SemeAd 2024
XXVII Seminários em Administração

05, 06, 07 e 08 de novembro de 2024
ISSN 2177-3866

PERCEPÇÃO DOS GESTORES DE TI SOBRE O USO DA SHADOW IT NO CONTEXTO DA GESTÃO DE RISCOS EM ORGANIZAÇÕES PÚBLICAS E PRIVADAS

AUGUSTO JORGE SILVA DE SOUSA
UNIVERSIDADE FEDERAL DO CEARÁ (UFC)

JULIANA SALES CORDEIRO FERREIRA
UNIVERSIDADE FEDERAL DO CEARÁ (UFC)

HANDERSON BEZERRA FERREIRA
UNIVERSIDADE FEDERAL DO CEARÁ (UFC)

TIBERIO CESAR JOCUNDO LOUREIRO
UNIVERSIDADE FEDERAL DO CEARÁ (UFC)

ALESSANDRA CARVALHO DE VASCONCELOS
UNIVERSIDADE FEDERAL DO CEARÁ (UFC)

PERCEPÇÃO DOS GESTORES DE TI SOBRE O USO DA *SHADOW IT* NO CONTEXTO DA GESTÃO DE RISCOS EM ORGANIZAÇÕES PÚBLICAS E PRIVADAS

1 Introdução: Problema de Pesquisa e Objetivo

Shadow IT é o uso de tecnologias de informação não aprovadas ou não gerenciadas pela área de gestão de Tecnologia da Informação (TI) de uma organização, capaz de alavancar a produtividade, resolver problemas com eficiência e agilizar a comunicação (Silic; Back, 2014). Pode incluir parte física (*hardware*), programa (*software*), serviços em nuvem, recurso de TI que não esteja sob o controle da equipe de TI central (Silic; Back, 2014), ou qualquer outra solução usada pelos funcionários dentro do ecossistema organizacional que não recebeu nenhuma aprovação formal do departamento de TI (Monteiro Junior, 2018).

Györy *et al*. (2012) consideram a *shadow IT* um fenômeno incompreendido e relativamente inexplorado. No mesmo sentido, Machado (2023) e Silic, Silic e Oblakivic (2016) afirmam que a *shadow IT* é um fenômeno que pode ser considerado emergente e está trazendo uma série de desafios para a gestão, além de riscos para a segurança organizacional. Esses desafios da *shadow IT* envolvem a aprovação ética, privacidade e a confusão de papeis, aspectos contemplados pela governança de TI nas organizações (Van Der Weele; Bredewold, 2021).

Conforme Machado (2023) e Monteiro Junior (2018) explicam, a *shadow IT* tem ganhado proporção por conta do crescente acesso à tecnologia e à facilidade de sua utilização, permitindo que as pessoas tenham maior familiaridade com essa prática. Dessa forma, considera-se que o conhecimento da *shadow IT* por parte dos gestores e da governança pode transformar riscos em oportunidades de negócio e requer, a todo momento, profissionais preparados e proativos, com respostas rápidas e assertivas das organizações públicas e privadas.

Considerando essa breve contextualização, surge a pergunta norteadora desta pesquisa: Qual a percepção dos gestores de TI sobre o uso da *shadow IT* no contexto da gestão de riscos? Com o intuito de responder a essa questão, o objetivo geral do estudo é analisar a percepção dos gestores de TI sobre o uso da *shadow IT* no contexto da gestão de riscos.

Para o alcance do objetivo geral, têm-se os seguintes objetivos específicos: i) avaliar o conhecimento dos gestores de TI sobre *shadow IT* e a existência na sua organização; ii) identificar a percepção dos gestores de TI sobre a responsabilidade da área de TI quanto ao uso da *shadow IT*; e iii) identificar a percepção dos gestores de TI quanto à prática de *shadow IT* no contexto da gestão de riscos, considerando o tipo da sua organização (pública ou privada).

Nessa perspectiva, o presente estudo se justifica devido à relevância prática e teórica do tema nos ambientes corporativo e acadêmico, contribuindo para identificar os possíveis riscos associados ao uso da *shadow IT*, considerando também temas cruciais para organizações públicas e privadas, como governança de TI, segurança cibernética e controles internos.

Conforme enunciam Silic e Back (2014), a *shadow* IT, também conhecida como TI invisível, tem influenciado negativamente questões de segurança da informação nas organizações e provocado a ocorrência de inconsistências em regras e processos de negócio (Moura Jr., 2017; Strong; Volkoff, 2004). Assim, a realização de pesquisas nesse campo de estudo pode beneficiar gestores de negócio e de TI, oferecendo direcionamentos práticos e *insights* valiosos para organizações de forma geral, promovendo o desenvolvimento de estratégias, traduzindo conhecimentos acadêmicos em ferramentas práticas e tangíveis.

Destaca-se, ainda, que o estado do Ceará (foco desta investigação) foi selecionado intencionalmente para o presente estudo devido à pujança do setor de tecnologia da informação e comunicação (TIC) no estado, cujo crescimento alcançou 20% nos últimos três anos, sendo responsável pela geração de 43 mil empregos e movimentando mais de R$ 1 bilhão de reais por ano (ASSESPRO, 2023). Ademais, a presença do setor de TIC é transversal a todos os outros segmentos da economia cearense, o que reforça a importância da temática em tela para que

quaisquer tipos de organizações tenham a capacidade de explorar a *shadow IT* como uma vantagem competitiva.

2 Fundamentação Teórica

2.1 A evolução da *shadow IT*

Conforme Machado (2022), existem vários termos diferentes para descrever o fenômeno *shadow IT* (como *rogue IT*, *shadow systems*, *workaround systems* ou *feral systems*), além de TI invisível (Silic; Back, 2014). O termo *shadow IT* é aqui utilizado porque parece ser o mais amplamente aceito na literatura. Desde 2012, estudos sobre *shadow IT* têm ganhado relevância, sendo que a maioria deles é recente (publicados entre 2014 e 2020). Neste sentido, o assunto pode ser considerado emergente (Silic; Silic; Oblakivic, 2016), mesmo que tenha ganhado notoriedade na academia com o passar dos anos.

Mallmann, Pinto e Maçada (2019) explicam que os primeiros estudos sobre *shadow IT* abordam o seu surgimento após a adoção de sistemas *Enterprise Resource Planning* (ERP), por meio do uso de planilhas alternativas ao uso do sistema contratado. No âmbito do tratamento do uso de *shadow IT* pela governança de TI, Györy *et al*. (2012) estudaram as possíveis decisões em relação ao uso de *shadow IT* dentro da organização. Na mesma época, um modelo de avaliação de *shadow IT* foi proposto por Rentrop e Zimmermann (2012), o qual foi utilizado em estudos posteriores, dentre os quais se destacam os trabalhos desenvolvidos por Fuerstenau, Rothe e Sandner (2017), Klotz, Westner e Strahringer (2020) e Zimmermann e Rentrop (2014).

Machado (2023) analisou as bases de dados *Scopus*, *Web of Science* (WoS) e os principais periódicos da *Association of Information Systems* (AIS), tendo como parâmetro os anos de 2002 a 2021, e observou a evolução de publicações sobre o tema *shadow IT* a partir de 2012. Machado (2023) examinou 114 artigos e identificou que 105 (92,1%) foram publicados nos últimos 10 anos (2012-2021), demonstrando que as discussões sobre *shadow IT* podem ser consideradas recentes e emergentes, haja vista o aumento considerável de publicações nesse período (Haag; Eckhardt, 2017; Klotz *et al.*, 2019; Silic; Barlow; Back, 2017).

A evolução das publicações do *shadow IT* é evidenciada por diversas categorias que englobam práticas relacionadas ao uso não autorizado de tecnologias nas organizações. Uma dessas categorias é a utilização de serviços de nuvem não aprovados, que envolve o emprego de *software* baseado na internet e *Software-as-a-Service* (SaaS) sem a devida aprovação ou conhecimento do departamento de TI. Mallmann, Pinto e Maçada (2019) e Machado (2023) apontam exemplos para compreensão desse fenômeno, como *WhatsApp, Facebook, Skype* para *Web, Dropbox* e *Google Apps*, que caracterizam o *Mobile shadow IT*, por possibilitarem acesso fora do ambiente de trabalho.

