Contemporânea
Contemporary Journal
Vol. 5 N°. 6: p. 01-14, 2025
ISSN: 2447-0961

Artigo

GESTÃO DE SHADOW IT: PRÁTICAS PARA REDUZIR RISCOS E POTENCIALIZAR A INOVAÇÃO

SHADOW IT MANAGEMENT: PRACTICES TO REDUCE RISKS AND ENHANCE INNOVATION

GESTIÓN DE TI EN LA SOMBRA: PRÁCTICAS PARA REDUCIR RIESGOS Y POTENCIAR LA INNOVACIÓN

DOI: 10.56083/RCV5N6-037
Receipt of originals: 5/9/2025
Acceptance for publication: 5/30/2025

Bruno Pereira Joca
Doutorando em Ciências Contábeis e Administração
Instituição: Fucape Pesquisa e Ensino S/A
Endereço: Vitória, Espiríto Santo, Brasil
E-mail:brunojoca@yahoo.com

RESUMO: O presente artigo aborda o fenômeno do Shadow IT, caracterizado pelo uso de soluções tecnológicas sem aprovação formal da área de Tecnologia da Informação (TI), analisando seus riscos e potenciais para a inovação. No contexto da transformação digital, especialmente em setores regulados como o financeiro, o Shadow IT tem se expandido como resposta à lentidão dos processos tradicionais de TI, oferecendo agilidade e aderência às necessidades dos usuários. A pesquisa adota abordagem qualitativa e revisão bibliográfica exploratória, com apoio em estudos de caso e na literatura especializada. Foram identificadas sete práticas essenciais para gestão eficaz do Shadow IT, como o mapeamento ativo de ferramentas, a criação de políticas inclusivas, a adoção de modelos de governança federada, e o fortalecimento da cultura de inovação segura. A análise demonstra que, quando corretamente gerido, o Shadow IT pode ser transformado em alavanca estratégica, desde que alinhado às diretrizes institucionais e às exigências regulatórias. Conclui-se que uma governança adaptativa, participativa e baseada na confiança é essencial para mitigar os riscos associados e potencializar os benefícios dessa prática. A articulação entre autonomia e segurança, inovação e conformidade, deve guiar a construção

de uma TI mais ágil, resiliente e orientada ao valor. O estudo reforça a importância de compreender o Shadow IT não como ameaça, mas como oportunidade estratégica a ser integrada aos processos de transformação digital.

PALAVRAS-CHAVE: Shadow IT, inovação digital, governança de TI, gestão de riscos, transformação digital, tecnologia organizacional.

ABSTRACT: This article addresses the phenomenon of Shadow IT, characterized by the use of technological solutions without formal approval from the Information Technology (IT) area, analyzing its risks and potential for innovation. In the context of digital transformation, especially in regulated sectors such as the financial sector, Shadow IT has expanded as a response to the slowness of traditional IT processes, offering agility and adherence to user needs. The research adopts a qualitative approach and exploratory bibliographic review, supported by case studies and specialized literature. Seven essential practices for effective Shadow IT management were identified, such as active mapping of tools, creation of inclusive policies, adoption of federated governance models, and strengthening of a culture of secure innovation. The analysis demonstrates that, when properly managed, Shadow IT can be transformed into a strategic lever, as long as it is aligned with institutional guidelines and regulatory requirements. It is concluded that adaptive, participatory, and trust-based governance is essential to mitigate the associated risks and enhance the benefits of this practice. The connection between autonomy and security, innovation and compliance, should guide the construction of a more agile, resilient and value-oriented IT. The study reinforces the importance of understanding Shadow IT not as a threat, but as a strategic opportunity to be integrated into digital transformation processes.

KEYWORDS: Shadow IT, digital innovation, IT governance, risk management, digital transformation, organizational technology.

