Congresso Internacional de Administração
ADM 2021
Administração Ágil
Inovação e Trabalho Remoto
25 a 27 de outubro
Ponta Grossa - Paraná - Brasil

ANÁLISE DA CONCEPÇÃO DA GESTÃO DE RISCOS DE UMA INSTITUIÇÃO FEDERAL DE ENSINO SUPERIOR

ANALYSIS OF THE RISK MANAGEMENT CONCEPTION OF A FEDERAL HIGHER EDUCATION INSTITUITION

ÁREA TEMÁTICA: ADMINISTRAÇÃO PÚBLICA

Aline Pacheco Primão, Universidade Federal de Santa Catarina, Brasil, aline.pacheco.pr@gmail.com

Leonardo Flach, Universidade Federal de Santa Catarina, Brasil, leonardo.flach@gmail.com

Rogério da Silva Nunes, Universidade Federal de Santa Catarina, rognunes@msn.com

Resumo

A pesquisa fez uma análise das ferramentas COSO GRC 2004, COSO GRC 2017, The IIA - Três Linhas de Defesa, ABNT NBR ISO/IEC 31000:2018, ABNT NBR ISO/IEC 31010:2012 que são utilizadas para realizar o processo de avaliação dos riscos e também a ferramenta utilizada pelo Tribunal de Contas da União para avaliar as instituições. A pesquisa tem como objetivo fazer uma análise da gestão de riscos em uma instituição federal de ensino superior (IFES), a fim de verificar em que ponto está sendo cumprido o decreto 9.203/2017, como estão dispostas políticas, planos e relatórios e também apontar pontos fortes, fracos e possíveis melhorias da instituição. No artigo foi utilizado uma abordagem qualitativa, descritiva e exploratória, fazendo uma análise documental a partir de documentos relacionados diretamente à gestão de riscos e também analisando documentos norteadores da instituição, por fim a pesquisa foi complementada com entrevistas para a confirmação dos dados e análise de acompanhamento.

Palavras-chave: Gestão de Riscos; Avaliação da Gestão de Riscos; IFES.

Abstract

The research analyzed the tools COSO GRC 2004, COSO GRC 2017, The IIA -Three Lines of Defense, ABNT NBR ISO/IEC 31000:2018, ABNT NBR ISO/IEC 31010:2012which are used to carry out the risk assessment process and also the toolused by the Federal Court of Accounts to assess institutions. The search has howobjective to carry out an analysis of risk management in a federal institution of higher education(IFES), in order to verify at what point Decree 9.203/2017 is being complied with, such aspolicies, plans and reports are laid out, as well as pointing out strengths, weaknesses andpossible improvements of the institution. In the article a qualitative approach was used,descriptive and exploratory, making a document analysis from documentsdirectly related to risk management and also analyzing guiding documents of theinstitution, finally the research was complemented with interviews to confirm thefollow-up data and analysis.

Keywords: *Risk Management; Risk Management Assessment.*

1. INTRODUÇÃO

A governança começou a ganhar importância no Brasil a partir da implantação do Plano Diretor da Reforma do Aparelho do Estado, em 1995, com o então presidente Fernando Henrique Cardoso, tendo como um de seus objetivos globais “aumentar a governança do Estado, ou seja,

sua capacidade administrativa de governar com efetividade e eficiência, voltando a ação dos serviços do Estado para o atendimento dos cidadãos" e não apenas orientados para o simples controle do próprio estado (BRASIL,1995).

Riscos começaram a ser tratados na administração pública com influência do Comitê das Organizações Patrocinadoras (COSO), da Organização de Padronização Internacional (ISO) e do Instituto dos Auditores Internos (IIA) (RÊGO, 2020). O COSO publicado em 2004 introduz o gerenciamento de riscos corporativos e propõe o tratamento dos riscos através dos níveis hierárquicos e categorias de níveis de gestão (RÊGO, 2020).

O TCU disponibiliza desde 2011 objetivos estratégicos voltados a práticas de gestão de riscos para a administração pública, através de documentos (BRASIL, 2018a; BRASIL, 2018b).

O governo federal brasileiro intensifica seu foco na governança da administração pública, através do decreto 9.203/2017, o qual dispõe da política de governança da administração pública federal direta, autárquica e fundacional (BRASIL, 2017). O artigo 17 do decreto especifica a gestão de riscos:

> A alta administração das organizações da administração pública federal direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional (BRASIL, 2017).

