Revista Matiz Online
ISSN 21794022

SEGURANÇA DA INFORMAÇÃO NA ERA DIGITAL: ANÁLISE DA PERCEPÇÃO E PRÁTICAS NO CONTEXTO BRASILEIRO

BERNARDO, P. R. A.[1], VERGA, M. D.[2], GRAZIOSI, S. E.[3]

1 Docente em Administração e Sistemas de Informação no Instituto Matonense Municipal de Ensino Superior (IMMES). 2 Docente em Administração e Sistemas de Informação no Instituto Matonense Municipal de Ensino Superior (IMMES) 3 Docente em Sistemas de Informação no Instituto Matonense Municipal de Ensino Superior (IMMES).

RESUMO: Este artigo investiga a segurança da informação no contexto brasileiro, com foco nos comportamentos de internautas e práticas organizacionais. Utiliza como base dados da pesquisa TIC Domicílios e Usuários 2010, bem como estudos acadêmicos sobre políticas de segurança e vulnerabilidades digitais. A metodologia é qualitativa, de natureza exploratória e bibliográfica. Os resultados indicam que o aumento no acesso à internet é acompanhado por riscos crescentes, exacerbados pela falta de capacitação técnica e políticas de segurança ineficazes, especialmente em pequenas empresas. Constatou-se que, apesar da crescente consciência sobre ameaças como phishing e invasões, muitas organizações ainda carecem de medidas estruturadas para proteção da informação. Conclui-se que a segurança da informação deve ser tratada como um ativo estratégico, exigindo políticas claras, treinamentos constantes e investimento contínuo em infraestrutura. O estudo contribui para a conscientização sobre a relevância da gestão da informação segura como diferencial competitivo na economia digital.

Palavras-chave: Segurança da Informação, Política de Segurança, TIC, Cibersegurança, Internet no Brasil

Abastract: *This article investigates information security in the Brazilian context, focusing on Internet user behavior and organizational practices. It uses data from the 2010 ICT Households and Users survey as a basis, as well as academic studies on security policies and digital vulnerabilities. The methodology is qualitative, exploratory and bibliographic in nature. The results indicate that increased Internet access is accompanied by increasing risks, exacerbated by the lack of technical training and ineffective security policies, especially in small companies. It*

was found that, despite the growing awareness of threats such as phishing and hacking, many organizations still lack structured measures to protect information. It is concluded that information security should be treated as a strategic asset, requiring clear policies, constant training and continuous investment in infrastructure. The study contributes to raising awareness of the importance of secure information management as a competitive advantage in the digital economy.

KEYWORDS: *Information Security, Security Policy, ICT, Cybersecurity, Internet in Brazil*

1. INTRODUÇÃO

A sociedade contemporânea é marcada pela intensa circulação de informações, mediada por tecnologias digitais cada vez mais presentes na vida pessoal e profissional. Com a popularização da internet e a consolidação da sociedade da informação (Machlup, 1962), tornou-se evidente o papel estratégico da informação como ativo fundamental. No Brasil, a expansão do acesso domiciliar à internet reflete um avanço significativo, porém, traz consigo novos desafios relacionados à segurança e proteção da informação (CGI/CETIC, 2010).

A literatura especializada aponta que, apesar dos avanços tecnológicos, muitas organizações ainda não possuem políticas eficazes de segurança da informação. Para Santos e Sott (s.d.), a ausência de cultura organizacional voltada à proteção de dados expõe as empresas a riscos operacionais e reputacionais. Por outro lado, Carvalho (2009) argumenta que a adoção de normas como a ISO/IEC 27001 pode transformar a segurança da informação em vantagem competitiva. Esse embate revela a complexidade do tema, que exige diálogo entre a técnica e a gestão.

análise do comportamento dos internautas brasileiros demonstra que fatores como desconhecimento, desconfiança nos serviços online e ausência de capacitação agravam a vulnerabilidade digital. Cunha e Fenato (s.d.) destacam que, sem uma abordagem preventiva e estratégica, a informação perde valor, tornando-se passivo em vez de ativo. No entanto, estudos como o de Coutinho et al. (2017) revelam que empresas que investem em políticas claras e treinamento conseguem mitigar riscos e aumentar sua resiliência.

