MUST UNIVERSITY
MASTER OF SCIENCE IN BUSINESS ADMINISTRATION

MATHEUS ROCHA GARCEZ MACEDO

O impacto da cibersegurança na tomada de decisão estratégica em organizações brasileiras

Uma análise da relação entre gestão de riscos, governança e estratégia organizacional

FLORIDA – USA
Junho/2026

MATHEUS ROCHA GARCEZ MACEDO

O impacto da cibersegurança na tomada de decisão estratégica em organizações brasileiras

Uma análise da relação entre gestão de riscos, governança e estratégia organizacional

Trabalho de Conclusão Final apresentado como requisito parcial para obtenção do título de Mestre no Curso de Master of Science In Business Administration da MUST University – Florida USA.

Orientador (a): Prof. (a) Dr. (a) Luciane de Paula Soutello

FLORIDA – USA

Junho/2026

MUST UNIVERSITY
70 SW 10th St, Deerfield Beach, FL 33441, USA | info@mustedu.com | www.mustedu.com
MUST University®: licensed by Florida Commission for Independent Education. License: 5593.

Lista de Figuras

Lista de Quadros

Lista de Tabelas

Lista de Abreviaturas e Siglas

APA – *American Psychological Association*

CIA – Confidentiality, Integrity and Availability (Confidencialidade, Integridade e Disponibilidade)

IIA – Institute of Internal Auditors

ISO – International Organization for Standardization

ISO/IEC – International Organization for Standardization / International Electrotechnical Commission

LGPD – Lei Geral de Proteção de Dados

MIS – Management Information Systems

TI – Tecnologia da Informação

WEF – World Economic Forum

Resumo

O presente estudo analisa o impacto da cibersegurança na tomada de decisão estratégica em organizações brasileiras, no contexto da transformação digital. Diante do aumento dos riscos cibernéticos e da crescente dependência tecnológica, a pesquisa busca responder de que forma a cibersegurança influencia a tomada de decisão estratégica em organizações brasileiras. A relevância do estudo reside na necessidade de compreender a cibersegurança para além de uma abordagem exclusivamente técnica, reconhecendo-a como um fator estratégico capaz de influenciar o planejamento, a gestão de riscos e a competitividade organizacional. Do ponto de vista acadêmico, o trabalho contribui para ampliar as discussões sobre a integração entre segurança da informação e gestão estratégica, temática que ainda apresenta espaço para aprofundamento na literatura. Metodologicamente, trata-se de uma pesquisa qualitativa, de caráter exploratório e descritivo, fundamentada em revisão bibliográfica, com levantamento de dados em bases científicas e análise por meio de categorização temática. Como principais resultados, evidenciou-se que a cibersegurança exerce influência significativa na tomada de decisão estratégica, contribuindo para a mitigação de riscos, o fortalecimento da governança, a continuidade dos negócios e a sustentabilidade das organizações em ambientes digitais.

Palavras-chave: Cibersegurança; Tomada de decisão estratégica; Gestão de riscos; Segurança da informação; Transformação digital.

Abstract

This study analyzes the impact of cybersecurity on strategic decision-making in Brazilian organizations within the context of digital transformation. Given the increasing exposure to cyber risks and the growing dependence on digital technologies, the research seeks to understand how cybersecurity influences strategic decision-making in Brazilian organizations. The relevance of this study lies in addressing cybersecurity beyond a purely technical perspective, recognizing it as a strategic factor capable of influencing organizational planning, risk management, and competitiveness. From an academic standpoint, the study contributes to expanding discussions on the integration between information security and strategic management, a topic that still offers opportunities for further development in the literature. Methodologically, this is a qualitative, exploratory, and descriptive study based on a literature review, using scientific databases and thematic content analysis. The results showed that cybersecurity plays a significant role in strategic decision-making, contributing to risk mitigation, stronger governance practices, business continuity, and organizational sustainability in digital environments.

Keywords: Cybersecurity; Strategic decision-making; Risk management; Information security; Digital transformation.

Sumário

1. Introdução

A transformação digital tem modificado de forma significativa a dinâmica das organizações, ampliando o uso de tecnologias e, consequentemente, a exposição a riscos cibernéticos. Nesse contexto, a cibersegurança deixa de ser apenas um suporte técnico e passa a ocupar um espaço relevante nas decisões organizacionais, especialmente aquelas relacionadas à estratégia e à continuidade dos negócios.

