Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i8.29284

PROCESSOS DE SEGURANÇA DA INFORMAÇÃO E SUA RELEVÂNCIA PARA A GESTÃO EMPRESARIAL

Helder Silva de Paiva[1]
Anna Anita Almeida e Sousa[2]
Claudineide Leite da Silva[3]
Geane de Luna Souto[4]
Maria do Socorro Fernandes de Macedo[5]
Vanessa Alessandra Lucena Ferreira de Castro[6]
Rosa Sylvana da Silva Mousinho[7]
Maria Dalvanir Fausto de Lima[8]

RESUMO: O avanço das tecnologias digitais e a crescente dependência das organizações em relação aos ativos informacionais tornaram a segurança da informação um elemento estratégico para a continuidade dos negócios, a gestão de riscos e a competitividade empresarial. Nesse contexto, este estudo tem como objetivo analisar a relevância dos processos de segurança da informação para a gestão empresarial, destacando a contribuição dos mecanismos de proteção de dados, da prevenção de ameaças cibernéticas e da gestão de vulnerabilidades para o alcance dos objetivos organizacionais. A pesquisa caracteriza-se como bibliográfica, de abordagem qualitativa e de caráter exploratório e descritivo, desenvolvida por meio da análise de livros, artigos científicos, documentos institucionais e legislações especializadas, selecionados nas bases Google Scholar (Google Acadêmico) e SciELO, utilizando descritores relacionados à segurança da informação, proteção de dados, gestão empresarial, governança de TI e Lei Geral de Proteção de Dados (LGPD), combinados conforme os objetivos da pesquisa, além de obras clássicas da área e estudos contemporâneos publicados predominantemente entre 2006 e 2026. A literatura analisada evidencia que a adoção de políticas de segurança da informação, associada ao cumprimento das diretrizes da Lei Geral de Proteção de Dados (LGPD) e à capacitação contínua dos colaboradores, contribui para reduzir riscos cibernéticos, proteger ativos informacionais e fortalecer a governança organizacional. Os resultados demonstram que práticas eficazes de segurança da informação favorecem a continuidade das operações, o cumprimento das exigências legais, a confiabilidade dos processos, a proteção da reputação institucional e o fortalecimento da competitividade empresarial. Conclui-se que a segurança da informação deve ser compreendida como um componente estratégico da gestão organizacional, indispensável para a sustentabilidade, a inovação e a geração de valor em um ambiente caracterizado pela transformação digital e pelo crescimento das ameaças cibernéticas.

Palavras-chave: Segurança da informação. Gestão empresarial. Proteção de dados. Governança de TI. Cibersegurança.

[1]Mestrando em Administração pela MUST University.
[2]Mestre em Administração Pública pela Universidade Federal de Campina Grande.
[3]Mestre em Administração pela MUST University.
[4]Mestre em Ciência da Informação pela UFPB.
[5]Mestre em Administração de Empresas pela Must University.
[6]Mestre em Mestrado Profissional em Organizações Aprendentes (MPGOA)/UFPB.
[7]Mestre em Mestrado Profissional em Organizações Aprendentes (MPGOA)/UFPB.
[8]Especialização em Biblioteconomia - Faculdades Integradas de Jacarepaguá.

ABSTRACT: The advancement of digital technologies and the growing dependence of organizations on information assets have made information security a strategic element for business continuity, risk management, and organizational competitiveness. In this context, this study aims to analyze the relevance of information security processes for business management, highlighting the contribution of data protection mechanisms, prevention of cyber threats, and vulnerability management to the achievement of organizational objectives. This research is characterized as a bibliographic study with a qualitative, exploratory, and descriptive approach, developed through the analysis of books, scientific articles, institutional documents, and specialized legislation selected from the Google Scholar and SciELO databases, using descriptors related to information security, data protection, business management, IT governance, and the Brazilian General Data Protection Law (LGPD), combined according to the research objectives, in addition to classical works in the field and contemporary studies published predominantly between 2006 and 2026. The analyzed literature demonstrates that the adoption of information security policies, combined with compliance with the guidelines established by the General Data Protection Law (LGPD) and continuous employee training, contributes to reducing cyber risks, protecting information assets, and strengthening organizational governance. The results show that effective information security practices support business continuity, compliance with legal requirements, process reliability, institutional reputation protection, and the strengthening of organizational competitiveness. It is concluded that information security should be understood as a strategic component of organizational management, essential for sustainability, innovation, and value creation in an environment characterized by digital transformation and the increasing growth of cyber threats.