RESUMEN: Este artículo aborda el fenómeno de las TI en la sombra, caracterizado por el uso de soluciones tecnológicas sin la aprobación formal del área de Tecnologías de la Información (TI), analizando sus riesgos y su potencial de innovación. En el contexto de la transformación digital, especialmente en sectores regulados como el financiero, las TI en la sombra se han expandido como respuesta a la lentitud de los procesos de TI tradicionales, ofreciendo agilidad y adaptación a las necesidades de los usuarios. La investigación adopta un enfoque cualitativo y una revisión bibliográfica exploratoria, con el apoyo de estudios de caso y literatura especializada. Se identificaron siete prácticas esenciales para una gestión eficaz de las TI en la sombra, como el mapeo activo de herramientas, la

creación de políticas inclusivas, la adopción de modelos de gobernanza federada y el fortalecimiento de una cultura de innovación segura. El análisis demuestra que, con una gestión adecuada, las TI en la sombra pueden transformarse en una herramienta estratégica, siempre que se ajusten a las directrices institucionales y los requisitos regulatorios. Se concluye que una gobernanza adaptativa, participativa y basada en la confianza es esencial para mitigar los riesgos asociados y potenciar los beneficios de esta práctica. La conexión entre autonomía y seguridad, innovación y cumplimiento normativo debe guiar la construcción de una TI más ágil, resiliente y orientada al valor. El estudio refuerza la importancia de entender Shadow IT no como una amenaza, sino como una oportunidad estratégica para integrarse en los procesos de transformación digital.

PALABRAS CLAVE: Shadow IT, innovación digital, gobernanza de TI, gestión de riesgos, transformación digital, tecnología organizacional.

1. Introdução

No atual cenário de transformação digital acelerada, organizações de todos os setores enfrentam uma pressão crescente por inovação, agilidade e personalização dos serviços. Essa nova dinâmica, impulsionada por tecnologias emergentes e pelo empoderamento dos usuários finais, tem contribuído para a intensificação de um fenômeno cada vez mais relevante: o Shadow IT. Trata-se do uso de aplicações, sistemas, dispositivos e serviços tecnológicos sem o conhecimento, supervisão ou autorização explícita das áreas formais de Tecnologia da Informação (TI) das empresas. Embora por muito tempo tenha sido considerado um risco a ser eliminado, o Shadow IT hoje é compreendido por muitos estudiosos e profissionais como uma resposta espontânea à lentidão, burocracia e falta de aderência das soluções oficiais às necessidades do negócio.

Pesquisas recentes indicam que entre 50% e 70% dos colaboradores utilizam, em alguma medida, ferramentas e tecnologias não autorizadas para

desempenhar suas funções (Kopper et al., 2020). O mais alarmante, porém, é que menos da metade dos profissionais de TI e das áreas de negócio acredita que os Chief Information Officers (CIOs) tenham plena consciência das tecnologias que realmente afetam o dia a dia das operações. Isso sugere uma desconexão crítica entre a governança de TI tradicional e a realidade vivida nos setores operacionais, sobretudo em contextos de alta volatilidade e exigência por inovação contínua.

No setor financeiro, esse panorama adquire contornos ainda mais sensíveis. Trata-se de um ambiente altamente regulado, com exigências rigorosas de conformidade (compliance), proteção de dados e segurança cibernética. Qualquer uso não autorizado de soluções tecnológicas pode resultar em sérios riscos institucionais, como vazamentos de informações sigilosas, violações à Lei Geral de Proteção de Dados (LGPD), falhas de interoperabilidade e exposição a ataques cibernéticos. Tais incidentes não apenas comprometem a integridade dos sistemas, mas também a confiança do público, elemento central na reputação de instituições financeiras.

Paradoxalmente, o surgimento do Shadow IT também revela uma demanda legítima por autonomia, flexibilidade e inovação nas pontas da organização. Ferramentas como planilhas avançadas, aplicativos em nuvem, plataformas de análise de dados e serviços colaborativos são frequentemente adotados por usuários de negócio justamente por preencherem lacunas que as soluções institucionais ainda não cobrem com eficiência. Em outras palavras, o Shadow IT surge como um sintoma da inadequação das estruturas tradicionais de TI frente às exigências do novo paradigma digital.