Com o aumento de incidentes como ataques cibernéticos, vazamentos de dados e outras ameaças digitais, as organizações passaram a enfrentar novos desafios na proteção de suas informações e na manutenção de suas operações. De acordo com o World Economic Forum (2023), os riscos cibernéticos estão entre as principais ameaças globais para organizações e governos, exigindo maior atenção por parte dos gestores e tomadores de decisão. No Brasil, esse cenário ganha ainda mais relevância com a intensificação da digitalização e com a necessidade de adequação a normas como a Lei Geral de Proteção de Dados (LGPD), reforçando a importância da cibersegurança no ambiente organizacional.

Diante desse contexto, surge a necessidade de compreender de que forma a cibersegurança influencia a tomada de decisão estratégica em organizações brasileiras. Embora existam estudos relevantes sobre segurança da informação e gestão estratégica, ainda são limitadas as abordagens que analisam essas dimensões de forma integrada.

Essa lacuna torna-se particularmente relevante diante da crescente dependência tecnológica das organizações e da necessidade de incorporar a gestão dos riscos cibernéticos aos processos estratégicos. Nesse contexto, compreender a relação entre cibersegurança e tomada de decisão estratégica contribui para ampliar a compreensão dos desafios enfrentados pelas

organizações contemporâneas, especialmente em ambientes caracterizados pela rápida evolução tecnológica e pela crescente complexidade dos riscos digitais.

Diante desse cenário, estabelece-se como problema de pesquisa a seguinte questão: de que forma a cibersegurança influencia a tomada de decisão estratégica em organizações brasileiras, considerando sua relação com a gestão de riscos, a governança corporativa e a continuidade dos negócios? Embora a literatura reconheça a crescente importância da cibersegurança para as organizações, observa-se que parte significativa dos estudos aborda o tema sob uma perspectiva predominantemente técnica, havendo menor aprofundamento acerca de sua influência sobre os processos de gestão estratégica e tomada de decisão. Essa lacuna justifica o desenvolvimento da presente pesquisa, ao buscar integrar diferentes perspectivas teóricas da Administração Estratégica, da Governança e da Segurança da Informação.

Assim, este estudo tem como objetivo geral analisar de que forma a cibersegurança influencia a tomada de decisão estratégica em organizações brasileiras públicas e privadas inseridas em contextos de transformação digital. Como objetivos específicos, busca-se: (i) compreender os principais fundamentos teóricos da cibersegurança aplicados ao contexto organizacional; (ii) identificar os fatores que relacionam cibersegurança, gestão de riscos e governança corporativa; (iii) analisar as contribuições da literatura acerca da influência da cibersegurança sobre os processos de tomada de decisão estratégica; e (iv) discutir as implicações gerenciais decorrentes da incorporação da cibersegurança ao planejamento estratégico das organizações. Para isso, adota-se uma abordagem qualitativa, de caráter exploratório e descritivo, com base em revisão bibliográfica e análise interpretativa da literatura.

A delimitação da pesquisa concentra-se em organizações brasileiras que desenvolvem processos de transformação digital, tanto no setor público quanto no privado, considerando que a crescente dependência de tecnologias digitais amplia a exposição aos riscos cibernéticos e torna a cibersegurança um fator estratégico para a gestão, a governança e a tomada de decisão.

Este trabalho contribui para a ampliação das discussões sobre o papel da cibersegurança na gestão estratégica, além de oferecer reflexões que podem auxiliar organizações na condução de decisões mais seguras em um ambiente cada vez mais digital. Ao integrar conceitos relacionados à segurança da informação, gestão de riscos, governança e estratégia organizacional, busca-se evidenciar a importância da cibersegurança como elemento fundamental para a sustentabilidade, a resiliência e a competitividade das organizações na era digital.

2. Metodologia

A presente pesquisa caracteriza-se como qualitativa, de natureza exploratória e descritiva, fundamentada em revisão bibliográfica. De acordo com Gil (2019), a pesquisa bibliográfica permite analisar e interpretar contribuições teóricas já consolidadas sobre determinado tema, possibilitando a construção de um referencial teórico consistente. A abordagem qualitativa foi escolhida por possibilitar a compreensão aprofundada de fenômenos organizacionais complexos, especialmente aqueles relacionados à influência da cibersegurança nos processos de tomada de decisão estratégica.

