GT - USO, COMUNICAÇÃO E GESTÃO DA INFORMAÇÃO E DO CONHECIMENTO

A IMPORTÂNCIA DA AUDITORIA DE INFORMAÇÃO PARA O PROCESSO DE GESTÃO DE RISCOS

Ana Carolina Freire Oliveira Aragão de Medeiros, Andréa Vasconcelos Carvalho

RESUMO

Os órgãos de controle da administração pública, em suas auditorias, têm dedicado atenção especial ao nível de maturidade da política de gestão de riscos adotada por cada instituição. A falta, o excesso ou a má qualidade dos ativos informacionais expõe a organização a riscos e impede o alcance dos objetivos estratégicos. Diante disso, objetiva-se analisar a importância da Auditoria de Informação para o processo de gestão de riscos, visando contribuir para o alcance dos objetivos estratégicos organizacionais e melhorar a sua maturidade em gestão de riscos. Com foco na consecução desse objetivo, o processo metodológico se realiza por meio de pesquisa básica, sob uma abordagem qualitativa, fundamentada em pesquisa bibliográfica acerca de Sistemas de Informação , Gestão da Informação, Auditoria de Informação e Gestão de Riscos . Constata-se, portanto, que a auditoria de informação é um instrumento de mitigação de riscos e aplicar um dos seus métodos é uma forma de agregar valor ao processo de gestão de riscos, especialmente quanto ao uso, aos recursos e aos fluxos da informação.

Palavras-chave: Gestão da informação, Sistema de Informação, Gestão de Riscos e Auditoria de Informação.

1 INTRODUÇÃO

Historicamente, os serviços oferecidos pelos órgãos públicos brasileiros são passíveis de críticas e, em algumas situações, considerados ineficientes, muito embora, sabe-se que existem ações positivas, mesmo diante da complexidade que envolve a gestão pública e suas diversas atuações. A sociedade contemporânea almeja uma administração pública eficaz, capacitada para gerar resultados positivos e que atenda às suas necessidades, como, por exemplo, mediante a oferta de serviços de educação e saúde de excelência.

Nesse contexto, o gerenciamento de riscos vem sendo implementado nas organizações visando ao alcance dos objetivos estratégicos e, consequentemente, protegendo os interesses da sociedade no uso de bens e serviços públicos de qualidade. Os riscos são inerentes às organizações públicas ou privadas e, quando não gerenciados, podem comprometer o alcance dos objetivos traçados. Para Miranda (2021, p. 32), entende-se risco "como uma possibilidade de algo dar errado", contudo o autor defende que o conceito é mais amplo e "envolve a quantificação e a

qualificação da incerteza tanto no que diz respeito às perdas quanto aos ganhos por indivíduos ou organização". Nesse sentido, a Gestão de Riscos (GR) permite que a administração pública trate de forma mais eficaz as incertezas - riscos e oportunidades - com foco na sua capacidade de criar valor, seja através dos serviços prestados à sociedade, seja por meio da melhoria dos processos de trabalho, contribuindo para a tomada de decisão e o alcance dos objetivos institucionais.

Duque (2021, p. 1) reforça que uma organização, independentemente de sua natureza, tamanho ou ramo, sempre irá produzir informação por meio dos seus processos e sistemas de informação disponíveis aos usuários. Por sua vez, a Associação Brasileira de Normas Técnicas (ABNT) através da NBR ISO 30301:2016 (2016, p. VI) reforça que "o êxito das organizações depende, em grande medida, da implementação e manutenção de um sistema de gestão desenhado para a melhoria contínua de seu desempenho" e devem oferecer metodologias que contribuam com "a tomada de decisões e a gestão de recursos para atingir os objetivos da organização". Diante da relevância da informação para as organizações, pondera-se o quão imprescindível os sistemas de informações também o são, inclusive por serem veículo captador, condutor, disseminador e meio de acesso à informação.

Sistemas devem ser desenvolvidos com o apoio dos usuários, trabalhadores detentores do conhecimento, satisfazendo as necessidades informacionais pertinentes. É essencial que eles consigam utilizar as informações contidas nos sistemas para interpretar, gerar novos conhecimentos e tomar decisões apropriadas. Os sistemas de informação quando não disponibilizam a informação certa, para as pessoas certas, no momento e no formato certos, não cumprem com seu propósito. A má qualidade informacional resultará em comprometimento do desempenho dos processos, expondo a organização a riscos. Gerir riscos de informação visa garantir que os ativos informacionais úteis sejam protegidos e disponibilizados adequadamente. O processo que busca a mitigação desses riscos é a auditoria de informação, pois audita o uso da informação pelos trabalhadores, os recursos de informação e seus respectivos fluxos na organização.

