REVISTA TÓPICOS

DESVENDANDO A INFLUÊNCIA DO ENFOQUE SOCIAL NA SEGURANÇA DA INFORMAÇÃO E NO DESEMPENHO ORGANIZACIONAL

DOI: 10.5281/zenodo.14627157

Lauren Aparecida Barcelos Sanches[1]

RESUMO

O presente estudo tem como objetivo apresentar a influência do enfoque social na segurança da informação e no desempenho organizacional. Com esse propósito, foram abordados temas como a definição e as características da segurança da informação, de que forma a segurança da informação contribui para a inovação e o crescimento dos objetivos organizacionais, além da importância do enfoque social na proteção dos seus dados. A metodologia utilizada para esse estudo foi uma revisão bibliográfica, realizando pesquisas em fontes atualizadas e confiáveis sobre o assunto. A partir dos assuntos apresentados, observou-se que a segurança da informação é um aspecto fundamental dentro do ambiente empresarial, uma vez que a proteção de dados e informações sensíveis é essencial para o bom funcionamento e a sustentabilidade do negócio. Com o enorme crescimento da tecnologia e da internet, as informações estão cada vez mais expostas a ameaças cibernéticas, o que torna essencial a adoção de práticas relacionadas ao enfoque social para a consolidação da proteção e

segurança. Esse investimento é uma estratégia importante para o sucesso e durabilidade das organizações diante das ameaças que estão em constante evolução. Portanto, a implementação de processos contribui significativamente para a preservação da integridade, confidencialidade e disponibilidade das informações, garantindo a confiança dos stakeholders e o cumprimento de normas e regulamentações vigentes.
Palavras-chave: Confidencialidade. Disponibilidade. Integridade. Organizações. Segurança da Informação.

ABSTRACT

The present study aims to present the influence of the social focus on information security and organizational performance. For this purpose, topics such as the definition and characteristics of information security were addressed, how information security contributes to innovation and the growth of organizational objectives, in addition to the importance of a social focus on protecting your data. The methodology used for this study was a bibliographic review, carrying out research in updated and reliable sources on the subject. From the topics presented, it was observed that information security is a fundamental aspect within the business environment, since the protection of sensitive data and information is essential for the proper functioning and sustainability of the business. With the enormous growth of technology and the internet, information is increasingly exposed to cyber threats, which makes it essential to adopt practices related to a social approach to consolidate protection and security. This investment is an important strategy for the success and durability of organizations in the face of constantly evolving threats. Therefore, the

implementation of processes significantly contributes to preserving the integrity, confidentiality and availability of information, ensuring stakeholder trust and compliance with current rules and regulations.
Keywords: Confidentiality. Availability. Integrity. Organizations. Information Security.

1 Introdução

A segurança da informação tem sido uma preocupação constante para as organizações, uma vez que a quantidade de dados digitais armazenados e transmitidos aumentou consideravelmente nas últimas décadas. Dessa forma, é preciso que as empresas estabeleçam objetivos organizacionais claros e bem definidos quando se trata de garantir a proteção de suas informações.

Quando a segurança da informação não é adequada, a organização corre o risco de sofrer ataques cibernéticos, vazamento de dados, perda de informações críticas e danos a sua reputação. Isso pode afetar negativamente a produtividade, a eficiência operacional, a confiança dos clientes e parceiros, bem como causar prejuízos financeiros.

Nesse sentido, o objetivo do estudo é que se compreenda como a influência do enfoque social na segurança da informação pode impactar os objetivos organizacionais. Uma vez que, esse tipo de segurança compreende um conjunto de estratégias e procedimentos elaborados com o intuito de resguardar as informações de uma organização contra acessos não autorizados. Suas características incluem a identificação de ameaças, a

implementação de controles de acesso e a realização de avaliações contínuas de riscos.

Para melhor compreensão acerca do tema, o paper está estruturado em três capítulos. A primeira parte aborda a definição e as características da segurança da informação. Em seguida, é apresentado de que maneira esse tipo de segurança contribui para a inovação e o crescimento dos objetivos organizacionais. Por último, é realizada uma análise sobre a forma como o enfoque social impacta na segurança da informação das organizações.

A metodologia utilizada é a de revisão bibliográfica realizada a partir do referencial teórico abordado na disciplina, pesquisas em livros, artigos e outros materiais relacionados para trazer o embasamento às referidas temáticas. Com base nisso, considera-se que a segurança da informação não está apenas relacionada à proteção contra-ataques de hackers, mas também envolve a prevenção de perda de dados, garantindo a disponibilidade, a integridade e a confidencialidade das informações.