O levantamento bibliográfico foi realizado em bases de dados científicas reconhecidas, como SciELO, Scopus, Web of Science e Portal de Periódicos CAPES, além de periódicos indexados nas áreas de gestão, tecnologia e segurança da informação, como MIS Quarterly e

MIS Quarterly Executive. Foram utilizados descritores como “cibersegurança”, “segurança da informação”, “gestão estratégica”, “tomada de decisão”, “governança”, “gestão de riscos” e “riscos cibernéticos”, tanto em português quanto em inglês.

A busca bibliográfica foi realizada de forma sistemática, contemplando inicialmente o levantamento de estudos potencialmente relevantes a partir dos descritores previamente definidos. Em seguida, procedeu-se à leitura dos títulos, resumos e palavras-chave das publicações recuperadas, sendo selecionados apenas os trabalhos que apresentavam aderência ao objetivo da pesquisa. Posteriormente, realizou-se a leitura integral dos estudos considerados mais relevantes, permitindo a identificação das principais abordagens teóricas, conceitos e evidências relacionadas à influência da cibersegurança sobre a gestão estratégica, a governança corporativa e a tomada de decisão organizacional.

Foram considerados estudos publicados preferencialmente nos últimos dez anos, com o objetivo de garantir atualidade e relevância acadêmica. Os critérios de inclusão compreenderam publicações diretamente relacionadas ao tema proposto, com consistência teórica, rigor metodológico e aderência aos objetivos da pesquisa. Foram excluídos trabalhos que não apresentavam relação direta com a temática investigada, publicações duplicadas e estudos sem fundamentação científica adequada. Além disso, foram utilizados autores clássicos das áreas de Administração, Estratégia e Tomada de Decisão, cujas contribuições permanecem relevantes para a compreensão dos fundamentos teóricos que sustentam a análise proposta neste estudo.

A análise dos dados foi realizada por meio de abordagem qualitativa interpretativa, buscando identificar, comparar e compreender os principais conceitos, perspectivas e contribuições presentes na literatura relacionada à cibersegurança, gestão de riscos, governança corporativa,

conformidade regulatória, continuidade dos negócios e tomada de decisão estratégica. Para organizar a análise, os estudos selecionados foram agrupados em categorias temáticas, permitindo identificar convergências, divergências e lacunas teóricas entre os autores. As categorias temáticas foram definidas a partir da recorrência dos temas identificados na literatura selecionada, permitindo organizar a discussão em eixos analíticos relacionados à cibersegurança, gestão de riscos, governança e tomada de decisão estratégica. Essa sistematização possibilitou compreender como diferentes abordagens explicam a influência da cibersegurança sobre os processos decisórios e sobre o planejamento estratégico das organizações.

Por fim, os resultados foram sistematizados de forma a identificar convergências, divergências, lacunas e contribuições teóricas presentes na literatura analisada. Essa abordagem permitiu compreender como a cibersegurança influencia a tomada de decisão estratégica nas organizações, fornecendo subsídios para a discussão dos impactos dos riscos cibernéticos sobre a gestão organizacional contemporânea.

Quadro 1 – Síntese do percurso metodológico da pesquisa

Etapa	**Procedimento realizado**
Tipo de pesquisa	Pesquisa qualitativa, exploratória e descritiva
Estratégia metodológica	Revisão bibliográfica

Bases consultadas	SciELO, Scopus, Web of Science, Portal CAPES, MIS Quarterly e MIS Quarterly Executive
Descritores utilizados	Cibersegurança, segurança da informação, gestão estratégica, governança, gestão de riscos, tomada de decisão e riscos cibernéticos
Critérios de inclusão	Estudos relacionados ao tema, com consistência teórica e metodológica
Critérios de exclusão	Trabalhos sem aderência ao objetivo, duplicados ou sem fundamentação científica
Procedimento de análise	Leitura dos estudos, agrupamento por categorias temáticas e análise qualitativa interpretativa

Fonte: Elaborado pelo autor (2026).

A organização dos estudos em categorias temáticas permitiu desenvolver uma análise interpretativa da literatura, buscando identificar convergências, divergências e contribuições relacionadas à influência da cibersegurança na tomada de decisão estratégica.