Outra categoria relevante na evolução do *shadow IT* é a adoção de soluções desenvolvidas pelo próprio empregado, como é observado por Mallmann, Pinto e Maçada (2019) e Machado (2023), como planilhas do *software Excel* ou aplicativos desenvolvidos internamente, para realizar suas tarefas de trabalho. Nesse sentido, os autores ressaltam a autonomia dos funcionários na criação de ferramentas adaptadas às suas necessidades específicas (Mallmann; Pinto; Maçada, 2019; Machado, 2023).

Pode-se observar que, na categoria de aplicativos auto instalados, Mallmann, Pinto e Maçada (2019) e Machado (2019) destacam o uso de *software* instalado independentemente pelos funcionários em seus dispositivos de trabalho. Autores como Silic e Back (2014) discutem esse fenômeno, evidenciando a instalação de *software* disponível gratuitamente na internet sem a devida autorização do departamento de TI.

Já na categoria de dispositivos auto adquiridos, Machado (2019) e Mallmann, Pinto e Maçada (2019) revelam a utilização de dispositivos pessoais pelos funcionários no ambiente de trabalho, adquiridos diretamente no varejo. Silic e Back (2014) abordam essa prática, evidenciando a preferência dos funcionários por dispositivos não oficiais, muitas vezes contornando os processos estabelecidos pelo departamento de TI. Essas categorias refletem a

complexidade e a constante evolução do *shadow IT*, destacando a importância de abordagens mais flexíveis e estratégias de gestão eficazes para lidar com esse fenômeno emergente.

Pode-se então destacar, por meio dos achados de Mallmann, Pinto e Maçada (2019) e Machado (2023), que muitas vezes os funcionários não têm ciência de que estão utilizando ferramentas de *shadow IT*, o que demonstra ainda mais a importância dos gestores de explorarem o assunto nas organizações, principalmente no período pós pandemia de Covid-19, em que as ferramentas de trabalho *online* avançaram para níveis mais elevados.

Pesquisa realizada em grandes empresas em 2021 pela Gartner Group revelou que 30% a 40% dos gastos com TI são consumidos pela *shadow IT* e que uma empresa utiliza em média 57 serviços diferentes de compartilhamento de arquivos (Mitrovich, 2021). Ademais, Chaleff (2020) aponta que 83% dos profissionais de TI relataram que os funcionários armazenam dados da empresa em serviços de nuvem não autorizados, fato também constatado na pesquisa de Machado, Maçada e Dolci (2022).

Embora os sistemas *shadow IT* sejam geralmente vistos de forma negativa, eles também oferecem vantagens que permitem que os indivíduos alcancem resultados de trabalho mais positivos. Esses resultados podem ser uma solução mais eficaz e eficiente do que as que estão disponíveis nos sistemas corporativos (Aragão; Streit, 2023; Behrens; Sedera, 2004).

Assim, as organizações precisam promovê-la e incentivá-la de modo que os funcionários se sintam livres para não apenas explorar suas ideias e processos inovadores, mas também falar sobre elas e compartilhar seus *insights* que podem ser implementados em toda a estrutura organizacional, se forem úteis. No entanto, isso depende do tipo de cultura organizacional existente (Aragão; Streit, 2023; Kopper *et al.*, 2019).

Dito isto, se demonstra a importância do estudo da temática e discussão com os gestores de TI de diferentes organizações (públicas e privadas), devido às implicações nas instituições, em que não se pode ignorar o fenômeno que está acontecendo.

Silic e Back (2014) consideram que o uso da *shadow IT* nas organizações pode alavancar a produtividade, resolver problemas com eficiência e ainda agilizar a comunicação. No entanto, os riscos de TI com a adoção dessa prática são muito aumentados, devendo as organizações aprenderem a lidar com o seu uso, ao invés de simplesmente restringi-lo.

Na perspectiva dos riscos, Klotz *et al*. (2019) definem que os principais riscos associados ao uso da *shadow IT* são os relacionados à segurança de dados, falta de privacidade, perda da sinergia e a criação de ineficiência. Kopper e Wertner (2016) citam que são reconhecidos na literatura, apesar dos benefícios, aspectos negativos como a falta de segurança, risco de conformidade (*compliance*) e problemas de eficiência – aspectos que são conectados à governança de TI.

Na mesma linha, Silic e Back (2014) afirmam que a expansão do uso de dispositivos pessoais no trabalho, como *smartphones*, *notebooks* e *tablets*, e a popularização da computação em nuvem, fez com que a *shadow IT* invadisse os sistemas organizacionais, trazendo riscos de segurança sem precedentes para os departamentos de TI. Problemas de *compliance*, perda de tempo, lógica de negócios inconsistente, riscos aumentados de perda ou vazamento de dados e investimentos desperdiçados são apenas alguns dos riscos que podem ter sérios impactos (Silic; Back, 2014).

Quanto ao desperdício de recursos, Rentrop e Zimmermann (2012) comentam que a construção ou contratação de diversos aplicativos paralelos tem altos custos. No entanto, quando se constrói algo de forma centralizada e colaborativa, a organização pode ter ganhos de escala, além de ser possível elaborar um planejamento para as integrações e para o uso de conexões entre outras aplicações já utilizadas. Além disso, os autores advertem que o uso de tecnologias não autorizadas aumenta a vulnerabilidade e os riscos nos processos de trabalho.

Outro risco relevante trazido pela *shadow IT* é causado pela falta ou ausência de controle das atividades do usuário, visto que a TI deve realizar a manutenção e melhorias

contínuas apenas daqueles dispositivos e sistemas oficiais que são determinados no planejamento tecnológico da organização. Essa falta de controle pode tanto complicar e atrasar a solução de falhas quanto criar pontos cegos na gestão das informações (Györy *et al*., 2012).

Contudo, apesar dos riscos envolvidos, a utilização da *shadow IT* também pode trazer vantagens competitivas e benefícios para a organização. Para Klotz *et al*. (2019), os principais benefícios da *shadow IT* estão associados ao ganho de produtividade e agilidade, melhoria da satisfação do usuário e aprimoramento da colaboração. Ademais, a *shadow IT* possibilita o alcance de resultados de trabalho de maneira diferenciada, sem a dependência do departamento de TI da organização, por vezes sobrecarregado com demandas mais genéricas e impossibilitado de atender as demandas na mesma rapidez com que elas surgem. Por esse motivo, Behrens e Sedera (2004) consideram que a *shadow IT* pode ser uma solução mais eficaz e eficiente do que o sistema oficial oferece.

Os benefícios do uso da *shadow IT* podem ser observados também à medida que ela preenche uma lacuna deixada pela TI, cuja falha consiste em deixar de fornecer todos os serviços para atender as necessidades dos clientes. Não se pode, portanto, ignorar sua utilização, mas aprender a como lidar com ela (Raden, 2005).

Silic e Back (2014) constataram que, em geral, os funcionários usam extensivamente a *shadow IT*, pois os torna mais rápidos e produtivos, além de melhorar a colaboração e comunicação. Apesar de os riscos de TI aumentarem muito no contexto de utilização da *shadow IT*, as organizações têm controles e contramedidas que podem mitigá-los, sendo a restrição do uso uma solução válida, mas não definitiva, tendo em vista que os desafios encontrados podem se tornar oportunidades para todo o ecossistema organizacional.

Outrossim, Mallmann, Maçada e Eckhardt (2018) argumentam que ao invés de evitar o uso de *shadow IT*, as organizações deveriam encontrar formas de mitigar os riscos, ao mesmo tempo em que reconhecem as oportunidades de melhorias proporcionadas por ela, a partir da aplicação da gestão de riscos no contexto da governança de TI.

2.2 Gestão de riscos

A literatura acerca da gestão de risco oferece uma base robusta para compreender os desafios enfrentados nas organizações sejam elas públicas ou privadas. O manual de riscos do Tribunal de Contas da União - TCU (2020) mostra a complexidade crescente dos ambientes tecnológicos e a necessidade de conformidade com regulamentações em constantes mudanças e camadas adicionais de desafio. Aragão e Streit (2023) identificam a necessidade da agilidade na adaptação de estratégias e a implementação de medidas de mitigação inovadoras para enfrentar esses desafios em constante evolução.

