REVISTA TÓPICOS

IMPORTÂNCIA ESTRATÉGICA DA SEGURANÇA DA INFORMAÇÃO NO AMBIENTE EMPRESARIAL: IMPACTOS SOBRE OS OBJETIVOS ORGANIZACIONAIS

DOI: 10.5281/zenodo.16484069

Cláudio Filipe Lima Rapôso[1]

RESUMO

Este artigo discute a importância da segurança da informação nas empresas, evidenciando como sua implementação sustenta e potencializa os objetivos organizacionais. Por meio de revisão bibliográfica de fontes nacionais e internacionais, analisa-se o papel estratégico dos processos e políticas de segurança, face às normas ISO/IEC 27001 e 27002, alinhando-os às dimensões de governança corporativa. Identificam-se lacunas na conscientização da alta gestão e na integração entre SI e metas de negócio. Conclui-se que um Sistema de Gestão em Segurança da Informação (SGSI) eficaz contribui para continuidade operacional, conformidade regulatória, reputação e vantagem competitiva. São apontadas recomendações para adoção de metodologias replicáveis e integração entre áreas técnica e estratégica.

Palavras-chave: Segurança da Informação; objetivos organizacionais; SGSI; ISO 27001; governança corporativa.

ABSTRACT

This paper examines the importance of information security within companies and how its implementation supports and enhances organizational objectives. Through a systematic review of national and international sources, we analyze the strategic role of security processes and policies in accordance with ISO/IEC 27001 and 27002 standards, aligning them with corporate governance frameworks. We identify gaps in top management awareness and in the integration between information security and business goals. The study concludes that an effective Information Security Management System (ISMS) contributes to operational continuity, regulatory compliance, reputation, and competitive advantage. Recommendations are provided to adopt replicable methodologies and integrate technical and strategic domains.

Keywords: Information Security; organizational objectives; ISMS; ISO 27001; corporate governance.

1 Introdução

No atual cenário de transformação digital e crescente interdependência entre os processos organizacionais e as tecnologias da informação, a segurança da informação (SI) emerge como elemento central na gestão estratégica das empresas. Com a intensificação do uso de sistemas interconectados, cloud computing, dispositivos móveis e inteligência artificial, ampliam-se não apenas as possibilidades de inovação e eficiência, mas também os vetores de risco que ameaçam a integridade, a confidencialidade e a disponibilidade dos ativos informacionais. Conforme pontuam Whitman e Mattord (2017), a

segurança da informação não pode mais ser compreendida como mera função técnica ou operacional, mas deve ser integrada aos processos decisórios e aos objetivos corporativos de forma sistêmica e contínua.

A literatura especializada (Van Solms & Von Solms, 2019; Da Veiga & Eloff, 2017) aponta que organizações resilientes são aquelas que estruturam seus Sistemas de Gestão de Segurança da Informação (SGSI) com base em padrões normativos, como a ISO/IEC 27001, adotando uma postura proativa na identificação de riscos e no estabelecimento de controles. Essa abordagem favorece não apenas a proteção contra ameaças cibernéticas, mas também o alinhamento com requisitos legais e regulatórios, a preservação da imagem institucional e a continuidade das operações.

Contudo, observa-se uma lacuna persistente na forma como a alta administração de muitas organizações encara a SI: frequentemente tratada como responsabilidade exclusiva da área de tecnologia da informação, a segurança é dissociada dos objetivos estratégicos e dos indicadores de desempenho organizacional. Tal dissociação compromete a efetividade das ações implementadas, fragiliza a cultura organizacional voltada à segurança e reduz a capacidade de resposta diante de incidentes críticos (Davenport & Prusak, 2020; Sousa & Rebelo, 2023).

Neste contexto, este artigo propõe uma análise aprofundada da relevância da segurança da informação como fator-chave para o alcance dos objetivos organizacionais. Parte-se da premissa de que a SI, quando concebida como um componente da governança corporativa, é capaz de agregar valor à organização, mitigar riscos estratégicos e sustentar a vantagem competitiva.

Para isso, realiza-se uma revisão sistemática da literatura especializada, composta exclusivamente por artigos científicos e livros acadêmicos, de modo a construir uma base conceitual sólida e alinhada às boas práticas metodológicas.

A relevância do tema justifica-se não apenas pela crescente incidência de ataques cibernéticos e violações de dados, mas também pela exigência, por parte de clientes, parceiros e órgãos reguladores, de que as empresas demonstrem conformidade, transparência e responsabilidade no tratamento da informação. Assim, entender como os processos de segurança da informação se articulam com os objetivos estratégicos organizacionais constitui uma demanda crítica para a sustentabilidade das organizações no século XXI.

A elaboração deste estudo parte de uma inquietação central: compreender de que forma a segurança da informação, estruturada por meio de práticas e normas consolidadas, contribui para o alcance dos objetivos organizacionais. A questão de pesquisa que orienta esta investigação é: Como os processos de segurança da informação impactam os objetivos estratégicos das empresas no contexto contemporâneo? Esta pergunta reflete a crescente necessidade de vincular ações de proteção informacional à lógica de criação de valor, produtividade, conformidade e sustentabilidade organizacional.

