de continuidade dos serviços, treinamento e preparação da equipe, melhoria na tomada de decisão, melhoria da resiliência organizacional, proteção de reputação, redução de perdas financeiras e identificação e correção de vulnerabilidades.

2.5. Gerenciamento e monitoramento de riscos

Para o Gerenciamento de Riscos foi observado a suficiência, capacitação, responsabilidades/competências, atuação e registro do setor ao atuar no monitoramento dos planos de ação.

Para isso foram aplicados os seguintes testes:

- Verificar a suficiência de capacidade operacional na 2ª linha
- Verificar a existência de plano de capacitação em riscos
- Verificar a aplicação das responsabilidades e competências das unidades envolvidas.
- Verificar se a área detentora do risco atua proativamente na identificação e tratamento dos riscos envolvidos.
- Verificar o registro do processo de gerenciamento de riscos na organização

Embora fora do escopo da presente auditoria, a qual se limitou a avaliar o gerenciamento de riscos em nível estratégico, se faz importante registrar que, ao avaliar a capacidade funcional da 2ª Linha, foi constatada a inexistência de controles específicos voltados para o acompanhamento dos riscos operacionais da empresa. A ausência destes controles compromete a eficácia no monitoramento e na mitigação dos riscos associados, podendo resultar

em possíveis consequências como falhas operacionais, não conformidade com regulamentações ou perdas financeiras.

A capacidade operacional da 2ª linha (suficiência) é fundamental para garantir que a equipe possa desempenhar de modo eficaz seu papel de monitoramento e controle dos riscos nas três esferas (operacional, tático e estratégico). Isso inclui garantir que a equipe tenha recursos adequados, conhecimentos e habilidades para identificar, avaliar e mitigar os riscos de forma apropriada.

Ao ser questionada sobre o quantitativo de colaboradores na unidade, a SUINT informou que atualmente a equipe é composta por um Gerente e uma Assessora Técnica nível III e que não há necessidade de ampliação em seu quadro funcional pois afere-se ser *"suficiente para executar as atividades da GRCOI"* e que *"tal aferição leva em consideração a quantidade de projetos executados bem como o universo no qual a empresa está inserida, seu quadro de colaboradores e a quantidade de projetos e programas finalísticos de sua competência."*

Contudo, conforme previsto no Estatuto Social, Regimento Interno, Política de Gestão de Riscos e Controles Internos e Manual de Gestão de Riscos, são atribuições da Segunda Linha: coordenar os processos de identificação, classificação e avaliação dos riscos a que está sujeita a empresa, coordenar a elaboração e monitorar os planos de ação para mitigação dos riscos identificados, verificar continuamente a adequação e a eficácia da gestão de risco, gerenciar e monitorar o sistema de controles internos, dentre outras.

Atualmente a área realiza o monitoramento para os riscos táticos e estratégicos, não atuando sobre os riscos operacionais e seus controles internos. A causa informada para o não monitoramento dos riscos operacionais é a ausência de mapeamento dos processos existentes e, devido ao tamanho da equipe, o alto custo-benefício para que seja realizado o mapeamento dos riscos operacionais, já que a Unidade teria que parar de acompanhar o monitoramento dos riscos táticos e estratégicos.

Embora o quantitativo de pessoal da área esteja alinhado com o escopo atual dos trabalhos da SUINT, a ausência de acompanhamento das ações de tratamento dos riscos operacionais e o gerenciamento e monitoramento do sistema de controles internos neste nível fica em desencontro ao que está previsto nas diretrizes da Política de Gestão de Riscos e Controle Interno.

Assim, não podemos afirmar, em razão das ressalvas apresentadas e do achado a seguir, que as unidades possuem pessoas capacitadas e em quantitativo suficiente para monitoramento dos planos de tratamento.

Ainda, após a realização dos testes previamente mencionados, observou-se que as áreas realizam a identificação, análise, avaliação, tratamento e monitoramento dos riscos estratégicos em conjunto com a SUINT, área competente, nos termos do art. 85, inciso VI do Estatuto Social desta Infra S.A., por meio de oficinas de instrução, as quais são registradas em reuniões que culminam em Relatórios Trimestrais de Riscos. Apesar deste procedimento estar registrado em processo, à exceção do processo pertencente à Diretoria de Planejamento, não foi possível identificar documentos que demonstrem a atuação proativa da Primeira Linha na identificação e tratamento dos riscos envolvidos, sendo o processo de gerenciamento de riscos impulsionado sempre a partir da provocação da Segunda Linha.

Entretanto, considera-se adequado o acompanhamento e monitoramento dos riscos estratégicos e controles-chave pelas áreas responsáveis e pela Alta Administração.

2.5.1. Achado de auditoria: Ausência de Programa de Capacitação

Critério

Art. 3º da Política de Gestão de Riscos e Controle Interno: *"VIII - disseminar a cultura de Gestão de Riscos, especificando o perfil de risco adotado, introduzindo uma linguagem comum para o assunto "riscos" em todos os níveis da organização;"*

Análise e evidência

Inexistência de capacitação contínua efetiva tanto para os colaboradores da 1ª linha, quanto para a própria 2ª linha.

No que pese a área ter apresentado as oficinas trimestrais como uma ferramenta de capacitação utilizada e ter informado em resposta à Solicitação de Auditoria nº 01 que está previsto para o segundo semestre de 2024 uma capacitação formal para todos os colaboradores e empregados da empresa (o que não ocorreu), observa-se a necessidade de elaborar uma trilha de capacitação em riscos contínua, com treinamentos que auxiliem os colaboradores da primeira linha na construção e elaboração dos riscos, bem como a elaboração de um cronograma de treinamento para os colaboradores da segunda linha como previsto no Art. 3º, parágrafo VIII da Política de Gestão de Riscos e Controle Interno.