A auditoria de informação (AI), também chamada de auditoria de ativos informacionais (AAI), vem contribuir para adicionar valor à informação por meio dos sistemas, do uso, dos fluxos, bem como avaliar quais informações são necessárias,

mas estão ausentes, provocando erros e impossibilitando a construção do conhecimento; ou que estão disponíveis, mas não são claras, acessíveis ou são desnecessárias (CARVALHO, 2021, p. 236).

É importante observar que desenvolvimento e investimento unicamente em tecnologia não têm êxito sem a percepção de que pessoas são a razão de existir dos sistemas e organizações, pois trazem consigo uma bagagem de conhecimento e informações (DAVENPORT, 1998, p. 12). Os sistemas de informação devem ser desenvolvidos por pessoas, com pessoas e para pessoas considerando seu comportamento, competências e necessidades. Computadores e sistemas expandem o acesso aos dados e às informações, mas se os usuários não os compreendem, não recuperam e não utilizam em benefício da organização, tornam-se ineficientes. Ademais, se o processo, o fluxo e o sistema de gestão de riscos não disponibilizam as informações necessárias, no momento e formato oportunos, aos seus agentes há comprometimento da segurança, confiabilidade da informação e eficácia da gestão de riscos.

Diante do exposto, o objetivo precípuo desta pesquisa é analisar a importância da auditoria de informação para o processo de gestão de riscos, visando contribuir para o alcance dos objetivos estratégicos organizacionais.

Com foco na consecução desse objetivo, o processo metodológico se realiza por meio de pesquisa básica, sob uma abordagem qualitativa fundamentada em pesquisa bibliográfica.

2. REFERENCIAL TEÓRICO

A consecução do objetivo do presente trabalho demanda a discussão sobre Sistemas de Informação, Gestão da Informação, Auditoria de Informação e Gestão de Riscos.

2.1. Sistemas de Informação

A finalidade de uso dos sistemas de informação tem sido ampliada significativamente ao longo das últimas décadas, causando impactos importantes às organizações, aos usuários e à sociedade. Praticidade para o usuário realizar compra segura sem precisar de deslocamento; painéis visuais que expõe dados da organização com a finalidade de contribuir com a gestão e suas decisões; acesso às

contas correntes e realização de operações financeiras em aparelhos de comunicação móvel; comunicação em tempo real com indivíduos de qualquer parte do mundo sem necessitar longas viagens ou maiores investimentos. São infinitas as possibilidades de aplicação dos sistemas de informação.

Pode-se afirmar que, nos dias atuais, os sistemas têm a função de integrar os usuários por meio da comunicação e de tornar os processos mais transparentes garantindo o acesso à informação de forma segura.

O´Brien (2004, p. 6) define SI como "um conjunto organizado de pessoas, hardware, software, redes de comunicação e recursos de dados que coleta, transforma e dissemina informações em uma organização". Stair (2011, p. 8) compartilha entendimento semelhante quando diz que SI é "um conjunto de elementos ou componentes inter relacionados que coleta (entrada), manipula (processo), armazena e dissemina (saída) dados e informações." Tem-se que *entrada* (ou *input*) é a atividade que alimenta e fornece o dado bruto ao sistema; o *processo* é a etapa responsável pela transformação do dado em informação útil; a *saída (output)* é o estágio em que a informação é disseminada ao usuário promovendo o conhecimento e contribuindo para a tomada de decisão gerencial.

As organizações devem garantir aos seus servidores os meios, sistemas de TI ou não, para que os dados e as informações sejam registrados, transformados, armazenados e disseminados, facilitando o seu uso a fim de que haja a construção do conhecimento, que por sua vez, é construído pelo processo de transformação de conhecimento tácito em explícito. Esse processo envolve etapas de socialização e troca de experiências; "reflexão coletiva"; busca de conhecimento teórico às fontes diversas; até assimilar e incorporar o conhecimento nas mentes das pessoas e nas rotinas de trabalho (CHOO, 2006, p. 36-40).

Davenport (1998, p. 11) defende que sistemas não conceberão informações oportunas aos consumidores, se seus desenvolvedores não tiverem o apoio de usuários (especialistas) abertos a socializar seu conhecimento, durante o desenvolvimento da arquitetura da informação. Além de que, não é produtivo uma organização utilizar diversos sistemas de informação se eles não interagem entre si ou se as pessoas não conseguem utilizá-los para interpretar, gerar novos conhecimentos e tomar decisões apropriadas (DAVENPORT, 1998, p. 67). O

conhecimento tácito dos especialistas somado ao conhecimento teórico dos desenvolvedores devem construir sistemas em benefício da organização, contribuindo para que o conhecimento extraído dos sistemas de informação seja integrado e centralizado, contudo, de forma disseminada a toda organização.

