XII SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
CIK 12th INTERNATIONAL CONFERENCE

PERCEPÇÃO DA GOVERNANÇA DE TI SOBRE PRÁTICAS DE SHADOW IT: UM ESTUDO NA SECRETARIA DE FINANÇAS DE FORTALEZA

PERCEPTION OF IT GOVERNANCE ON SHADOW IT: A STUDY IN THE FINANCE SECRETARIAT OF FORTALEZA

LUCAS GABRIEL BEZERRA COSTA DA SILVA
UNIVERSIDADE FEDERAL DO CEARÁ

AUGUSTO JORGE SILVA DE SOUSA
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, ATUÁRIA E CONTABILIDADE DA UFC

AUGUSTO CÉZAR DE AQUINO CABRAL
UNIVERSIDADE FEDERAL DO CEARÁ

SANDRA MARIA DOS SANTOS
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, ATUÁRIA E CONTABILIDADE DA UFC

Comunicação:
O XII SINGEP foi realizado em conjunto com a 12th Conferência Internacional do CIK (CYRUS Institute of Knowledge) e com o Casablanca Climate Leadership Forum (CCLF 2024), em formato híbrido, com sede presencial na ESCA Ecole de Management, no Marrocos.

PERCEPÇÃO DA GOVERNANÇA DE TI SOBRE PRÁTICAS DE SHADOW IT: UM ESTUDO NA SECRETARIA DE FINANÇAS DE FORTALEZA

Objetivo do estudo
O objetivo principal do estudo é identificar como os profissionais da governança de TI da SEFIN lidam com as práticas de Shadow IT.

Relevância/originalidade
Nas organizações, uma realidade observada é o fenômeno do Shadow IT, onde recursos de TI são usados sem conhecimento ou anuência do Departamento de TI, gerando alerta e instigando os profissionais da governança de TI a refletir essa questão e mitigar riscos.

Metodologia/abordagem
No que se refere aos procedimentos metodológicos, a pesquisa é de natureza exploratória-descritiva, com abordagem quantitativa, sendo utilizados dados primários coletados mediante um questionário aplicado junto a profissionais do Departamento de TI da SEFIN. Na análise dos dados, utilizou-se a estatística descritiva.

Principais resultados
Quanto aos pesquisados, atuam na instituição há mais de 15 anos. Compreendem o ambiente de trabalho e práticas de negócios, assim como riscos e benefícios do Shadow IT. Quanto às práticas, emergem pela lentidão nas soluções de TI.

Contribuições teóricas/metodológicas
Este estudo proporcionou uma visão abrangente das percepções dos colaboradores em relação a Shadow IT, destacando a importância da governança de TI e da gestão de riscos para lidar com os desafios associados a essa prática.

Contribuições sociais/para a gestão
As contribuições incluem a identificação das percepções dos colaboradores em relação à existência, necessidade e controle da Shadow IT, bem como a atribuição de responsabilidade pela utilização, reconhecimento dos riscos associados, incluindo exposição à fraude, perdas financeiras e danos irreparáveis à organização.

Palavras-chave: Gestão da tecnologia, Shadow IT, Setor público, Governança de TI, Riscos

PERCEPTION OF IT GOVERNANCE ON SHADOW IT: A STUDY IN THE FINANCE SECRETARIAT OF FORTALEZA

Study purpose
The main objective of the study is to identify how IT governance professionals at SEFIN deal with Shadow IT practices.

Relevance / originality
In organizations, a reality observed is the phenomenon of Shadow IT, where IT resources are used without the knowledge or consent of the IT Department, generating alert and encouraging IT governance professionals to reflect on this issue and mitigate risks.

Methodology / approach
Regarding methodological procedures, the research is exploratory-descriptive in nature, with a quantitative approach, using primary data collected through a questionnaire applied to professionals from the SEFIN IT Department. In data analysis, descriptive statistics were used.

Main results
About that surveyed, they have worked at the institution for more than 15 years. They understand the work environment and business practices, like that risks and benefits of Shadow IT. As for practices, they emerge due to the slowness in IT solutions.

Theoretical / methodological contributions
This study provided a comprehensive view of employee perceptions regarding Shadow IT, highlighting the importance of IT governance and risk management to deal with the challenges associated with this practice.

Social / management contributions
Contributions include identifying employee perceptions regarding the existence, need and control of Shadow IT, as well as assigning responsibility for its use, recognizing associated risks, including exposure to fraud, financial losses and irreparable damage to the organization.

Keywords: Technology management, Shadow IT, Public sector, IT Governance, Risks

PERCEPÇÃO DA GOVERNANÇA DE TI SOBRE PRÁTICAS DE *SHADOW IT*: UM ESTUDO NA SECRETARIA DE FINANÇAS DE FORTALEZA

1 Introdução

A Tecnologia da Informação (TI) tem evoluído significativamente ao longo das últimas décadas, advindo desta evolução uma variedade de tecnologias, tais como: bancos de dados, dispositivos inteligentes, hardwares e softwares de computador. No contexto das organizações, inclusive no setor público, foco deste estudo, cresce a demanda por mais investimentos em TI, justificados pelos resultados que geram na eficiência, na otimização de processos, na segurança da informação e na redução de custos (Sengik & Lunardi, 2023). Conjuntamente, todos estes fatores contribuem para a melhoria dos serviços prestados (Benbunan-Fich *et al*., 2020).

Na esteira deste desenvolvimento, há benefícios e oportunidades, mas também malefícios e riscos (Behrens & Sedera, 2004). Neste trabalho, toma-se por objeto de pesquisa as transformações no uso dos recursos tecnológicos, em particular na computação pessoal, que levaram ao fenômeno cunhado de *Shadow IT*, investigando-se esta questão no âmbito de uma organização pública, a Secretaria de Finanças do Município de Fortaleza – SEFIN. Significando, literalmente, TI nas sombras, tende a ser denominada, no Brasil, como TI invisível, referindo-se, conforme Kopper *et al*. (2019), às instâncias de TI, nas mais diversas áreas de uma organização, inclusive no setor de TI, que não são conhecidas nem envolvidas na governança formal de TI.

Shadow IT configura-se como uma estratégia de dupla face (Fürstenau *et al*., 2021). Por um lado, impulsiona a inovação, ao quebrar amarras nos processos; por outro lado, gera descontrole no gerenciamento pela falta de monitoramento, podendo ocasionar danos sérios que tendem a permanecer invisíveis, como a expressão sugere, vindo a causar problemas de grande impacto, em especial quanto à segurança das informações. Sua abrangência envolve os mais diversos tipos de *softwares* e dispositivos, bem como aplicativos e programas sem a legítima aprovação para acessar e manipular os dados de uma organização.