As Instituições Federais de Ensino Superior (IFES) estão inseridas neste cenário e infere-se que a governança pública voltada à educação superior deve ser exercida a fim de satisfazer aos interesses da comunidade, formando profissionais capazes de resolver os problemas da sociedade, resultando no aumento da qualidade de vida, na medida que se comprometem com a evolução social e econômica.

Com isso, a governança, utilizando-se do instrumento de gestão de riscos, quando bem implementado em uma IFES, pode colaborar com a tomada de decisões mais oportuna, minimizando incertezas, criando e protegendo valor institucional.

A pesquisa tem como objetivo avaliar a gestão de riscos de uma instituição federal de ensino superior, verificando como é realizado os planos e relatórios de acompanhamento e apontando pontos fortes, fracos e possíveis melhorias.

2. GESTÃO DE RISCOS

Segundo Brasil (2018b), o desafio da governança pública é determinar quanto de risco é possível aceitar para entregar valor aos cidadãos prestando serviços de interesse público da melhor maneira equilibrando riscos e benefícios. Com isso a gestão de riscos se torna imprescindível, pois ela ajuda na tomada de decisão e, consequentemente na confiança dos cidadãos, prevenindo perdas e auxiliando na gestão de incidentes (BRASIL, 2018b).

A ISO 31000 de 2018 define risco como o efeito da incerteza nos objetivos (ABNT, 2018). Bezerra (2011) explica que os riscos se apresentam no dia-a-dia de toda e qualquer atividade humana desenvolvida e que convivemos com duas certezas no ciclo de vida: os objetivos, aquilo que deve acontecer, e as incertezas, aquilo que pode acontecer. (BEZERRA, 2011).

O Decreto 9.203 de 2017 apresenta o conceito da gestão de riscos como sendo:

> Processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos (BRASIL, 2017).

Segundo Brasil (2018a, 2018b), a gestão de riscos implementada corretamente consegue fornecer informações para que as instituições consigam tomar decisões de alocações de recursos e seu uso apropriado para otimizar o desempenho organizacional, aumentando a eficiência e eficácia na entrega do valor público impactando positivamente toda sociedade (BRASIL, 2018a; BRASIL, 2018b).

A ISO 31000 de 2018 denota que o propósito da gestão de riscos é a criação e proteção de valor, onde ela apoia o alcance dos objetivos institucionais melhorando o desempenho e encorajando a inovação (ABNT, 2018).

2.1. Gestão de Riscos

O COSO GRC 2004 - Gerenciamento de Riscos - Estrutura Integrada, é um modelo de gestão de riscos, predominante no cenário mundial, apresentado na forma tridimensional representado na Figura 1: 1) Face superior - categorias de objetivos comuns a todas as organizações; 2) Face frontal - componentes presentes no funcionamento de uma gestão de riscos eficaz e; 3) Face lateral - estrutura da organização (unidades, áreas, processos, funções, etc) (BRASIL, 2018b). A Figura 1 apresenta o modelo do Cubo do COSO GRC 2004.

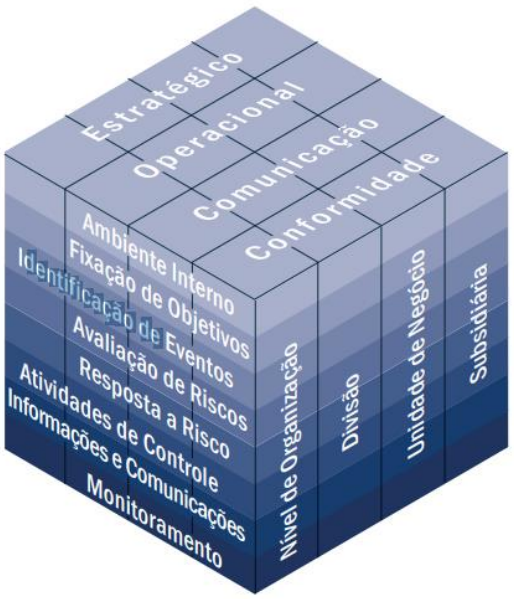

Figura 1 - Cubo COSO 2004 - Modelo de Gestão de Riscos

Fonte: Brasil (2018b).

O COSO GRC 2017 - Integrado com Estratégia e Desempenho, integra os processos de governança, que o 2004 não possuía, e melhora a integração com a gestão de desempenho (BRASIL, 2018b). A Figura 2 apresenta o processo do COSO GRC 2017.