Keywords: Information Security. Business Management. Data Protection. IT Governance. Cybersecurity.

1 INTRODUÇÃO

O cenário organizacional contemporâneo encontra-se inserido em um processo contínuo de transformação digital, impulsionado pelo avanço acelerado das tecnologias da informação, pela expansão dos sistemas informatizados e pela crescente utilização de recursos digitais nos processos empresariais. A incorporação dessas tecnologias modificou significativamente a forma como as organizações produzem, armazenam, processam e compartilham informações, tornando os ativos informacionais elementos essenciais para a tomada de decisões, a continuidade dos negócios e a obtenção de vantagem competitiva. Nesse sentido, a informação deixa de representar apenas um recurso operacional e passa a constituir um ativo estratégico indispensável ao desenvolvimento organizacional. Conforme destacam Laudon e Laudon (2022), as informações assumem papel fundamental na gestão das organizações, apoiando o planejamento, o controle dos processos e a tomada de decisões em ambientes cada vez mais dinâmicos e competitivos.

O avanço das tecnologias digitais proporcionou importantes benefícios às organizações, como o aumento da eficiência operacional, a integração entre setores, a automatização de processos, a ampliação da capacidade de armazenamento de dados e o aprimoramento da

comunicação com clientes, fornecedores e demais públicos de interesse. Além disso, recursos como computação em nuvem, sistemas integrados de gestão, inteligência artificial, análise de dados e Internet das Coisas (IoT) vêm transformando a maneira como as empresas desenvolvem suas atividades e estruturam seus modelos de negócio. Entretanto, a crescente dependência desses recursos tecnológicos também ampliou a exposição das organizações a riscos relacionados à segurança da informação, tornando indispensável a adoção de mecanismos capazes de proteger seus ativos informacionais.

Nesse cenário, observa-se um crescimento significativo das ameaças cibernéticas, incluindo ataques de ransomware, vazamentos de dados, fraudes eletrônicas, acessos não autorizados e outras vulnerabilidades capazes de comprometer a confidencialidade, a integridade e a disponibilidade das informações. Segundo Stallings e Brown (2015), a segurança da informação constitui um conjunto de práticas, políticas e mecanismos destinados à proteção dos sistemas e das informações contra ameaças internas e externas, assegurando a continuidade das operações e reduzindo os riscos associados ao ambiente digital. De forma complementar, Sêmola (2014) destaca que a segurança da informação deve ser compreendida como um processo contínuo de gestão, fundamentado na integração entre tecnologia, pessoas e processos, e não apenas como um conjunto de soluções tecnológicas.

A crescente complexidade dos ambientes digitais também evidencia a necessidade de fortalecer a governança da informação e a gestão de riscos organizacionais. Além da implementação de controles tecnológicos, torna-se fundamental estabelecer políticas institucionais, promover programas permanentes de capacitação dos colaboradores e desenvolver estratégias voltadas à prevenção, identificação e tratamento de vulnerabilidades. Dessa maneira, a adequação às diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018 – representa um importante instrumento para assegurar a conformidade legal, fortalecer a proteção das informações e ampliar a confiança de clientes, parceiros e demais partes interessadas.

Diante dessa realidade, este estudo tem como objetivo geral analisar a relevância dos processos de segurança da informação para a gestão empresarial, considerando a contribuição dos mecanismos de proteção de dados, da prevenção de ameaças cibernéticas, da gestão de vulnerabilidades e da conformidade com a LGPD para o fortalecimento da governança organizacional e para o alcance dos objetivos estratégicos das organizações. Busca-se compreender de que maneira a adoção de práticas eficazes de segurança da informação contribui

para reduzir riscos, proteger ativos informacionais, assegurar a continuidade das operações e fortalecer a competitividade empresarial.