O fato é que, apesar dos altos níveis de investimentos em TI pelas organizações, seus empregados não têm se restringido ao uso das ferramentas fornecidas pelo departamento de TI para realizar suas tarefas de trabalho (Mallmann; Pinto; Maçada, 2019; Vargas Pinto; Beerepoot; Maçada, 2023). Acerca desta questão, Klotz *et al*. (2022) destacam a relevância de se desenvolver uma eficaz estrutura de governança de TI, capaz de identificar e monitorar as instâncias de TI que operam em unidades de negócios ou no próprio setor de TI, à margem do devido monitoramento e nem sempre em alinhamento aos objetivos estratégicos da organização. Como argumentam Zimmermann, Rentrop e Felden (2014), por serem implementadas de forma autônoma, as práticas de *Shadow IT* não possuem relação técnica nem estratégica com a gestão de serviços de TI da organização.

No setor público, esta questão ganha relevância especial, dado seu impacto potencial na eficiência da gestão e no alcance dos objetivos. Como argumentam Moraes, Löbler e Bobsin (2006), a função do gestor público, inclusive na esfera municipal, foco de análise neste estudo, passa por uma fase crítica de responsabilidades e cobranças por parte da sociedade. Nesse sentido, ainda conforme o autor, cabe ao gestor público definir metodologias e ferramentas de apoio à decisão, tais como indicadores contábeis, *softwares* de gestão integrada (ERP) e Sistemas de Informações Gerenciais ou de Apoio à Decisão (SIG e SAD), assim buscando informações gerenciais de maior abrangência e qualidade para suporte aos serviços prestados.

Neste contexto, a governança de TI desempenha papel fundamental na melhoria da qualidade dos serviços (Tonelli *et al*., 2017). Além dos ganhos na eficiência operacional, mediante a padronização de processos e práticas, a otimização de recursos e a redução de custos, a governança de TI é essencial para o alinhamento estratégico das inovações com os objetivos

e metas da organização (Lunardi *et al*., 2014), dando suporte ao processo decisório e, assim, contribuindo, para o desempenho da missão organizacional. Ademais, uma adequada estrutura de governança de TI contribui para a agilidade e flexibilidade face à dinâmica do contexto organizacional, ao mesmo tempo em que permite a conformidade regulatória, a redução de riscos e a transparência e prestação de contas (Santos Filho, 2018), medidas essenciais no combate a desvios e ameaças à segurança da informação, que tendem a ocorrer na *Shadow IT*, em especial quanto a seus pilares, confidencialidade, integridade e disponibilidade e autenticidade, citados na norma ISO 27001, como destacam Hintzbergen *et al*. (2018).

Em face dos impactos potenciais das práticas de *Shadow IT*, em especial em organizações públicas, e da relevância de uma eficaz estrutura de governança nestas entidades, esta pesquisa tomou como ponto de partida o seguinte questionamento: Como os profissionais da governança de TI da Secretaria de Finanças de Fortaleza (SEFIN) lidam com as práticas de *Shadow IT* que ocorrem na organização? Visando responder esta questão, o objetivo geral é investigar como os profissionais da governança de TI da SEFIN lidam com as práticas de *Shadow IT*. Para isto, foram definidos os seguintes objetivos específicos: 1) mapear o perfil dos profissionais da governança de TI da instituição; 2) Analisar as práticas de *Shadow IT* na instituição; e 3) Verificar os riscos associados ao uso de *Shadow IT* na instituição.

Quanto à justificativa para realização do estudo, destaca-se o fato que, como corolário da crescente aceleração e disseminação dos avanços no campo das tecnologias de comunicação e informação, a aplicação destas inovações tem modificado a forma como o trabalho é realizado. No âmbito das organizações, particularmente neste estudo, no contexto da SEFIN, uma realidade observada tem sido o fenômeno do *Shadow IT*, em que recursos de TI são, por vezes, usados sem o conhecimento ou anuência do Departamento de TI, gerando alerta e instigando os profissionais da governança de TI a refletir sobre esta questão, de modo a mitigar riscos.

Na perspectiva acadêmica, a literatura corrobora a percepção que o departamento de TI não é mais o único ponto de solução para todos os processos que precisam ser automatizados (Alt *et al*., 2020). De fato, já há alguns anos estudos apontam que as unidades de negócios, de modo autônomo, estão se envolvendo na adoção de novas tecnologias de TI, utilizando uma diversidade de ferramentas e, assim, se tornando protagonistas na resolução dos seus próprios problemas (Andriole, 2015). Face este cenário, investigar como os profissionais de TI lidam com esta realidade assume relevância estratégica.

Quanto ao enfoque adotado, o estudo se justifica pelo comportamento de uso de *Shadow IT* a partir da perspectiva individual, pois, como argumenta Gregor (2006), as pesquisas em Sistemas de Informação estão na interseção do conhecimento dos objetos físicos (máquinas) e o conhecimento do comportamento humano, uma vez que *Shadow IT* tem origem no usuário, assim sendo, compreender como e por que os usuários utilizam *Shadow IT* no trabalho é fundamental. Com o aumento do uso de tecnologias não autorizadas pelo departamento de TI, desvendar as motivações, impactos e estratégias de combate, permitirá à SEFIN definir estratégias de ação, de modo a garantir a eficiente alocação de seus recursos e otimizar sua capacidade de prestação de serviços com transparência e qualidade. Deste modo, o estudo busca contribuir para pesquisas futuras sobre a temática no que se refere às práticas de *Shadow IT* no contexto das organizações públicas e nas ações de governança a serem implementadas.

No que se refere aos procedimentos metodológicos, a pesquisa é de natureza exploratória-descritiva, com abordagem quantitativa, sendo utilizados dados primários coletados mediante um questionário aplicado junto a profissionais do Departamento de TI da SEFIN. Na análise dos dados, utilizou-se a estatística descritiva.

Quanto à organização do artigo, estruturou-se em 5 seções. Nesta primeira, de introdução, são apresentados os elementos centrais do estudo, com destaque para a questão de pesquisa, os objetivos e a justificativa. A segunda traz o embasamento teórico, contemplando os temas de governança de TI e de *Shadow IT*. A seção três discorre sobre o percurso

metodológico da pesquisa, seguida da seção quatro, em que são apresentadas a análise e discussão dos resultados, inicialmente com a descrição e análise do questionário aplicado aos profissionais da governança de TI da SEFIN Fortaleza e, posteriormente, com as discussões dos resultados. Por fim, na quinta e última seção, são apresentadas as conclusões, considerações finais e contribuições do estudo, sucedidas pelas referências.

2 Referencial Teórico

2.1 Governança de TI

Governança de TI é o termo usado para descrever a forma como as pessoas responsáveis pela governança de uma organização considerarão a TI em supervisão, monitoramento, controle e direção (Teodoro, Przeybilovicz e Cunha, 2014). A governança de TI tem como objetivo estabelecer o melhor alinhamento entre o negócio e a tecnologia da informação da instituição para serem alcançados os objetivos organizacionais (Weill e Ross, 2006). Para Haes e Grembergen (2009), é importante compreender como é a estrutura da empresa em relação às tomadas de decisão de TI, como comitês, cerimônias e papéis dos envolvidos.