Figura 2 - COSO GRC 2017

Fonte: Brasil (2018b)

O The IIA (*Institute of Internal Auditors*) forneceu o modelo das Três Linhas de Defesa, o qual ajuda a melhorar a comunicação e conscientização da governança, gestão de riscos e controles para diversos tipos de organização, dispondo de forma simples, uma explicação direta dos diversos papéis e responsabilidades que compõem o gerenciamento de riscos e controles (IIA, 2019).

Segundo Brasil (2018b), as três linhas de defesas, ou grupo de responsáveis envolvidos com o gerenciamento de riscos no The IIA são: 1) funções que gerenciam e têm prioridade de riscos - gestão operacional e procedimentos diários; 2) funções que supervisionam riscos - funções específicas para garantir que a primeira linha funcione como planejado e; 3) funções que fornecem avaliações independentes - auditoria interna (BRASIL, 2018b). A Figura 3 fornece o processo de gestão de riscos de Três Linhas de Defesa apresentado pelo IIA.

Figura 3 - The IIA - Três Linhas de Defesa

Fonte: IIA (2013).

ABNT NBR ISO/IEC 31000:2018 fornece princípios e diretrizes para a gestão de riscos, servindo para qualquer tipo de organizações, onde estas podem personalizar conforme seu contexto. Também apresenta o processo de gestão de riscos desde a identificação do risco até o registro e relato, considerando contextos internos e externos da instituição, incluindo fatores humanos e culturais (ABNT, 2018).

A ISO 31000 segue os princípios que a gestão de riscos deve ser integrada, estruturada e abrangente, personalizada no contexto da organização, inclusiva nas percepções de todas as partes interessadas, dinâmica, influenciada por fatores humanos e culturais, e melhorada continuamente (ABNT, 2018). O processo de gestão de riscos inicia com o contexto, escopo e critérios, avaliação dos riscos, tratamento dos riscos, registro e relato, onde em todo o processo há atividades de comunicação e consulta e monitoramento e análise crítica.

A norma NBR ISO/IEC 31010:2012 é uma norma de apoio da 31000 e dispõe de boas práticas para o processo de avaliação de riscos através de orientações de seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos (ABNT, 2012).

O processo de avaliação de riscos disposto na norma ISO/IEC 31010 de 2012 engloba as atividades de identificação de riscos, análise de riscos e avaliação que pode variar conforme as técnicas e métodos utilizados para a condução do processo. Na Identificação de Riscos é onde devem ser identificados os ativos da organização, desde processos, recursos humanos, sistemas, estrutura física, entre outros. Para cada ativo levantado é necessário identificar ameaças e suas fontes, controles existentes e assegurá-los que realmente funcionam, as vulnerabilidades associadas aos ativos, ameaças e controles e, por fim, as consequências e prejuízos caso um incidente venha a ocorrer. Após a identificação, é preciso priorizar os riscos, avaliar as consequências, probabilidades de um risco vir a ocorrer e estimar seu nível, com isso, será gerado uma lista dos riscos com os níveis e valores designados, podendo agora realizar o

tratamento (ABNT, 2012). O Tratamento de Riscos está descrito na ISO 31000, e é efetivado a partir do Plano de Tratamento de Riscos. A Figura 4 apresenta o processo de avaliação de riscos para o processo de gestão de riscos fornecido pela norma NBR ISO/IEC 31010:2012.