O modelo defendido por Davenport (1998, p. 12) é baseado em uma organização que investe na promoção da informação em todas as dimensões do seu ecossistema, seja cultural, comportamental, processual, política e, por último, tecnológica. Para o autor, construir uma cultura informacional é fundamental, porém uma tarefa árdua, pois instiga mudanças principalmente na dimensão comportamental.

O benefício advindo pela utilização de sistemas pode ser medido pela relação entre melhoria da gestão organizacional promovida pelo sistema, o custo de implantá-lo/desenvolvê-lo/mantê-lo e a avaliação do seu desempenho.

Stair (2011, p. 371) explica que "o desempenho desses sistemas é, em geral, uma função da qualidade da decisão e da complexidade do problema. A qualidade da decisão pode resultar em aumento da eficácia e da eficiência, maior produtividade e muitas outras medidas". A complexidade do problema trata-se de uma medida intangível, pois "depende da dificuldade de ser resolvido e implantado". Quanto maior for o desempenho de um sistema, maior será o impacto sob seus benefícios. Os custos correspondem aos elementos de Tecnologia da Informação (TI) e quanto maior é custo de um sistema de informação maior será o impacto negativo em seus benefícios.

Sistemas devem ser projetados e usados em favor das instituições para atingir suas metas e objetivos, aumentar lucro e baixar custos e desenvolver novos e melhores produtos. A informação é o elo de ligação entre o desempenho do sistema e o benefício que ele proporciona à organização. Informação confiável, disseminada de forma adequada e transparente contribui para apoiar as ações gerenciais.

Levando em consideração que tanto os *sistemas de informação* quanto seus *usuários* estão inseridos em um contexto que influencia, por exemplo, a decisão, o engajamento e eficiência de processos, como o de gestão de riscos, por exemplo, é importante que se atente aos aspectos de ambos os pontos de vista. Dedicando

atenção predominante aos usuários, que devem ser os protagonistas nessa relação homem-máquina.

2.2. Gestão da Informação

Quando são desenvolvidos visando disseminar a informação correta, no tempo certo às pessoas certas, os SI proporcionam às organizações fluidez em seus processos de trabalho gerando confiabilidade, transparência, satisfação pessoal, segurança, ajudando para o alcance das metas e dos objetivos estratégicos. Esse cenário ótimo, concretiza-se mediante foco, esforço e comprometimento organizacional em favor da Gestão da Informação, "processo pelo qual os recursos são utilizados com o objetivo de otimizar o uso e a disseminação da informação dentro de uma organização" (LATEEF e OMOTAYO, 2019, p. 17, tradução nossa) mediante identificação dos ativos informacionais necessários aos respectivos utilizadores da informação.

As pesquisadoras argumentam que o GI não é um assunto unicamente de Tecnologia da Informação (TI), mas envolve questões multifatoriais que a organização precisa desenvolver a capacidade de "adquirir, processar, gerenciar, armazenar, preservar e entregar as informações certas para as pessoas certas, no momento certo e no formato certo" (LATEEF e OMOTAYO, 2019, p. 17, tradução nossa). Entender os processos de gestão é imprescindível para um GI eficaz nas organizações. Relacionar as informações necessárias com os respectivos processos, é uma forma eficiente de disseminá-las aos usuários certos, de eliminar informações desnecessárias e aumentar o valor de utilidade.

É importante entender as necessidades de informação (NI) específicas a cada organização (ou processo de trabalho). As NI podem surgir do dever de resolver um fato ocorrido, por meio de um impulso cognitivo, ou quando o conhecimento possuído é insuficiente para alcançar um objetivo ou solucionar um problema (MIRANDA, 2014, p. 62). A autora ainda argumenta que :

Estudos de NI interessam-se pela forma com que uma pessoa analisa necessidades, entra em contato com um sistema de informação e constrói sentido para suas atividades. A NI traduz o estado em que um usuário se encontra quando se confronta com a exigência de uma informação que lhe falta (e é necessária) para prosseguir seu trabalho. (MIRANDA, 2014, p. 62)

Para identificar quais informações são essenciais para os processos e que precisam estar disponíveis, por exemplo, em um sistema de TI, é importante refletir sobre questões como: por que o usuário precisa buscar aquela informação? Para qual finalidade ela acredita precisar da informação? O que fará com a informação? Perguntas como essas devem ser respondidas para que se analise a real necessidade (e disponibilização) de uma informação (MIRANDA, 2014, p. 62).

O valor de utilidade da informação está diretamente relacionado à sua qualidade. A má qualidade da informação resultará em comprometimento do desempenho do processo, expondo a organização a riscos.