A governança de TI é utilizada nas organizações por meio de um conjunto de mecanismos, que são métodos adotados para a implementação da governança de TI e, segundo Lunardi *et al*. (2014), o sucesso da implementação depende de mecanismos bem concebidos cujas estruturas, processos e comunicações tenham sido pensados de forma prioritária. Conforme Ribbers, Peterson e Parker (2002), os mecanismos de governança de TI ligados a processos fazem com que os responsáveis por TI e pelas áreas de negócio trabalhem em conjunto para que as decisões de TI e o negócio estejam alinhados, executando e monitorando a aplicação das decisões, em um processo de aprendizado dessas iniciativas. Segundo Haes e Van Grembergen (2005), os mecanismos de governança de TI relacionados aos processos são: o planejamento estratégico de sistemas de informação, a utilização de indicadores de desempenho, a utilização de metodologias como *Information Technology Infrastructure Library* (ITIL) e *Control Objectives for Information and Related Technology* (Cobit), e a utilização de acordos de nível de serviço (SLA – *Software Level Agreement*).

Conforme Lunardi (2008), o relacionamento entre as áreas do negócio e a TI permite que as soluções para problemas possuam saídas mais ligadas às reais necessidades de negócio, ultrapassando as fronteiras funcionais. Contudo, ainda conforme o autor, pode haver casos em que os processos e a estrutura da TI estejam bem ajustados, mas, mesmo assim, em virtude de problemas de relacionamento entre a TI e o negócio, a área de TI não funcione de forma satisfatória. Quanto mais a organização comunica os mecanismos de governança e seu funcionamento, mais eficaz será sua governança (Weill e Ross, 2004). Dessa forma, os mecanismos de relacionamento são indispensáveis para a organização, tendo em vista a importância da comunicação para atender os diversos públicos da organização.

A governança de TI nas organizações constitui fator essencial para garantir o alinhamento estratégico da tecnologia com os objetivos do negócio, podendo, assim, impactar positivamente seus processos operacionais, estratégicos e financeiros. Conforme Haes & Van Grembergen (2004), um fator determinante na eficácia da governança de TI é a forma como a função de TI é organizada e onde a autoridade de tomada de decisão de TI está localizada na organização. Com os novos modelos de entrega de tecnologia baseados em nuvem e a disseminação de dispositivos de consumo, a estrutura da governança de TI fica mais susceptível a arranjos informais, inclusive no tocante ao uso de *Shadow IT* (Andriole, 2015), o que reforça a necessidade de se repensar a configuração da estrutura de governança utilizada e, também, de se estabelecer mecanismos de controle.

2.2 *Shadow IT*

A tendência dos empregados de proverem suas próprias soluções tecnológicas nas organizações vem sendo motivada pelo fenômeno da consumerização da TI, que é o termo utilizado para o uso de tecnologias de consumo, como *tablets*, *smartphones* ou aplicações em nuvem, que tem facilitado a adoção e uso de tecnologias pelo próprio usuário, que não são autorizadas pelo departamento de TI (Goodwin, 2014; Köffer; Ortbach; Niehaves, 2014).

Haag e Eckhardt (2017) definem *Shadow IT* como qualquer *hardware*, *software* ou serviço desenvolvido, introduzido e/ou utilizado para o trabalho, sem aprovação explícita ou conhecimento da organização. Conforme Rentrop e Zimmermann (2012), *Shadow IT* pode ser definido como uma coleção de sistemas, desenvolvidos pela área de negócios, sem o suporte do departamento de TI, sendo assim desenvolvidos e implementados de forma independente.

A compreensão dos tipos de *Shadow IT* facilita na identificação das práticas mais recorrentes. De acordo com Huber *et al.* (2016), podem ser consideradas *Shadow IT*, planilhas, bancos de dados, aplicativos instalados no local de trabalho, serviços de nuvem, dispositivos periféricos, uma solução combinada ou até mesmo um sistema legado. Para Siqueira e Larieira (2019), outro exemplo é a compra ou desenvolvimento interno, para dar suportes para soluções de *Business Inteligence*, pelos próprios funcionários, sem intermédio da TI corporativa.

As organizações enfrentam diversos riscos devido a adoção da *Shadow IT*, tendo em vista que geralmente essas iniciativas são desenvolvidas e implementadas de forma autônoma, sem o conhecimento, sem possuir relação técnica e nem estratégica com a gestão de serviços da organização (Silic & Back, 2014). Diversos autores abordam os riscos das práticas de *Shadow IT*, conforme sumarizado no Quadro 1.

Risco	Justificativa	Autor
Dispersão e falta de organização	As iniciativas desenvolvidas em *Shadow IT* geralmente carecem de formalização, padronização ou documentação, o que causa retrabalhos em sua manutenção e na dificuldade de manutenção a longo prazo.	Huber *et al.* (2016)
Vazamento de informações confidenciais	Soluções desenvolvidas e/ou utilizadas pelas áreas de negócios geralmente não são submetidas aos protocolos da TI corporativa, gerando vulnerabilidades, por expor informações estratégicas e confidenciais.	Silic & Back (2014)
Perda de dados	O controle de qualidade a que são submetidos os aplicativos corporativos não é aplicado em Shadow *IT* e possíveis falhas, como ausência de controle, rotinas de *backup* e processos, podem acarretar perdas de dados críticos.	
Ausência ou controle de atividades	A equipe de TI realiza melhorias contínuas daquilo que é determinado como norma de conduta tecnológica. A falta de controle pode complicar e atrasar a solução de falhas, gerando pontos cegos na gestão das informações.	Gyory *et al.* (2012)
Elevado risco de erros e prejuízos financeiros	O uso de tecnologias não autorizadas aumenta a vulnerabilidade e os riscos nos processos da organização, que no que lhe concerne acaba retardando a identificação dos problemas e dos aplicativos paralelos.	Rentrop & Zimmermann (2012)
Desperdício de recursos	A construção ou contratação de diversos aplicativos paralelos muitas vezes tem altos custos e desperdício de recursos.	
Quebra do *compliance*	Sem o controle das atividades dos usuários e das transferências de dados, a instituição fica fragilizada em relação às obrigações legais, ficando exposta a equívocos e ao descumprimento de normas ou legislações, o que pode acarretar multas e restrições pelo governo ou órgãos reguladores.	Silic & Back (2014)

Quadro 1 – Possíveis riscos de *Shadow IT*.
Fonte: Elaboração própria baseado nos conceitos de Siqueira e Larieira (2019).

No entanto, os impactos positivos da utilização de *Shadow IT* são bastante discutidos na literatura. De acordo com Furstenau e Rothe (2014), *Shadow IT* permite melhorias na produtividade dos funcionários e na inovação, uma vez que suas aplicações são desenvolvidas para atender as necessidades dos usuários das áreas de negócio, sendo a eficácia na execução dos trabalhos um dos principais impulsionadores do desenvolvimento desse fenômeno.

3 Metodologia

Conforme Creswell, J. W. e Creswell, J. D. (2021), uma importante definição em uma pesquisa científica são os métodos específicos que envolvem as formas de coleta, análise e interpretação dos dados que os pesquisadores utilizarão em seus estudos. No que diz respeito à natureza, a pesquisa pode ser tipificada como qualitativa, quantitativa ou de métodos mistos. Considerando os objetivos específicos do presente estudo, o método quantitativo é o mais adequado, tendo em vista que possibilita testar ou verificar situações, a partir da utilização de procedimentos estatísticos adequados.