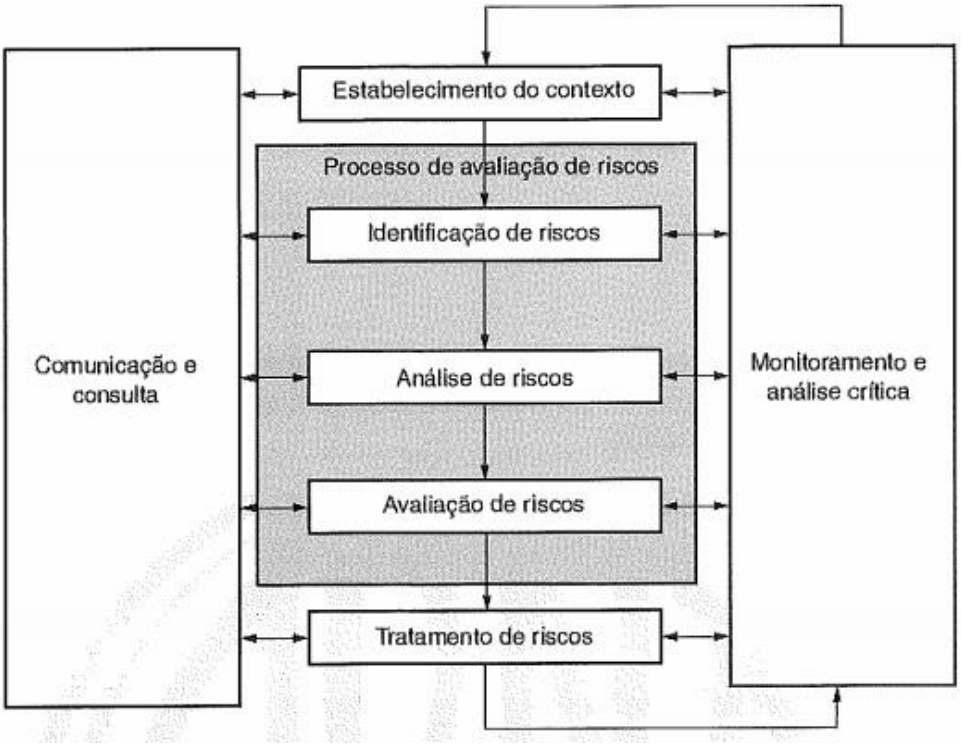

Figura 4 - Processo de Avaliação de Riscos para o Processo de Gestão de Riscos

Fonte: ABNT NBR ISO/IEC 31010:2012.

O Tribunal de Contas da União (TCU) disponibiliza alguns documentos que podem ajudar as organizações a implantar a gestão de riscos, um deles é a cartilha "10 passos para a boa gestão de riscos", estes passos são (BRASIL, 2018a): 1) Decidir gerenciar riscos de forma proativa; 2) Aprender sobre gestão de riscos; 3) Definir papéis e responsabilidades; 4) Estabelecer a política de gestão de riscos; 5) Definir o processo de gestão de riscos; 6) Identificar os riscos-chave; 7) Tratar e monitorar os riscos-chave; 8) Manter canais de comunicação com as partes interessadas; 9) Incorporar a gestão de riscos aos processos organizacionais e; 10) Avaliar e aprimorar a gestão de riscos (BRASIL, 2018a).

Outro documento fornecido pelo TCU é o "Roteiro de Avaliação de Maturidade em Gestão de Riscos, com o objetivo de apoiar os gestores públicos na autoavaliação, conseguindo elaborar iniciativas e colocar em prática planos, também colabora com a avaliação da maturidade de gestão de riscos das instituições identificando pontos a serem aperfeiçoados para melhorar a entrega de produtos e serviços à sociedade (BRASIL, 2018b).

O TCU avalia a governança e gestão pública através de um questionário de autoavaliação encaminhado às instituições. A partir do ano de 2021 a aplicação deste questionário será realizada por uma ferramenta chamada e-Governança. Entre os itens levantados na avaliação, a

gestão de riscos é avaliada na Estratégia e na Tecnologia da Informação. Os questionamentos incluem se a estrutura de gestão de riscos está definida, se o processo de gestão de riscos está implantado, se os riscos críticos são geridos, se executa o processo de gestão de riscos de tecnologia da informação, se executa o processo de gestão de riscos de segurança da informação e, se executa processo de gestão de ativos associados à informação (BRASIL, 2021).

2.2. Políticas e Planos de Gestão de Riscos

A política se refere à pluralidade dos homens, e trata da convivência entre os diferentes, de como estes se organizam para o bem comum (ARENDT, 2002). A ABNT ISO GUIA 73:2009 define a política de gestão de riscos como uma declaração de intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.

O Plano de Gestão de Riscos é considerado um esquema dentro da estrutura de gestão de riscos que especifica a abordagem, componentes e recursos aplicados para gerenciar riscos (BRASIL, 2018a). O Plano pode ser aplicado a um determinado processo, projeto ou produto, em partes ou em toda a instituição.

No plano de gestão de riscos também é englobado o tratamento de riscos, com o Plano de Tratamento de Riscos, onde é descrito todas as formas de tratamentos dos riscos que foram identificados, em sua implementação serão executadas as ações de segurança de informação incluídas no plano aprovado, onde deve haver um acompanhamento dos gestores das ações e prazos estabelecidos (ABNT, 2018b). O tratamento de riscos começa quando finalizado a avaliação dos riscos, cada risco pode ser reduzido, retido, evitado ou transferido.