Riscos de informação, quando não identificados, classificados, tratados e mitigados, podem se desdobrar em novos riscos, tais como: financeiros, de conformidade, de integridade, dentre outros. Gerir riscos de informação visa garantir que os ativos informacionais úteis sejam protegidos e disponíveis adequadamente. O processo que busca a mitigação desses riscos é a Auditoria de Informação.

2.3. Auditoria de Informação

Na atualidade, as organizações e os trabalhadores estão expostos a sobrecarga de informações, dados e conhecimento, *inputs* ou *outputs*. O excesso ou a má qualidade dos ativos informacionais, além de expor a organização a riscos, impedem o alcance dos objetivos estratégicos e a efetividade dos processos de trabalho, por exemplo, podendo afetar o fluxo das atividades, provocar prejuízos emocionais e operacionais causados pelo esforço excessivo dos funcionários para filtrar, identificar a informação correta e preencher lacunas (LATEEF e OMOTAYO, 2019, p. 16) .

Com o intuito de superar esses obstáculos, Carvalho (2021, p. 233) apresenta a "auditoria como ferramenta efetiva de *avaliação* e de *consultoria* voltada para o conteúdo, os processos, os fluxos e os usos da informação e do conhecimento."

O termo auditoria é habitualmente associado ao processo de adequação de uma situação a padrões legais e à identificação de erros e fraudes. No entanto, o conceito é muito mais amplo. A ABNT NBR ISO 19011:2018 (2018a, p. 1) define auditoria como "processo sistemático, independente e documentado para obter evidência objetiva e avaliá-la objetivamente, para determinar a extensão na qual os

critérios de auditoria são atendidos". Na esfera governamental, a CGU (2017b, p. 12) define auditoria interna como "uma atividade independente e objetiva de *avaliação* e de *consultoria*, desenhada para adicionar valor e melhorar as operações de uma organização" com vistas a "avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos".

No que se refere ao processo de *avaliação*, a auditoria busca obter e examinar evidências, a fim de formar opinião sobre o objeto que pode ser financeiro, de conformidade ou operacional. Em todos os casos, a auditoria de avaliação relaciona-se com os processos de governança, de gerenciamento de riscos e de controles internos, em busca de atingir seus objetivos (BRASIL, 2017b, p. 14).

Sobre a *consultoria,* a CGU diz tratar de atividade de "assessoramento, aconselhamento e outros serviços relacionados fornecidos à alta administração com a finalidade de respaldar as operações da unidade" (BRASIL, 2017b, p. 17). A auditoria consultiva é realizada mediante solicitação do serviço e deve se debruçar sobre temas estratégicos que visem ao fortalecimento da Governança e da Gestão de Riscos.

Transpondo as colocações para o tema sob análise, temos que AI é um "processo que facilita a avaliação da gestão da informação e do conhecimento e da produção e uso de inteligência e contribui para melhorar o planejamento destas ações" (CARVALHO; ESTEBAN NAVARRO, 2010).

Para Elisabeth Orna (2004 apud Pestana, 2014, p. 51), AI é definida como "avaliação sistemática do uso, recursos e fluxos da informação" relacionando as necessidades individuais das pessoas envolvidas e documentos existentes com os objetivos organizacionais. Da mesma forma, Buchanan e Gibb (1998) entendem que AI é um "processo para descobrir, monitorar e avaliar os fluxos e os recursos de informação da organização, a fim de implementar, manter ou melhorar a gestão da informação", visando atribuir valor aos ativos informacionais tornando-os mais úteis e alinhados com a estratégia organizacional.

Carvalho (2019, p. 61) resume os principais métodos e etapas propostos por pesquisadores para realizar AI, conforme quadro 1 a seguir.

Quadro 1 - Principais modelos de AI e suas respectivas etapas

BUCHANAN, GIBB (1998)	BURK, HORTON (1998)	ORNA (1999)	HENCZEL (2001)
1. promover; 2. identificar; 3. analisar; 4. contabilizar; 5. sintetizar.	1. indagar a equipe utilizando questionários e surveys; 2. medir os recursos de informação em relação a custo/valor; 3. analisar os recursos; 4. sintetizar os resultados, elaborar matriz swot dos recursos de informação.	1. análise preliminar para confirmar a direção estratégica; 2. obter apoio e recursos da gestão; 3. obter compromisso dos stakeholders; 4. planejar; 5. identificar os recursos e fluxos de informação; 6. interpretar os resultados obtidos.	1. planejamento; 2. coleta de dados; 3. análise de dados; 4. avaliação de dados; 5. comunicação das recomendações; 6. implantação das recomendações.

Fonte: adaptado de Carvalho, 2019.