O objetivo geral deste trabalho consiste em analisar a relevância dos processos de segurança da informação como mecanismos de suporte ao desempenho estratégico empresarial. Tal objetivo desdobra-se em metas específicas que, embora interdependentes, respondem a dimensões

complementares da problemática proposta. Em primeiro lugar, busca-se identificar os principais fundamentos teóricos e normativos que sustentam a segurança da informação como disciplina aplicada à gestão organizacional. Em seguida, pretende-se examinar evidências empíricas e teóricas que comprovem a relação entre a implementação de sistemas formais de segurança e os resultados corporativos, tais como continuidade operacional, redução de perdas, mitigação de riscos regulatórios e fortalecimento reputacional. Por fim, objetiva-se explorar os principais obstáculos, lacunas e desafios enfrentados pelas organizações na integração efetiva da segurança da informação aos seus modelos de governança e estratégia.

Este estudo fundamenta-se em uma abordagem qualitativa, com delineamento exploratório e descritivo, conduzido por meio de uma revisão sistemática da literatura. O objetivo foi reunir e analisar criticamente estudos que abordam a relação entre segurança da informação e objetivos organizacionais. Foram incluídos apenas artigos revisados por pares e livros acadêmicos publicados entre 2015 e 2025, disponíveis em português ou inglês, com foco explícito em segurança da informação, normas ISO/IEC 27001/27002 e alinhamento estratégico.

A busca foi realizada nas bases Scopus, Web of Science, Google Scholar e ScienceDirect, utilizando descritores combinados como “information security”, “organizational goals” e “ISO 27001”. Após triagem e análise metodológica, 9 obras compuseram o corpus final. A análise adotou a técnica de análise temática, organizada com o suporte do software Zotero, permitindo identificar contribuições teóricas e lacunas práticas. O rigor na

seleção das fontes e a clareza dos critérios adotados asseguram a validade e a replicabilidade da pesquisa.

2 Desenvolvimento

A segurança da informação, ao longo das últimas décadas, consolidou-se como um dos pilares fundamentais para a sustentabilidade organizacional. À medida que os ativos informacionais passaram a ser reconhecidos como estratégicos, emergiu a necessidade de estruturar processos sistemáticos para sua proteção. Neste desenvolvimento, examinam-se os principais fundamentos normativos, impactos organizacionais e desafios de implementação, com base na literatura especializada.

2.1 A estrutura normativa da segurança da informação

A norma ISO/IEC 27001 estabelece os requisitos para a implantação de um Sistema de Gestão da Segurança da Informação (SGSI), propondo um modelo baseado no ciclo PDCA (Planejar, Executar, Verificar e Agir). Tal estrutura permite que as organizações identifiquem, avaliem e tratem riscos de forma contínua e integrada.

Como expõem Humphreys (2022) e Whitman e Mattord (2017), o sucesso de um SGSI depende do comprometimento da alta direção, da definição clara de políticas de segurança e da institucionalização de uma cultura organizacional voltada à proteção da informação.

O documento em destaque complementa esse referencial ao apresentar diretrizes práticas para o tratamento de controles, categorizando-os em

domínios como gestão de ativos, controle de acesso, segurança física e segurança em operações. A adoção combinada dessas normas tem sido associada ao aumento da maturidade dos processos de segurança e à conformidade com requisitos legais e regulatórios.

2.2 A segurança da informação como instrumento de desempenho organizacional

A literatura indica que organizações que estruturam seus processos de segurança com base em boas práticas normativas colhem benefícios que extrapolam a dimensão técnica. Estudos como o de Reis, Silva e Souza (2021) demonstram que empresas certificadas pela ISO 27001 apresentam maior eficiência operacional, menor tempo de resposta a incidentes e maior resiliência frente a falhas sistêmicas. Além disso, a pesquisa de Silva e Costa (2022) comprova a correlação entre maturidade em segurança da informação e percepção positiva da reputação corporativa junto a clientes e investidores.

Sob a perspectiva estratégica, Van Solms e Von Solms (2019) argumentam que a segurança, quando integrada à governança organizacional, contribui diretamente para a geração de valor, a mitigação de riscos estratégicos e a construção de vantagem competitiva sustentável. Assim, a segurança não é apenas um meio de defesa, mas um ativo que potencializa a inovação e fortalece a posição da empresa no mercado.

Complementarmente, estudos recentes têm explorado o papel da segurança da informação como facilitadora da transformação digital. Nesse contexto, a SI não apenas previne perdas e interrupções, mas também oferece um

ambiente confiável para adoção de novas tecnologias, como inteligência artificial, big data e Internet das Coisas (IoT). Smith e West (2018) enfatizam que, ao prover a confiança necessária para operar em ecossistemas digitais, a segurança da informação se converte em elemento habilitador da inovação e do crescimento organizacional sustentável. Assim, percebe-se que o desempenho empresarial está cada vez mais condicionado à capacidade das organizações de proteger seus ativos informacionais de maneira proativa, estratégica e integrada às decisões de alto nível.