Para alcançar esse objetivo, foi realizada uma pesquisa bibliográfica, abordagem qualitativa e objetivos exploratórios e descritivos, fundamentada na análise de livros, artigos científicos, documentos institucionais, normas técnicas e legislações relacionadas à segurança da informação, à gestão de riscos, à governança de tecnologia da informação e à proteção de dados. A busca bibliográfica foi realizada nas bases Google Scholar, SciELO, considerando publicações em português e inglês, priorizando estudos publicados entre 2006 e 2026, sem desconsiderar obras clássicas indispensáveis à fundamentação teórica. Foram utilizados descritores como "segurança da informação", "gestão de riscos", "governança de TI", "proteção de dados", "LGPD", "cybersecurity" e "information security", combinados por operadores booleanos. Os critérios de inclusão contemplaram estudos diretamente relacionados ao tema, enquanto foram excluídos trabalhos duplicados, publicações sem rigor científico e estudos que não apresentavam relação com os objetivos da pesquisa. A análise do material selecionado ocorreu por meio de leitura exploratória, seletiva, analítica e interpretativa. Posteriormente, os conteúdos foram organizados em categorias temáticas relacionadas à proteção de dados, prevenção de incidentes cibernéticos, gestão de vulnerabilidades e contribuição estratégica da segurança da informação para a gestão empresarial. O estudo está estruturado em quatro seções principais. Após esta introdução, a segunda seção apresenta os fundamentos da segurança da informação, abordando os protocolos de proteção de dados, as práticas de prevenção contra incidentes cibernéticos e os métodos utilizados para redução de vulnerabilidades em sistemas de segurança. A terceira seção discute a influência da proteção da informação para a concretização das metas organizacionais, evidenciando sua contribuição para a continuidade dos negócios, a conformidade legal, a governança organizacional, a proteção dos ativos informacionais e a competitividade empresarial. Por fim, a quarta seção apresenta as considerações finais, reunindo as principais reflexões desenvolvidas ao longo do estudo.

Dessa forma, o presente trabalho busca contribuir para o aprofundamento das discussões acerca da segurança da informação como elemento estratégico da gestão empresarial, evidenciando que a proteção dos ativos informacionais ultrapassa os aspectos exclusivamente tecnológicos e envolve fatores relacionados à governança, à gestão de riscos, à conformidade legal e ao desenvolvimento de uma cultura organizacional voltada para a proteção da informação. Em um cenário marcado pela transformação digital e pelo crescimento contínuo

das ameaças cibernéticas, compreender esses aspectos torna-se fundamental para que as organizações fortaleçam sua capacidade de inovação, assegurem a continuidade de suas operações e mantenham sua competitividade em um ambiente empresarial cada vez mais dinâmico e digital.

2 Fundamentos da Segurança da Informação: Proteção de Dados, Defesa contra Ameaças Cibernéticas e Gestão de Vulnerabilidades

Com o avanço da transformação digital e a crescente integração entre sistemas, a proteção das informações passou a ocupar um papel central nas organizações, independentemente de seu tamanho ou área de atuação. Nesse cenário, os dados deixaram de ser considerados apenas elementos operacionais e passaram a representar ativos estratégicos capazes de influenciar diretamente a tomada de decisões, a continuidade dos negócios e a competitividade empresarial.

Segundo Rapôso (2025), a segurança da informação no ambiente empresarial deve ser compreendida como um componente estratégico da gestão organizacional, uma vez que seus processos e políticas contribuem para a continuidade operacional, a conformidade regulatória, a preservação da reputação institucional e o alcance dos objetivos corporativos. Dessa forma, a segurança deixa de ser exclusivamente uma responsabilidade técnica da área de tecnologia e passa a integrar as práticas de governança e planejamento estratégico das organizações.

Por conseguinte, torna-se fundamental compreender os princípios relacionados aos protocolos de proteção de dados, às formas de prevenção contra ataques virtuais e às estratégias utilizadas para reduzir impactos causados por falhas de segurança. A segurança da informação está fundamentada na preservação de três princípios essenciais: confidencialidade, integridade e disponibilidade. A confidencialidade garante que as informações sejam acessadas apenas por usuários autorizados; a integridade assegura que os dados permaneçam corretos e protegidos contra alterações indevidas; enquanto a disponibilidade permite que os recursos informacionais estejam acessíveis quando necessários para a continuidade das atividades organizacionais (STALLINGS; BROWN, 2015).

