GESTÃO DE RISCOS EM ATIVOS DE TECNOLOGIA DA INFORMAÇÃO EM UNIVERSIDADE FEDERAL

STEFANY BRIER COSTA[1]; VIVIANE COSTA TOUGUINHA BAUER[2]; HENRIQUE BERTOCHI GRIGOL[3]; JULIANA FAUSTO FLORES[4]; RAFAEL LIPINSKI PAES[5]; e RICARDO PINKOSKI LUZZARDI[6]

[1]*Universidade Federal do Rio Grande – stefanybrier@furg.br*
[2]*Universidade Federal do Rio Grande – vivianetouguinha@furg.br*
[3]*Universidade Federal do Rio Grande – henriquebg.bg@furg.br*
[4]*Universidade Federal do Rio Grande – julianafausto@furg.br*
[5]*Universidade Federal do Rio Grande – rpaes@furg.br*
[6]*Universidade Federal do Rio Grande – ricardoluzzardi@hotmail.com*

1. INTRODUÇÃO

A gestão de riscos é fundamental para apoiar as organizações no alcance de objetivos, no cumprimento de regulamentos e na mitigação de danos institucionais. No setor público brasileiro, sua relevância foi destacada pela Instrução Normativa Conjunta MP/CGU nº 01/2016 e pelo Decreto nº 9.203/2017 que instituíram a Política de Gestão de Riscos, Controles Internos e Governança da Administração Pública Federal (BRASIL, 2016; BRASIL, 2017), orientando órgãos e universidades a implementarem metodologias de controle e monitoramento de riscos.

Na área de tecnologia da informação (TI), ativos como redes, servidores e sistemas são estratégicos à continuidade de processos acadêmicos, administrativos e de pesquisa, sendo vulneráveis a falhas e ameaças de segurança que afetam a governança institucional.

Assim, este estudo aplica uma metodologia de gestão de riscos em ativos de TI de uma universidade federal, fundamentando-se em normas internacionais (ISO 31000:2018; ISO/IEC 27005:2019, e ISO/IEC 27001:2022), com foco no inventário, classificação e priorização dos ativos, visando fortalecer a governança e a continuidade dos serviços essenciais.

2. METODOLOGIA

O estudo de caso qualitativo (YIN, 2015), desenvolvido no Centro de Gestão de Tecnologia da Informação (CGTI) com apoio do Núcleo de Apoio Executivo (NUEX), foi fundamentado nas diretrizes da ISO 31000 (2018), ISO/IEC 27005 (2019), ISO/IEC 27001 (2022) e nas recomendações do Tribunal de Contas da União – TCU (2018). A Tabela 1 apresenta a síntese das etapas da metodologia de gestão de riscos aplicada.

Tabela 1 – Estrutura da Metodologia de Gestão de Riscos

Metodologia de Gestão de Riscos da Universidade		**Normas e Ferramentas complementares**
1. Estabelecimento do contexto	1. Estabelecimento do Contexto da unidade 1.2 Desenvolvimento da Matriz SWOT 1.3 Construção do mapa de processos da unidade	BPMN (via Software Bizagi)
2. Identificação e Análise dos Riscos	2.1 Identificação dos Riscos 2.2 Identificação dos Eventos de Risco 2.3 Identificação das Causas 2.4 Identificação das Consequências 2.5 Classificação dos Tipos de Riscos 2.6 Identificação das Fontes de Risco	ISO/IEC 27001, ISO/IEC 27005 e boas práticas de órgãos públicos (TCU, 2018) para a categorização de ameaças e vulnerabilidades.