As oficinas são consideradas uma ferramenta de identificação, análise e elaboração do contexto dos riscos junto às áreas, porém não podem ser classificadas como única forma de capacitação, especialmente por terem participação de público limitado, contemplando apenas reduzida parcela do corpo funcional da empresa, na maioria gestores e a Alta Administração.

Para o adequado fomento da cultura de gestão de riscos, as ações de capacitação e reciclagem devem alcançar toda empresa, em todos os seus níveis.

Causa

Possíveis causas: falta de capacitação contínua da equipe da SUINT e falta de capacitação contínua para os colaboradores da empresa.

Efeito

São efeito ao presente achado: falha na identificação sistemática do risco.

Manifestação das Unidades examinadas

A SUINT concorda com o achado de auditoria.
Em relação ao programa de treinamento e capacitação, este achado também foi identificado na auditoria realizada que teve como objeto verificar atendimento de obrigações da CGPAR (CGPAR) nº 30, 31, 35, 39, 42, 48 e 50.
Para o referido achado foi elaborado Plano de Ação com medidas e prazos em andamento.
Dentre as etapas consta a cerificação da equipe da SUINT na ISO 31.000/2018, processo 50050.007310/2024-13.

Manifestação da Auditoria Interna

Manifestação acatada.

Recomendações

3) Recomenda-se intensificar o programa de treinamento, conscientização e divulgação dos riscos na empresa.

4) Recomenda-se elaborar um programa de treinamento e reciclagem contínuos para os colaboradores da SUINT, com temas inerentes à área como forma a manter o conhecimento atualizado e que possam desenvolver novas habilidades reforçar as atuais e corrigir possíveis lacunas.

Benefícios Esperados

Apresenta-se os seguintes benefícios esperados: conformidade legal e regulatória; melhoria da eficiência operacional; melhoria da tomada de decisões; melhoria da gestão de riscos.

3. RECOMENDAÇÕES

Apresenta-se, em síntese as recomendações oferecidas ao longo deste Relatório, correlacionando-as com os respectivos achados:

Quadro 3 - Síntese das Recomendações.

RECOMENDAÇÃO	ITEM DO ACHADO
1) A etapa de identificação dos riscos no processo de gerenciamento, por meio das oficinas, deve estar documentada de modo a garantir completa rastreabilidade da informação, realizando as atividades previstas no normativo interno e instruindo os artefatos necessários ao processo administrativo, tal como a Tabela de Identificação dos Riscos, de modo a demonstrar o exaurimento da identificação de todos os eventos possíveis relacionados aos empreendimentos, programas, negócios, objetivos, dentre outros, assim como as consequências relacionadas.	**2.2.1**
2) Recomenda-se a implantação de um plano de contingência abrangente, contemplando ações de mitigação e estratégias de recuperação a fim de assegurar a resiliência organizacional para os riscos gerenciados, em especial àqueles cujo impacto for considerado significativo para a Empresa, seus objetivos e suas operações.	**2.4.1**
3) Recomenda-se intensificar o programa de treinamento, conscientização e divulgação dos riscos na empresa.	**2.5.1**
4) Recomenda-se elaborar um programa de treinamento e reciclagem contínuos para os colaboradores da SUINT, com temas inerentes à área como forma a manter o conhecimento atualizado e que possam desenvolver novas habilidades reforçar as atuais e corrigir possíveis lacunas.	**2.5.1**

Fonte: AUDIN.

4. CONCLUSÃO

A Auditoria Interna concluiu que o nível de implementação dos Planos de Ação para mitigação de riscos estratégicos apresenta avanços significativos em diversas áreas, mas ainda requer melhorias em pontos críticos. A análise demonstrou que o processo de gerenciamento de riscos adota práticas relevantes, com base em normativos internos e internacionais, mas enfrenta lacunas que podem comprometer a eficácia plena do sistema.

Como pontos positivos identificados citam-se: (i) Análise de Contexto – a área de gestão de riscos demonstrou preocupação com o estabelecimento de contextos interno e externo para atingir os objetivos organizacionais, utilizando fontes diversas como planejamento estratégico e relatórios trimestrais; e (ii) Planos de Tratamento – para todos os riscos estratégicos identificados, há planos de tratamento correspondentes, abrangendo ações de melhoria nos controles internos.

Principais Achados e Recomendações

Registros incompletos na identificação de riscos: os registros não documentam de forma exaustiva os riscos relacionados aos objetivos estratégicos. Recomenda-se a documentação completa das etapas de identificação, conforme normativos internos.

Ausência de Plano de Contingência: a falta de um plano formal compromete a capacidade de resposta a eventos inesperados. Sugere-se a implantação de um plano abrangente de contingência e continuidade de negócios.

Necessidade de capacitação contínua: verificou-se a carência de um programa formal e contínuo de capacitação em gestão de riscos. Recomenda-se a implementação de trilhas de capacitação abrangentes para toda a organização.

As melhorias sugeridas visam fortalecer a governança, reduzir lacunas nos processos de gestão de riscos e aumentar a resiliência organizacional. Espera-se que a adoção das recomendações possibilite decisões mais informadas, maior eficiência operacional e melhor alinhamento estratégico.

Embora a Infra S.A. tenha avançado na mitigação de riscos, a implementação das recomendações será essencial para consolidar a maturidade do gerenciamento de riscos e assegurar o cumprimento pleno dos objetivos organizacionais.

Brasília, 17 de fevereiro de 2025.

ICP Brasil
Documento assinado digitalmente
WAGNER ROSA DA SILVA
Data: 17/02/2025 11:26:41-0300
Verifique em https://validar.iti.gov.br

WAGNER ROSA DA SILVA
Auditor Chefe