Nesse contexto, as organizações precisam desenvolver mecanismos capazes de proteger seus ativos informacionais contra ameaças internas e externas. Para Sêmola (2014), a segurança da informação deve ser tratada como um processo contínuo de gestão, envolvendo tecnologia, pessoas e processos, pois a simples adoção de ferramentas tecnológicas não é suficiente para

garantir níveis adequados de proteção. É necessário estabelecer políticas institucionais, controles de acesso, procedimentos de monitoramento e uma cultura organizacional voltada à segurança.

A adoção de protocolos de segurança, mecanismos de prevenção contra invasões e práticas de gestão de vulnerabilidades constitui uma estratégia essencial para reduzir riscos e preservar a integridade, a confidencialidade e a disponibilidade das informações corporativas. Essas práticas permitem que as organizações desenvolvam maior capacidade de prevenção, identificação e resposta diante de incidentes de segurança, reduzindo impactos financeiros, operacionais e reputacionais.

Nesse sentido, a implementação de Sistemas de Gestão da Segurança da Informação (SGSI), conforme estabelecido pela ABNT NBR ISO/IEC 27001:2022 (ABNT, 2022), permite que as organizações adotem uma abordagem estruturada para identificar riscos, implementar controles de proteção e promover melhorias contínuas nos processos de segurança. A adoção dessas práticas contribui para reduzir vulnerabilidades, fortalecer a governança da informação e aumentar a capacidade organizacional de resposta diante de incidentes cibernéticos.

A gestão de vulnerabilidades representa uma etapa fundamental da segurança da informação, pois possibilita identificar fragilidades existentes em sistemas, aplicações, redes e processos organizacionais antes que sejam exploradas por agentes mal-intencionados. A realização periódica de avaliações de segurança, aplicação de atualizações, análise de riscos, testes de vulnerabilidade e monitoramento contínuo contribuem para reduzir a superfície de ataque e fortalecer a resiliência das organizações diante das ameaças digitais.

Além dos controles tecnológicos, destaca-se a importância do fator humano na proteção das informações. A capacitação dos colaboradores, a conscientização sobre ameaças digitais e o desenvolvimento de uma cultura organizacional de segurança são aspectos fundamentais para reduzir riscos relacionados a comportamentos inadequados, como compartilhamento indevido de informações, utilização de senhas frágeis e exposição a ataques de engenharia social.

Portanto, a segurança da informação deve ser compreendida como uma estratégia organizacional ampla, que integra aspectos tecnológicos, humanos e administrativos. Em um ambiente empresarial cada vez mais dependente de recursos digitais, proteger informações significa preservar a continuidade das operações, fortalecer a confiança dos stakeholders e garantir condições favoráveis para o crescimento sustentável das organizações.

2.1 Protocolos de Segurança no Gerenciamento de Dados

No cenário atual de transformação digital, a informação tornou-se um ativo estratégico para as organizações, sendo essencial para a tomada de decisões, continuidade operacional e competitividade empresarial. Entretanto, o aumento do uso de sistemas informatizados, redes conectadas e ambientes digitais também ampliou os riscos relacionados ao acesso indevido, perda, alteração ou indisponibilidade dos dados. Dessa forma, os protocolos de segurança assumem papel fundamental na proteção dos ativos informacionais, garantindo os princípios da confidencialidade, integridade e disponibilidade.

Segundo Rapôso (2025), a segurança da informação deve ser compreendida como um componente estratégico da gestão organizacional, pois contribui para a continuidade dos negócios, conformidade regulatória, preservação da reputação institucional e alcance dos objetivos corporativos. Nesse sentido, a proteção dos dados deixa de ser uma responsabilidade exclusiva da área de tecnologia e passa a integrar as práticas de governança e gerenciamento de riscos.

De acordo com Schneier (2015), a segurança dos dados deve envolver não apenas ferramentas tecnológicas, mas também processos estruturados capazes de reduzir vulnerabilidades e fortalecer a confiabilidade dos sistemas. Entre os principais mecanismos utilizados destacam-se a criptografia, os protocolos de comunicação segura, como HTTPS e TLS, e os controles de autenticação e acesso, que permitem restringir o uso das informações apenas a usuários autorizados.

A adoção desses mecanismos deve ocorrer de forma integrada às políticas organizacionais e aos controles de segurança. Para Whitman e Mattord (2022), a proteção da informação depende da combinação entre medidas técnicas, administrativas e físicas, considerando que a segurança não está relacionada somente à tecnologia, mas também aos processos e ao comportamento dos usuários.