Vergara (2008) classifica uma pesquisa a partir de dois critérios básicos: os fins e os meios. No que se refere aos fins, este estudo tem propósito exploratório, tendo em vista que possibilita o melhor entendimento de um fenômeno, no caso, como os profissionais de governança em TI lidam com as práticas de *Shadow IT* numa instituição; e descritivo, pois também tem a pretensão de expor características e comportamentos de uma população, formada pelos profissionais que atuam nessa área. Já no que concerne aos meios, o estudo foi desenvolvido a partir de uma pesquisa de campo.

A coleta de dados foi de natureza primária, tendo ocorrido no período de novembro de 2023 a dezembro de 2023, por meio da aplicação de questionário disponibilizado em um Formulário no *Google Forms*. O questionário estava estruturado em três partes, sendo a primeira voltada para o mapeamento do perfil do profissional de governança em TI na instituição; na segunda parte, para a análise das práticas de *Shadow IT* na instituição; e na terceira parte, para a verificação dos riscos associados ao uso da *Shadow IT* na instituição.

Esta pesquisa contou, voluntariamente e obedecendo aos critérios éticos de privacidade, com a participação de profissionais que compõem a governança de TI da SEFIN de Fortaleza, sendo esse o critério de seleção dos respondentes. A escolha da SEFIN com foco da pesquisa deu-se por sua relevância estratégica e pelo fato da instituição contar com uma área de TI bem estruturada, mas com relatos de práticas de *Shadow IT*. No total, participaram 56 profissionais na pesquisa. A última etapa foi a análise e discussão dos resultados, mediante o uso de estática descritiva e apresentação dos achados em gráficos, com considerações dos pesquisadores.

4 Análise e discussão dos resultados

Nesta seção, apresentam-se a descrição e a análise dos resultados obtidos com a aplicação do questionário aos profissionais de TI da SEFIN Fortaleza, em conformidade com os objetivos específicos previamente definidos.

4.1 Perfil dos respondentes

A maioria dos respondentes, devido ao tempo de atuação, tem uma boa compreensão do ambiente de trabalho e das práticas de negócios, o que pode influenciar suas opiniões sobre a necessidade e o controle da TI na organização. Em comparação com outros departamentos da organização, isto pode indicar que eles têm uma melhor compreensão dos riscos e benefícios de práticas que constituem *Shadow IT*, embora não necessariamente tais práticas sejam assim denominadas ou reconhecidas na organização.

Tabela 1 – Perfil dos respondentes.

Item de perfil	Categorias	Qtd. de Respondentes
Gênero	Masculino	31
	Feminino	25

Faixa etária	20 – 30 anos	6
	31 – 40 anos	17
	41 – 50 anos	20
	51 – 60 anos	10
	mais de 60 anos	3
Tempo de atuação	até 5 anos	4
	6 a 10 anos	5
	11 a 15 anos	8
	16 a 20 anos	16
	mais de 20 anos	23

Fonte: Dados da pesquisa (2023).

Os profissionais de governança em TI na instituição, e que participaram da pesquisa, 58,9% têm mais de quarenta anos e quase 70% dos respondentes atuam há mais de quinze anos na instituição; o gênero masculino predomina, constituindo 55% dos participantes, conforme sumarizado na Tabela 1.

4.2 Práticas de *Shadow IT*

Quanto ao conhecimento dos respondentes em relação ao termo Shadow *IT*, constatou que a maioria 57, 1% não estão familiarizados com o termo, enquanto, 42,9% informaram conhecê-lo (Figura 1).

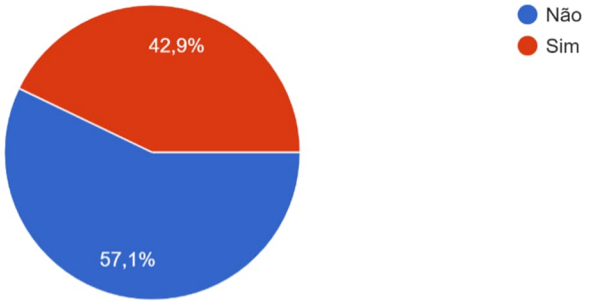

Figura 1 – Conhecimento sobre o termo *Shadow IT*.
Fonte: Dados da pesquisa (2023).

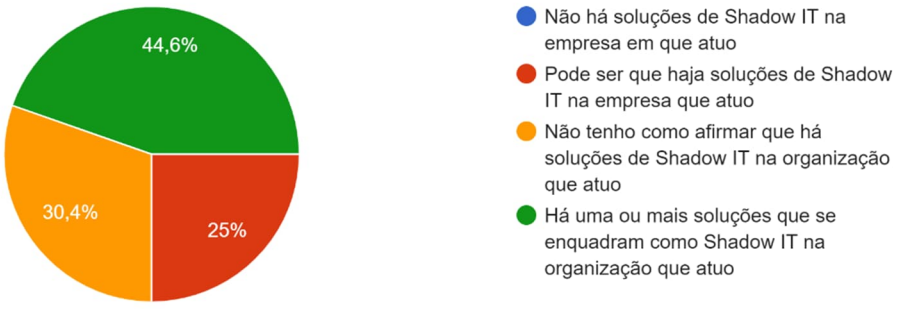

Figura 2 – Soluções de *Shadow IT* na organização.
Fonte: Dados da pesquisa (2023).

Para os respondentes do questionário, foi destacado que o termo *Shadow IT* se refere a programas, *softwares*, dispositivos, planilhas e serviços que estejam fora do controle do departamento de TI e que não possuem aprovação explícita da organização (canvas, PowerBI, Access etc.). A partir desta informação, 44,6% dos pesquisados informaram que há a existência de uma ou mais soluções que se enquadram de *Shadow IT*, seguidos por 30,4% que não confirmam se há a existência de soluções para tal fenômeno (Figura 2).

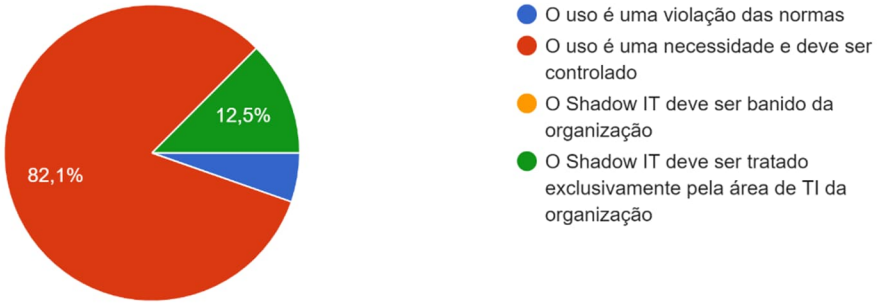

Figura 3 – Uso da *Shadow IT* nas organizações.
Fonte: Dados da pesquisa (2023).