Contudo, destaca-se que a implementação eficaz da segurança da informação é primordial para proteger os ativos da organização, contribuir para a inovação e alcançar os objetivos organizacionais. É preciso que se tenha um olhar diferenciado para o enfoque social, conscientizando os colaboradores dos seus riscos. As empresas devem investir não apenas em tecnologia, mas também na capacitação e conscientização deles para garantir uma segurança da informação eficaz e sustentável.

2 Segurança da informação: definição e características

A segurança da informação é um tema determinante atualmente, com o avanço da tecnologia e a crescente dependência de sistemas informatizados em diferentes áreas da sociedade. Em vista disso, a proteção dos dados e informações se tornou uma preocupação inevitável para organizações, governos e indivíduos, visando garantir a confidencialidade, integridade e disponibilidade das informações.

Segundo Hintzbergen, Hintzbergen, Smulders e Baars (2018), a segurança da informação consiste em estratégias e procedimentos implementados para resguardar as informações e dados de uma empresa contra intrusos, furtos, perdas, danos e quaisquer ameaças potenciais. Em outras palavras, tem por objetivo assegurar que somente indivíduos autorizados possam ter acesso aos dados, garantindo sua integridade e proteção. Esse conceito envolve tanto aspectos tecnológicos, como o uso de firewall, antivírus e criptografia, quanto aspectos organizacionais e de gestão, como políticas de segurança, processos de controle de acesso e conscientização dos colaboradores.

Desse modo, a segurança da informação desempenha um papel fundamental no sucesso e crescimento das organizações na era digital. Para Leme e Blank, 2020, a proteção dos dados sensíveis e confidenciais de uma empresa não apenas impede potenciais violações de segurança, mas também cria um ambiente propício para a inovação e o alcance dos objetivos organizacionais.

Dentre as principais características, destacam-se a confidencialidade, que diz respeito à proteção dos dados contra acessos não autorizados,

garantindo que apenas pessoas autorizadas tenham acesso às informações sensíveis. A integridade, que consiste em assegurar que os dados não sejam alterados ou corrompidos, mantendo sua consistência e veracidade. E a disponibilidade, refere-se à garantia de que os sistemas e informações estejam sempre acessíveis quando necessário, evitando interrupções e indisponibilidades (ALMEIDA, 2022).

Além disso, salienta-se a autenticidade e a rastreabilidade que são características que garantem a identificação correta dos usuários e a capacidade de rastrear as ações realizadas nos sistemas, facilitando a investigação em caso de incidentes de segurança. Conforme a percepção de Carloto (2023), a segurança da informação também envolve a conformidade com leis e regulamentos, como a Lei Geral de Proteção de Dados (LGPD), que estabelecem regras e diretrizes para o tratamento e proteção de dados pessoais. Penalidades são impostas para as empresas que não protegem de forma adequada as informações dos indivíduos.

Uma vez identificadas essas características, compreende-se que a segurança da informação é indispensável para as organizações assegurarem a proteção dos seus ativos mais valiosos: as informações. Ao implementar medidas de segurança adequadas, as empresas podem evitar prejuízos financeiros, proteger sua reputação no mercado e manter a confiança de seus clientes e colaboradores. Consequentemente, um investimento como esse é mais do que uma necessidade, é uma questão de sobrevivência no mundo empresarial atual.

3 Como a segurança da informação contribui para a inovação e o crescimento dos objetivos organizacionais

A partir do momento em que uma organização investe em segurança da informação, ela está protegendo não apenas seus ativos digitais, mas também seu capital intelectual. A confidencialidade e integridade das informações são essenciais para o desenvolvimento de novas ideias e soluções inovadoras. Barreto e Lima (2022), argumentam que os colaboradores se sentem mais confiantes em compartilhar suas ideias quando sabem que suas informações estão seguras e protegidas. Isso cria um ambiente de confiança e colaboração que favorece a inovação e o crescimento da organização.

Nesse sentido, percebe-se que a inovação é essencial para a competitividade e o sucesso das organizações no mercado globalizado atual. A capacidade de desenvolver novas ideias, produtos e serviços é um diferencial competitivo que impulsiona o crescimento e a expansão das empresas. No entanto, a inovação só pode ser eficaz se baseada em informações precisas e atualizadas.

A proteção dos ativos e recursos da organização é garantida através do importante papel desempenhado pela segurança da informação. Diante desse cenário, Neves, de Almeida Lopes, Pavani e Sales (2021) alegam que dados corporativos, propriedade intelectual, Sistemas de Tecnologia da Informação (TI) e informações estratégicas são resguardados de maneira eficaz. A perda ou comprometimento desses ativos pode resultar em prejuízos financeiros, danos à reputação da empresa e perda de

competitividade no mercado. Assim sendo, a implementação de processos de segurança da informação é imperiosa para garantir a continuidade dos negócios e a proteção dos interesses da organização.