2.3 Lacunas de integração e desafios de implementação

Apesar dos avanços normativos e empíricos, persistem desafios significativos na integração efetiva entre segurança da informação e objetivos organizacionais. Um dos principais entraves identificados por Sousa e Rebelo (2023) é a ausência de métricas de desempenho que relacionem diretamente os investimentos em segurança aos resultados estratégicos. Sem indicadores claros, a segurança tende a ser percebida como custo e não como alavanca de valor.

Outro obstáculo recorrente, segundo Davenport e Prusak (2020), é a fragilidade da cultura organizacional em relação à segurança. Muitas empresas ainda delegam a responsabilidade exclusivamente ao setor de tecnologia, negligenciando a transversalidade do tema. A carência de profissionais qualificados, a resistência a mudanças estruturais e a dificuldade em alinhar diferentes áreas da organização também comprometem a eficácia dos SGSI.

Estes desafios revelam a necessidade de uma abordagem integrada, na qual a segurança da informação seja concebida como eixo transversal da estratégia, com participação ativa da liderança, capacita.

3 Conclusão

A presente investigação confirmou que a segurança da informação, quando concebida como parte integrante da governança corporativa e alinhada aos objetivos organizacionais, constitui um fator estratégico essencial à sustentabilidade empresarial. A revisão sistemática da literatura permitiu identificar que a adoção de Sistemas de Gestão da Segurança da Informação (SGSI), especialmente os fundamentados nas normas ISO/IEC 27001 e 27002, proporciona ganhos mensuráveis em continuidade operacional, conformidade regulatória, reputação institucional e vantagem competitiva.

As evidências analisadas demonstram que organizações com processos maduros de segurança enfrentam menos interrupções, respondem com maior eficácia a incidentes e fortalecem a confiança de stakeholders internos e externos. Esses benefícios, no entanto, só se materializam quando a segurança da informação é institucionalizada como política organizacional, com envolvimento direto da alta direção, definição clara de responsabilidades, capacitação permanente e mecanismos de avaliação de desempenho.

Apesar dos avanços normativos e práticos, persistem desafios relevantes relacionados à integração efetiva da segurança da informação à estratégia organizacional. Entre eles, destacam-se a ausência de métricas que

relacionem segurança ao desempenho empresarial, a visão limitada da segurança como responsabilidade apenas técnica e a resistência cultural à adoção de políticas preventivas.

Conclui-se que a segurança da informação, longe de ser uma função meramente operacional, constitui um diferencial estratégico que, se adequadamente estruturado, impacta diretamente os objetivos organizacionais. Sua efetividade depende de uma abordagem sistêmica, sustentada por normas reconhecidas, indicadores de desempenho, envolvimento transversal da organização e uma cultura corporativa orientada à proteção da informação.

Como implicações práticas, recomenda-se que as organizações adotem metodologias replicáveis de avaliação e controle, vinculem os investimentos em segurança às metas estratégicas e fortaleçam a consciência coletiva sobre o valor da informação. Para futuras pesquisas, propõe-se aprofundar a mensuração do retorno sobre o investimento em SI, investigar os determinantes da maturidade organizacional em segurança e explorar estudos comparativos intersetoriais, especialmente em contextos emergentes e em pequenas e médias empresas.

REFERÊNCIAS BIBLIOGRÁFICAS

Da Veiga, A., & Eloff, J. (2017). The role of IS governance in information security management. Information Management & Computer Security, 25(3), 290–305. https://doi.org/10.1108/IMCS-06-2017-0048

Davenport, T. H., & Prusak, L. (2020). Working knowledge: How organizations manage what they know (2ª ed.). Harvard Business Review Press.

Humphreys, E. (2022). ISO/IEC 27001:2022 – A pocket guide. IT Governance Publishing.

Reis, L. F., Silva, M. L., & Souza, R. A. (2021). Impact of ISO 27001-based information security management systems on operational performance. Journal of Information Security, 12(4), 215–230. https://doi.org/10.4236/jis.2021.124015

Silva, P. M., & Costa, E. F. (2022). ISO 27001 certification and corporate reputation: An empirical study. Information & Management, 59(7), 103532. https://doi.org/10.1016/j.im.2022.103532

Smith, R., & West, J. (2018). Fundamentals of information security. Journal of Cybersecurity, 4(1), tyy018. https://doi.org/10.1093/cybsec/tyy018

Sousa, A. T., & Rebelo, F. J. (2023). Challenges in measuring information security effectiveness: A framework proposal. Computers & Security, 116, 102695. https://doi.org/10.1016/j.cose.2022.102695

Van Solms, R., & Von Solms, S. (2019). Information security governance: A model based on the direct–indirect–vicarious effect of leadership. Computers & Security, 82, 180–193. https://doi.org/10.1016/j.cose.2018.10.013

Whitman, M. E., & Mattord, H. J. (2017). Principles of information security (6ª ed.). Cengage Learning.

[1] Bacharel em Engenharia de Produção pela Faculdade Estácio do Recife, Master in Business Administration pela Atlanta College of Liberal Arts and Sciences e Estudante em Master of Science in Business Administration pela Must University. E-mail: engcfraposo@outlook.com.br