Quando questionados sobre o a prática de *Shadow IT*, 82,1% informaram que o uso é uma necessidade e deve ser controlado, 5,4% informam que o uso é uma violação das normas e 12,5% informam que a prática deveria ser tratada apenas pela equipe de TI. As respostas corroboram o que foi exposto na literatura por Furstenau e Rothe (2014), que afirma que a *Shadow IT* permite melhorias na produtividade dos funcionários e na inovação, uma vez que suas aplicações são desenvolvidas para atender as necessidades dos usuários das áreas de negócio, sendo a eficácia na execução dos trabalhos um dos principais impulsionadores do desenvolvimento desse fenômeno.

Ao serem questionados se o uso de *Shadow IT* é uma necessidade para a organização, 53,6% dos entrevistados concordam parcialmente, enquanto 42,9% concordam totalmente, seguidos por 3,6% que discordam (Figura 4).

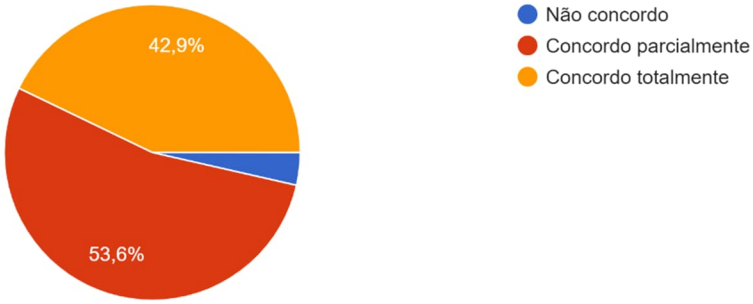

Figura 4 – Necessidade do uso de soluções de *Shadow IT* na organização.
Fonte: Dados da pesquisa (2023).

No que diz respeito ao questionamento sobre as práticas de *Shadow IT*, onde a área de TI não possui controle sobre os programas desenvolvidos, 62,5% dos respondentes informaram que a prática deve ser controlada, seguidos por 21,4% que a prática se trata de uma necessidade e, portanto, precisa existir, 14,3% informaram que a prática deve ser tratada apenas pela equipe de TI e 1,8% acreditam que a prática deva ser eliminada.

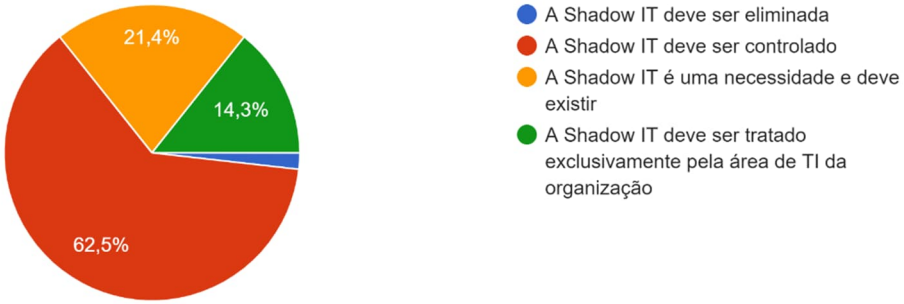

Figura 5 – Posicionamento da área de TI quanto a *Shadow IT*.
Fonte: Dados da pesquisa (2023).

Ao serem questionados sobre a culpa pela utilização de *Shadow IT* na organização, 46,4% responderam que não há tempo suficiente para se desenvolver uma solução urgente para o usuário, 30,4% discordam que os profissionais de TI compartilham a culpa pelas práticas de *Shadow IT*, 10,7% informaram que há falta de interesse entre as áreas e 10,7% reconheceram que a área de informática não está alinhada com a organização (Figura 6). Diante disso, infere-se pela maioria das respostas que em alguns momentos por não terem a resolução de alguma necessidade, devido à ausência de tempo ou outros fatores, os usuários acabam recorrendo a práticas de *Shadow IT*, para atender demandas emergentes.

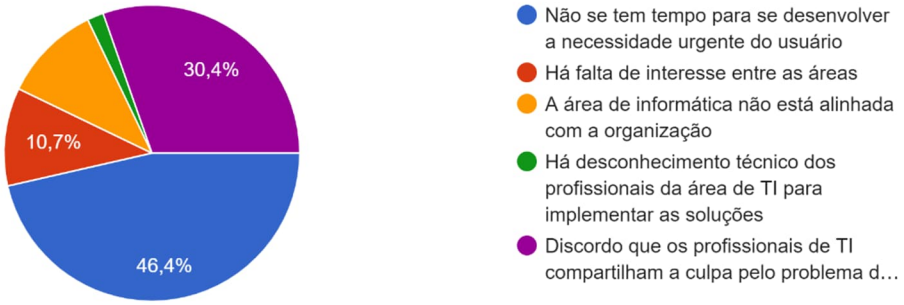

Figura 6 – Fatores motivadores do uso de *Shadow IT* na organização.
Fonte: Dados da pesquisa (2023).

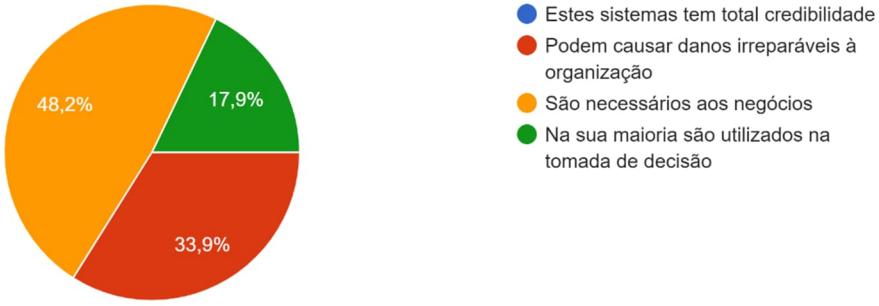

Figura 7 – Credibilidade dos sistemas desenvolvidos na *Shadow IT*.
Fonte: Dados da pesquisa (2023).

Quando questionados sobre a credibilidade do que está sendo utilizado atualmente na organização que pode ser considerado como *Shadow IT*, 48,2% dos respondentes consideraram que tais práticas são necessárias, sendo, em sua maioria, utilizadas na tomada de decisão, enquanto 33,9% consideram que podem causar danos irreparáveis à organização (Figura 7).

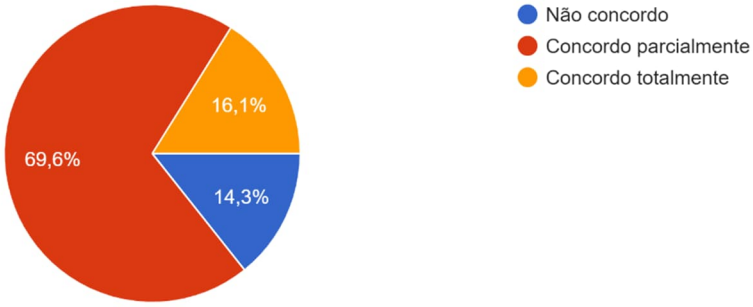

Figura 8 – *Shadow IT* como um problema a ser resolvido pela área de TI da organização.
Fonte: Dados da pesquisa (2023).