Nesse sentido, a implementação de Sistemas de Gestão da Segurança da Informação (SGSI), conforme estabelecido pela ABNT NBR ISO/IEC 27001:2022 (ABNT, 2022), possibilita às organizações identificar riscos, estabelecer controles e promover melhorias contínuas nos processos de proteção da informação. Além dos aspectos tecnológicos, a segurança empresarial exige uma abordagem integrada entre diferentes setores. Conforme Hass (2026), a proteção dos ativos informacionais envolve políticas internas, monitoramento,

capacitação dos colaboradores e desenvolvimento de uma cultura organizacional voltada à prevenção de riscos digitais.

Portanto, os protocolos de segurança no gerenciamento de dados representam elementos essenciais para a proteção das informações corporativas. A integração entre tecnologias, normas, processos e pessoas permite reduzir vulnerabilidades, fortalecer a governança da informação e ampliar a capacidade das organizações de enfrentar ameaças cibernéticas.

2.2 Práticas de Proteção contra Incidentes Cibernéticos

A crescente dependência dos recursos digitais tornou os incidentes cibernéticos um dos principais desafios das organizações. Além disso, compreender as vulnerabilidades dos sistemas e adotar medidas preventivas torna-se essencial para reduzir riscos e proteger os ativos informacionais. A segurança da informação envolve aspectos tecnológicos, administrativos e humanos, considerando a integração entre ferramentas, processos e comportamento organizacional.

Segundo Rapôso (2025), a segurança da informação deve ser compreendida como um elemento estratégico da gestão empresarial, contribuindo para a continuidade operacional, redução de riscos, conformidade regulatória e preservação da confiança institucional. Dessa forma, a prevenção contra incidentes deixa de ser apenas uma atividade técnica e passa a integrar as práticas de governança organizacional.

Segundo Whitman e Mattord (2022), a avaliação contínua dos ambientes tecnológicos permite identificar vulnerabilidades, corrigir falhas e implementar controles capazes de ampliar a proteção dos sistemas corporativos. Entre as principais práticas preventivas destacam-se a atualização de sistemas, realização de backups, utilização de mecanismos de proteção, como antivírus e firewalls, além do monitoramento contínuo dos ambientes digitais.

Para Stallings e Brown (2015), a segurança da informação deve preservar os princípios da confidencialidade, integridade e disponibilidade dos dados, garantindo proteção contra ameaças internas e externas. Além dos controles tecnológicos, o fator humano também possui papel fundamental. Segundo Sêmola (2014), a segurança deve ser tratada como um processo contínuo de gestão, envolvendo tecnologia, pessoas e processos.

Nesse sentido, a capacitação dos colaboradores e o desenvolvimento de uma cultura organizacional de segurança são fundamentais para reduzir riscos relacionados a falhas humanas, engenharia social e uso inadequado das informações. Conforme Hass (2026), a

proteção dos dados exige uma abordagem multissetorial, envolvendo políticas internas, treinamentos e participação integrada dos diferentes setores da organização.

Portanto, as práticas de proteção contra incidentes cibernéticos devem combinar tecnologia, governança e conscientização dos usuários. Essa integração permite reduzir vulnerabilidades, fortalecer a gestão de riscos e ampliar a capacidade das organizações de prevenir, responder e recuperar-se diante de ameaças digitais.

2.3 Métodos para Redução de Vulnerabilidades em Sistemas de Segurança

Mesmo com a adoção de medidas preventivas, os ambientes digitais permanecem sujeitos a vulnerabilidades que podem comprometer a confidencialidade, integridade e disponibilidade das informações. Dessa forma, a gestão de vulnerabilidades torna-se uma prática essencial para identificar fragilidades, reduzir riscos e fortalecer a capacidade de proteção das organizações diante de ameaças cibernéticas.

Segundo Sêmola (2014), a segurança da informação deve ser conduzida como um processo contínuo de gestão de riscos, envolvendo a identificação de ameaças, análise de vulnerabilidades e implementação de controles capazes de reduzir impactos aos ativos informacionais. Sob essa perspectiva, empresas de diferentes portes precisam desenvolver estratégias adequadas de proteção, considerando que limitações de investimento, ausência de políticas estruturadas ou falhas de gerenciamento podem aumentar a exposição a incidentes.