3. Fundamentos da Cibersegurança

A crescente digitalização das organizações tem ampliado significativamente a dependência de sistemas tecnológicos, tornando a informação um dos principais ativos estratégicos no

ambiente organizacional contemporâneo. Nesse cenário, a cibersegurança surge como um elemento essencial para a proteção de dados, sistemas e processos, sendo cada vez mais incorporada às práticas de gestão e governança.

A evolução das tecnologias da informação, aliada ao aumento da conectividade, também tem contribuído para o crescimento dos riscos cibernéticos, exigindo das organizações uma postura mais estruturada na prevenção, detecção e resposta a incidentes de segurança. Dessa forma, compreender os fundamentos da cibersegurança torna-se indispensável para a análise de seu impacto na tomada de decisão estratégica.

Este capítulo tem como objetivo apresentar os principais conceitos relacionados à cibersegurança, bem como discutir a evolução das ameaças cibernéticas e a importância da segurança da informação no contexto organizacional. A partir dessa base teórica, busca-se fornecer os elementos necessários para a compreensão da relação entre cibersegurança e gestão estratégica, que será aprofundada nos capítulos seguintes.

3.1. Conceitos de cibersegurança e segurança da informação

A cibersegurança tem se consolidado como um elemento essencial no contexto organizacional contemporâneo, especialmente em função do avanço das tecnologias digitais e da crescente interconectividade entre sistemas. De forma geral, pode ser compreendida como o conjunto de práticas, ferramentas e estratégias voltadas à proteção de sistemas, redes e dados contra acessos não autorizados, ataques maliciosos e diferentes tipos de ameaças presentes no ambiente digital.

Nesse contexto, a segurança da informação apresenta-se como um conceito complementar, voltado à proteção das informações independentemente do meio em que estejam armazenadas ou transmitidas. Enquanto a cibersegurança concentra-se predominantemente na proteção dos

ambientes digitais e dos recursos tecnológicos conectados à internet, a segurança da informação possui uma abordagem mais ampla, abrangendo tanto informações digitais quanto físicas. Dessa forma, a cibersegurança pode ser compreendida como uma das áreas que compõem o campo mais abrangente da segurança da informação.

A segurança da informação baseia-se em princípios fundamentais que orientam sua aplicação no ambiente organizacional, destacando-se a confidencialidade, a integridade e a disponibilidade das informações, conhecidos internacionalmente como a tríade CIA (Confidentiality, Integrity and Availability). Esses elementos são essenciais para assegurar que os dados sejam acessados apenas por indivíduos autorizados, mantenham sua consistência ao longo do tempo e estejam disponíveis sempre que necessário para o funcionamento das atividades organizacionais (ISO/IEC 27001, 2013).

Esses princípios servem de base para a elaboração de políticas, controles e mecanismos de proteção utilizados pelas organizações na gestão da segurança da informação. Sua aplicação contribui para a redução de vulnerabilidades, para a proteção dos ativos informacionais e para o fortalecimento da confiança nos processos organizacionais.

Além da tríade CIA, autores da área destacam que a segurança da informação também está associada à autenticidade e à rastreabilidade das informações, aspectos que contribuem para aumentar a confiabilidade dos processos organizacionais. Em um cenário caracterizado pela transformação digital, a proteção das informações tornou-se um fator crítico para a continuidade dos negócios e para a manutenção da confiança de clientes, parceiros e demais stakeholders.

A crescente dependência tecnológica das organizações ampliou significativamente a relevância da cibersegurança. Processos que anteriormente eram executados de forma manual

passaram a ser conduzidos por sistemas digitais integrados, aumentando a eficiência operacional, mas também ampliando a exposição a vulnerabilidades. Nesse cenário, ataques cibernéticos, vazamentos de dados e interrupções de sistemas podem gerar impactos financeiros, operacionais e reputacionais significativos.

De acordo com o World Economic Forum (2023), os riscos cibernéticos figuram entre as principais ameaças globais enfrentadas por organizações e governos. Esse contexto demonstra que a cibersegurança deixou de ser uma preocupação restrita aos departamentos de tecnologia da informação e passou a integrar as discussões relacionadas à gestão estratégica e à governança corporativa.