Neste contexto, o presente estudo tem como objetivo geral analisar a percepção e as práticas de segurança da informação no Brasil, com base em dados de usuários e organizações. Os objetivos específicos incluem: identificar as principais ameaças percebidas por internautas; avaliar o nível de preparação das empresas; e discutir as implicações das práticas de segurança para a competitividade organizacional. Com isso, busca-se contribuir para o debate sobre o papel estratégico da informação na era digital.

2. OBJETIVOS

O objetivo geral deste estudo é analisar a percepção e as práticas de segurança da informação entre usuários e organizações brasileiras, à luz dos desafios impostos pela crescente digitalização da sociedade. A escolha do tema justifica-se pela crescente dependência de sistemas digitais para a condução de atividades críticas em empresas e na vida cotidiana, o que aumenta exponencialmente os riscos de incidentes de segurança (Cunha & Fenato, s.d.; Carvalho, 2009).

Os objetivos específicos são:

Investigar o comportamento de internautas brasileiros frente às ameaças cibernéticas, com ênfase em práticas de autoproteção e capacitação (CGI/CETIC, 2010; Radar n.15).

Avaliar o grau de implementação de políticas de segurança da informação em organizações de diferentes portes (Coutinho et al., 2017; Santos & Sott, s.d.).

Analisar a relação entre práticas de segurança da informação e a competitividade organizacional, destacando a adoção de normas como a ISO/IEC 27001 (Carvalho, 2009; Dantas, 2011).

3. REVISÃO DA LITERATURA

A segurança da informação (SI) tem se consolidado como um tema central nas organizações modernas, refletindo a necessidade de proteger dados sensíveis em um cenário cada vez mais digital. Segundo Ronan et al. (s.d.), SI refere-se à proteção das informações contra acessos não autorizados, alterações indevidas e indisponibilidades, com base nos pilares da confidencialidade, integridade e disponibilidade. De modo similar, a norma ISO/IEC 27001 estabelece padrões internacionais para garantir a confiabilidade e a continuidade das operações organizacionais (Carvalho, 2009).

Entretanto, a literatura indica lacunas na implementação prática dessas diretrizes, especialmente em empresas de pequeno e médio porte. Estudo de caso conduzido por Coutinho et al. (2017) revelou que, embora muitas organizações reconheçam a importância da informação, poucas adotam políticas estruturadas de proteção. Por outro lado, Cunha e Fenato (s.d.) reforçam que uma auditoria eficaz depende diretamente da existência de mecanismos de segurança que assegurem a qualidade e confiabilidade das informações auditadas.

Além das questões técnicas, autores como Santos & Sott (s.d.) enfatizam a relevância da cultura organizacional para o sucesso das políticas de segurança. A falta de conscientização e o despreparo de gestores e funcionários podem comprometer qualquer iniciativa técnica. Carvalho (2009), por sua vez, sugere que a participação ativa dos administradores na elaboração e disseminação da Política de Segurança da Informação (PSI) é decisiva para sua efetividade.

Do ponto de vista do comportamento dos usuários, o relatório do CGI/CETIC (2010) aponta que grande parte dos internautas brasileiros ainda hesita em realizar transações financeiras online, por receio de fraudes ou vazamento de dados. O estudo do Ipea (Radar n.15) complementa essa visão ao mostrar que muitos usuários preferem buscar capacitação informal, o que pode resultar em práticas de segurança inconsistentes e pouco eficazes.

Por fim, autores como Dantas (2011) e Beal (2005) argumentam que a segurança da informação deve ser compreendida de forma holística, integrando elementos físicos, lógicos e comportamentais. A SI não deve ser tratada apenas como uma questão técnica, mas como um processo contínuo e estratégico, capaz de agregar valor e garantir a sustentabilidade das organizações em um ambiente competitivo e digitalmente vulnerável.

4. METODOLOGIA

Este estudo adota uma abordagem qualitativa, de caráter exploratório e natureza bibliográfica, conforme defendido por Gil (2008), para a compreensão aprofundada das práticas e percepções sobre segurança da informação no contexto brasileiro. A escolha dessa abordagem justifica-se pela necessidade de examinar um fenômeno complexo e multifacetado, cuja análise exige sensibilidade contextual e interpretação crítica (Minayo, 2012).

Os dados utilizados foram coletados em fontes secundárias, incluindo relatórios oficiais, como a pesquisa TIC Domicílios e Usuários 2010 (CGI/CETIC), e literatura acadêmica composta por artigos científicos, estudos de caso e monografias (Radar n.15; Carvalho, 2009; Ronan et al., s.d.). Esta triangulação de fontes visa garantir maior confiabilidade às análises, conforme sugerido por Denzin (2006).