Entre os principais métodos utilizados para redução de vulnerabilidades destacam-se a realização de avaliações periódicas de segurança, atualização de sistemas, aplicação de correções, gerenciamento de acessos, monitoramento de redes e execução de cópias de segurança. Para Whitman e Mattord (2022), a proteção dos ativos informacionais depende da aplicação integrada de controles técnicos, administrativos e físicos, permitindo reduzir falhas e ampliar a capacidade organizacional de prevenção e resposta diante de eventos de segurança.

Em situações de comprometimento dos sistemas, torna-se fundamental adotar procedimentos de resposta a incidentes, incluindo identificação da origem do problema, isolamento dos recursos afetados, correção das vulnerabilidades existentes, alteração de credenciais e recuperação das informações por meio de backups confiáveis. De acordo com Stallings e Brown (2015), a preparação e a capacidade de resposta são elementos essenciais da segurança da informação, pois possibilitam minimizar impactos operacionais, financeiros e reputacionais.

No caso de ameaças como ransomware, a implementação de estratégias preventivas e planos de recuperação torna-se ainda mais importante, considerando o potencial de interrupção das atividades organizacionais. A adoção de políticas de backup, controle de acesso, atualização constante dos mecanismos de proteção e monitoramento contínuo contribui para reduzir os impactos causados por ataques digitais.

Nesse sentido, a ABNT NBR ISO/IEC 27001:2022 (ABNT, 2022) estabelece uma abordagem estruturada para a gestão da segurança da informação, permitindo que as organizações identifiquem riscos, implementem controles adequados e promovam melhorias contínuas nos processos relacionados à proteção dos dados.

Portanto, a redução de vulnerabilidades em sistemas de segurança depende da integração entre tecnologia, processos e pessoas. A adoção de práticas estruturadas de gestão de riscos, aliada à conscientização dos usuários e ao acompanhamento permanente dos ambientes digitais, fortalece a resiliência organizacional e amplia a capacidade das empresas de enfrentar ameaças cibernéticas.

3 A Influência da proteção da informação para a concretização das metas organizacionais

A segurança da informação exerce papel estratégico na concretização dos objetivos organizacionais, pois possibilita a proteção dos ativos informacionais contra ameaças como vazamentos de dados, acessos indevidos e ataques cibernéticos. Em um ambiente empresarial cada vez mais dependente de tecnologias digitais, a preservação da confidencialidade, integridade e disponibilidade das informações torna-se essencial para apoiar decisões, garantir a continuidade dos negócios e fortalecer a competitividade. Segundo Laudon e Laudon (2022), os sistemas de informação representam recursos estratégicos para as organizações, contribuindo para o gerenciamento eficiente dos dados e dos processos empresariais.

A adoção de práticas estruturadas de segurança também favorece a continuidade operacional, reduzindo impactos decorrentes de falhas e incidentes digitais. De acordo com Gordon e Loeb (2006), investimentos em segurança da informação contribuem para minimizar perdas financeiras e operacionais, por meio de estratégias de prevenção, recuperação e gerenciamento de riscos.

Além disso, a proteção das informações está diretamente relacionada ao cumprimento das exigências legais e regulatórias. No Brasil, a Lei Geral de Proteção de Dados (LGPD),

instituída pela Lei nº 13.709/2018, estabelece princípios e responsabilidades para o tratamento adequado dos dados pessoais, reforçando a necessidade de controles de segurança e práticas de governança (BRASIL, 2018).

Conforme Whitman e Mattord (2022), a segurança da informação deve ser compreendida como uma abordagem integrada entre tecnologia, processos e pessoas, envolvendo controles técnicos, administrativos e físicos. Dessa forma, organizações que desenvolvem uma cultura de segurança fortalecem sua reputação e ampliam a confiança de clientes, parceiros e demais partes interessadas.

Sob uma perspectiva estratégica, a segurança da informação deve estar integrada à governança organizacional e à gestão de riscos. Segundo Van Solms e Van Solms (2019), a governança da segurança da informação, quando associada à liderança e ao planejamento estratégico, contribui para reduzir riscos e gerar valor organizacional.