Dessa forma, a cibersegurança e a segurança da informação atuam de maneira integrada, contribuindo para a proteção dos ativos informacionais e para a redução de riscos no ambiente digital. Além disso, sua aplicação adequada fortalece a governança organizacional, auxilia no cumprimento de requisitos regulatórios e oferece suporte à tomada de decisão estratégica em um cenário marcado pela transformação digital e pela crescente complexidade tecnológica.

Quadro 2 – Principais conceitos relacionados à cibersegurança

Conceito	Definição	Relevância Organizacional
Cibersegurança	Conjunto de práticas, tecnologias e processos destinados à proteção de sistemas, redes e dados contra ameaças digitais.	Protege ativos digitais e reduz riscos operacionais.

Segurança da Informação	Área voltada à proteção das informações independentemente do meio em que estejam armazenadas.	Garante a confiabilidade das informações organizacionais.
Confidencialidade	Garante que apenas pessoas autorizadas tenham acesso às informações.	Evita acessos indevidos e vazamentos de dados.
Integridade	Assegura que as informações permaneçam completas e sem alterações indevidas.	Preserva a qualidade e a confiabilidade dos dados.
Disponibilidade	Garante que sistemas e informações estejam acessíveis quando necessários.	Mantém a continuidade das operações organizacionais.
Governança de Segurança	Conjunto de diretrizes, políticas e mecanismos de controle voltados ao gerenciamento da segurança da informação e dos riscos cibernéticos.	Auxilia na gestão de riscos, fortalece a governança corporativa e apoia a tomada de decisão estratégica.

Fonte: Elaborado pelo autor (2026), com base na ISO/IEC 27001 (2013).

Os conceitos apresentados no Quadro 1 demonstram que a cibersegurança não se limita à utilização de ferramentas tecnológicas para proteção de sistemas, mas envolve um conjunto de princípios e práticas que contribuem para a gestão organizacional. Observa-se que elementos como confidencialidade, integridade e disponibilidade constituem a base da segurança da informação, servindo como referência para a implementação de controles e políticas de proteção de dados. Além disso, a integração entre cibersegurança e governança evidencia que a proteção das informações passou a ocupar posição estratégica nas organizações, influenciando diretamente a gestão de riscos, a formulação de estratégias e os processos de tomada de decisão em ambientes cada vez mais digitalizados.

3.2 Evolução das ameaças cibernéticas

A evolução das ameaças cibernéticas está diretamente relacionada ao avanço das tecnologias da informação e à ampliação do uso de sistemas digitais nas organizações. Com o aumento da conectividade e da dependência de ambientes digitais, os riscos associados à segurança da informação tornaram-se mais complexos, exigindo mecanismos cada vez mais sofisticados de proteção.

Inicialmente, as ameaças cibernéticas eram caracterizadas por ataques mais simples, muitas vezes realizados de forma isolada e com objetivos limitados. No entanto, ao longo do tempo, esses ataques passaram a ser mais estruturados, frequentes e direcionados, envolvendo técnicas avançadas e, em muitos casos, organizações criminosas especializadas. Esse cenário demonstra uma mudança significativa no perfil das ameaças, que passaram de eventos pontuais para riscos estratégicos capazes de comprometer a continuidade das operações organizacionais.

Entre as principais ameaças cibernéticas contemporâneas destacam-se os ataques de ransomware, que consistem no sequestro de dados mediante pagamento de resgate; os ataques de phishing, que utilizam técnicas de engenharia social para obter informações sensíveis; os ataques de negação de serviço (DDoS), voltados à indisponibilidade de sistemas; e as invasões direcionadas a infraestruturas críticas e bases de dados corporativas.

Além disso, a popularização de tecnologias como computação em nuvem, Internet das Coisas (IoT), inteligência artificial e dispositivos móveis ampliou significativamente a superfície de ataque das organizações. Embora essas tecnologias proporcionem ganhos em produtividade e eficiência, também introduzem novas vulnerabilidades que podem ser exploradas por agentes maliciosos.

De acordo com a Cybersecurity Ventures (2023), os custos globais associados aos crimes cibernéticos apresentam crescimento contínuo e representam um dos maiores desafios para organizações públicas e privadas. Esse cenário evidencia que os riscos digitais não se limitam a perdas financeiras, podendo afetar a reputação institucional, a confiança dos clientes e a continuidade das operações.