A implementação de melhores práticas, como os *frameworks* internacionalmente reconhecidos ISO 31000 e NIST *Cybersecurity Framework*, fornece uma base sólida para abordar proativamente os riscos (Kopper *et al.*, 2018). Almém disso, Siqueira e Larieira (2021) ressaltam que a gestão de riscos permeia diversas áreas, desde as dimensões financeiras até as operacionais, desempenhando um papel na sustentabilidade e na tomada de decisões estratégicas.

No contexto organizacional mais dinâmico e interconectado, Behrens e Sedera, (2004) salientam que a gestão de riscos se torna uma ferramenta base que garante a resiliência e a continuidade dos negócios. Além de mitigar ameaças, a abordagem sistemática busca identificar oportunidades que impulsionam o crescimento e a inovação. Desta forma, ao abranger facetas operacionais, financeiras e estratégicas, a gestão de riscos busca antecipar, compreender e responder a eventos incertos que podem influenciar negativamente os objetivos da organização (Behrens; Sedera, 2004). Para tanto, a gestão de riscos de TI deve ser alinhada estrategicamente à gestão de riscos tradicional, reconhecendo as particularidades do cenário tecnológico.

2.3 Gestão de riscos de TI e a *shadow IT*

A gestão de riscos de TI é um dos pilares fundamentais para se considerar as complexidades do ambiente tecnológico nas organizações contemporâneas (Parreira, 2019). Parreira (2019) afirma que, enquanto a dependência em sistemas informatizados cresce exponencialmente, a integridade, confidencialidade e disponibilidade das informações tornam-se prioridades críticas. Nesse contexto, Behrens (2022) ressalta que a gestão de riscos de TI focaliza desafios específicos, abordando ameaças como falhas de segurança, interrupções de serviço e questões de conformidade regulatória.

Machado, Maçada e Dolci (2022) ressaltam que além de enfrentar ameaças iminentes, a gestão de riscos de TI incorpora práticas para garantir a conformidade regulatória e a governança efetiva dos recursos tecnológicos. Isso não apenas promove a segurança operacional, mas também fortalece a resiliência organizacional em face de desafios dinâmicos.

Nos ambientes dinâmicos e altamente conectados, estratégias proativas tornam-se essenciais. Parreira (2019) destaca a implicação da implementação de controles de segurança robustos, avaliação constante de vulnerabilidades e o cultivo de uma cultura organizacional que prioriza a conscientização sobre a importância da segurança nas áreas de tecnologia.

A gestão de riscos de TI, para Behrens (2022), não é apenas uma resposta a ameaças, mas uma postura proativa para mitigar riscos, proteger ativos tecnológicos e manter a confiança dos *stakeholders*. Assim, é possível afirmar que a gestão de riscos de TI não é estática, mas sim um campo em constante evolução. Machado (2023) aponta que a integração harmoniosa entre as estratégias de gestão de riscos tradicional e de TI é vital para garantir uma abordagem holística e eficaz, garantindo a proteção dos ativos e fomentando operações seguras e sustentáveis.

Assim, coexistindo sobre a mesma linha de pensamento, Machado (2023) e Parreira (2019) identificam que a gestão de riscos de TI não apenas enfrenta os desafios específicos do ambiente tecnológico, mas contribui de maneira significativa para a resiliência e prosperidade organizacional em um cenário empresarial cada vez mais digitalizado. Assim, ao incorporar essa perspectiva abrangente e dinâmica, as organizações podem posicionar-se de maneira mais eficaz diante das rápidas mudanças e complexidades inerentes ao mundo da TI (Silva, 2020).

Destarte, no contexto da gestão de riscos de TI, a ascensão da *shadow IT* é caracterizada pelo uso não autorizado ou não supervisionado de tecnologias e serviços pelos colaboradores. Aragão e Streit (2023) apresentam a *shadow IT* como um desafio crescente para a segurança e governança de TI e menciona que por muitas vezes o fenômeno ocorre fora do escopo tradicional dos controles organizacionais, resultando em lacunas de segurança e riscos não identificados. Machado, Maçada e Dolci (2022) enfatizam que a gestão de riscos, quando estendida à *shadow IT*, visa compreender e mitigar os riscos dessas práticas não oficiais.

Siqueira e Larieira (2021) dizem que tem se percebido que muitos departamentos recorrem à *shadow IT* na tentativa de encontrar soluções mais ágeis e adaptáveis às suas necessidades específicas, muitas vezes não atendidas pelas vias formais de TI. Machado (2023) menciona que, no entanto, essa prática apresenta desafios consideráveis para as organizações, principalmente no que diz respeito à segurança da informação e que o uso não autorizado de tecnologia pode resultar em vulnerabilidades, elevando o risco de violações de dados e comprometimento da integridade do sistema.

Aragão e Streit (2023) ressaltam que outro desafio associado à *shadow IT* está relacionado à conformidade e governança. As soluções adotadas muitas vezes não estão em conformidade com as regulamentações, o que pode acarretar dificuldades na auditoria e rastreamento do uso de tecnologia. Por isso, evidencia-se a necessidade premente de estratégias para mitigar os riscos decorrentes da *shadow IT*.

A interconexão entre as áreas gestão de riscos, gestão de riscos de TI e governança de TI, mencionada por Aragão e Streit (2023), coaliza como estratégia essencial para uma

estratégia robusta e abrangente, para melhor compreensão sobre o uso da *shadow IT*. Monteiro Junior (2018) afirma que a gestão de riscos de TI precisa estar alinhada com os objetivos organizacionais gerais, considerando as nuances tecnológicas. Nos relatos de Siqueira e Larieira (2021), os autores colocam em evidência que a integração com a gestão de riscos tradicional permite uma visão holística, identificando interdependências e pontos de sinergia e que ao estender essas práticas à *shadow IT*, as organizações podem antecipar e responder proativamente aos riscos emergentes, promovendo uma cultura de segurança e conformidade.

Em suma, a gestão de riscos efetiva, quando associada à *shadow IT*, não apenas aborda ameaças convencionais, mas também reconhece as motivações dos usuários finais. Esta abordagem integrada é crucial para enfrentar os desafios contemporâneos, promovendo a segurança, conformidade e inovação dentro das organizações.

3 Metodologia

A pesquisa se enquadra como descritiva, visando a descrição das características de uma determinada população ou fenômeno, caracterizando-se pela utilização de técnicas padronizadas de coleta de dados (Gil, 2002). No caso em comento, objetiva-se analisar a percepção dos gestores de TI sobre o uso da *shadow IT* no contexto da gestão de riscos. Com relação aos procedimentos, foi aplicado um questionário através da plataforma *Google Forms.*

A pesquisa tem natureza qualitativa, dado que não utiliza modelos matemáticos e/ou de aplicações estatísticas, mas da interpretação de textos, sons, imagens e até de linguagem não verbal (Guba; Lincoln, 2005). Marconi e Lakatos (2017) explicam que a abordagem qualitativa tem como premissa analisar aspectos mais profundos, fornecendo análises mais detalhadas sobre as investigações, atitudes e tendências de comportamento.

O universo de gestores de TI, escolhido propositalmente para a pesquisa, é o Grupo de Gestores de Tecnologia da Informação e Comunicação do Estado do Ceará (GGTIC). O GGTIC, formado por profissionais de TI do estado do Ceará, é uma associação civil de direito privado sediada em Fortaleza, sem fins econômicos, regida por leis nacionais e constituída por meio de estatuto. Seus objetivos sociais incluem a promoção da capacitação profissional dos associados por meio da troca de experiências, a provisão de informações éticas sobre fornecedores de TIC, a divulgação dos princípios do grupo para conscientizar os fornecedores de TIC e o apoio a organizações sem fins lucrativos solicitando informações sobre TIC, treinamentos e participação em campanhas de inclusão digital (GGTIC, 2023).

