Implantando Processo de Gestão de Riscos Enxuto na Gestão de TIC da UFRN

André Dantas, Adson Araceli, Erica Miranda

Universidade Federal do Rio Grande do Norte (UFRN)

{andre.dantas,adson.araceli,erica.miranda}@ufrn.br

Resumo. *Este artigo descreve a implantação de um processo de gestão de risco enxuto na gestão da Superintendência de Tecnologia da Informação (STI) da Universidade Federal do Rio Grande do Norte (UFRN). Grandes benefícios são percebidos a partir deste processo, em especial, torna mais eficiente a gestão de Tecnologia da Informação e Comunicação (TIC) a partir da mitigação completa ou parcial de ameaças que podem comprometer os objetivos institucionais. A STI, em conjunto com a Secretaria de Gestão de Projetos (SGP) da UFRN, adaptou o, já maduro, Processo de Gestão de Riscos da UFRN (PROGERIS-UFRN) para adequar-se ao contexto da gestão de TIC da Universidade. A etapa de monitoramento teve alguns aspectos adaptados para tornar o gerenciamento mais efetivo diante da organização estrutural da unidade, considerando os mais de 100 eventos de riscos operacionais e 18 estratégicos já mapeados da unidade. O modelo, o processo e os resultados deste trabalho podem servir como base para os gestores de TIC de outras Instituições Federais de Ensino Superior (IFES) que busquem o amadurecimento da sua prática de gestão de riscos.*

Palavras-chave*: gestão de riscos corporativos; gestão de TIC; IFES*

1. Introdução

A governança e a gestão de TIC nas IFES têm o compromisso de garantir a entrega de soluções tecnológicas que contribuam diretamente para os objetivos institucionais. Infelizmente, no setor público a relação desproporcional de desafios e recursos disponíveis comumente leva a ineficiências indesejadas. Diante desta realidade e dessa necessidade, é preciso buscar implantar práticas de gestão e governança enxutas que agreguem valor da forma mais eficiente e efetiva possível. Gerenciar os riscos que influenciam diretamente no cumprimento dessa missão precisa ser um dos principais focos dos gestores.

Administrar as ameaças e oportunidades ao serviço prestado é essencial à eficiência da gestão, especialmente no contexto de incertezas e volatilidade do gerenciamento de TI no setor público. Nesta esfera somos suscetíveis a mudanças de normas e regulamentações, sérias restrições orçamentárias, e ainda, mais recentemente, muita dificuldade de retenção de talentos, principalmente para órgãos (como as IFES) cuja carreira de TIC tem salários muito menores que os do setor privado. Neste cenário é primordial que se maximize as chances de sucesso com os recursos disponíveis. Portanto, mitigar, pelo menos, riscos críticos como a perda de um storage com dados institucionais, vazamentos de dados pessoais, ou a indisponibilidade do sistema acadêmico no período de matrícula on-line, precisa ser tão prioritário e importante quanto qualquer outra atividade da gestão.

A governança corporativa da UFRN já endereça essa questão através da implantação de seu modelo de Gestão de Riscos (GR) abrangendo riscos estratégicos da Universidade e operacionais dos processos de trabalho das dezenas de unidades. Recentemente, a STI, em parceria com a SGP, iniciou a implantação efetiva da GR adaptando-se às especificidades do setor. A implantação abrange o gerenciamento (desde a concepção até o monitoramento) de riscos operacionais e estratégicos da unidade, contando ainda com uma forma de acompanhamento diferenciada diante do volume de eventos de riscos e processos envolvidos.

Este trabalho tem o intuito de apresentar o modelo de gestão de riscos da UFRN[1] e como está sendo implantado na STI. Nele serão apresentados como os riscos operacionais são gerenciados, bem como a importância e motivação de também tratar os riscos estratégicos da unidade. Visa ainda demonstrar que o método desta implantação e o modelo adaptado para realidade da STI podem servir de base para outros setores de TIC de IFES com cenários similares.

2. Gestão de Riscos

Segundo Fabozzi (2003), o risco é um fenômeno que, por natureza e por definição, não pode ser eliminado. Embora o risco e a incerteza sejam frequentemente usados como sinônimos, há uma distinção entre eles. A incerteza refere-se a não ter certeza do que vai acontecer no futuro e o risco é o grau dessa incerteza. A gestão de riscos pode ser considerada uma medida defensiva que contribui para reduzir as incertezas e evitar resultados indesejados. É também o processo de identificação de riscos críticos em uma organização, quantificando seus impactos nos objetivos financeiros, estratégicos e operacionais, e desenvolve e implementa estratégias de gerenciamento de riscos integrados (BERRY, 1998; BERKOWITZ, 2001).