Além disso, incidentes cibernéticos podem comprometer processos decisórios, gerar perda de informações estratégicas e afetar a confiança dos stakeholders, ampliando seus impactos sobre a gestão organizacional. Dessa forma, os riscos cibernéticos deixam de representar apenas uma preocupação operacional e passam a influenciar aspectos relacionados ao planejamento, à governança e à sustentabilidade das organizações.

Outro aspecto relevante refere-se à profissionalização do cibercrime. Atualmente, grupos organizados utilizam modelos sofisticados de atuação, comercializando ferramentas de invasão e serviços ilegais em ambientes conhecidos como dark web. Essa realidade contribui

para ampliar a escala e a complexidade dos ataques, tornando insuficientes abordagens exclusivamente reativas de segurança.

Nesse contexto, torna-se fundamental que as organizações adotem uma postura preventiva e estratégica em relação à cibersegurança, investindo em monitoramento contínuo, capacitação de usuários, gestão de vulnerabilidades e planos de resposta a incidentes. A compreensão da evolução das ameaças cibernéticas é, portanto, essencial para a construção de políticas eficazes de segurança da informação e para o suporte à tomada de decisão estratégica em ambientes digitais cada vez mais complexos.

Tabela 1 – Evolução estimada dos custos globais do cibercrime

Ano	Custos globais estimados (US$ trilhões)	Crescimento acumulado
2015	3,0	-
2021	6,0	+100%
2025	10,5	+250%

Fonte: Elaborado pelo autor (2026), com base em Cybersecurity Ventures (2023).

Os dados apresentados na Tabela 1 demonstram o crescimento expressivo dos impactos econômicos associados aos crimes cibernéticos ao longo da última década. Observa-se que os custos globais praticamente triplicaram entre 2015 e 2025, evidenciando que a cibersegurança deixou de representar apenas uma preocupação operacional para assumir relevância

estratégica nas organizações. Esse cenário reforça a necessidade de investimentos contínuos em prevenção, monitoramento e gestão de riscos cibernéticos, especialmente em ambientes caracterizados pela intensa dependência tecnológica. Além dos prejuízos financeiros, o aumento dos custos do cibercrime está associado a impactos reputacionais, operacionais e regulatórios, ampliando a necessidade de integração entre cibersegurança, governança e tomada de decisão estratégica.

3.3 Importância da segurança no contexto organizacional

A segurança da informação tem se tornado um elemento estratégico no contexto organizacional, especialmente diante da crescente digitalização dos processos e da valorização dos dados como ativos essenciais. Nesse cenário, a proteção das informações ultrapassa o campo técnico e passa a influenciar diretamente a sustentabilidade, a reputação e a competitividade das organizações.

O avanço da transformação digital fez com que empresas e instituições passassem a depender cada vez mais de sistemas informatizados para execução de suas atividades. Como consequência, a interrupção desses sistemas ou o comprometimento de informações sensíveis pode gerar impactos significativos sobre o desempenho organizacional. Dessa forma, a segurança da informação assume papel fundamental na proteção dos ativos digitais e na continuidade das operações.

A ocorrência de incidentes de segurança, como vazamentos de dados, ataques cibernéticos e falhas em sistemas críticos, pode resultar em prejuízos financeiros expressivos, perda de confiança por parte dos clientes e danos à imagem institucional. Em muitos casos, os impactos reputacionais podem ser mais duradouros que os próprios prejuízos financeiros, afetando diretamente a capacidade competitiva das organizações.

Além dos aspectos econômicos e operacionais, a segurança da informação também está relacionada ao cumprimento de exigências legais e regulatórias. No Brasil, a Lei Geral de Proteção de Dados (LGPD) estabeleceu diretrizes para o tratamento de dados pessoais, exigindo que organizações adotem medidas adequadas para garantir a proteção dessas informações (Brasil, 2018). O descumprimento dessas exigências pode acarretar sanções administrativas, multas e danos à reputação institucional.

Outro aspecto relevante refere-se à relação entre segurança da informação e governança organizacional. Organizações que incorporam práticas estruturadas de segurança tendem a desenvolver processos mais eficientes de gestão de riscos, permitindo maior previsibilidade e controle sobre ameaças que possam comprometer seus objetivos estratégicos. Nesse sentido, a segurança da informação passa a ser compreendida como um componente essencial da governança corporativa.