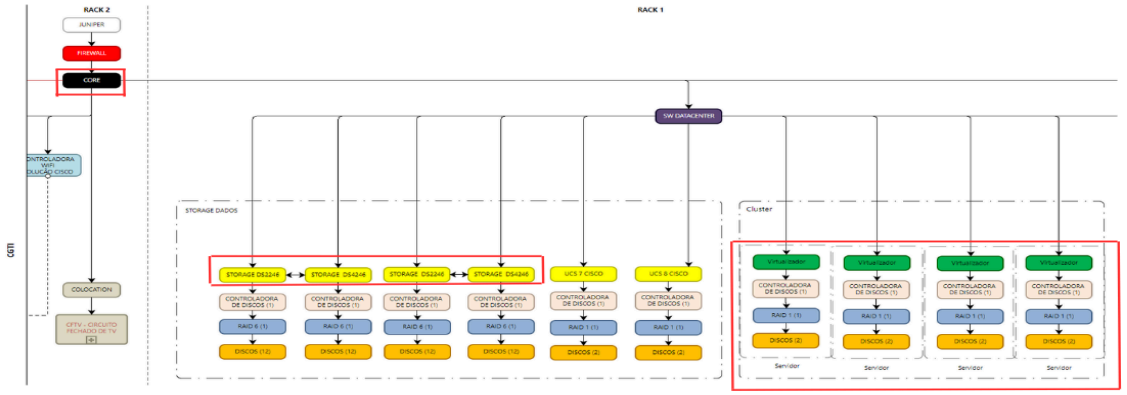
3. Avaliação dos Riscos	3.1 Identificação da Probabilidade (P) 3.2 Identificação do Impacto (I) 3.3 Identificação dos Controles	Matriz de Gravidade x Urgência x Tendência Matriz GUT (KEPNER; TREGOE, 1981); TCU (2018)
4. Tratamento dos Riscos	4.1 Resposta aos Riscos	Método BowTie (CCPS, 2008)

Fonte: Autores (2025)

3. RESULTADOS E DISCUSSÃO

A aplicação da metodologia de gestão de riscos evidenciou as vulnerabilidades críticas da infraestrutura de TI do Centro de Gestão de Tecnologia da Informação (CGTI), especificamente nas Coordenações de Engenharia de Rede e de Serviços de Rede e na Divisão de Segurança da Informação. O mapeamento realizado com Bizagi destacou a interdependência entre os ativos Core, Storage e Servidor (Virtualizador), permitindo reconhecer aqueles de maior relevância estratégica (Figura 1).

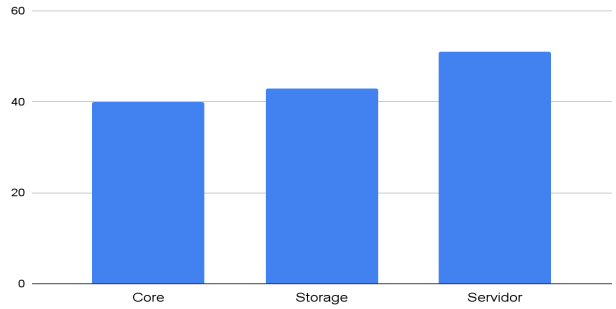
Figura 1 – Árvore de Processos



Fonte: NUEX (2024)

Na etapa de identificação, com base na ISO/IEC 27005:2019, foram categorizadas as principais ameaças e vulnerabilidades, utilizando-se o método BowTie para relacionar causas e consequências, além da matriz GUT como ferramenta de priorização. Esse processo resultou em 134 riscos identificados, distribuídos entre os três ativos (40 no Core, 43 no Storage e 51 no Servidor), conforme ilustrado na Figura 2.

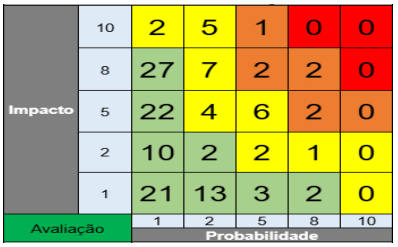
Figura 2 – Riscos Identificados nos Ativos



Fonte: Autores (2025)

A avaliação de probabilidade e impacto permitiu calcular o risco inerente e, posteriormente, o risco residual considerando os controles existentes. A Figura 3 apresenta a matriz consolidada, que revelou predominância de riscos médios e altos, confirmando a necessidade de reforço em medidas preventivas e mitigatórias.

Figura 3 – Matriz de Riscos



Fonte: NUEX (2025)

Como resultado final, sete riscos residuais foram priorizados, sendo quatro classificados como altos e três como médios. Destaca-se a recorrência de determinados riscos em mais de um ativo, o que demonstra a importância de planos de ação integrados, capazes de tratar vulnerabilidades comuns de forma coordenada. Esses achados convergem com a literatura (ISO 31000, 2018; TCU, 2018), que ressalta a necessidade de governança e controles sistêmicos em ambientes de TI de instituições públicas.