Um aspecto relevante é que a segurança da informação é necessária para o cumprimento de regulamentações e legislações vigentes. Para Santos (2020), organizações que não protegem adequadamente seus dados estão sujeitas a multas e sanções legais, o que pode afetar significativamente sua reputação e credibilidade no mercado. Por outro lado, empresas que investem em segurança da informação demonstram comprometimento com a proteção dos dados de seus clientes e parceiros, reforçando sua imagem no mercado e aumentando a confiança dos stakeholders (todas as pessoas envolvidas no processo).

Outro aspecto muito impactado são os objetivos organizacionais, uma vez que a proteção dos dados e informações corporativas está diretamente relacionada à eficiência, eficácia e qualidade dos processos e operações empresariais. A implementação de medidas de segurança adequadas contribui para a redução de incidentes de segurança, a melhoria da produtividade e a minimização de custos relacionados à recuperação de dados e à reparação de danos (ARAÚJO, BATISTA e ARAÚJO, 2020).

Quando se analisa sobre a ótica dos objetivos organizacionais, entende-se que esse nível de segurança tem como principal finalidade proteger os dados confidenciais e sensíveis da empresa, evitando assim possíveis violações de segurança e vazamentos de informações. É imprescindível priorizar a disponibilidade, integridade e autenticidade dos dados a fim de

garantir a perpetuidade das atividades e preservar a confiança dos clientes e colaboradores.

Conforme as percepções de Sêmola (2014), outro ponto a destacar é a tentativa de minimizar os riscos associados ao uso de TI, como ataques cibernéticos, falhas de segurança e desastres naturais. Para isso, é importante investir em tecnologias de segurança da informação, como firewalls, antivírus, criptografia e backups regulares, além de promover a conscientização e treinamento dos colaboradores em relação às práticas de segurança.

A segurança da informação também contribui para a eficiência operacional e a inovação dentro da empresa. Ao garantir a integridade dos dados e a disponibilidade dos sistemas, as organizações podem tomar decisões mais assertivas e explorar novas oportunidades de negócio de forma segura.

Em síntese, a segurança da informação é um pilar vital para a inovação e o crescimento das organizações. Investir em medidas protetivas para garantir a integridade e confidencialidade das informações não só protege os ativos digitais da empresa, mas também cria um ambiente propício para o desenvolvimento de novas ideias e soluções inovadoras. As organizações que reconhecem essa importância estão mais bem preparadas para enfrentar os desafios do mundo digital e alcançar seus objetivos organizacionais.

4 A importância do enfoque social na proteção dos dados de uma organização

Nos dias de hoje, o aspecto social da segurança da informação tem ganhado destaque em meio à era digital em que as pessoas estão imersas. Não se trata apenas de proteger dados e sistemas contra ameaças cibernéticas, mas também de assegurar a privacidade e a integridade das informações pessoais dos indivíduos.

Ao adotar uma abordagem social para a proteção dos dados, Leme e Blank (2020) consideram que a organização demonstra preocupação com a privacidade e segurança das informações dos seus funcionários, clientes e parceiros. Isso ajuda a construir confiança e credibilidade com essas partes interessadas, mostrando que a empresa está comprometida em proteger os seus dados e respeitar a sua privacidade.

O enfoque social na proteção dos dados, também contribui para a proteção da reputação da organização (SOUZA, 2020). Casos de vazamento de dados e violações de privacidade podem ter um impacto significativo na imagem e credibilidade da empresa, afetando a sua relação com clientes, colaboradores e o público em geral.

Essa segurança, por sua vez, envolve a proteção de dados, sistemas e infraestrutura contra ameaças cibernéticas, como hackers, malwares e ataques de phishing. Segundo Carloto (2023), a ênfase tem sido em adotar medidas técnicas para garantir a segurança dos sistemas. No entanto, com a crescente quantidade de dados pessoais armazenados online, ocorreu um grande destaque para o impacto social dessas práticas.

O enfoque social da segurança da informação reconhece que a proteção dos dados pessoais dos indivíduos é fundamental para a manutenção da confiança e da privacidade online. Maletta, e Silva (2021) argumentam que isso significa que as empresas e organizações devem adotar políticas e práticas transparentes e éticas em relação ao tratamento e armazenamento de informações dos usuários. Além disso, é importante garantir que medidas de segurança sejam acessíveis e compreensíveis para todos, independentemente do nível de conhecimento técnico.

Ao considerar o aspecto social, é crucial abordar questões de inclusão digital e disparidades de acesso à tecnologia. Muitas vezes, indivíduos em situações de vulnerabilidade têm menos recursos e conhecimento para proteger suas informações pessoais online, o que os torna alvos mais fáceis para ataques cibernéticos (SCHUENCK, 2022). Nesse viés, compreende-se que as políticas adotadas devem levar em consideração essas desigualdades e buscar garantir a proteção de todos os usuários, independentemente de sua condição socioeconômica.