Diante disso, torna-se evidente que adotar uma postura exclusivamente reativa, pautada na proibição e no controle rígido, tende a ser contraproducente. A proposta deste artigo é defender uma abordagem mais estratégica e propositiva para a gestão do Shadow IT. Em vez de combatê-lo como uma ameaça isolada, sugere-se tratá-lo como uma oportunidade de escuta organizacional e modernização da governança

tecnológica. Propõe-se, assim, um conjunto de práticas recomendadas que permita às organizações — especialmente no setor financeiro — equilibrar dois objetivos muitas vezes percebidos como antagônicos: mitigar riscos operacionais e regulatórios, e ao mesmo tempo fomentar a inovação orientada às necessidades reais dos usuários.

Ao criar diretrizes práticas, mecanismos de engajamento intersetorial e políticas flexíveis de governança, é possível construir um modelo de TI mais resiliente, inclusivo e adaptável. Tal modelo não apenas reduz a incidência de Shadow IT nocivo, como também canaliza sua energia criativa para dentro de uma estratégia corporativa consciente e eficiente. Esta é a proposta central que sustenta o presente trabalho.

2. Referencial Teórico

2.1 Shadow IT: Riscos Reais e Oportunidades Estratégicas

O fenômeno do Shadow IT, caracterizado pelo uso de tecnologias e soluções digitais sem o conhecimento ou aprovação formal da área de Tecnologia da Informação (TI), tem ganhado crescente atenção tanto no meio acadêmico quanto nas práticas organizacionais. A literatura especializada alerta para os riscos substanciais que o Shadow IT pode acarretar, incluindo vulnerabilidades de segurança, perda de controle sobre dados sensíveis, duplicidade de sistemas e falhas na integração tecnológica (Györy et al., 2012; Gartner, 2021). Em especial no setor financeiro, onde a conformidade regulatória é estrita e os padrões de segurança são elevados, a proliferação de tecnologias paralelas pode representar um ponto crítico de falha na arquitetura de TI corporativa.

No entanto, a compreensão do Shadow IT apenas como ameaça é reducionista. Diversos autores reconhecem que sua emergência está profundamente associada à busca por agilidade e inovação nas áreas de

negócio. Behrens (2009) argumenta que os chamados "sistemas-sombra" surgem como resposta às limitações percebidas da TI centralizada, e frequentemente proporcionam soluções mais rápidas, personalizadas e economicamente viáveis para problemas específicos. Zimmermann, Rentrop e Felden (2014) acrescentam que o Shadow IT pode ser interpretado como uma expressão legítima de inovação orientada pelo usuário final, especialmente em ambientes organizacionais que sofrem com a lentidão dos processos de governança tecnológica.

Estudos recentes reforçam essa perspectiva ao indicar que as iniciativas de Shadow IT podem aumentar a eficiência operacional e promover o alinhamento mais direto com as necessidades reais dos usuários (Kopper, Westner & Strahringer, 2020). Segundo os autores, "a TI gerenciada pelas unidades de negócio é percebida de forma positiva quando existe alinhamento com o departamento de TI e quando se restringe a requisitos locais" (Kopper et al., 2020, p. 221). Essa constatação remete à proposta de uma TI federada, onde a autonomia das áreas de negócio é compatibilizada com os padrões e diretrizes institucionais.

Neste contexto, György et al. (2012) sugerem que a governança do Shadow IT não deve ser pautada apenas pela lógica da proibição, mas sim pela compreensão do papel estratégico dessas iniciativas. É necessário desenvolver mecanismos de identificação, avaliação e incorporação dessas soluções ao ecossistema tecnológico da organização. Isso pode ser feito por meio de abordagens de governança adaptativa, em que políticas são elaboradas para reconhecer e orientar o uso legítimo do Shadow IT, em vez de simplesmente reprimi-lo (Haag & Eckhardt, 2017).

Além disso, pesquisas sobre práticas de TI emergentes destacam a importância de promover uma cultura organizacional que estimule a inovação segura. Segundo Iivari, Sharma e Ventä-Olkkonen (2020), a aceitação do Shadow IT como componente legítimo da estratégia digital pode fortalecer a resiliência organizacional, desde que sejam implementadas

estruturas claras de responsabilidade, mecanismos de monitoramento e canais de colaboração entre as áreas de TI e de negócio.