4. CONCLUSÕES

O estudo permitiu aplicar e adaptar a metodologia de gestão de riscos ao contexto da Coordenação de Sistemas de Informação, com foco nos ativos de TI. O uso combinado das normas ISO 31000:2018, ISO/IEC 27005:2019 e das diretrizes do TCU (2018), aliado a ferramentas como Bizagi, matriz GUT e método BowTie, mostrou-se eficaz para estruturar a análise de riscos de forma sistemática e visual.

Os resultados evidenciaram a criticidade dos ativos Core, Storage e Servidor (Virtualizador), dos quais foram identificados 134 riscos, sendo priorizados sete riscos residuais (quatro altos e três médios). Essa priorização favoreceu a elaboração de planos de ação direcionados, fortalecendo os controles internos e a governança de TI da instituição.

A análise também demonstrou que muitos riscos se repetem entre diferentes ativos, ressaltando a necessidade de tratamento integrado e de uma abordagem coordenada para aumentar a resiliência organizacional. Além disso, a matriz de riscos consolidada possibilitou uma visão clara do nível de exposição e apoiou a tomada de decisão estratégica pelo Comitê de Governança, Riscos e Controle Interno.

Como limitações, destaca-se que a aplicação foi restrita a três ativos centrais, não abrangendo todos os sistemas e serviços da unidade. Todavia, a sistematização apresentada neste trabalho fornece um modelo prático e replicável, que pode ser aplicado em outros setores da universidade e em diferentes instituições públicas, servindo como guia metodológico para futuras análises de riscos em ambientes de TI. Para estudos futuros, recomenda-se expandir a análise para outros ativos de TI e avaliar periodicamente a efetividade

dos planos de tratamento, garantindo um ciclo contínuo de monitoramento e melhoria.

5. REFERÊNCIAS BIBLIOGRÁFICAS

Livros

YIN, R. K. **Estudo de caso: planejamento e métodos.** 5. ed. Porto Alegre: Bookman, 2015.

KEPNER, Charles Higgins; TREGOE, Benjamin B. **O administrador racional: uma abordagem sistemática a solução de problema e tomada de decisões**. 2. ed. São Paulo: Atlas, 1965. 238 p. ISBN (Broch.).

Documentos legais e normativos

BRASIL. Decreto nº 9.203, de 22 de nov. 2017. **Política de governança da administração pública federal.** Diário Oficial da União, Brasília, DF, n. 224, p. 3, 23 nov. 2017.

BRASIL. **Instrução Normativa Conjunta MP/CGU nº 01**, **de 10 de maio de 2016. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do** Poder Executivo Federal. Diário Oficial da União: Seção 1, Brasília, DF, n. 89, p. 54, 11 maio 2016.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão**. Brasília: MPDG, 2017. Disponível em: https://bibliotecadigital.economia.gov.br/bitstream/777/438/1/170609_Manual%20de%20GIRC_v1.2.pdf. Acesso em: 12 mai. 2025.

BRASIL. Tribunal de Contas da União. **Referencial básico de gestão de riscos: estabelecendo o contexto, identificação, análise e avaliação de riscos.** Brasília: TCU, 2018. Disponível em: https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf. Acesso em: 12 mai. 2025.

Documentos institucionais

FURG – UNIVERSIDADE FEDERAL DO RIO GRANDE. **Conselho Universitário**. **Resolução nº 027/2019. Dispõe sobre a Política de Gestão de Riscos da FURG**. Rio Grande: FURG, 2019. Disponível em: https://www.furg.br/arquivos/institucional/gestao-de-riscos/politica-gestao-riscos-furg.pdf. Acesso em: 12 mai. 2025.

FURG. **Metodologia de Gestão de Riscos**. Rio Grande: FURG, 2020. Disponível em: https://www.furg.br/arquivos/institucional/gestao-de-riscos/metodologia-gestao-riscos-furg.pdf. Acesso em: 12 mai. 2025.

Documentos internacionais

UNITED KINGDOM. HM Treasury. **The Orange Book: management of risk – principles and concepts.** London: HM Treasury, 2023. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154709/HMT_Orange_Book_May_2023.pdf. Acesso em: 12 mai. 2025.