O grupo, formado informalmente em 2005 por amigos da área de TIC, foi oficializado em 2010, com a assinatura de um estatuto pelos 20 *Chief Information Officers* (CIOs) fundadores. Representando empresas em diversos setores (têxtil, alimentício, metalmecânico, químico, gás, comércio, serviços, educação, construção civil, entretenimento e seguro saúde), o GGTIC tem crescido e se fortalecido desde então, contando hoje com mais de 130 CIOs associados, com plenas condições de representar a amostra para a presente pesquisa, composta por gestores de TI que atuam em organizações públicas e privadas do Ceará (GGTIC, 2023).

A coleta de dados da pesquisa foi realizada nos meses de novembro e dezembro de 2023, por meio de aplicação de questionário adaptado de Kopper (2017), Mallman, Pinto e Maçada (2019) e Monteiro Junior (2018), junto aos 130 membros do Grupo GGTIC. O questionário foi estruturado com 18 perguntas, buscando compreender a percepção dos gestores de TI sobre o uso da *shadow IT* no contexto da gestão de riscos.

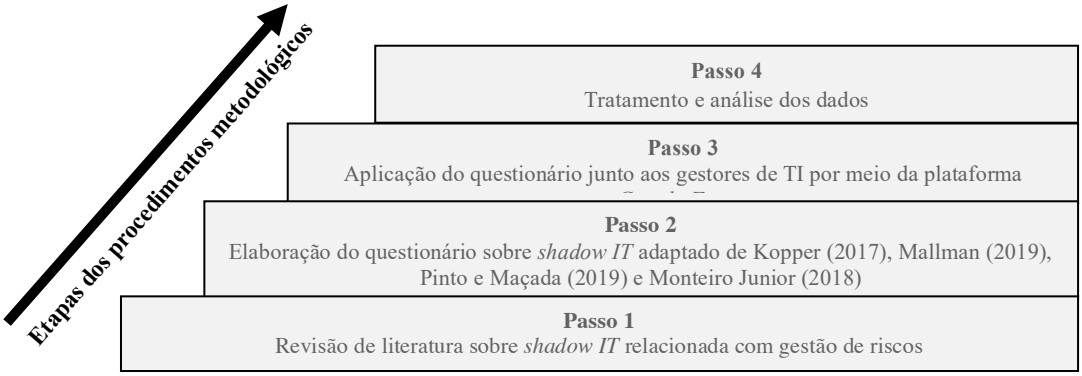
Quadro 1 - Questões que contemplaram o questionário aplicado na pesquisa

Perfil do gestor de TI e da sua organização
1. Informe seu gênero: ( ) feminino; ( ) masculino; ( ) outro; ( ) prefiro não informar
2. Qual sua faixa etária (idade)? de 20 a 30; de 31 a 40; de 41 a 50; de 51 a 60; acima de 60 anos
3. Tempo de atuação como gestor de TI (em anos): até 5; de 6 a 10; de 11 a 15; de 16 a 20; acima de 20 anos
4. Você exerce suas atividades em uma organização: ( ) privada; ( ) pública
Conhecimento dos gestores de TI sobre *shadow IT* e sua existência na sua organização (Fonte: adaptado de Monteiro Junior, 2018)
5. Você conhece o termo *shadow IT*? ( ) sim; ( ) não
6. No contexto da organização em que você atua, considerando que a *shadow IT* refere-se a programas, *softwares*, dispositivos, planilhas e serviços que estejam fora do controle do departamento de TI e que não possuem aprovação explícita da organização, pode-se afirmar que: ( ) não há *shadow IT* na organização; ( ) pode ser que haja *shadow IT* na organização; ( ) não tenho como afirmar que há *shadow IT* na organização; ( ) tem alguma solução que se enquadra como *shadow IT* na organização
Responsabilidade da área de TI quanto às práticas de *shadow IT* no âmbito das organizações (Fonte: adaptado de Monteiro Junior, 2018)
7. Considerando que a *shadow IT* pode ser um problema, onde a área de TI não tem controle dos programas desenvolvidos: ( ) a *shadow IT* deve ser eliminada; ( ) a *shadow IT* deve ser controlada; ( ) a *shadow IT* é uma necessidade e deve existir; ( ) a *shadow IT* deve ser tratada exclusivamente pela área de TI
8. Na perspectiva de neutralizar e afastar: Previsão de uso da *shadow IT:* ( ) o uso é uma violação das normas; ( ) o uso é uma necessidade e deve ser controlado; ( ) a *shadow IT* deve ser banida da organização; ( ) a *shadow IT* deve ser tratada exclusivamente pela área de TI
9. Os profissionais de TI compartilham a culpa pelo problema da *shadow IT*, posso afirmar que: ( ) não se tem tempo para se desenvolver a necessidade urgente; ( ) falta de interesse entre as áreas; ( ) a área de TI não está alinhada com a organização; ( ) há desconhecimento técnico dos profissionais da área de TI para implementar as soluções
10. Sobre a credibilidade da informação, o impacto dos sistemas desenvolvidos no ambiente *shadow IT,* e a tomada de decisões gerenciais: ( ) estes sistemas tem total credibilidade; ( ) podem causar danos irreparáveis à organização; ( ) são necessários aos negócios; ( ) frequentemente são utilizados na toma da de decisão
11. Falta de consciência da segurança e análise na exposição ao risco do uso da *shadow IT:* ( ) não concordo; ( ) concordo parcialmente; ( ) é uma necessidade o uso mesmo com risco; ( ) deve ser negado seu uso
Prática de *shadow IT* no contexto da gestão de riscos na organização em que você atua (Fonte: adaptado de Kopper, 2017; Mallman, Pinto e Maçada, 2019; Monteiro Junior, 2018)
12. As pessoas usam *shadow IT,* mas desconhecem, principalmente seus riscos: ( ) não concordo; ( ) concordo parcialmente; ( ) é uma necessidade o uso mesmo com risco; ( ) deve ser negado seu uso
13. Qual o maior risco que se destaca no uso da *shadow IT*?: ( ) exposição da organização à fraude; ( ) exposição da imagem da empresa; ( ) exposição da empresa a perdas financeiras;( ) integração pobre das soluções de *shadow IT* às demais soluções de TI da organização; ( ) alto custo na manutenção das soluções de *shadow IT*
14. Colaboradores que são detectados violando regras de segurança com aplicações de *shadow IT* são punidos: ( ) não concordo; ( ) concordo parcialmente; ( ) concordo totalmente
15. A área de TI tem conhecimento dos colaboradores que violam as regras quanto ao uso de soluções tecnológicas: ( ) não concordo; ( ) concordo parcialmente; ( ) concordo totalmente
16. A organização define políticas para tratamento de riscos de *shadow IT* como requisitos de licenciamento, segurança e privacidade: ( ) não concordo; ( ) concordo parcialmente; ( ) concordo totalmente
17. A área de TI tem capacidade para avaliação dos riscos das soluções de *shadow IT* detectadas: ( ) não concordo; ( ) concordo parcialmente; ( ) concordo totalmente
18. A organização define ações específicas de detecção de *shadow IT*, como monitoramento de tráfego de rede: ( ) não concordo; ( ) concordo parcialmente; ( ) concordo totalmente

Fonte: Elaborado pelos autores a partir de Kopper (2017), Mallman, Pinto e Maçada (2019) e Monteiro Junior (2018).

A Figura 1 ilustra o percurso metodológico adotado no estudo para o alcance dos objetivos propostos.

Figura 1 - Etapas dos procedimentos metodológicos



Fonte: elaborada pelos autores.

O percurso metodológico iniciou-se com a busca de trabalhos sobre *shadow IT* envolvendo gestão de riscos nas plataformas Google Acadêmico, *Spell* e *Web of Science*. Após a revisão de literatura, iniciou-se a elaboração de um questionário que proporcionasse o alcance dos objetivos propostos. Sendo assim, utilizou-se uma adaptação dos instrumentos de pesquisa utilizados nos trabalhos de Kopper (2017), Mallman, Pinto e Maçada (2019) e Monteiro Junior (2018). A seguir, o referido questionário foi aplicado junto aos 130 gestores do grupo GGTIC-CE por meio da plataforma *Google Forms* e o seu resultado foi compilado por meio de planilha no *software* Excel e exposto a seguir por meio de tabelas e figuras.