3. METODOLOGIA

A pesquisa é considerada qualitativa, pois pretende analisar a gestão de riscos em uma instituição de ensino superior através de documentos existentes e entrevistas. Terence (2006) afirma que na abordagem qualitativa o pesquisador tem como objetivo aprofundar-se no tema para compreender seus fenômenos, interpretando-os na perspectiva dos participantes do contexto sem possuir uma representação numérica, podendo analisar opiniões, reações, hábitos e atitudes, buscando compreender uma determinada situação social, um fato, grupo ou uma interação (TERENCE, 2006).

Quanto a estratégia a pesquisa se enquadra em um estudo de casos, pois esta procura responder sobre a gestão de riscos em instituições de ensino, de forma a avaliar uma instituição e conseguir apontar pontos fracos e fortes, e desta forma, propor melhorias. Segundo Gil (2008) um estudo de caso permite o conhecimento mais amplo e detalhado de um estudo, que em outros tipos de delineamento são muito difíceis. A pesquisa se enquadra no tipo descritivo, pois segundo Yin (2015) um caso de uso descritivo é aquele que o pesquisador consegue descrever fenômenos contemporâneos dentro de um contexto real, procurando ilustrar uma situação complexa e os aspectos que estão envolvidos.

Os dados analisados foram retirados do portal da instituição e do sistema acadêmico (resoluções), disponível na parte pública. Primeiramente, foram analisados documentos diretos referentes à Gestão de Riscos: Plano de Integridade, Plano de Gestão de Riscos de TIC, Política de Segurança da Informação e Comunicação, Sistema de Governança de Tecnologia da

Informação e Comunicação e Política de Governança, Integridade, Riscos, Controle Internos da Gestão, e também verificado se a instituição possui setores e comitês que trabalham com a governança institucional. Após analisados se estes setores/comitês dispõe de políticas e planos de gestão de riscos. Em um segundo momento, foram avaliados documentos considerados norteadores da instituição, investigando Plano de Desenvolvimento Institucional (PDI), Plano de Permanência e Êxito, Plano Estratégico de TIC (PETIC) e Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC).

Para a complementação de análise dos dados documental, confirmar os dados levantados e também verificar o acompanhamento realizado para as políticas e planos desenvolvidos foi utilizado o protocolo de entrevistas usando a plataforma Google Meet, onde foi gravada para não perder nenhuma informação importante. Entrevistas em estudos descritivos podem ser utilizadas para identificar padrões gerais (SAUNDERS *et al.*, 2009). Segundo Silva (*et al.*, 2006), na entrevista tem como objetivo de investigar determinada questão e podem ser levadas por uma conversação espontânea, fácil comunicação. Dentre as modalidades de entrevista, a escolhida foi a entrevista baseada em um roteiro, em que teve uma preparação de um roteiro a seguir pelo entrevistador, porém é mais flexível, podendo ser formuladas novas perguntas durante a entrevista (SILVA *et al.*, 2006).

As entrevistas foram realizadas com o Coordenador de Governança de TIC e um representante do Comitê de Governança Digital. Os questionamentos realizados foram: Como foi realizado o plano/política? Como é realizado o acompanhamento do plano/política? Além destes planos/políticas você vê outro que envolva a gestão de riscos na instituição?

Com o levantamento dos dados coletados foi feita a tabulação para comparação dos resultados e colaboração com críticas e sugestões para aprimoramento da gestão de riscos da organização.

4. RESULTADOS

A Instituição analisada não possui um departamento destinado a governança institucional, porém foi informado por um dos entrevistados que a instituição possui uma diretoria de gestão do conhecimento, a qual desenvolve algumas ações referentes a governança quando necessário. A coordenadoria de processos e riscos, dentro da diretoria informada, realiza algumas ações referentes a riscos. A coordenadoria foi alterada recentemente para atender as demandas do Decreto 9.203/2017, nas solicitações de gestão de riscos institucionais.

Já relacionado a TIC, existe uma coordenação de governança de TIC, a qual foi criada, segundo o entrevistado, que é o coordenador da área, por se tratar de um requerimento do governo federal. Esta desenvolve, entre outras coisas, toda a documentação referente à gestão de riscos de TIC. Para o entrevistado, a coordenação pode ser considerada uma área técnica consultiva, onde propõe resoluções, normativas, planos, políticas seguindo as documentações e solicitações do governo e as encaminha para aprovação dos responsáveis.