Conforme respostas do questionário, 69,6% concordam de maneira parcial que a prática deve ser resolvida pela área de informática, enquanto 16,1% concordam totalmente e 14,3% discordam da afirmação. A maioria concordou de maneira parcial, pois ocorrem situações que a TI não possui conhecimento sobre a prática (Figura 8).

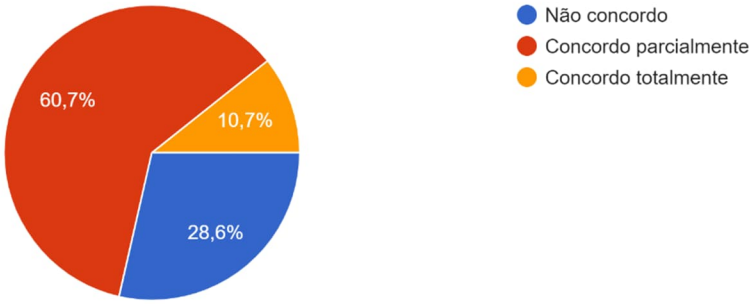

Figura 9 – Percepção dos usuários quanto à lentidão e insatisfação dos serviços prestados pela área de TI.
Fonte: Dados da pesquisa (2023).

Quando questionados quanto à avaliação dos usuários sobre os serviços fornecidos pela TI, 60,7% dos respondentes concordaram parcialmente que os serviços podem ser considerados como lentos ou insatisfatórios, 28,6% discordam da afirmação e 10,7% concordaram totalmente. Dessa forma, pode-se concluir que por julgarem o atendimento dos serviços com uma característica lenta, os usuários buscam soluções externas para a solução e adotam a prática de *Shadow IT* (Figura 9).

De modo geral, em alinhamento ao que é apontado na literatura, por exemplo, por Kopper *et al.* (2020), os gestores compreendem a necessidade de balancear controle e autonomia na governança de TI, apesar do grande desafio que isto representa no contexto específico da SEFIN, dado o estágio incipiente da governança no enfrentamento desta questão.

4.3 Riscos associados ao uso da *Shadow IT* na instituição

As respostas dos colaboradores em relação aos riscos associados a *Shadow IT* revelaram percepções significativas sobre a exposição da organização a potenciais ameaças. A maioria dos participantes expressou preocupação com a exposição à fraude, indicando que a utilização de soluções de *Shadow IT* poderia aumentar a vulnerabilidade da organização a atividades fraudulentas. Além disso, muitos colaboradores reconheceram o risco de perdas financeiras decorrentes da utilização não autorizada de tecnologias e serviços de informação, destacando a possibilidade de impactos negativos nos resultados financeiros da empresa. Outra preocupação manifestada pelos colaboradores foi a percepção de que a *Shadow IT* poderia causar danos

irreparáveis à organização, indicando a gravidade dos potenciais impactos negativos decorrentes dessa prática. Em alinhamento ao que argumentam Rentrop & Zimmermann (2012), os gestores apontam que há um elevado risco de erros e prejuízos financeiros, bem como de desperdício de recursos, uma vez que o uso de tecnologias não autorizadas aumenta a vulnerabilidade e os riscos nos processos da organização, retardando a identificação dos problemas e acarretando o desenvolvimento ou contratação de diversos aplicativos paralelos muitas vezes tem altos custos e desperdício de recursos.

Essas percepções têm implicações significativas para a governança de TI e a gestão de riscos. Em primeiro lugar, as preocupações dos colaboradores em relação à exposição à fraude destacam a importância de se estabelecer controles eficazes para mitigar os riscos de segurança associados à utilização de soluções de *Shadow IT*. Isso inclui a implementação de políticas de segurança da informação, a adoção de medidas de controle de acesso e a realização de auditorias regulares para identificar e mitigar vulnerabilidades. Além disso, a percepção dos colaboradores sobre o risco de perdas financeiras e danos irreparáveis à organização ressalta a necessidade de se promover a conscientização e a educação sobre os potenciais impactos negativos da *Shadow IT*. Isso pode incluir a realização de treinamentos, a divulgação de boas práticas e a promoção de uma cultura organizacional que valorize a conformidade e a segurança da informação.

Em suma, as percepções dos colaboradores em relação aos riscos associados a *Shadow IT* destacam a importância de se adotar uma abordagem proativa para a governança de TI e a gestão de riscos, visando mitigar os potenciais impactos negativos dessa prática e promover a segurança e a conformidade no uso de tecnologias e serviços de informação.

Na figura 10, tem-se a percepção dos respondentes quanto à falta da segurança e exposição ao risco do uso de soluções de *Shadow IT*. Observa-se que 53,6% dos participantes concordaram parcialmente sobre a falta da segurança e exposição ao risco do uso de soluções de SIT, enquanto 41,1% concordaram totalmente e 5,4% não concordaram com a afirmação.

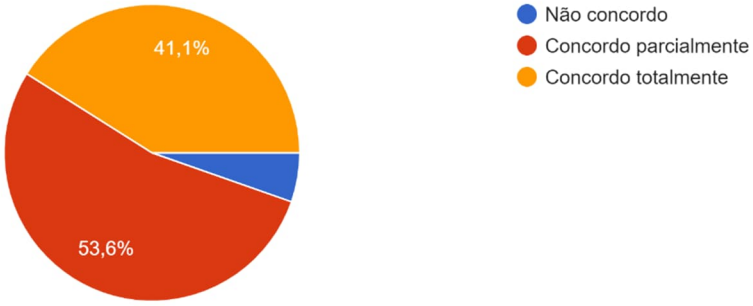

Figura 10 – Falta de consciência quanto às questões de segurança e riscos da *Shadow IT*.
Fonte: Dados da pesquisa (2023).

Figura 11 – Riscos na utilização de *Shadow IT*.
Fonte: Dados da pesquisa (2023).

No que diz respeito aos riscos na utilização de *Shadow IT*, todos os respondentes reconhecem que há danos potenciais, com impactos mais significativos em diferentes dimensões, conforme evidenciado na Figura 11. A este respeito, 35,7% identificam o risco de exposição da organização à fraude, 32,1% afirmaram que a integração pobre da solução de *Shadow IT*, quando comparado com a solução da própria equipe de TI, 16,1% reconhecem a exposição a perdas financeiras e 10,7% a exposição da imagem da organização.

Quando questionados sobre as punições relacionadas à detecção dos colaboradores que são detectados realizando a prática de *Shadow IT*, 53,6% responderam que há punição e 44,6% discordam da afirmação (Figura 12).