4 Resultados

Nesse ponto, cabe esclarecer que o universo da pesquisa é composto apenas pelos 130 gestores de TI membros do GGTIC-CE no mês de novembro de 2023, não sendo objeto de avaliação a percepção de usuários finais a respeito da *shadow IT*. Findo o prazo estabelecido para respostas (08/12/2023), obteve-se 43 respostas válidas, representando 33% dos gestores membros do GGTIC-CE.

4.1 Perfil dos gestores de TI

As questões iniciais do questionário possibilitaram a identificação do perfil dos 43 gestores de TI do estado do Ceará participantes da pesquisa (Tabela 1), de forma a melhor compreender as análises posteriores.

Tabela 1 - Perfil dos gestores

Caraterística	Categorias	Quantidade
Gênero	feminino	3
	masculino	40
Faixa etária	de 20 a 30 anos	1
	de 31 a 40 anos	13
	de 41 a 50 anos	16
	de 51 a 60 anos	8
	acima de 60 anos	5
Tempo de atuação como gestor de TI	até 5 anos	2
	de 6 a 10 anos	10
	de 11 a 15 anos	12
	de 16 a 20 anos	7
	acima de 20 anos	12
Tipo da organização em que atua	privada	21
	pública	22

Fonte: dados da pesquisa (2023).

Quanto ao perfil dos gestores participantes da pesquisa, em linhas gerais, nota-se que a maioria é homem (93%), com idade entre 31 e 50 anos (67%) e tem de 6 a 15 anos de experiência como gestor de TI (51%). Sobre o gênero dos gestores, onde observa-se que apenas

três respondentes são mulheres (7%). Importante lembrar que, segundo a Pesquisa Nacional por Amostra de Domicílios (PNAD, 2018), no Brasil, tem-se que 20% dos profissionais de TI são mulheres, e, por outro lado, a parcela feminina da população nacional supera a marca de 52,5%.

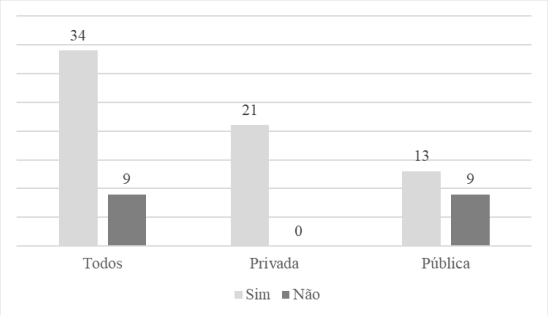
Ainda é possível verificar que há uma distribuição equilibrada entre gestores de TI que atuam em organizações públicas e privadas (Tabela 1). Esse fato proporciona a análise comparativa da prática de *shadow IT* e da gestão de riscos nos dois cenários (setor público x inciativa privada).

4.2 Conhecimento sobre o termo *shadow IT*

Após a identificação do perfil dos gestores de TI e do tipo de organização em que eles atuam, verificou-se qual o conhecimento dos gestores sobre o termo *shadow IT* e constatou-se que 34 gestores de TI (74%) conhecem o termo, enquanto que 9 gestores (26%) indicaram desconhecer o termo.

Para melhor compreensão sobre o conhecimento dos gestores de TI quanto ao termo *shadow IT*, agora considerando o tipo de organização em que atua, apresenta-se a Figura 2.

Figura 2 - Conhecimento dos gestores de TI sobre o termo *shadow IT*, distribuídos conforme tipo de organização em que atuam

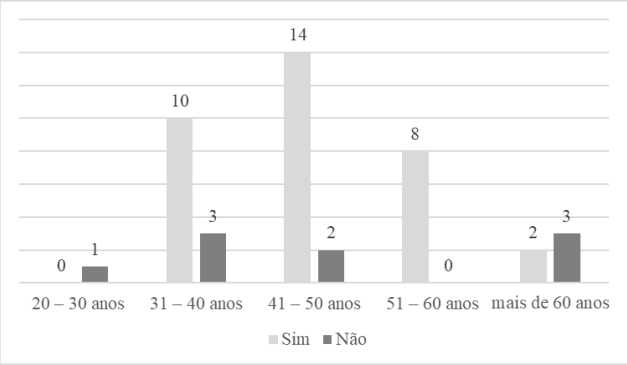


Fonte: dados da pesquisa (2023).

A partir da Figura 2 percebe que 100% dos gestores de TI que atuam em organizações privadas conhecem o termo *shadow IT*, enquanto 45% dos gestores que atuam no setor público declaram não ter conhecimento sobre o termo, caracterizando importante achado da pesquisa. Cabe aqui mencionar que Monteiro Junior (2018) ressalta a importância do conhecimento do termo para a gestão eficaz dos riscos associados.

Na sequência, buscou-se identificar o conhecimento dos gestores de TI quanto ao termo *shadow IT*, considerando a faixa etária dos mesmos (Figura 3).

Figura 3 - Conhecimento dos gestores sobre o termo *shadow IT*, distribuídos conforme a faixa etária

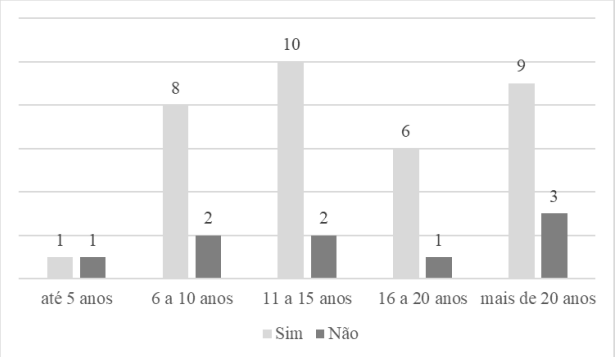


Fonte: dados da pesquisa (2023).

Na Figura 3, nota-se que a maior parte dos gestores com mais de 60 anos desconhece o termo *shadow IT*. Mas observa-se que parte dos gestores que apontou desconhecer o termo possui até 50 anos de idade.

A Figura 4 ilustra a distribuição dos gestores, conforme o tempo de atividade como gestor de TI, visando identificar o conhecimento deles quanto ao termo *shadow IT*.

Figura 4 - Conhecimento dos gestores sobre o termo *shadow IT*, distribuídos conforme o tempo de atividade como gestor de TI



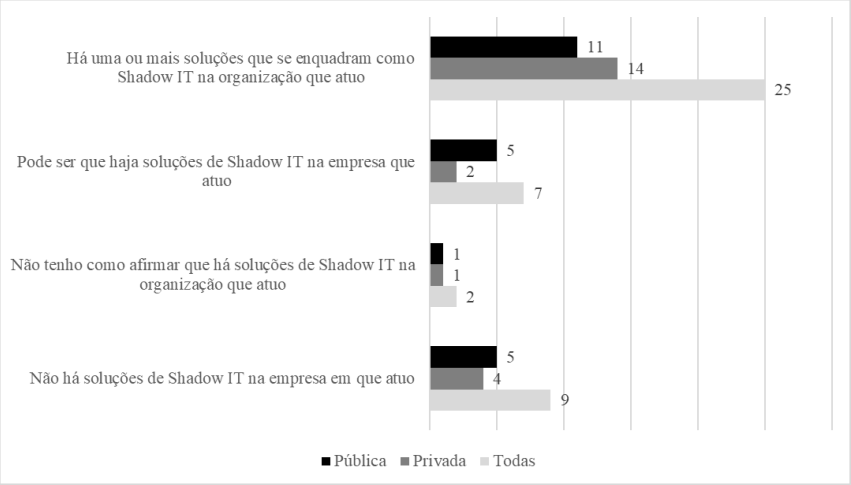
Fonte: dados da pesquisa (2023).

Verifica-se, a partir das informações da Figura 4 que é possível identificar diferenças quanto ao conhecimento dos gestores sobre o termo *shadow IT* em função do seu tempo de atividade como gestor de TI, evidenciando algumas peculiaridades na percepção dos gestores de TI em função do seu perfil.