Em 2021 foi instituído o "Comitê de Governança, Integridade, Riscos e Controles Internos da Gestão", porém a resolução de criação e composição do mesmo não está pública.

Neste ano também foi extinto o "Comitê gestor de tecnologia da informação e comunicação" e o "Comitê de Segurança da Informação" e criado o "Comitê de Governança Digital (CGD)",

que tem natureza deliberativa de caráter permanente e trata assuntos relativos à implementação de ações do governo digital, uso de recursos de tecnologia da informação e comunicação, e políticas de governança e segurança da informação. Segundo o entrevistado, que representa o CGD, a junção dos dois comitês em apenas um foi importante para inserir requisições referentes à transformação digital, mas também para facilitar demandas que necessitavam passar pelos dois comitês para obter aprovação, como é o caso da gestão de riscos de TIC.

A instituição possui uma "Política de Governança, Integridade, Riscos e Controles Internos da Gestão", publicada em 2021. Ela está organizada da seguinte forma: 1) Princípio e Objetivos Organizacionais; 2) Diretrizes; 3) Instrumentos; 4) Instâncias de Supervisão onde apresenta as linhas de defesa, composição e responsabilidades e; 5) Disposições Finais. O documento também apresenta dois anexos com um fluxograma do sistema de governança e gestão da instituição e outro dos Campi da mesma. Nas disposições finais da política é apresentada as próximas etapas a serem desenvolvidas, a qual fornece o prazo até 2024 para que todos os riscos sejam identificados e gerenciados. Por ser incipiente, o documento não possui nenhum acompanhamento, assim como no disposto anteriormente, o comitê responsável pela política não possui nenhuma fundamentação.

O tópico da integridade está nos princípios da governança pública do decreto 9.203/2017 no artigo 3° e também no item III do artigo 19 que descreve "análise, avaliação e gestão de riscos associados ao tema da integridade". A Controladoria Geral da União (CGU), conforme o decreto, foi responsável por disponibilizar os procedimentos, fases e prazos para a elaboração e execução do plano de integridade na administração pública, o qual está com prazos para 2018. A instituição avaliada possui o Plano de Integridade institucional, que foi publicado em 2020, este define medidas para se trabalhar de forma preventiva com riscos relacionados à integridade.

A instituição possui a "Política de Segurança de Informação e Comunicação", aprovada em 2016. Em um dos capítulos da política (Diretrizes Específicas), uma seção trata da gestão de riscos em apenas um artigo e expõe que a avaliação dos riscos relativos à segurança da informação e comunicação devem ser tratados conforme exigências legais e regulatórias. O entrevistado relatou que com a mudança dos comitês, o CGD abarcou a responsabilidade pela política, e que o documento deve sofrer alterações devido à Lei Geral de Proteção de Dados Pessoais (LGPD).

A Coordenação de Governança de TIC desenvolveu o "Sistema de Governança de Tecnologia da Informação e Comunicação", que descreve as políticas de TIC, entre elas, princípios e diretrizes de gestão de riscos. Esta política é datada de 2018, e segundo o entrevistado o acompanhamento é realizado pelo, agora Comitê de Governança Digital, que garante o cumprimento da mesma.

O Plano de Gestão de Riscos de TIC foi publicado em 2020 e possui planilhas de mapeamento de ativos e identificação de riscos, seguindo a ISO/IEC 27005:2008, que é específica para a gestão de riscos de segurança da informação, a ISO/IEC 31000:2009 e a ISO/IEC 31010/2012, também segue o "Guia de Governança de Tecnologia da Informação e Comunicação" do Sistema de Administração de Recursos de Tecnologia da Informação (SISP) da Secretaria de Governo Digital (SGD), parte do Ministério da Economia. O plano foi subdividido em fases e abrange toda parte de infraestrutura e sistemas, recursos humanos e processos de negócios. Em

seu anexo, é desenvolvido o Plano de Tratamento de Riscos e Riscos Residuais, onde foram apresentados os riscos, níveis de risco, ação e controle a implantar. Os controles foram especificados e priorizados e gerados os riscos residuais, os quais também foram tratados. Em conversa com o entrevistado, foi informado que o desenvolvimento do plano começou em 2019 e a versão publicada abrange apenas uma parte da instituição, o qual possui um planejamento de execuções e que a gestão de riscos de TIC completa está prevista para 2024. Também foi inteirado que o tratamento de riscos foi definido com o comitê responsável, onde os representantes deliberaram as prioridades e devem realizar o acompanhamento.