A partir da análise do quadro 1, depreende-se que os modelos propostos tendem a se enquadrar como uma auditoria consultiva. Entretanto, os modelos propostos por Orna e Henczel possuem perspectivas, também, avaliativas. Uma análise simples sobre os quatro métodos revela destaques importantes, tais como: inventariar os ativos de informação e mapear o seu fluxo, avaliar o uso e necessidades informacionais dos trabalhadores, analisar se os recursos disponíveis para armazenar, registrar, processar e disseminar a informação são adequados, analisar o custo da informação, avaliar o cenário encontrado, propor recomendações e implementá-las.

Predomina também entre os métodos, etapa que, mesmo que indiretamente, integra trabalhadores ao processo de AI, uma vez que irá analisar se as informações que a instituição detém são suficientes e capazes de agregar valor ao trabalho deles, como também precisa-se entender se os recursos existentes (sistemas de informação, por exemplo) são capazes de disponibilizar aos trabalhadores certos, a informação útil, na quantidade e tempo corretos. Então, é coerente que os usuários sejam consultados, examinados e ativos no processo de AI.

Independente do método adotado, a AI também é capaz de promover benefícios a outros processos organizacionais, além da própria gestão da informação e do conhecimento. Nesse sentido, Ariffin *et al* (2014) e Henczel e Robertson (2016) defendem que a AI é útil para a transparência, acessibilidade e melhoria regulatória, no que se refere à governança institucional, assim como contribui para o planejamento e o desenvolvimento dos sistemas de informação, por meio do

mapeamento dos fluxos informacionais necessários para o desenvolvimento e funcionamento desses sistemas.

Lateef e Omotayo (2019, p. 17-18) apresentam benefícios da AI relacionados à gestão de riscos informacionais. Argumentam que quando tratados, controlados e mitigados, são capazes de aumentar a qualidade informacional e melhorar o comprometimento dos trabalhadores para com os ativos de informação. A AI interessa-se pela forma como as informações que a organização detém estão sendo armazenadas, processadas e protegidas, sempre buscando mitigar os riscos que estão comprometendo esses processos informacionais.

2.4. Gestão de riscos na administração pública

A administração pública deve ser capaz de suprir os anseios da sociedade através de serviços e políticas públicas eficientes, o que corrobora com a disseminação da cultura de gerenciar com base em riscos (BRASIL, 2018, p. 5).

Os riscos são inerentes às organizações públicas ou privadas e, quando não gerenciados, podem comprometer o alcance dos objetivos traçados. Para Miranda (2021), entende-se risco "como uma possibilidade de algo dar errado", contudo o autor defende que o conceito é mais amplo e "envolve a quantificação e a qualificação da incerteza tanto no que diz respeito às perdas quanto aos ganhos por indivíduos ou organização". Nesse sentido, a GR permite que a administração pública trate de forma mais eficaz as incertezas - riscos e oportunidades com foco na sua capacidade de criar valor, seja através dos serviços prestados à sociedade, seja por meio da melhoria dos processos de trabalho, contribuindo para a tomada de decisão e o alcance dos objetivos institucionais.

Hill (2006) diz que risco "é a probabilidade de que um evento, seja ele bom ou mau, ocorra no futuro". A GR investe esforços para prever os possíveis eventos, aos quais os objetivos organizacionais estão expostos, com a intenção de mitigá-los por meio da implantação de controles internos e monitoramento.

No Brasil, a GR é regulamentada pela Instrução Normativa nº 01/2016 (BRASIL, 2016) destinada ao Poder Executivo federal e determina que os órgãos "deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos, e à governança."

A norma além de disciplinar os princípios de GR que os órgãos do Poder Executivo federal devem observar, também diz que cada órgão deve formalizar sua própria política e modelo de GR, objetivando garantir aos servidores tomadores de decisão acesso a informações relativas aos riscos aos quais a instituição está exposta; ampliar a probabilidade de atingir os objetivos institucionais reduzindo os riscos a um nível possível; e promover a melhoria do processo de tomada de decisão e tratamento dos riscos.

O Decreto 9.203/2017 (BRASIL, 2017), dispõe sobre a política de governança da administração pública e define GR como um conjunto de atividades contínuas e ininterruptas, que deve ocorrer conforme disciplinado pela alta administração, devendo igualmente prever "as atividades de identificar, avaliar e gerenciar potenciais eventos" que possam vir a impactar e/ou comprometer o alcance dos objetivos.