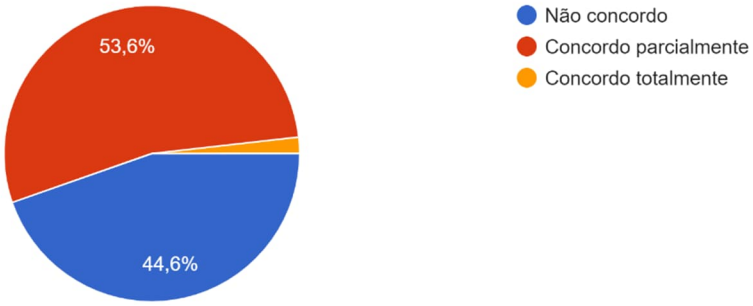

Figura 12 – Ocorrência de punição por violação de regras por uso de *Shadow IT*.
Fonte: Dados da pesquisa (2023).

Na figura 13, constata-se que 81,7% dos respondentes concordam que a área de TI possui conhecimento dos colaboradores que violam a regra quanto ao uso de TI e 17,9% discordam da afirmação. Além disso, 94,6% dos entrevistados concordam que a área de TI tem capacidade de avaliar os riscos das soluções de *Shadow IT* detectadas (Figura 14).

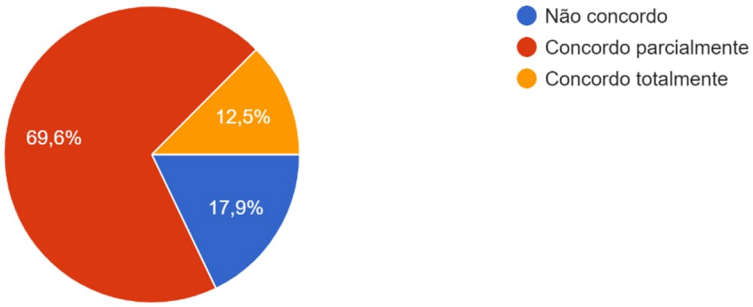

Figura 13 – Conhecimento da área de TI sobre violação das regras quanto ao uso de TI.
Fonte: Dados da pesquisa (2023).

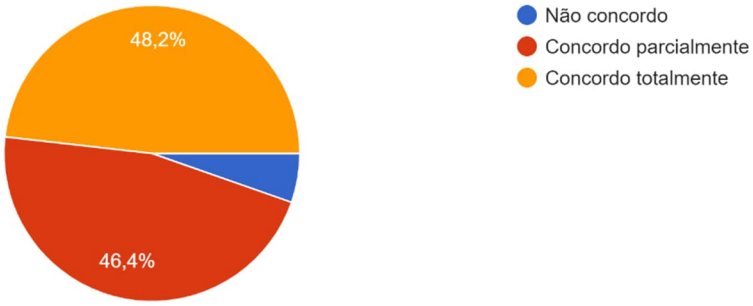

Figura 14 – Capacidade de avaliação dos riscos das soluções de Shadow *IT* pela área de TI.
Fonte: Dados da pesquisa (2023).

Quanto ao tratamento de riscos, 82,2% dos respondentes informaram que há políticas para tratamento da prática de *Shadow IT*, para os requisitos de segurança, licenciamento e privacidade, enquanto 17,7% discordaram. (Figura 15)

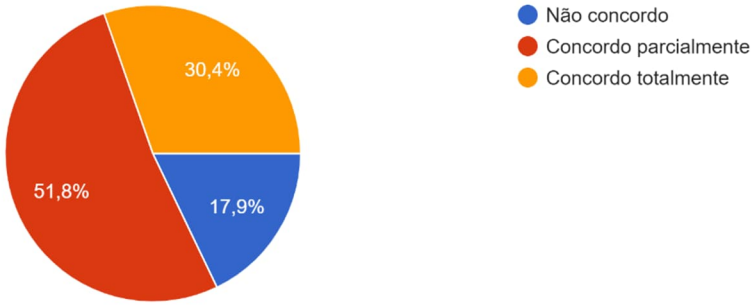

Figura 15 – Políticas para tratamento de riscos pela organização.
Fonte: Dados da pesquisa (2023).

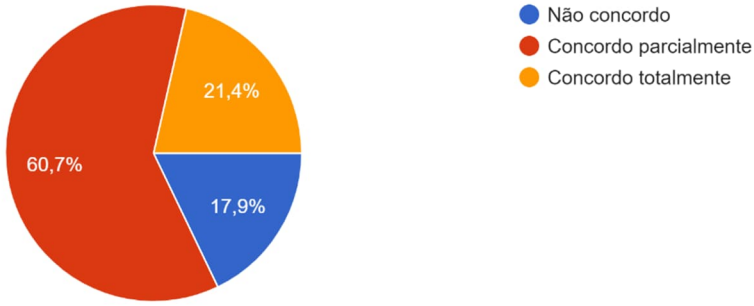

Figura 16 – Ações específicas de detecção de *Shadow IT* pela organização.
Fonte: Dados da pesquisa (2023).

E, por último, 82,1% dos respondentes concordaram que a organização realiza ações para evitar a prática de *Shadow IT*, utilizando da ação de monitoramento de tráfego de rede, algo que 17,9% discordaram (Figura 16).

Em síntese, contata-se que a visão dos gestores reflete a compreensão que *Shadow IT* representa desafios e oportunidades, assim como argumentam Fürstenau *et al*. (2021). Embora o tratamento da temática no âmbito da organização carece de sistematização, prevalece no grupo encarregado da governança a percepção da relevância de se instituir uma estrutura de governança capaz de minimizar as desvantagens e promover as vantagens das práticas de *Shadow IT*, em conformidade com o que defende Raković *et al*. (2020).

5 Conclusões, considerações finais e contribuições

Este estudo proporcionou uma visão abrangente das percepções dos colaboradores em relação a *Shadow IT*, destacando a importância da governança de TI e da gestão de riscos para lidar com os desafios associados a essa prática. Os principais achados e contribuições do estudo incluem: a) identificação das percepções dos colaboradores em relação à existência, necessidade e controle da *Shadow IT*, bem como a atribuição de responsabilidade pela sua utilização; b) reconhecimento dos riscos associados a *Shadow IT*, incluindo exposição à fraude, perdas financeiras e danos irreparáveis à organização, conforme percebido pelos colaboradores.

Sugestões para pesquisas futuras e aprimoramento das práticas relacionadas à *Shadow IT* incluem a realização de estudos adicionais para investigar as percepções dos profissionais de TI e líderes organizacionais em relação a *Shadow IT*, a fim de obter uma compreensão abrangente das diferentes perspectivas sobre o tema; b) exploração de estratégias específicas para a implementação de políticas de governança de TI voltadas para a gestão da *Shadow IT*,

levando em consideração as melhores práticas e os desafios enfrentados pelas organizações e c) avaliação do impacto das iniciativas de conscientização e educação dos colaboradores sobre a *Shadow IT*, visando entender como essas ações podem influenciar o comportamento e as práticas relacionadas à utilização de tecnologias não autorizadas.

Em resumo, este estudo forneceu *insights* valiosos sobre as percepções dos colaboradores em relação a *Shadow IT* e ofereceu recomendações para aprimorar as práticas de governança de TI. Ao considerar as sugestões para pesquisas futuras, as organizações poderão desenvolver estratégias mais eficazes para lidar com os desafios e riscos associados a *Shadow IT*, promovendo uma abordagem mais segura e alinhada com as necessidades e objetivos organizacionais.