Cabe também observar que o crescimento do Shadow IT está vinculado à democratização do acesso à tecnologia, com a popularização de ferramentas SaaS, plataformas low-code e aplicativos de produtividade em nuvem (Gartner, 2021). Tais recursos, ao mesmo tempo em que capacitam os usuários finais a inovar, aumentam a complexidade da governança de TI e exigem novos modelos de gestão baseados em confiança, capacitação e responsabilização.

Portanto, a gestão eficaz do Shadow IT exige uma mudança de paradigma: é preciso sair de uma lógica reativa e repressiva para adotar uma postura proativa, estratégica e integradora. A organização que consegue equilibrar controle e autonomia, segurança e inovação, constrói um ecossistema tecnológico mais dinâmico, participativo e aderente às transformações digitais contemporâneas. Como enfatiza Weill e Ross (2004), uma governança de TI eficaz não se faz pela centralização extrema, mas pela capacidade de criar mecanismos flexíveis de tomada de decisão tecnológica que considerem os múltiplos atores envolvidos.

Em síntese, o Shadow IT representa não apenas um desafio, mas uma oportunidade estratégica. Reconhecê-lo como tal é o primeiro passo para transformá-lo em aliado da inovação organizacional. A literatura mostra que, com políticas claras, envolvimento das lideranças e adoção de boas práticas, é possível mitigar seus riscos e amplificar seus benefícios — criando, assim, um ambiente mais ágil, seguro e alinhado às exigências do mercado digital.

3. Metodologia

Este artigo adota uma abordagem qualitativa, com base em revisão bibliográfica exploratória e análise de estudos de caso previamente documentados na literatura acadêmica, com foco especial no setor

financeiro. A metodologia teórico-prática foi fundamentada em autores relevantes da área de Sistemas de Informação, como Behrens (2009), Kopper et al. (2020), e Györy et al. (2012), com o objetivo de identificar padrões, riscos e boas práticas associados à gestão do Shadow IT. Utilizou-se também a análise de recomendações de governança e segurança da informação, a fim de estruturar um conjunto de práticas aplicáveis à realidade organizacional. Essa abordagem permitiu construir um guia baseado em evidências empíricas e contribuições teóricas consolidadas.

4. Resultados e Discussões

A partir da análise de estudos de caso conduzidos por Kopper et al. (2020), somada à revisão da literatura sobre governança de tecnologia e transformação digital, foi possível estruturar um conjunto de sete práticas estratégicas voltadas à gestão eficaz do Shadow IT. Longe de buscar sua erradicação total — o que se mostra, na prática, inviável —, este guia tem como objetivo canalizar o potencial inovador do Shadow IT de forma segura, controlada e alinhada à estratégia organizacional, especialmente em setores críticos como o financeiro.

O primeiro passo para compreender e gerir o Shadow IT é o reconhecimento explícito da sua existência. Muitas vezes, as áreas de TI subestimam o volume e a variedade de soluções adotadas autonomamente pelas unidades de negócio. Portanto, torna-se essencial implementar mecanismos sistemáticos de detecção — como auditorias periódicas, escaneamento de tráfego de rede, entrevistas com usuários-chave e análise de logs — que permitam mapear ferramentas, dispositivos, plataformas e aplicativos em uso fora do controle formal.

Esse mapeamento não se limita à identificação de riscos, mas também permite capturar boas práticas e soluções inovadoras que emergem das "pontas" da organização, potencializando a inteligência coletiva interna.

A repressão pura e simples ao uso não autorizado de tecnologia tende a gerar resistência e estimular comportamentos ocultos. Em vez disso, propõe-se a construção de políticas orientativas, elaboradas de forma participativa entre TI e as áreas de negócio. Essas diretrizes devem estabelecer critérios transparentes para a adoção, experimentação e integração de novas ferramentas, definindo com clareza: o que pode ou não ser adotado autonomamente; quais os pré-requisitos técnicos e de segurança devem ser atendidos; quais são os limites de responsabilidade de cada área; como submeter novas soluções à homologação.