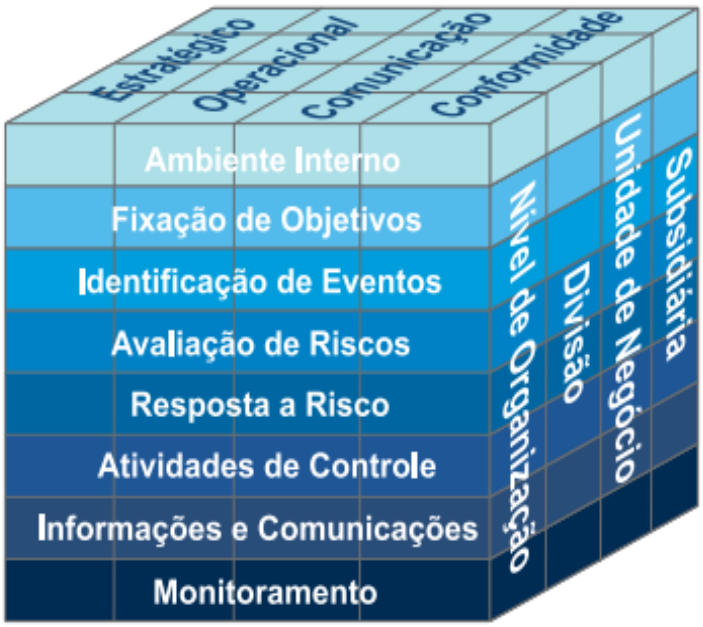
Diante desses instrumentos normativos, depreende-se que cada organização pública deve adotar seu próprio modelo de GR, podendo ser fundamentado nas metodologias disponíveis que melhor se adequa à organização, como por exemplo: *Committee of Sponsoring Organizations of the Treadway Commission* (COSO, 2007) e ISO 31000. Essas são as estruturas de gerenciamento de riscos que as organizações ao redor do mundo mais utilizam e apresentam semelhanças entre si, devendo ser ajustadas a cada instituição (MIRANDA, 2021, p. 49).

O COSO em 2004 publicou o documento *Enterprise risk management - integrated framework* (*Gerenciamento de riscos corporativos Estrutura integrada,* traduzido para o português em 2007 pela PriceWaterhouseCoopers), também conhecido como COSO II. Esse modelo entende que risco é a chance de ocorrência de um evento capaz de comprometer o alcance do objetivo.

A figura 1, conhecida como Cubo do Coso, mostra as três dimensões abordadas na metodologia. Na dimensão superior do cubo, estão os objetivos que devem ser alcançados pela organização, classificados como: estratégico, operacional, de comunicação e de conformidade. A amplitude dos objetivos torna claro o espectro de atuação da GR em todos os níveis da organização. Esses níveis estão representados na dimensão lateral do cubo. Na dimensão frontal, estão os oito componentes do gerenciamento de riscos: ambiente interno; fixação de objetivos; identificação de eventos; avaliação de riscos; resposta a risco; atividade de controle;

informações e comunicação; e monitoramento. O cubo representa a relação entre os objetivos que a organização almeja alcançar com os componentes do gerenciamento de riscos que viabilizam seu alcance, perpassando por toda a organização. Cada componente de gerenciamento relaciona-se com todos objetivos (COSO, 2007, p. 23).

Figura 1 - Cubo do Coso: Relacionamento entre objetivos e componentes



Fonte: COSO (2007)

A norma brasileira ISO 31000:2009, publicada pela Associação Brasileira de Normas Técnicas (ABNT), diz que todas as atividades organizacionais estão cercadas por riscos. Ademais, argumenta que o processo de gerir riscos compreende as atividades de definir o contexto, identificar, analisar, avaliar e tratar o risco. Todo o processo deve ser monitorado e analisado criticamente para acompanhamento da efetividade dos procedimentos adotados pela instituição, dos riscos identificados e dos controles internos, se foram suficientes para mitigar e diminuir o grau de risco (ABNT, 2009, p. v).

A norma diz que o processo de GR (figura 2) deve ser parte integrante da gestão organizacional, pois promove a disseminação de informações, conhecimento e ferramentas gerenciais que subsidiam a tomada de decisão (ABNT, 2018, p. 9).

Figura 2 - Processo de gestão de riscos conforme a norma ABNT NBR ISO 31000:2018

Fonte: adaptado de ABNT NBR ISO 31000:2018

O processo proposto pela ISO 31000 possibilita à organização a melhoria contínua tanto dos seus processos/unidades de trabalho que são submetidos à gestão de riscos, como a própria GR, pois o monitoramento ativo durante todo o processo ajuda a perceber as necessidades de ajustes e adequações, tempestivamente.

Seja qual for a estrutura de gerenciamento de riscos aplicada pelo órgão, seus objetivos e metas devem estar subordinados ao interesse público. A cultura de servir à sociedade deve estar enraizada nos servidores, procedimentos e processos, por meio de sua cultura organizacional. A GR deve ser utilizada como um meio para se atingir esse macro objetivo, proporcionando aprendizagem e disseminação do conhecimento organizacional.