REFERÊNCIAS

Alt, R., Leimeister, J. M., Priemuth, T., Sachse, S., Urbach, N., & Wunderlich, N. (2020). Software-defined business: implications for IT management. *Business & Information Systems Engineering*, *62*, 609-621.

Andriole, S. J. (2015). Who owns IT?. *Communications of the ACM*, *58*(3), 50-57.

Behrens, S., & Sedera, W. (2004). Why do shadow systems exist after an ERP implementation? Lessons from a case study. In Proceedings of the Pacific Asia Conference on Information Systems (PACIS2004), Shanghai, China, (pp. 153-166). Electronic Commerce Research Centre, Sun Yat-sen University.

Benbunan-Fich, R., Desouza, K. C., & Andersen, K. N. (2020). IT-enabled innovation in the public sector: introduction to the special issue. *European Journal of Information Systems*, *29*(4), 323-328.

Creswell, J. W., & Creswell, J. D. (2021). *Projeto de pesquisa-: Métodos qualitativo, quantitativo e misto*. Penso Editora.

Fürstenau, D., Rothe, H., & Sandner, M. (2021). Leaving the shadow: A configurational approach to explain post-identification outcomes of shadow IT systems. Business & information systems engineering, 63, 97-111. https://doi.org/10.1007/s12599-020-00635-2

Fürstenau, D., Rothe, H., & Sandner, M. (2021). Leaving the shadow: a configurational approach to explain post-identification outcomes of shadow IT systems. Business & information systems engineering, 63, 97-111. https://doi.org/10.1007/s12599-020-00635-2.

Fürstenau, D., & Rothe, H. (2014, June). Shadow IT Systems: Discerning the Good and the evil. In *ECIS*.

Gil, A. C. (2007). *Como elaborar projetos de pesquisa*. Editora Atlas SA.

Goodwin, B. (2014). IT governance in the era of shadow IT. *ComputerWeekly. Available on: http://www. computerweekly. com/feature/CW500-IT-governance-in-the-era-of-shadow-IT*.

Gregor, S. (2006). The nature of theory in information systems. *MIS quarterly*, 611-642.

György, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation.

Haag, S., & Eckhardt, A. (2017). Shadow IT. Business & Information Systems Engineering, 59 (6), 469–473.

Haes, S., & Van Grembergen, W. (2005, January). IT governance structures, processes and relational mechanisms: Achieving IT/business alignment in a major Belgian financial group. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences* (pp. 237b-237b). IEEE.

HAES, S. D., GREMBERGEN, W. V. An exploratory study into IT Governance implementations and its impacts on business/IT Alignment. Information Systems Management, 26(2), 123-137, 2009.

Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2018). Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002.(3oed). Brasport.

Huber, M., Zimmermann, S., Rentrop, C., & Felden, C. (2016). The relation of shadow systems and ERP systems—Insights from a multiple-case study. *Systems*, *4*(1), 11.

Klotz, S., Westner, M., & Strahringer, S. (2022). Critical success factors of business-managed IT: it takes two to tango. *Information systems management*, *39*(3), 220-240.

Köffer, S., Ortbach, K. C., & Niehaves, B. (2014). Exploring the relationship between IT consumerization and job performance: a theoretical framework for future research. *Communications of the Association for Information Systems*, *35*(1), 14.

Kopper, A., Klotz, S., Westner, M., & Strahringer, S. (2019). Shadow IT and business-managed IT: practitioner perceptions and their comparison to literature. *Journal of Information Technology Management*, *30*(4), 1-25.

LAKATOS, E. M.; MARCONI, M. de A. (2010) *Técnicas de pesquisa***:** planejamento e execução de pesquisas, amostragens e técnicas de pesquisas, elaboração, análise e interpretação de dados. 3. ed. São Paulo: Atlas.

Lunardi, G. L., Dolci, P. C., Maçada, A. C. G., & Becker, J. L. (2014). Análise dos mecanismos de governança de TI mais difundidos entre as empresas brasileiras. *Alcance. Itajaí. Vol. 21, n. 1 (jan./mar. 2014), p. 46-76.*

Lunardi, G. L. (2008). Um estudo empírico e analítico do impacto da governança de TI no desempenho organizacional. Tese de Doutorado de Administração.

Mallmann, G. L., de Vargas Pinto, A., & Maçada, A. C. G. (2019). 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* (pp. 63-79). Springer International Publishing.

Moraes, G. M., Löbler, M. L., & Bobsin, D. (2006). Percepção dos usuários quanto ao desempenho de Sistemas de Informação em Secretarias de Finanças de três grandes municípios do Rio Grande do Sul. *Sistemas & Gestão*, *1*(2), 156-173.

Rentrop, C., & Zimmermann, S. (2012). Shadow it. *Management and Control of Unofficial IT. ICDS*, 98-102.

Ribbers, P. M., Peterson, R. R., & Parker, M. M. (2002, January). Designing information technology governance processes: Diagnosing contemporary practices and competing theories. In *Proceedings of the 35th annual Hawaii international conference on system sciences* (pp. 3143-3154). IEEE.

Röder, N., Wiesche, M., Schermann, M., & Krcmar, H. (2014). Why managers tolerate workarounds–the role of information systems.

Santos Filho, J. W. (2018). Governança de TI: Análise das Contribuições de Mecanismos Privados no Gerenciamento Público de TI. *Interfaces Científicas-Exatas e Tecnológicas*, *2*(3), 71-84.

Sengik, A. R., & Lunardi, G. L. (2023). Information technology governance in the government public sector: a systematic mapping of the scientific production. *International Journal of Services Technology and Management*, *28*(3-4), 248-271.

Silic, M., & Back, A. (2014). Shadow IT–A view from behind the curtain. *Computers & Security*, *45*, 274-283.

Siqueira, W., & Larieira, C. L. (2019). Proposal of a method for evaluating Shadow IT Applications in corporate companies: a case study. CONTECSI USP – *International Conference on Information Systems and Technology Management*.

Teodoro, A. N., Przeybilovicz, É., & Cunha, M. A. (2014). Governança de tecnologia da informação: uma investigação sobre a representação do conceito. *Revista de Administração*, *49*(2), 307-321.

Tonelli, A. O., de Souza Bermejo, P. H., Aparecida dos Santos, P., Zuppo, L., & Zambalde, A. L. (2017). It governance in the public sector: a conceptual model. *Information Systems Frontiers*, *19*, 593-610.

Vargas Pinto, A., Beerepoot, I., & Maçada, A. C. G. (2023). Encourage autonomy to increase individual work performance: the impact of job characteristics on workaround behavior and shadow IT usage. *Information Technology and Management*, *24*(3), 233-246.

Vergara, S. C. (2008). *Métodos de pesquisa em administração*. Atlas.

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.

Zimmermann, S., Rentrop, C., & Felden, C. (2014). Managing shadow IT instances–a method to control autonomous IT solutions in the business departments.