4.3 Percepção dos gestores de TI sobre a existência da *shadow IT* na sua organização e a responsabilidade da área de TI quanto ao seu uso

Após a explanação sobre o que está contido na *shadow IT*, os gestores de TI apresentaram suas percepções sobre a ocorrência de práticas de *shadow IT* em suas organizações (Figura 5).

Figura 5 - Percepção dos gestores de TI sobre a existência da *shadow IT* na organização



Fonte: dados da pesquisa (2023).

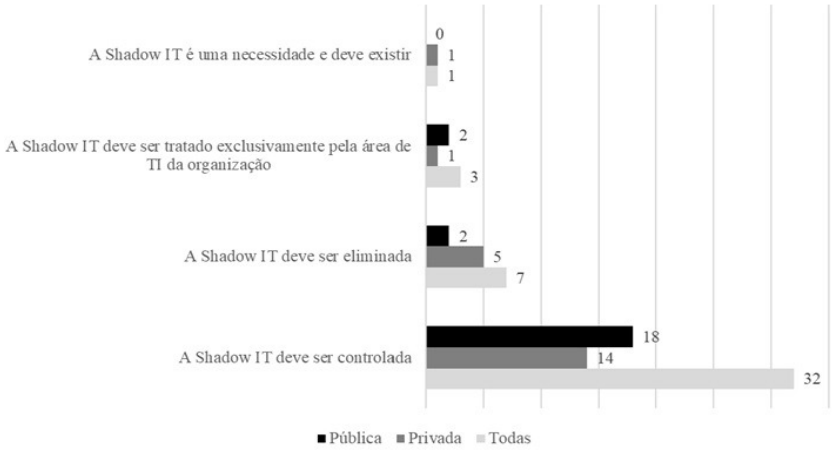
As informações evidenciadas na Figura 5 revelam que 58% dos gestores de TI está ciente do uso de tecnologias não autorizadas em suas organizações, sendo mais comum em organizações privadas. Esse fato pode refletir a maior cobrança por produtividade e resultados nas organizações privadas, o que faz com que os empregados busquem soluções isoladas para atender suas necessidades. Destaca-se que Silic e Back (2014) ponderam que a *shadow IT* é uma prática comum, devido à busca por soluções rápidas e eficazes pelos colaboradores.

Cabe ainda salientar que 21% dos gestores de TI informam que não há práticas de *shadow IT* em suas organizações, sendo que tal proporção é semelhante nas organizações públicas e privadas e 16% dos gestores de TI consideram que pode ser que haja o uso da *shadow*

IT na organização, mas não têm certeza do fato. Nesse caso, a proporção de gestores de TI que atuam no setor público é preponderante.

A Figura 6 apresenta o posicionamento dos gestores de TI quanto ao endereçamento do que deve ser feito quando da detecção de práticas de *shadow IT* nas organizações.

Figura 6 - Percepção dos gestores de TI quanto à responsabilidade da área de TI sobre o uso da *shadow IT*



Fonte: dados da pesquisa (2023).

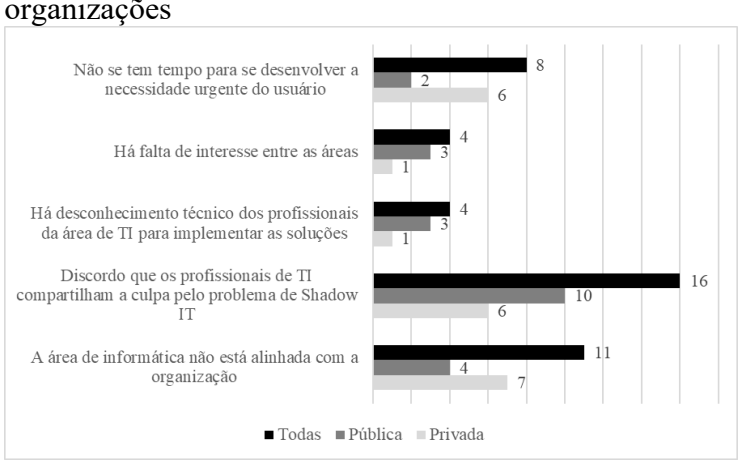
De acordo com a Figura 6, verifica-se que a maioria dos gestores de TI entende que a área de TI da organização deve ter instrumentos que possibilitem o controle das práticas de *shadow IT* (70%), comportamento esse que se mantém tanto para gestores de TI que atuam tanto em organizações públicas quanto privadas. Esse achado está alinhado com Györy *et al.* (2012), que defendem a necessidade de mecanismos de controle na governança de TI.

Por sua vez, 15% dos gestores de TI participantes da pesquisa consideram que a *shadow IT* deve ser eliminada da organização, provavelmente em função dos aspectos negativos que a prática pode proporcionar à organização, como a falta de segurança, risco de conformidade (*compliance*) e problemas de eficiência – aspectos que são conectados à governança de TI (Kopper; Wertner, 2016).

Uma outra observação menos expressiva, mas importante é que há gestores de TI (7%) que apontam que a *shadow IT* não deve ser tratada exclusivamente pela área de TI das organizações, ou seja, entendem que essa questão deve ser enfrentada por toda a organização.

A Figura 7 elucida a percepção dos gestores de TI sobre a responsabilidade (culpa) pelo uso da *shadow IT* nas organizações.

Figura 7 - Percepção dos gestores de TI sobre a responsabilidade pelo uso da *shadow IT* nas organizações



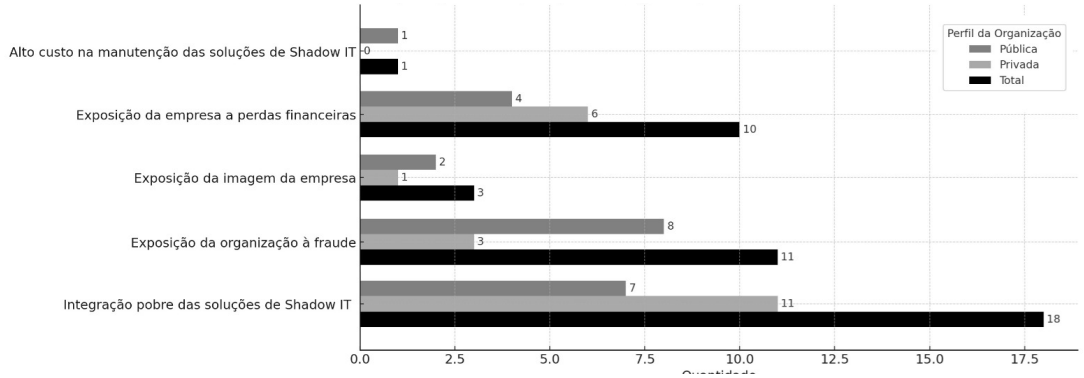
Fonte: dados da pesquisa (2023).

A partir da Figura 7 observa-se que há diferentes percepções entre os gestores de TI sobre a responsabilidade dos profissionais de TI pelo uso da *shadow IT*, com maior predominância para: discordância que os profissionais de TI compartilham a culpa pelo problema de *shadow IT,* a área de TI não está alinhada com a organização e não se tem tempo para se desenvolver a necessidade urgente do usuário.

Com relação à real necessidade de os colaboradores de se valerem de práticas de *shadow IT* para desempenhar suas funções, foi possível constatar que 74% dos gestores de TI concordam totalmente ou parcialmente que a utilização de *shadow IT* é necessária pela organização. Essa proporção se mantém semelhante entre os gestores de TI que atuam nos setores privado e público, com 71% e 77%, respectivamente. Ou seja, verifica-se que a maior parte dos referidos gestores está consciente do uso do fenômeno.

A Figura 8 exibe a percepção dos gestores quanto ao maior risco no uso da *shadow IT* nas organizações.

Figura 8 - Percepção dos gestores quanto ao maior risco no uso da *shadow IT* nas organizações



Fonte: dados da pesquisa (2023).