Diante do exposto, percebe-se que os temas explanados se conectam e formam um ciclo contínuo de produção de conhecimento, sendo a informação o seu elo promotor (CURVELO *et al.*, 2022, p. 120). As informações são a base de trabalho da gestão de riscos e demanda sistemas de TI eficientes e pensados nas necessidades do usuário, entregando, de forma acessível e intuitiva, informações que permitam identificar, interpretar e mitigar os riscos, contribuindo para a tomada de decisões organizacionais.

6 CONSIDERAÇÕES FINAIS

Cada organização representa um ambiente informacional composto por diversos subsistemas independentes, mas que interagem entre si. Fazer com que a informação percorra seu fluxo ideal, realizando as diversas interações entre os subsistemas do ambiente e alcance o objetivo global é uma tarefa que requer gestão sistêmica e multidisciplinar.

O objetivo deste trabalho foi o de analisar a importância da AI para o processo de gestão de riscos, visando verificar se o fluxo da informação está a contribuir para o alcance dos objetivos estratégicos organizacionais.

Considerando que a AI é um instrumento de mitigação de riscos, realizá-la agrega valor ao processo de gestão de riscos quanto ao *uso,* aos *recursos* e aos *fluxos* da informação.

Quanto ao *uso* da informação e da documentação relativos a riscos a AI possibilitará, por exemplo, verificar se o mapa de riscos está adequado ao formato definido no plano de gestão de riscos, se o mapeamento de processos foi realizado corretamente ou se estão disponíveis e sendo aplicados pelas respectivas unidades, se o plano de implementação de controles está preenchido corretamente e sendo usado para monitorar os controles efetivamente e se estes foram capazes de mitigar ou não os riscos.

No que diz respeito aos *recursos*, a AI auditará o sistema de informação utilizado na GR, para verificar se seus dados registrados são confiáveis e transparentes; se as informações que são necessárias aos gestores para acompanhamento do risco que a organização está exposta - se houve mitigação ou não - estão disponíveis; se existem informações ausentes no sistema, mas que deveria contemplar; se há informações presentes, mas que não são necessárias tornando o sistema robusto em informações que não agregam valor, podendo confundir o usuário; se o sistema é intuitivo ao usuário; e se proporciona ao gestor uma visão gerencial da GR, disponibilizando indicadores, dashboards, dentre outros. Nos recursos, informáticos ou não, a informação é coletada, registrada, transformada, armazenada, recuperada e disseminada. Logo, a AI deve verificar se os recursos estão sendo eficazes quanto à execução desse processo de informação.

Os sistemas utilizados na GR devem contribuir para organizar o processo, promover a sua transparência e medir a evolução organizacional. É importante que também monitore a eficácia da própria gestão de riscos visando medir o seu desempenho, calculando indicadores definidos pela organização, como: percentual de riscos mitigados, percentual de unidades com riscos gerenciados, percentual de processos estratégicos com riscos altos/muito altos, percentual de processos estratégicos com riscos mitigados, dentre outros.

O *fluxo* da GR precisa ser mapeado, institucionalizado e disseminado entre os trabalhadores - inclusive por meio de política ou plano de gestão de riscos - e deve ser reproduzido em todos os recursos utilizados na gestão de riscos - sistemas informáticos ou não. A AI responsabiliza-se em auditar o fluxo informacional da GR em termos de eficiência e conformidade com as normas. Questões como essas, devem ser atendidas: o fluxo estabelecido está sendo seguido pela unidade responsável pela GR? o fluxo definido apresenta entraves institucionais? O fluxo possibilita a disseminação das informações geradas pela GR e promove o alcance dos objetivos estratégicos? As unidades estão tendo acesso aos ativos informacionais? o fluxo pode ser melhorado? O sistema está adequado ao fluxo? As pessoas envolvidas estão sendo atuantes no fluxo?

Por fim, entende-se que a AI contribui ao avaliar a informação no que diz respeito às necessidades dos usuários, seu uso, recursos e fluxos, visando melhorar a qualidade informacional do processo de GR.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 19011: Diretrizes para auditoria de sistemas de gestão. 3. ed. Rio de Janeiro: ABNT, 2018a. Disponível em: https://pdfcoffee.com/abnt-nbr-iso-19011-2018-3-pdf-free.html Acesso em: 23. jan. 2023

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO 30301: Informação e documentação — Sistemas de gestão de documentos de arquivo — Requisitos. 3. ed. Rio de Janeiro: ABNT, 2016. Disponível em: https://fatecsenai.com.br/arquivos/30301-Informacao-e-documentacao-Sistemas-de-Gestao-de-Documentos-de-arquivo-Requisitos.pdf Acesso em: 14. jan. 2023.