A análise dos dados foi realizada por meio de leitura crítica e categorização temática dos conteúdos encontrados nas fontes. As categorias analíticas foram definidas com base nos pilares da segurança da informação — confidencialidade, integridade e disponibilidade —, bem como em conceitos como política de segurança e cultura organizacional (Carvalho, 2009; Dantas, 2011). Essa estrutura permitiu comparar práticas e percepções em diferentes contextos organizacionais.

Optou-se por não realizar entrevistas ou levantamentos primários, dado que o objetivo era revisar e integrar o conhecimento já produzido sobre o tema. Essa decisão segue a recomendação de Severino (2007), que destaca o valor dos estudos bibliográficos na formulação de diagnósticos e construção de referenciais teóricos.

Por fim, o estudo considerou diretrizes metodológicas da norma ISO/IEC 27001 como parâmetro para análise das práticas de segurança encontradas nas organizações estudadas. O uso dessa norma como referência permite aferir a aderência das ações organizacionais aos padrões internacionais e identificar oportunidades de melhoria (Coutinho et al., 2017; Carvalho, 2009).

5. RESULTADOS

A análise dos dados da pesquisa TIC Domicílios e Usuários 2010 revelou um crescimento constante no número de domicílios brasileiros com acesso à internet, passando de 13% em 2005 para 38% em 2010 (CGI/CETIC, 2010). Esse crescimento indica uma maior inserção da população no ambiente digital, porém, traz consigo o aumento proporcional dos riscos cibernéticos, especialmente entre usuários inexperientes.

Os dados também indicaram que, apesar da popularidade da internet para fins de lazer e comunicação, apenas uma parcela reduzida dos internautas realiza atividades financeiras online. O relatório identificou que 29% dos entrevistados evitam compras pela internet devido a preocupações com a privacidade e segurança dos dados (Radar n.15). Além disso, somente 11% dos usuários relataram problemas nas compras online, como fraudes ou atrasos.

Em relação às empresas, o estudo de Coutinho et al. (2017) apontou que muitas organizações de pequeno porte não implementam políticas formais de segurança da informação.

Dentre as principais falhas observadas, destacam-se a ausência de controle de acesso físico e lógico, a falta de capacitação dos funcionários e a inexistência de planos de contingência.

A pesquisa de Carvalho (2009) complementa essa visão ao demonstrar que, mesmo em organizações que adotam a norma ISO/IEC 27001, muitas vezes o envolvimento da alta gestão é limitado. Isso compromete a efetividade das políticas implementadas, tornando o processo de segurança mais técnico do que estratégico.

Por fim, dados extraídos do relatório da Symantec (2010), citado no Radar n.15, indicaram que o Brasil ocupava, à época, a terceira colocação mundial em atividades maliciosas. Este dado reforça a percepção de que a infraestrutura de segurança da informação no país ainda carece de maturidade, tanto do ponto de vista organizacional quanto da conscientização do usuário.

6. DISCUSSÃO

Os dados evidenciam que o crescimento do acesso à internet no Brasil tem ocorrido de forma acelerada, porém sem o devido acompanhamento por parte de políticas educacionais voltadas à segurança da informação. Conforme alerta Santos & Sott (s.d.), o despreparo técnico de gestores e usuários compromete a eficácia das práticas de segurança e eleva a exposição a riscos. Esta constatação é reforçada pelos dados do Radar n.15, que mostram como grande parte da população não utiliza serviços bancários online por receio de fraudes.

Além da questão comportamental, observa-se um descompasso entre o avanço tecnológico e a maturidade organizacional para lidar com ameaças digitais. Enquanto Carvalho (2009) destaca a importância de alinhar as políticas de segurança à estratégia da empresa, estudos como o de Coutinho et al. (2017) mostram que muitas empresas, especialmente as de pequeno porte, sequer implementam normas básicas de controle. Isso indica um cenário em que a segurança é tratada de forma reativa e fragmentada.

Outro aspecto relevante é a centralidade da cultura organizacional. Conforme argumenta Cunha e Fenato (s.d.), a ausência de uma cultura voltada à segurança dificulta a internalização de práticas preventivas e a colaboração entre setores. Mesmo organizações que adotam normas como a ISO/IEC 27001 podem fracassar se não houver engajamento dos líderes e clareza na comunicação dos valores da segurança (Dantas, 2011).