Dentre os aspectos apontados pelos gestores de TI sobre o maior risco para as organizações no uso da *shadow IT,* observa-se destaque para a integração pobre das soluções de *shadow IT*, exposição da organização à fraude e exposição a perdas financeiras. Esses achados convergem com Klotz *et al*. (2019) ao discutirem a segurança de dados e a conformidade como desafios principais da *shadow IT*. Exposição da imagem da empresa e alto custo na manutenção das soluções de *shadow IT* foram pouco observadas como aspectos de maior risco das práticas de *shadow IT*.

4.4 *Shadow IT* e a gestão de riscos

A Tabela 2 apresenta a percepção dos gestores de TI com relação ao uso da *shadow IT* no contexto da gestão de riscos na percepção dos gestores de TI participantes da pesquisa, atuantes em organizações públicas e privadas.

Tabela 2 - Nível de concordância dos gestores de TI sobre o uso da *shadow IT* no contexto da gestão de riscos, distribuídos conforme o tipo de organização em que atuam

***Shadow IT* e a gestão de riscos**	**Nível de concordância**	**Privada**	**Pública**	**Total**
Há falta de consciência da segurança e da exposição ao risco do uso de soluções de *shadow IT*	Não concordo	0	0	0
	Concordo parcialmente	12	9	22
	Concordo totalmente	9	13	21
Em minha organização, colaboradores que são detectados violando regras de segurança com aplicações de *shadow IT* são punidos	Não concordo	7	14	21
	Concordo parcialmente	13	7	20
	Concordo totalmente	1	1	2

***Shadow IT* e a gestão de riscos**	**Nível de concordância**	**Privada**	**Pública**	**Total**
A área de TI da minha organização tem conhecimento dos colaboradores que violam as regras quanto ao uso de soluções tecnológicas	Não concordo	1	6	7
	Concordo parcialmente	18	12	30
	Concordo totalmente	2	4	6
Minha organização define políticas para tratamento de riscos de *shadow IT*, tais como requisitos de licenciamento, segurança e privacidade	Não concordo	3	14	17
	Concordo parcialmente	12	6	18
	Concordo totalmente	6	2	8
A área de TI da minha organização tem capacidade para avaliação dos riscos das soluções de *shadow IT* detectadas	Não concordo	2	7	9
	Concordo parcialmente	11	6	17
	Concordo totalmente	8	9	17
Minha organização define ações específicas de detecção de *shadow IT*, como monitoramento de tráfego de rede	Não concordo	6	10	16
	Concordo parcialmente	13	8	21
	Concordo totalmente	2	4	6

Fonte: dados da pesquisa (2023).

A partir das informações da Tabela 2, verifica-se que 84% dos gestores de TI concordam total ou parcialmente que a área de TI tem conhecimento que os colaboradores da organização violam as regras quanto ao uso de soluções tecnológicas. Esse achado é relevante para o setor de segurança da informação da organização, que tem condições de desenvolver ações de controle e conscientização desses usuários finais e deve estabelecer ações visando à conscientização dos usuários.

Diferentemente do esperado, constata-se que 81% dos gestores de TI não concordam ou concordam apenas parcialmente que sua organização define políticas para tratamento de riscos de *shadow IT*, tais como requisitos de licenciamento, segurança e privacidade. Sobre o assunto, Parreira (2019) enfatiza a importância de políticas claras e bem definidas.

Uma questão relevante observada na Tabela 2 é a verificação se a área de TI das organizações está capacitada para realizar a gestão de riscos das práticas de *shadow IT*. Nesse sentido, verifica-se que 79% concorda parcial ou totalmente que a área de TI tem condições de realizar a gestão de riscos. Nesse sentido, tem-se que a maior parte das organizações tem as condições mínimas necessárias para tratar dos riscos de *shadow IT,* em consonância com Behrens (2022), que destaca a necessidade de uma gestão de riscos eficaz.

Um outro ponto crítico de análise em relação à gestão de riscos de *shadow IT* indica que 86% gestores de TI não concorda ou concorda parcialmente que a organização em que atua define ações específicas de detecção de *shadow IT*, como monitoramento de tráfego de rede, indicando a necessidade implementação de melhores práticas de governança de TI e controles internos, conforme alertam Mallmann, Maçada e Eckhardt (2018).

5. Conclusão

O presente estudo objetivou analisar a percepção dos gestores de TI sobre o uso da *shadow IT* no contexto da gestão de riscos. Para tanto, foi aplicado um questionário junto ao Grupo de Gestores de Tecnologia da Informação e Comunicação do Estado do Ceará (GGTIC), formado, no período de coleta, por 130 profissionais de TI que atuam tanto em empresas privadas como públicas do estado do Ceará.

Quanto ao perfil dos 43 gestores de TI participantes da pesquisa (amostra), foi possível observar que a maioria é homem, com faixa etária entre 31 e 50 anos e tem de 6 a 15 anos de experiência como gestor de TI. Verificou-se ainda que há uma distribuição equilibrada entre gestores de TI que atuam em organizações públicas e privadas, proporcionando uma análise comparativa sobre o uso da *shadow IT* e da gestão de riscos nos diferentes ambientes organizacionais.

Constatou-se que 34 gestores de TI (74%) conhecem o termo *shadow IT*. Por sua vez, 9 gestores (26%) desconhecem o termo, sendo todos atuantes em organizações públicas e a maior parte deles possui mais de 60 anos de idade.

Em linhas gerais, foi possível verificar que 58% dos gestores de TI está ciente do uso

de tecnologias não autorizadas em suas organizações, sendo mais comum em organizações privadas. Ademais, os resultados demonstram que a maioria dos gestores de TI entende que a área de TI da organização deve ter instrumentos que possibilitem o controle das práticas de *shadow IT* (70%), comportamento esse que se mantém tanto para gestores de TI que atuam tanto em organizações públicas quanto privadas. Apesar disso, 15% dos gestores de TI consideram que a *shadow IT* deve ser eliminada da organização, provavelmente em função dos aspectos negativos que a prática pode proporcionar à organização.

Sobre a necessidade de os colaboradores de se valerem de práticas de *shadow IT* para desempenhar suas funções, observou-se que 74% dos gestores de TI concordam total ou parcialmente que a utilização de *shadow IT* é necessária pela organização, sugerindo que a maior parte dos gestores de TI pesquisados está consciente do uso do fenômeno na sua organização.

No que tange ao nível de concordância dos gestores de TI sobre o uso da *shadow IT* no contexto da gestão de riscos, notou-se que 84% concorda total ou parcialmente que a área de TI tem conhecimento que os colaboradores da organização violam as regras quanto ao uso de soluções tecnológicas. Além disso, 81% dos gestores de TI não concordam ou concordam apenas parcialmente que sua organização define políticas para tratamento de riscos de *shadow IT*, mas que 79% concorda parcial ou totalmente que a área de TI tem condições de realizar a gestão de riscos.

Cabe advertir o achado relacionado à análise da gestão de riscos de *shadow IT* que apontou que 86% gestores de TI não concorda ou concorda apenas parcialmente que sua organização define ações específicas de detecção de *shadow IT*, como monitoramento de tráfego de rede, indicando a necessidade implementação de melhores práticas de governança de TI e controles internos.

A partir dos resultados obtidos, é possível concluir que a maioria dos gestores de TI conhece o termo *shadow IT* e reconhece a prática na sua organização. Apesar de considerarem a *shadow IT* necessária, a maioria acredita que a prática deve ser controlada pela área de TI. A falta de políticas específicas para a gestão de riscos, especialmente no setor público, foi destacada como um ponto crítico. Esses achados reforçam a necessidade de um alinhamento maior entre a governança de TI e as práticas organizacionais para transformar a *shadow IT* de uma ameaça em uma oportunidade para inovação.

Por fim, frente à fragilidade peculiar deste tipo de estudo com a aplicação de questionário em populações restritas, sugere-se que pesquisas futuras direcionem a investigação para as percepções de líderes organizacionais de outras áreas de negócio, a fim de obter uma compreensão abrangente das diferentes perspectivas sobre o tema, visto que ele é transversal e impacta as organizações de maneira geral. Instiga-se, ainda, a avaliação do impacto das iniciativas de conscientização e educação dos colaboradores sobre a *shadow IT*, com o intuito de entender como essas ações podem influenciar o comportamento e as práticas relacionadas à utilização de tecnologias não autorizadas no contexto da gestão de riscos.