Outro ponto explanado é que o registro de incidentes é apresentado em outro plano chamado "Sistema Gestor de Continuidade de Negócios", o qual é acionado quando um risco ocorre, este possui um anexo com uma tabela de incidentes passados, porém este plano não possui atualização desde 2018, o que segundo o entrevistado, deve acontecer ao findar da pandemia. Para ele, a dificuldade de atualização dos planos cessaria com um sistema de transparência dos dados, onde a sociedade pode acompanhar as ações realizadas. Hoje os riscos são internos à instituição e somente ficam externos quando há um problema que leva um tempo maior para ser resolvido, os quais para o entrevistado é importante prestar contas para a comunidade. O entrevistado afirma que o acompanhamento do Plano de Gestão de Riscos deve ser realizado pelo CGD e que mudanças também devem advir destes, salvo mudanças de leis e solicitações dos órgãos de controle.

Quando questionado ao entrevistado sobre outros planos que possuem gestão de riscos do documento (documentos indiretos), foi referenciado o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e o Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC), que se enquadram em documentos norteadores da instituição. Os dois documentos, em sua atual versão, possuem uma avaliação de riscos bem completa, para cada ação do plano existe uma análise de risco, avaliando ameaças, probabilidades, tratamento, aceitação e impacto.

Outro documento norteador da instituição é o Plano de Desenvolvimento Institucional (PDI), este documento tem como objetivo pensar em estratégias, formalizá-las e definir um plano de ação, envolvendo metas e prazos, dentro das legalidades e exigências dispostas pelo Ministério da Educação (MEC) (BRASIL, 2004). O PDI da organização avaliada possui um objetivo estratégico de consolidar a governança institucional, com iniciativas de aprimorar a gestão de TIC e estruturar o processo de gestão estratégica baseada em indicadores e riscos. Porém, não é possível identificar a gestão de riscos do documento.

Na Tabela 1 é apresentado os documentos que a instituição tem referente a gestão de riscos. Os documentos diretos são aqueles que definem a gestão de riscos na instituição e os documentos indiretos são os que apresentam o tratamento de gestão de riscos do documento. A aba Acompanhamento está descrito quem é responsável pelo acompanhamento.

DOCUMENTOS DIRETOS	ANO/VERSÃO	ACOMPANHAMENTO	
Política de Governança, Integridade, Riscos e Controles Internos de Gestão	2021	Comitê de Governança, Integridade, Riscos e Controles Internos de Gestão	
Sistema de Governança de Tecnologia da Informação e Comunicação	2018	Comitê de Governança Digital	
Plano de Gestão de Riscos de TIC	2020	Comitê de Governança Digital	
Política de Segurança de Informação e Comunicação	2016	Comitê de Governança Digital	
Plano de Integridade Institucional	2020	Comitê de Governança, Integridade, Riscos e Controles Internos de Gestão	
DOCUMENTOS INDIRETOS	**ANO/VERSÃO**	**ACOMPANHAMENTO**	**POSSUI GR?**
Plano Diretor de Tecnologia da Informação e Comunicação	2021/2022	Comitê de Governança Digital	Sim
Planejamento Estratégico de Tecnologia da Informação e Comunicação	2020/2024	Comitê de Governança Digital	Sim
Plano de Desenvolvimento Institucional	2020/2024		Não
Plano de Permanência e Êxito	2018		Não
Plano Anual de Trabalho	2021 e 2022		Não

Tabela 1 - Documentos Institucionais

Fonte: O próprio autor.

5. CONSIDERAÇÕES FINAIS

A organização avaliada possui alguns processos institucionais bem incipientes de gestão de riscos, com a avaliação de documentos, percebe-se que as publicações realizadas do tema são de 2021. Quando avaliamos publicações mais específicas, cenário de TICs, elas já estão em andamento há mais tempo, onde vimos publicações de 2018, caso do Sistema de Governança de Tecnologia da Informação e Comunicação.

Pode-se verificar que a gestão de riscos de TIC está mais avançada do que a institucional, com políticas bem definidas, planos em andamento, processos estabelecidos, porém ainda tem um

caminho longo a percorrer para realizar uma gestão total e efetiva, principalmente com relação a transposição de informações das ações realizadas. Com isso, é possível inferir que uma área bem estruturada de governança produz resultados mais expressivos, fazendo-se necessário a instituição, para melhorar seus processos de gestão de riscos institucionais, que tenha um setor específico de governança institucional.