Nesse contexto de transformação digital, a segurança também possibilita a adoção confiável de tecnologias emergentes, como inteligência artificial, computação em nuvem, big data e Internet das Coisas (IoT). Assim, a proteção dos ativos informacionais deixa de ser apenas uma medida defensiva e passa a representar um elemento estratégico para inovação, sustentabilidade e crescimento empresarial.

4 CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objetivo analisar a relevância dos processos de segurança da informação para a gestão empresarial, considerando sua contribuição para a proteção dos ativos informacionais, prevenção de ameaças cibernéticas, gestão de vulnerabilidades e fortalecimento da governança organizacional. A partir da revisão bibliográfica realizada, verificou-se que a segurança da informação deixou de ser uma atividade exclusivamente técnica e passou a representar um elemento estratégico para a continuidade dos negócios, a redução de riscos e a competitividade empresarial.

Os resultados evidenciaram que a proteção das informações depende da integração entre tecnologia, processos e pessoas. A implementação de protocolos de segurança, sistemas de gestão da informação, controles de acesso, políticas institucionais e práticas contínuas de monitoramento contribui para reduzir vulnerabilidades e ampliar a capacidade das organizações de prevenir, responder e recuperar-se diante de incidentes cibernéticos.

Além dos recursos tecnológicos, destacou-se a importância do fator humano e da conformidade legal como elementos essenciais para a segurança organizacional. A capacitação dos colaboradores, o desenvolvimento de uma cultura de proteção de dados e a adequação às diretrizes da Lei Geral de Proteção de Dados (LGPD) fortalecem a confiança de clientes e parceiros, preservam a reputação institucional e favorecem uma gestão mais eficiente e responsável das informações.

Dessa forma, conclui-se que a segurança da informação deve ser incorporada ao planejamento estratégico das organizações, integrando práticas de governança, gestão de riscos e inovação tecnológica. Em um cenário marcado pela transformação digital e pelo crescimento das ameaças cibernéticas, a capacidade de proteger e administrar os ativos informacionais torna-se fundamental para garantir a continuidade das operações, promover a sustentabilidade empresarial e manter a competitividade no mercado. Sugere-se que estudos futuros investiguem empiricamente a implementação de políticas de segurança da informação em organizações públicas e privadas, permitindo ampliar a compreensão dos impactos dessas práticas sobre o desempenho organizacional

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022: segurança da informação, segurança cibernética e proteção à privacidade — sistemas de gestão da segurança da informação — requisitos**. Rio de Janeiro: ABNT, 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 4 ago. 2026.

GORDON, Lawrence A.; LOEB, Martin P. *Managing cyber security resources: a cost-benefit analysis*. New York: McGraw-Hill, 2006.

HASS, Ana Paula Von Zuben. A segurança da informação empresarial: uma necessidade multissetorial. *Revista Tópicos*, 2026. Disponível em: https://revistatopicos.com.br/artigos/a-seguranca-da-informacao-empresarial-uma-necessidade-multissetorial. Acesso em: 4 ago. 2026.

LAUDON, Kenneth C.; LAUDON, Jane P. *Sistemas de informação gerenciais*. 17. ed. São Paulo: Pearson, 2022.

RAPÔSO, Cláudio Filipe Lima. Importância estratégica da segurança da informação no ambiente empresarial: impactos sobre os objetivos organizacionais. *Revista Tópicos*, 2025. Disponível em: https://revistatopicos.com.br/artigos/importancia-estrategica-da-seguranca-

da-informacao-no-ambiente-empresarial-impactos-sobre-os-objetivos-organizacionais. Acesso em: 4 ago. 2026.

SCHNEIER, Bruce. *Data and Goliath: the hidden battles to collect your data and control your world*. New York: W. W. Norton & Company, 2015.

SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva*. 2. ed. Rio de Janeiro: Elsevier, 2014.

STALLINGS, William; BROWN, Lawrie. *Segurança de computadores: princípios e práticas*. 3. ed. São Paulo: Pearson Education do Brasil, 2015.

VAN SOLMS, Rossouw; VAN SOLMS, Basie. Information security governance: a model based on the direct–indirect–vicarious effect of leadership. *Computers & Security*, v. 82, p. 180-193, 2019. DOI: https://doi.org/10.1016/j.cose.2018.10.013.

WHITMAN, Michael E.; MATTORD, Herbert J. *Principles of information security*. 7. ed. Boston: Cengage Learning, 2022.