Essa abordagem aumenta a legitimidade das regras e fortalece o engajamento dos usuários no processo de governança.

A centralização excessiva das decisões tecnológicas é um dos fatores que alimenta o Shadow IT. Para mitigar esse risco e, ao mesmo tempo, garantir segurança e coerência organizacional, recomenda-se a adoção de modelos federados de governança, nos quais a responsabilidade pelas tecnologias é compartilhada entre a TI e os usuários de negócio.

Nesse modelo, a TI mantém o papel de orquestradora da arquitetura corporativa, da segurança e da interoperabilidade, enquanto as áreas de negócio ganham autonomia operacional e capacidade de inovação supervisionada. Trata-se de uma lógica de empoderamento responsável, onde a descentralização é acompanhada de alinhamento normativo e técnico.

O fortalecimento das capacidades digitais das áreas de negócio é um pilar fundamental na mitigação do Shadow IT nocivo. Investir em formações contínuas voltadas para segurança da informação, proteção de dados, boas práticas em cloud computing e uso consciente de tecnologia é essencial. Além disso, a disponibilização de ferramentas validadas de low-code/no-code, ambientes seguros de sandbox e catálogos de APIs internas permite que os usuários inovem com autonomia dentro de um perímetro seguro.

Essa prática reduz a fricção entre TI e negócio, encoraja soluções criativas e contribui para uma cultura de colaboração multidisciplinar na resolução de problemas.

Um dos principais motivadores do Shadow IT é a falta de acesso rápido a ferramentas úteis e atualizadas. Para contornar isso, é recomendável manter um catálogo corporativo de soluções homologadas, constantemente revisado e adaptado às necessidades emergentes das equipes. Esse repositório deve contemplar: aplicações de produtividade (gestores de tarefas, colaboração, dashboards); plataformas de analytics e BI; ferramentas de automação de processos; serviços de armazenamento e integração.

Ao ampliar e diversificar esse portfólio de soluções aprovadas, reduz-se a tentação de buscar ferramentas externas e não seguras, ao mesmo tempo em que se fortalece a coerência da infraestrutura digital da organização.

A proliferação de soluções tecnológicas não alinhadas aos objetivos da empresa tende a gerar sistemas redundantes, desconexos e ineficientes. Por isso, toda inovação tecnológica — seja originada pela TI, seja pelas áreas de negócio — deve passar por uma análise de aderência estratégica, na qual se avalie sua contribuição para os macrodesafios da organização: crescimento, eficiência operacional, experiência do cliente, conformidade regulatória, entre outros.

Esse alinhamento exige diálogo permanente entre líderes de TI, de negócio e de compliance, bem como o uso de ferramentas de priorização e análise de impacto. Iniciativas digitais que não agregam valor estratégico devem ser revistas ou descontinuadas.

A transformação cultural é a espinha dorsal de uma gestão eficaz do Shadow IT. Mais do que normas e controles, é necessário promover uma mudança de mentalidade que valorize a inovação segura, o diálogo intersetorial e a responsabilidade digital. Para isso, recomenda-se:

reconhecer publicamente iniciativas inovadoras que respeitam as diretrizes de TI; compartilhar boas práticas e aprendizados em eventos internos; incluir indicadores de governança de Shadow IT nos painéis de gestão; promover campanhas educativas sobre riscos e benefícios das tecnologias emergentes.

Uma cultura que valoriza a experimentação responsável, sem abrir mão da segurança e da conformidade, tende a reduzir os efeitos negativos do Shadow IT e a maximizar seu potencial criativo.

Essas sete práticas compõem um modelo integrado de gestão do Shadow IT que reconhece a complexidade do fenômeno e propõe soluções pragmáticas, centradas no equilíbrio entre controle e inovação. No setor financeiro, onde os riscos são amplificados por exigências legais, normativas e reputacionais, adotar esse modelo não é apenas desejável — é estratégico. Organizações que conseguirem integrar a energia inovadora das áreas de negócio à governança técnica da TI estarão mais bem posicionadas para competir em um ambiente digital dinâmico, seguro e resiliente.