Como apresentado por um dos entrevistados, a falta de um sistema de transparência de controle de informações, faz com que os dados não sejam repassados à sociedade de forma completa e atual, com isso, faz-se necessário vislumbrar uma solução que colabore com este processo para o progresso da gestão de riscos.

Com a pesquisa, vimos que a governança exercida nas IFES tende a sofrer melhoria contínua, oportunizando uma gestão de maior qualidade e, desta forma, que contribua para o aperfeiçoamento e melhoria das suas ações.

REFERÊNCIAS

ABNT ISO GUIA 73:2013 Gestão de riscos - Vocabulário.

ABNT NBR ISO/IEC 31000:2018. Gestão de Riscos - Princípios e Diretrizes.

ABNT NBR ISO/IEC 31010:2012. Gestão de Riscos - Técnicas para o processo de avaliação de riscos.

ARENDT, Hannah. (2002). O que é política? Ed. 3. Tradução Reinaldo Guarany. Rio de Janeiro: Bertrand Brasil. 240 pg. Disponível em: http://arquivos.eadadm.ufsc.br/somente-leitura/EaDADM/UAB_2017_1/Modulo_1/Ciencia%20Politica/Material%20Complementar/O%20que%20%C3%A9%20pol%C3%ADtica%20Hannah%20Arendt.pdf. Último acesso em 13/04/2021.

BEZERRA, Edson Kowask. Gestão de Riscos de TI - NBR 27005. Rio de Janeiro - RJ. RNP/ESR, 2011. 150 p.

BRASIL. Presidência da República. Decreto 9.203 de 22.11.2017 - política de governança da administração pública federal direta, autárquica e fundacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/D9203.htm.

BRASIL, Tribunal de Contas da União. (2018a). 10 passos para uma boa gestão de riscos. Brasília: TCU, Secretaria de Métodos e Suporte ao Controle Externo (Semec), 31p.

BRASIL, Tribunal de Contas da União. (2018b). Roteiro da Avaliação de Maturidade da Gestão de Riscos. Brasília - DF. Secretaria de Métodos e Suporte ao Controle Externo (Semec).

BRASIL, Presidência da República. Plano Diretor da Reforma do Aparelho do Estado. Disponível em: http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo /fhc/plano-diretor-da-reforma-do-aparelho-do-estado-1995.pdf. Último acesso em 12/04/2021.

BRASIL, Tribunal de Contas da União. (2021). Levantamento de Governança Pública. Disponível em: https://portal.tcu.gov.br/governanca/governancapublica/organizacional /levantamento-de-governanca/. Último acesso em 27/04/2021.

BRESSER PEREIRA, L. C. (2001). Uma nova gestão para um novo Estado: Liberal, Social e Republicano. Revista do Serviço Público. Disponível em: https://www.bresserpereira.org.br/papers/2001/78Otawa-ppdf.

TERENCE, Ana Cláudia Fernandes; ESCRIVÃO FILHO, Edmundo. (2006). Abordagem quantitativa, qualitativa e a utilização da pesquisa-ação nos estudos organizacionais. XXVI Encontro Nacional de Engenharia de Produção - ENEGEP, v.9, Fortaleza, CE.

SILVA, Pesquisa qualitativa em estudos organizacionais - paradigmas, estratégias e métodos. São Paulo. Saraiva. 2006.

GIL, Antonio Carlos. (2008). Métodos e técnicas de pesquisa social. Ed. 6. Editora Atlas. São Paulo-SP.

YIN, Robert K. Estudo de Caso - Planejamento e Métodos. 5 ed. Tradução: Cristhian Matheus Herrera. Porto Alegre: Bookman, 2015.

SAUNDERS, Mark; LEWIS, Philip; THORNHILL, Adrian. (2009). Research methods for business students. Ed. 5.

RÊGO, Lúcio Joaquim da Silva. Gestão de riscos no setor público do Brasil: análise da implantação no ministério da justiça e segurança pública (MJSP). Trabalho de Conclusão de Curso. Brasília - DF. 2020.

IIA, The Institute of Internal Auditors. (2019). Documento de Exposição - Três Linhas de Defesa.

IIA, The Institute of Internal Auditors. (2013). Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles. Disponível em: https://global.theiia.org/translations/PublicDocuments/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control%20Portuguese.pdf. Último acesso em 13/05/2021.