



ESTADO DO ACRE
SECRETARIA DE ESTADO DA FAZENDA

Rua Benjamin Constant, 946, - Bairro Centro, Rio Branco/AC, CEP 69900-062
- <http://www.sefaz.ac.gov.br/>

ANÁLISE DE RISCO Nº 16/2025/SEFAZ - DIPROJ

Processo nº 0715.007435.00044/2025-61

1. INTRODUÇÃO

1.1. O presente Mapa de Gerenciamento de Riscos (simplificado) tem como objetivo identificar e mitigar os principais riscos associados a contratação de *continuados de links de acesso à internet dedicados, serviços de proteção contra ataques DDoS e solução de proteção de perímetro gerenciado, com alta disponibilidade de hardware (cluster)*, para atender a demanda da Secretaria de Estado da Fazenda do Acre – SEFAZ/AC.

1.2. Este documento foi elaborado com base no Manual de Gestão de Riscos do TCU^[1] e o Código das Melhores Práticas de Governança Corporativa^[2], e segue a metodologia de análise qualitativa e quantitativa de riscos, considerando os impactos e probabilidades conforme os padrões definidos na ISO 31000:2009^[3].

1.3. O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso da contratação, da execução do objeto e da gestão contratual.

1.4. O Mapa de Gerenciamento de Riscos deve conter a identificação e a análise dos principais riscos, consistindo na compreensão da natureza e determinação do nível de risco, que corresponde à combinação do impacto e de suas probabilidades que possam comprometer a efetividade da contratação, bem como o alcance dos resultados pretendidos com a solução de TIC.

1.5. Para cada risco identificado, define-se: a probabilidade de ocorrência dos eventos, os possíveis danos e impacto caso o risco ocorra, possíveis ações preventivas e de contingência (respostas aos riscos).

1.6. A figura a seguir apresenta a **Matriz Probabilidade x Impacto**, instrumento responsável pela definição dos critérios quantitativos de classificação do nível de risco:

		Probabilidade (P)		
		Muito Provável 3	Provável 2	Pouco Provável 1
Impacto (I)	Alto	3 Médio	6 Alto	9 Alto
	Médio	2 Baixo	4 Médio	6 Alto
	Baixo	1 Baixo	2 Baixo	3 Médio
		1 Baixo	2 Médio	3 Alto

1.7. Parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão as ações relacionadas aos riscos durante as fases de contratação (planejamento, seleção de fornecedor e gestão do contrato).

1.8. **Classificação de Níveis de Risco:**

- Verde = Baixo risco (1,2)
- Amarelo = Médio risco (3,4)
- Vermelho = Alto risco (6,9)

1.9. A matriz permite avaliar o nível de risco combinando a probabilidade de ocorrência do evento e seu impacto, servindo como base para definir as ações mitigadoras.

2. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

2.1. Definição e especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição.

2.2. A tabela a seguir apresenta uma síntese dos riscos identificados e classificados neste documento.

ID	Risco Identificado	Consequências	Probabilidade (P) ¹	Impacto (I) ²	Nível de Risco NR=(P×I) ³
R01	Atraso no procedimento licitatório	Falhas no processo podem inviabilizar a contratação. Isso afeta diretamente o a comunicação e a segurança de dados da SEFAZ, provocando atrasos na contratação e sanções administrativas.	2	2	Médio(4)
R02	Falha na instalação e integração com os demais equipamentos do datacenter	A instalação de novos equipamentos envolve risco de compatibilidade.	2	3	Alto(6)
R03	Falhas no suporte técnico da contratada	Interrupção no fornecimento de internet e proteção de dados, afeta diretamente os sistemas críticos da SEFAZ, comprometendo a arrecadação tributária e a gestão fiscal do estado.	1	3	Médio(3)
R04	Falhas na segurança da informação e vazamento de dados	Comprometimento da segurança institucional e penalidades previstas na Lei Geral de Proteção de Dados (LGPD)	1	3	Médio(3)
R05	Atraso no pagamento à contratada	Descumprimento das obrigações pela contratante causando comprometimento na execução do objeto do contrato.	1	2	Baixo(2)

Legenda: P – Probabilidade; I – Impacto.

1 Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativa, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

2 Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

3 Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

3. MEDIDAS MITIGATÓRIAS

3.1. A tabela a seguir detalha as medidas mitigatórias para os principais riscos identificados:

ID	Risco Identificado	Medidas Mitigatórias
R01	Atrasos no processo licitatório	Aplicação de medidas mitigadoras, como a revisão jurídica rigorosa e registro no PNCP,

		reduz a chance, mas não anula a possibilidade de falha. Realizar prorrogação dos contratos vigentes ou contratações emergenciais.
R02	Falha na instalação e integração com os demais equipamentos do datacenter	Gestão ativa e técnica sobre o processo de instalação.
R03	Falhas no suporte técnico da contratada	Incluir penalidades contratuais, monitorar tempos de resposta e garantir suporte emergencial alternativo.
R04	Falhas na segurança da informação e vazamento de dados	Aplicar normas internacionais de segurança (ISO 27001), prever penalidades, fiscalizar constantemente e desenvolver treinamentos contínuos para mitigar riscos internos de vazamento de dados.
R05	Atraso no pagamento à contratada	Atuação do gestor junto à área de orçamento e finanças.

4. ACOMPANHAMENTO DAS AÇÕES DE TRATAMENTO DE RISCOS

4.1. O acompanhamento dos riscos será realizado por meio de revisões periódicas e auditorias internas, conduzidas pelo Departamento de Tecnologia da Informação, garantindo que eventuais desvios sejam identificados e tratados tempestivamente. Relatórios de conformidade serão elaborados regularmente, com indicadores específicos para cada risco identificado, permitindo a análise contínua da eficácia das medidas mitigatórias implementadas. Além disso, serão promovidas reuniões de monitoramento com os responsáveis pelas áreas impactadas, assegurando que as ações corretivas sejam aplicadas de forma proativa e alinhadas às melhores práticas de governança e segurança institucional.

Elaborado por:
DIVISÃO DE PROJETOS - DIPROJ

Requisitante:
ISRAEL JORDÃO SANTOS DE MELO
Chefe do Departamento de Tecnologia da Informação
Portaria nº 13/2023

Aprovado por:
JOSÉ AMARÍSIO FREITAS DE SOUZA
Secretário de Estado da Fazenda

[1] BRASIL. Tribunal de Contas da União. *Manual de gestão de riscos do TCU*. 2. ed. Brasília: TCU, 2020. 48 p. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/outros-documentos-externos/tcu_manual_gestao_riscos.pdf/view. Acesso em: 21 abr. 2025.

[2] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA – IBGC. *Código das Melhores Práticas de Governança Corporativa*. 6. ed. São Paulo: IBGC, 2023. 80 p. ISBN 978-65-5515-787-1. Disponível em: <https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=24640>

[3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000:2009 – *Risk management: principles and guidelines*. Geneva: ISO, 2009.



Documento assinado eletronicamente por **ZANIR NILSON DO NASCIMENTO DUARTE, Chefe de Divisão**, em 30/09/2025, às 10:40, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



Documento assinado eletronicamente por **ISRAEL JORDAO SANTOS DE MELO, Chefe(a) de Departamento**, em 30/09/2025, às 11:01, conforme horário oficial do Acre, com fundamento no art. 11, § 3º, da [Instrução Normativa Conjunta SGA/CGE nº 001, de 22 de fevereiro de 2018](#).



A autenticidade deste documento pode ser conferida no site <http://www.sei.ac.gov.br/autenticidade>, informando o código verificador **0017191391** e o código CRC **E2342D7F**.