BRASIL. Ministério da Transparência e Controladoria-Geral da União. Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal. Brasília, 2017b. Disponível em: https://www.gov.br/cgu/pt-

br/centrais-de-conteudo/publicacoes/auditoria-e-fiscalizacao/arquivos/manual-de-orientacoes-tecnicas-1.pdf. Acesso em: 22 jan. 2023.

CARVALHO, A. V. Auditoria e gestão da informação e do conhecimento: interações e perspectivas teórico-práticas. Ciência da Informação, *[S. l.]*, v. 48, n. 2, 2019. Disponível em: https://revista.ibict.br/ciinf/article/view/4693. Acesso em: 22 dez. 2022.

CARVALHO, Andréa Vasconcelos. A auditoria de informação e suas contribuições para a gestão estratégica. In: LILLIAN MARIA ARAUJO DE REZENDE ALVARES (Rio de Janeiro). Ibict (org.). Os múltiplos cenários da informação tecnológica no Brasil do século XXI. Rio de Janeiro: Ibict, 2021. Cap. 10. p. 233-251. Disponível em: https://repositorio.unb.br/browse?type=author&order=DESC&rpp=100&value=Alvares%2C+Lillian+Maria+Ara%C3%BAjo+de+Rezende+%28org.%29.. Acesso em: 28 jan. 2023.

CARVALHO, Andréa Vasconcelos; ESTEBAN NAVARRO, Miguel Ángel. Auditoria de Inteligência: um método para o diagnóstico de sistemas de inteligência competitiva e organizacional. In: XI ENANCIB - Encontro Nacional de Pesquisa em Ciência da Informação, 2010, Rio de Janeiro. Anais do XI ENANCIB. Rio de Janeiro: ANCIB, 2010. Disponível em: https://brapci.inf.br/index.php/res/v/180655. Acesso em 24. jan. 2022.

CHOO, CHUN WEI. A ORGANIZAÇÃO DO CONHECIMENTO. Como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. Senac, 2006. Disponível em: https://doceru.com/doc/n8e8xns. Acesso em: 20 jun. 2022.

CURVELO, Eduardo Felipe dos Santos *et al*. O PAPEL DA INFORMAÇÃO NOS INDICADORES DE DESEMPENHO E NOS PROCESSOS ORGANIZACIONAIS. P2P e Inovação, [*s. l*], v. 8, n. 2, p. 92-108, 29 mar. 2022. Semestral. Disponível em: https://revista.ibict.br/p2p/article/view/5881. Acesso em: 24 jul. 2022.

DAVENPORT, Thomas H. Ecologia da Informação: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998. Disponível em: https://ppgic.files.wordpress.com/2018/07/davenport-t-h-2002.pdf . Acesso em: 20 jun. 2022.

DUQUE, Vasco Nuno Amaral. Auditoria de informação: requisitos para um modelo. Dissertação (Mestrado em Ciências da Documentação e Informação) - Faculdade de Letras, Universidade de Lisboa, Lisboa, 2021. Disponível em: https://repositorio.ul.pt/handle/10451/49293. Acesso em: 08 jan. 2023.

LATEEF, A.; OMOTAYO, F. O. Information audit as an important tool in organizational management: A review of literature. Business Information Review, v. 36, n. 1, 2019. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/0266382119831458 Acesso em 19/01/2023

MIRANDA, Rodrigo Fontenelle de A.. Implementando a gestão de riscos no setor público. 2. ed. Belo Horizonte: Forum, 2021. 202 p. (9786555181500).

MIRANDA, S. V. de. Necessidades de informação e competências informacionais no setor público: um estudo de caso. Revista do Serviço Público, [S. l.], v. 59, n. 1, p. p. 61-80, 2014. DOI: 10.21874/rsp.v59i1.140. Disponível em: https://revista.enap.gov.br/index.php/RSP/article/view/140. Acesso em: 15. jul. 2022.

O'BRIEN, James A. Sistemas de informação e as decisões gerenciais na era da internet. 2. ed. São Paulo: Saraiva, 2004. 436 [66] p. ISBN: 8502044079.

PESTANA, O. Auditoria de informação: definição e evolução da atividade no contexto da gestão da informação e das organizações. Páginas A&B, Arquivos e Bibliotecas (Portugal), n. 2, p. 49-64, 2014. Disponível em: http://hdl.handle.net/20.500.11959/brapci/62568. Acesso em: 17 jan. 2023.

STAIR, Ralph M; REYNOLDS, George W. Princípios de sistemas de informação. São Paulo: Cengage learning, 2011. 590 p. ISBN: 9788522107971.