5. Conclusão

O Shadow IT não deve ser encarado como um adversário a ser eliminado, mas como uma realidade dinâmica que reflete as transformações contemporâneas nas práticas organizacionais e na relação entre tecnologia e negócios. Este artigo demonstrou que, embora os riscos relacionados ao Shadow IT sejam significativos — incluindo vazamento de dados, fragilidade na segurança da informação e desconexão entre sistemas — sua gestão estratégica pode converter tais desafios em alavancas de inovação e eficiência.

Evidências acadêmicas e práticas sugerem que iniciativas descentralizadas de TI, quando alinhadas às diretrizes institucionais e acompanhadas de políticas inclusivas, podem acelerar processos de transformação digital. No setor financeiro, por exemplo, onde os níveis de

risco são altos e as exigências regulatórias rigorosas, modelos federados de governança tecnológica — que conciliam a autonomia das áreas de negócio com o suporte e a supervisão da TI central — têm demonstrado eficácia na promoção de inovação com segurança.

Ao invés de se apoiar exclusivamente em proibições e controles rígidos, as organizações devem adotar mecanismos de mapeamento ativo, capacitação supervisionada, catálogos de ferramentas homologadas, e sobretudo, promover uma cultura organizacional baseada na confiança e na corresponsabilidade tecnológica. Como defendem Györy et al. (2012) e Kopper et al. (2020), a chave para lidar com o Shadow IT não está em eliminá-lo, mas em compreender suas motivações, integrar suas contribuições e garantir que elas estejam conectadas à estratégia da organização.

Em última instância, o Shadow IT oferece um termômetro da capacidade de adaptação das organizações à nova lógica digital, que exige agilidade, descentralização e proximidade com as necessidades reais dos usuários. Incorporar esse fenômeno à governança estratégica é reconhecer que a inovação, em muitas situações, nasce nas margens — e que é papel da liderança institucional canalizar essas iniciativas para que se tornem sustentáveis, seguras e transformadoras.

Portanto, a conclusão que se impõe é que a gestão inteligente do Shadow IT representa não apenas uma resposta aos desafios da transformação digital, mas um passo necessário rumo à construção de uma TI mais participativa, flexível e alinhada ao futuro dos negócios. Reconhecer, regular e integrar são verbos-chave de um novo modelo de governança — mais dialógico, adaptativo e orientado ao valor.

Referências

BEHRENS, S. **Shadow systems**: the good, the bad and the ugly. Communications of the ACM, v. 52, n. 2, p. 124–129, 2009.

GARTNER. **Emerging risks**: The top 10 for 2021. Stamford: Gartner, 2021.

GYÖRY, A. et al. **Exploring the shadow**s: IT governance approaches to user-driven innovation. ECIS 2012 Proceedings, Paper 222. 2012. Disponível em: http://aisel.aisnet.org/ecis2012/222. Acesso em: 3 jun. 2025.

HAAG, S.; ECKHARDT, A. **Shadow IT**. Business & Information Systems Engineering, v. 59, n. 6, p. 469–473, 2017.

IIVARI, N.; SHARMA, S.; VENTÄ-OLKKONEN, L. **Digital transformation of everyday life – How COVID-19 pandemic transformed the basic education of the young generation and why information management research should care**? International Journal of Information Management, v. 55, p. 102183, 2020.

KOPPER, A.; WESTNER, M.; STRAHRINGER, S. **From Shadow IT to Business-managed IT**: A qualitative comparative analysis to determine configurations for successful management of IT by business entities. Information Systems and E-Business Management, v. 18, p. 209–257, 2020.

WEILL, P.; ROSS, J. W. **IT governance**: How top performers manage IT decision rights for superior results. Boston: Harvard Business School Press, 2004.

ZIMMERMANN, S.; RENTROP, C.; FELDEN, C. **Managing shadow IT instances – a method to control autonomous IT solutions in the business departments**. In: Proceedings of the 20th Americas Conference on Information Systems, Savannah, USA, 2014. p. 1–12.