Referências

ARAGÃO, R. S.; STREIT, R. E. Shadow IT e TI gerenciada pelo negócio: uma análise das percepções sobre os riscos e benefícios em uma organização pública brasileira do setor financeiro. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. 51, p. 21-36, 2023.

ASSESPRO - Associação das Empresas Brasileiras de Tecnologia da Informação. Mercado de TI movimenta R$ 1 bilhão no Ceará. **O Povo**, Fortaleza, 15 de maio de 2023. Disponível em: <https://www.opovo.com.br/noticias/economia/2023/05/25/mercado-de-ti-movimenta-rs-1-bilhao-no-ceara.html> Acesso em: 26 nov. 2023.

BEHRENS, S.; SEDERA, W. Why do shadow systems exist after an ERP implementation? Lessons from a case study. Association for Information Systems, AIS Electronic Library

(AISeL). In: **Pacific Asia Conference on Information Systems (PACIS) 2004 Proceedings**. December, 2004, p. 1713-1726.
CHALEFF, D. **Want to keep your employees productivity?** Pay attention to shadow IT clues. Feb 6, 2020. Disponível em: <https://www.forbes.com/sites/googlecloud/2020/02/06/want-to-keep- your-employees-productive-pay-attention-to-shadow-it-lues/?sh=5a69caa2254b>. Acesso em: 28 nov. 2023.
FURSTENAU, D.; ROTHE, H.; SANDNER, M. Shadow systems, risk, and shifting power relations in organizations. **Communications of the Association for Information Systems**, v. 41, n. 1, p. 3, 2017.
GGTIC-CE - Grupo de Gestores de Tecnologia da Informação e Comunicação do Ceará. Disponível em: <https://ggtic-ce.org.br/>. Acesso em: 12 dez. 2023.
GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.
GUBA, E. G; LINCOLN, Y. S. Paradigmatic controversies, contradictions, and emerging confluences. In: DENZIN, N. K.; LINCOLN, Y. S. (Eds.). **The Sage handbook of qualitative research**. Sage Publications Ltd., 2005. p. 191-215.
GYÖRY, A. *et al*. **Exploring the shadows:** IT governance approaches to user-driver innovation. In: Proceedings of the 20th European Conference on Information Systems, ECIS 2012, Paper 222, Barcelona, Spain.
HAAG, S.; ECKHARDT, A. Shadow it. **Business & Information Systems Engineering**, v. 59, p. 469-473, 2017.
KLOTZ, S. *et al*. Causing factors, outcomes, and governance of shadow IT and business-managed IT: a systematic literature review. **International Journal of Information Systems and Project Management**, v. 7, n. 1, p. 15-43, 2019.
KLOTZ, S.; WESTNER, M.; STRAHRINGER, S. From shadow IT to business-managed IT and back again: how responsibility for IT instances evolves over time. In: XXIV Pacific Asia Conference on Information Systems (PACIS). 2020. **Proceedings…** Dubai, UAE: PACIS, 2020.
KOPPER, A.; WESTNER, M. **Towards a taxonomy for shadow IT**. In: Proceedings of the 22nd Americas Conference on Information Systems, San Diego, USA, 2016, p. 1-10.
KOPPER, A. Perceptions of IT managers on shadow IT. In: **Proceedings of the 23rd Americas Conference on Information Systems**, Boston. 2017, p. 1-10.
KOPPER, A. *et al*. Shadow IT and business-managed IT: a conceptual framework and empirical illustration. **International Journal of IT/Business Alignment and Governance**, v. 9, n. 2, p. 53-71, 2018.
KOPPER, A. *et al*. Shadow IT and business-managed IT: Practitioner perceptions and their comparison to literature. **Journal of Information Technology Management**, v. 30, n. 4, p. 1-25, 2019.
MACHADO, H. G.; MAÇADA, A. C. G.; DOLCI, P. C. **Ciclo de vida do uso de *shadow IT* nas organizações - uma revisão sistemática da literatura**. In: XXV SEMEAD Seminários em Administração, 2022, São Paulo. SEMEAD 2022. São Paulo: USP, 2022. v. 1. p. 1-12.
MACHADO, H. G. **O ciclo de vida do uso da *shadow IT* no contexto da governança de TI**. 127 f. Dissertação de Mestrado Acadêmico, Programa de Pós-Graduação em Administração, Universidade Federal do Rio Grande do Sul. Porto Alegre, 2023.
MALLMANN, G. L.; MAÇADA, A. C. G.; ECKHARDT, A. **We are social:** A social influence perspective to investigate shadow IT usage. In: Proceedings of the Twenty-Sixth European Conference on Information Systems (ECIS 2018), Portsmouth, 2018. p. 23-28.
MALLMANN, G. L.; PINTO, A. V.; MAÇADA, A. C. G. **Shedding light on shadow IT:** Definition, related concepts, and consequences. In: Information Systems for Industry 4.0:

Proceedings of the 18th Conference of the Portuguese Association for Information Systems. Springer International Publishing, Cham, 2019. p. 63-79.
MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.
MITROVICH, T. **How an agile approach can help eliminate shadow IT**. Forbes, 2021. Disponível em: https://www.forbes.com/sites/forbestechcouncil/2021/07/27/how-an-agileapproach-can-help-eliminate-shadow-it/. Acesso em: 28 nov. 2021.
MONTEIRO JUNIOR, A. G. **As práticas de Shadow IT nas empresas:** a visão de profissionais contadores. 2018. 75 f. Dissertação (Mestrado em Ciências Contábeis e Atuariais) - Programa de Estudos Pós-Graduados em Ciências Contábeis e Atuariais, Pontifícia Universidade Católica de São Paulo, São Paulo, 2018.
MOURA JR., P. J. Governança de tecnologia da informação: A meio caminho entre o isomorfismo e a comoditização. **Revista Electronica de Sistemas de Informação**, v. 16, n. 3, p. 1-24, 2017.
RADEN, N. **Shedding light on shadow IT:** Is Excel running your business?. Santa Barbara: Hired Brains Inc., 2005.
RENTROP, C; ZIMMERMANN, S. **Shadow IT management and control of unofficial IT**. ICDS: The Sixth International Conference on Digital Society Reference, 2012.
SIQUEIRA, W. Q.; LARIEIRA, C. L. C. Proposal of a method for evaluating shadow it applications in corporate companies: A case study. In: XXVIII CONTECSI – International Conference on Information Systems and Technology Management. **Anais…** São Paulo: TECSI–FEA/USP, 2021.
SILIC, M.; BACK, A. Shadow IT: A view from behind the curtain. **Computers & Security,** v. 45, p. 274-283, 2014.
SILIC, M.; BARLOW, J. B.; BACK, A. A new perspective on neutralization and deterrence: Predicting shadow IT usage. **Information & Management**, v. 54, n. 8, p. 1023-1037, 2017.
SILIC, M.; SILIC, D.; OBLAKOVIC, G. Influence of shadow IT on innovation in organizations. **Complex Systems Informatics and Modeling Quarterly**, n. 8, p. 68-80, 2016.
SILIC, M.; SILIC, D.; OBLAKOVIC, G. Shadow IT steroids for innovation. **SSRN Electronic Journal**, p. 113-120, 2016.
STRONG, D. M.; VOLKOFF, O. A roadmap for enterprise system implementation. **Computer**, v. 37, n. 6, p. 22-29, 2004.
TCU - Tribunal de Contas da União. **Manual de gestão de riscos do TCU**. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2020. 46 p.
VAN DER WEELE, S.; BREDEWOLD, F. Shadowing as a qualitative research method for intellectual disability research: Opportunities and challenges. **Journal of Intellectual & Developmental Disability**, v. 46, n. 4, p. 340-350, 2021.
ZIMMERMANN, S.; RENTROP, C. **On the emergence of shadow IT:** A transaction cost-based approach. In: Proceedings of the 22th European Conference on Information Systems, ECIS 2014.