2.1. Gestão de Riscos na UFRN

Desde 2018, a UFRN implanta e executa gradativamente o Processo de Gestão de Riscos (PROGERIS) baseado em padrões como ISO 31000 e COSO (Committee of Sponsoring Organizations of the Treadway Commission). A Figura 1 ilustra as dez etapas do PROGERIS executadas tanto nas perspectivas de riscos estratégicos quanto operacionais da instituição e suas unidades.

Figura 1. Processo da Gestão de Riscos da UFRN (OLIVEIRA et. al., 2020).

[1] Disponível em: http://sistemas.sgp.ufrn.br/riscos/

As etapas mais relevantes no contexto deste trabalho envolvem desde a definição do tratamento dos riscos até o ciclo de execução e monitoramento dos planos. A fase do tratamento compreende a definição da estratégia a ser aplicada para tratar o risco recém classificado na fase anterior (DANTAS, 2020). Dentre as quatro alternativas comuns como aceitar, transferir, evitar ou mitigar, esta última nos exige a definição complementar de mecanismos de controle que auxiliem na redução da probabilidade ou impacto do risco. Tipicamente os mecanismos podem servir para antecipadamente influenciarem o grau do risco através de planos de ação, ou através de planos de contingência, que buscam minimizar o grau após a concretização do risco. O monitoramento então passa a ser o momento em que os riscos são reavaliados, verificando a efetividade dos seus mecanismos de controle.

Além de um comitê próprio para tratar de questões sobre riscos e controles, gestores e servidores técnicos que implementam o processo, dois dos seus principais agentes são a Secretaria de Gestão de Projeto (SGP) e a Secretaria de Governança Institucional (SGI), cujas responsabilidades são, respectivamente, de desenvolver e executar o plano anual de GR e monitorar o modelo de GR. A partir do auxílio de um sistemas de informação (criado na UFRN) chamado Gerifes[2], a Universidade já mapeou mais de 800 riscos nos últimos cinco anos associados às principais unidades da instituição, e se mantém em constante evolução do processo, buscando formas mais eficientes, especialmente nos ciclos de monitoramento dos planos de controle.

3. Metodologia

Esta pesquisa caracteriza-se como qualitativa, cuja abordagem é estudo de caso. Do ponto de vista dos resultados, o estudo é descritivo. A pesquisa percorreu por três etapas e adotou diferentes meios na coleta, análise e tratamento dos dados: pesquisa documental, bibliográfica e grupo focal (SAMPIERI, 2013). O desenho da pesquisa obedeceu a: Diagnóstico da GR da IFE; Construção do modelo enxuto e ajustado ao GR de TICs e; Intervenção no curso do processo vigente de identificação ao monitoramento de riscos.

Para obtenção da etapa 1, o estudo buscou a literatura da GR e o arcabouço legal do tema, e levantou também dados contidos no sistema Gerifes da Instituição. Adiante, no passo 2, identificou riscos críticos de TIC e delineou os marcos para realização do seu monitoramento, adaptando-o ao modelo já estabelecido na UFRN. Por fim, aplicou o modelo enxuto junto aos atores da unidade de TIC observada. Também foi captada a experiência dos agentes via os times da STI pela técnica de grupos focais, visando a maturação dos planos de ação, de mitigação e dos ciclos de verificação do monitoramento desses riscos. Como meio de interpretação desses grupos, fez-se uso da análise do conteúdo (BARDIN, 2016), da qual resultou o modelo descrito na Figura 2, apresentado na seção seguinte deste trabalho.

4. Implantação do Modelo

A implantação do modelo de GR na STI acontece com foco em dois tipos de riscos: estratégicos e operacionais. De acordo com o enfoque, os perfis dos profissionais

[2] http://gerifes.net/

envolvidos no processo são diferentes. Para os operacionais, são envolvidas as equipes que executam os processos de trabalho, enquanto os estratégicos são os responsáveis pelas diretorias de sistemas e redes e a superintendente. Atualmente, os riscos estratégicos associados à STI envolvem as ameaças e seus mecanismos de controles vinculados às metas de TIC do Plano de Gestão vigente da UFRN.

A gestão dos riscos operacionais conta com mais de 100 eventos de riscos gerenciados agrupados em 40 processos de trabalho executados por 25 equipes diferentes da STI. Todos identificados através do PROGERIS, através de oficinas promovidas pelas SGP com times da STI para identificação, mapeamento e análise de processos, bem como identificação e classificação de riscos e seus mecanismos de controle. O modelo prevê ainda a designação do papel fundamental do gestor do risco, responsável pelo monitoramento dos riscos e acompanhamento dos planos de tratamento. Comumente esse papel seria atribuído às pessoas das equipes responsáveis pelos processos, porém no caso da STI, considerando as dezenas de processos e equipes diferentes, esse foi o elemento do modelo que precisou ser adaptado à realidade da unidade.