A preocupação dos usuários com a privacidade e a ausência de confiança nos sistemas digitais refletem não apenas uma percepção individual, mas um problema sistêmico. O dado de que o Brasil figurava entre os países com maior incidência de atividades maliciosas (Symantec,

2010) sugere que o ambiente digital brasileiro requer investimentos estruturais e ações coordenadas entre setor público e privado.

Finalmente, a análise dos documentos reforça a ideia de que a segurança da informação deve ser compreendida como um processo estratégico, e não apenas técnico. A visão de Beal (2005), ao considerar a segurança como elemento essencial para a continuidade dos negócios, amplia a compreensão sobre sua relevância. Proteger dados não é apenas evitar perdas — é sustentar a confiança e a competitividade em um mercado digitalizado.

7. CONCLUSÃO

Este estudo evidenciou que a segurança da informação continua sendo um desafio relevante para o contexto brasileiro, tanto no nível individual quanto organizacional. Apesar do avanço na conectividade, observado entre 2005 e 2010, a preparação dos usuários e das empresas para enfrentar ameaças digitais ainda é incipiente. Os dados analisados revelam lacunas significativas em termos de capacitação, políticas formais de segurança e infraestrutura de proteção.

Ficou claro que muitos usuários evitam transações digitais por receio de fraudes, e que organizações, principalmente de pequeno porte, negligenciam práticas fundamentais como controle de acesso e gestão de riscos. Esse cenário reforça a necessidade de maior conscientização e integração entre tecnologia, cultura e gestão estratégica da informação (Santos & Sott, s.d.; Coutinho et al., 2017).

Contudo, este estudo apresenta limitações. Por basear-se apenas em dados secundários, não foi possível captar percepções atualizadas ou aplicar metodologias empíricas. Além disso, o foco nos documentos disponíveis restringiu a análise a determinado período e contexto, não abrangendo plenamente as mudanças recentes na legislação ou nas práticas organizacionais pós-LGPD.

Para futuras pesquisas, recomenda-se a realização de estudos de campo que envolvam entrevistas com gestores de TI e usuários de diferentes perfis, bem como avaliações comparativas entre setores econômicos. Investigações sobre o impacto da LGPD e a maturidade em segurança digital em empresas brasileiras também são caminhos promissores.

REFERÊNCIAS

BEAL, Adriana. *Segurança da informação: uma abordagem gerencial*. São Paulo: Atlas, 2005.

CARVALHO, Rodrigo de Oliveira. *Segurança da Informação nas Organizações*. Brasília: UniCEUB, 2009.

CGI.br; CETIC.br. *Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil – TIC Domicílios e Usuários 2010*. São Paulo: CGI.br, 2010.

COUTINHO, Mateus Micael et al. Estudo de caso: principais pilares da segurança da informação nas organizações. *Revista Gestão em Foco*, n. 9, 2017.

CUNHA, Dalvan; FENATO, Marcos Alexandre. A segurança da informação e a sua importância para a auditoria de sistemas. *Faculdade São Francisco de Barreiras*, s.d.

DANTAS, Eduardo. *Segurança da informação na prática: como proteger sua empresa da ameaça digital*. São Paulo: Novatec, 2011.

DENZIN, Norman K. *The research act: a theoretical introduction to sociological methods*. New Brunswick: Aldine Transaction, 2006.

GIL, Antonio Carlos. *Métodos e técnicas de pesquisa social*. 6. ed. São Paulo: Atlas, 2008.

MACHLUP, Fritz. *The Production and Distribution of Knowledge in the United States*. Princeton: Princeton University Press, 1962.

MINAYO, Maria Cecília de Souza. *O desafio do conhecimento: pesquisa qualitativa em saúde*. 14. ed. São Paulo: Hucitec, 2012.

RONAN, Leandro C. dos Santos; SOTT, Mário Rubens W. Aspectos da segurança da informação: sua importância para as organizações. UNIPAC, s.d.

SANTOS, Ronan Leandro Coelho dos; SOTT, Mário Rubens W. Aspectos da Segurança da Informação. Universidade UNIPAC, s.d.

SYMANTEC. *Internet Security Threat Report 2010*. Mountain View: Symantec Corp., 2010.