O enfoque social da segurança da informação também pode contribuir para a promoção de uma cultura de privacidade e ética online. Ao educar os usuários sobre práticas seguras na internet e promover a conscientização sobre os riscos de segurança cibernética, é possível reduzir a incidência de ataques e proteger a privacidade das pessoas. Isso não apenas beneficia os indivíduos, mas também a sociedade como um todo, pois uma internet mais segura e confiável contribui para o desenvolvimento e o progresso tecnológico.

Além do mais, a proteção dos dados de uma organização está cada vez mais regulamentada por leis e normas de privacidade, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e a LGPD no Brasil (SANTOS, 2022). Ter um enfoque social na proteção dos dados ajuda a garantir o cumprimento dessas regulamentações e a evitar possíveis penalidades por não estar em conformidade com as leis de proteção de dados.

Em suma, é necessário que as organizações reconheçam a importância do enfoque social na segurança da informação e adotem medidas para promover um ambiente de trabalho saudável, inclusivo e comprometido com a proteção das informações. Somente assim será possível garantir a segurança dos dados, minimizar os riscos e impactos, e alcançar um desempenho organizacional sustentável e competitivo.

5 Considerações Finais

Ao longo do paper, observou-se que a segurança da informação é essencial para qualquer organização que lida com dados e informações sensíveis. Ao garantir a confidencialidade, integridade e disponibilidade dos dados, as empresas podem proteger seus ativos mais valiosos e manter a confiança de seus clientes e parceiros. É primordial adotar práticas e medidas de segurança da informação adequadas para garantir a proteção dos dados e informações de uma organização.

Por outro lado, ao considerar o enfoque social da segurança da informação, as organizações podem desenvolver políticas de segurança mais eficazes,

reduzindo incidentes de segurança, aumentando a produtividade e satisfação dos colaboradores, fortalecendo a imagem da empresa. Por isso, esse investimento é uma estratégia diferenciada para alcance do sucesso e a durabilidade das organizações diante das ameaças cibernéticas da atualidade.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, D. M. de. Segurança da Informação. [e-book] Flórida: Must University, 2022.

ARAÚJO, S. G. L.; BATISTA, R. R.; ARAÚJO, W. Práticas organizacionais em gestão do conhecimento que contribuem com a segurança da informação: estudo de caso na Universidade Federal da Paraíba. Perspectivas em Gestão & Conhecimento, 10, 38-53, 2020.

BARRETO, G. G.; ANTONIO, A. L. S.; LIMA, A. G. B. Governança em privacidade e proteção de dados: uma visão integrada aos negócios empresariais. Curitiba: Editorial Casa, 2022.

CARLOTO, S. Lei Geral da Proteção de Dados: Incluindo Modelos, Segurança da Informação e Fases de Implementação. LTr Editora, 2023.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Brasport, 2018.

LEME, R. S.; BLANK, M. Lei Geral de Proteção de Dados e segurança da informação na área da saúde. Cadernos Ibero-Americanos de Direito Sanitário, 9(3), 210-224, 2020.

MALETTA, G. V.; SILVA, A. L. D. Cibersegurança e Ciberdefesa: Uma nova abordagem da segurança nacional brasileira. Revista Brasileira de Inteligência Artificial e Direito-RBIAD, 1(1), 2021.

NEVES, D. L. F.; DE ALMEIDA LOPES, T. S.; PAVANI, G. C.; SALES, R. M. A segurança da informação de encontro às conformidades da LGPD. Revista Processando o Saber, 13, 186-198, 2021.

SANTOS, F. A. A lei geral de proteção de dados pessoais (LGPD) e a exposição de dados sensíveis nas relações de trabalho. Revista do Tribunal Regional do Trabalho da 10ª Região, 24(2), 145-151, 2020.

SCHUENCK, S. F. Políticas públicas de segurança da informação na prevenção e tratamento de incidentes cibernéticos na administração pública federal, 2024. Disponível em: <https://bdm.unb.br/handle/10483/31599> . Acesso em: 18 de junho de 2024.

SÊMOLA, M. Gestão de Segurança da Informação: uma visão executiva. 2.ed. Rio de Janeiro: Editora Elsevier Brasil, 2014.

[1] Graduada em Sistemas de Informação - UniRitter. Especialista em Tecnologias Aplicadas à Educação – Faculdade Descomplica. Especialista em Educação a Distância – SENAC RS. Mestra em Administração pela Must University. E-mail: laubarcelos@gmail.com .

REVISTA TÓPICOS – ISSN: 2965-6672