Diante do cenário particular da GR operacionais da STI, o papel dos gestores de riscos foi adaptado para, na prática, ser compartilhado entre 3 agentes: diretoria, Divisão de Apoio a Governança e Gestão (DAGG) e donos dos processos. Para efeitos formais, a responsabilidade máxima enquanto gestor de risco é da diretoria a qual o processo faz parte, no entanto é inviável que uma pessoa consiga gerenciar tantos riscos. Efetivamente, é compromisso do dono do processo em questão monitorar seus riscos associados e a execução dos planos de ação e de contingência relacionados. A DAGG, equipe da unidade responsável por fomentar a evolução das práticas de governança e gestão de TIC, se responsabiliza por, mensalmente, compilar informações sobre esses acompanhamentos das equipes e reportar às diretorias, com o objetivo de dar transparência do processo de forma eficiente para ajudar nas decisões dos diretores.

As adaptações aconteceram essencialmente nas etapas de monitoramento e execução dos planos de ação. Além desta separação de responsabilidades do gestor do risco, mais um elemento foi adicionado ao processo. Diante do alto número de riscos, foi necessário uma priorização de quais riscos serão monitorados através da definição de uma periodicidade de monitoramento baseado no grau de risco. A periodicidade em que o risco e seus mecanismos de controle devem ser monitorados é proporcional ao grau do risco, como ilustrado na Figura 2.

Figura 2. Matriz de risco categorizada a partir dos graus de risco e a periodicidade monitoramento associada para riscos da STI

5. Considerações Finais

Para que uma governança de TIC possa tornar a gestão de TIC efetiva na entrega de valor, em especial na prestação de serviços públicos, deve-se ter um foco especial em garantir uma gestão de riscos efetiva. No contexto das IFES, a GR ainda é uma prática com pouca maturidade, cujo nível de capacidade é inicial ou inexpressivo para 55% das IFES, segundo o levantamento de governança do TCU de 2021[3]. Este trabalho apresenta uma experiência de implantação de um modelo de gestão de riscos da UFRN, através de um processo maduro usado nos últimos 5 anos, e que, assim como foi adaptado às necessidades da STI, pode servir de base para outras instituições.

O processo de implantação é contínuo e atualmente a STI conta com o mapeamento de 18 riscos estratégicos (vinculados às metas do Plano de Gestão vigente da UFRN) e mais de 100 riscos operacionais, associados a 40 fluxos de trabalho, tratados por mais de 250 mecanismos de controle.

A UFRN, com unidades especializadas em práticas de gestão e governança como a SGP e a SGI, possui grande vantagem na implantação de práticas deste tipo. Além destas secretarias especializadas, o setor de TIC da instituição se beneficia de ter um núcleo dedicado para apoiar a gestão. Apesar disto, não estamos imunes aos desafios típicos que ameaçam a gestão pública, inclusive o próprio processo de gestão de riscos de TIC, como falta de recursos, muita demanda e engajamento inadequado das equipes. A boa notícia é que a partir de um processo enxuto como evidenciamos neste trabalho, apresentamos uma alternativa viável para melhorarmos nossos níveis de maturidade da gestão de riscos de TIC na educação.

Referências

BARDIN, L. (2016). Análise de conteúdo (3a reimp.). São Paulo: Edições 70.

BERKOWITZ, S. L. (2001). Enterprise risk management and healthcare risk management. Journal of healthcare risk management.

BERRY, A., PHILLIPS, J. (1998). Enterprise risk management: pulling it together. Risk Management, 45(9).

DANTAS, A. (2020) Proposta de Modelo de Monitoramento Ágil no Gerenciamento de Riscos Corporativos, Natal.

FABOZZI, F. J., PETERSON, P. P. (2003). Financial management and analysis (Vol. 100): John Wiley & Sons Inc.

OLIVEIRA, T.; SANTOS, L.; MEDEIROS JÚNIOR, J.; GURGEL, A.; SILVA, B. (2020). Proposta de framework para o processo de gestão de Riscos no setor Público (PROGERIS). Revista Gestão Universitária na América Latina - Gual.

SAMPIERI, H., COLLADO, F., & LUCIO, B. (2013). Metodologia de pesquisa [recurso eletrônico]. 5.ed. Porto Alegre: Penso.

[3] Disponível em: https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/