Essa integração torna-se especialmente relevante em ambientes organizacionais altamente digitalizados, nos quais a proteção das informações influencia não apenas a continuidade operacional, mas também a qualidade das decisões estratégicas. Dessa forma, a segurança da informação passa a fornecer suporte para escolhas mais seguras, reduzindo incertezas e fortalecendo a capacidade das organizações de responder aos desafios do ambiente competitivo.

A literatura também destaca que organizações com maior maturidade em segurança da informação apresentam maior capacidade de adaptação a cenários adversos e maior resiliência frente a crises tecnológicas. Essa capacidade de resposta contribui para a continuidade dos negócios e fortalece a confiança de investidores, parceiros e demais stakeholders.

Diante desse contexto, a segurança da informação deve ser compreendida como parte integrante da estratégia organizacional, contribuindo para a mitigação de riscos, para a proteção de ativos e para a tomada de decisões mais seguras. Assim, organizações que investem em práticas estruturadas de segurança tendem a apresentar maior resiliência frente às ameaças digitais e melhores condições para alcançar seus objetivos estratégicos em ambientes cada vez mais dinâmicos e tecnológicos.

Figura 1 – Principais impactos organizacionais associados a incidentes de cibersegurança

Fonte: Elaborado pelo autor (2026), com base em IBM Security (2024) e World Economic Forum (2023).

A Figura 1 evidencia que os impactos decorrentes de incidentes cibernéticos ultrapassam a esfera tecnológica e afetam diferentes dimensões organizacionais. Além dos prejuízos financeiros associados à recuperação de sistemas e à resposta a incidentes, organizações podem sofrer danos reputacionais significativos, comprometendo a confiança de clientes, parceiros e investidores. Somam-se a isso as possíveis sanções regulatórias decorrentes do descumprimento de normas de proteção de dados, bem como a interrupção de operações críticas. Esses fatores demonstram que a cibersegurança deve ser compreendida como um elemento estratégico, capaz de influenciar diretamente a sustentabilidade e a competitividade organizacional.

4. Tomada de Decisão Estratégica

A tomada de decisão estratégica constitui um dos principais processos organizacionais, influenciando diretamente a definição de objetivos, a alocação de recursos e a capacidade competitiva das organizações. Em ambientes caracterizados por mudanças constantes, elevada complexidade e intensa utilização de tecnologias digitais, as decisões estratégicas tornam-se cada vez mais dependentes de informações confiáveis e da adequada gestão dos riscos organizacionais.

Nesse contexto, compreender os fundamentos da estratégia organizacional e os fatores que influenciam os processos decisórios torna-se essencial para analisar como a cibersegurança pode impactar as escolhas realizadas pelos gestores. A crescente relevância dos riscos cibernéticos ampliou a necessidade de incorporar aspectos relacionados à segurança da informação no planejamento estratégico, tornando a proteção dos ativos digitais um elemento importante para a sustentabilidade e a continuidade das organizações.

Dessa forma, este capítulo apresenta os principais conceitos relacionados à estratégia organizacional, aos processos de tomada de decisão e aos fatores que influenciam as escolhas estratégicas, fornecendo a base teórica necessária para compreender a relação entre cibersegurança e gestão estratégica nas organizações.

4.1. Conceitos de estratégia organizacional

A estratégia organizacional representa um dos principais elementos para a orientação das ações e decisões das organizações. De forma geral, pode ser compreendida como o conjunto de diretrizes e escolhas que orientam a organização em direção aos seus objetivos de longo prazo, considerando o ambiente competitivo, os recursos disponíveis e as oportunidades de crescimento.

Ao longo das últimas décadas, diferentes autores desenvolveram abordagens para explicar o conceito de estratégia. Entre os mais influentes destaca-se Michael Porter (1985), que associa a estratégia à obtenção de vantagem competitiva sustentável. Segundo o autor, as organizações devem desenvolver posições diferenciadas no mercado por meio da criação de valor e da utilização eficiente de seus recursos, buscando alcançar desempenho superior em relação aos concorrentes.

Outra contribuição relevante é apresentada por Mintzberg (2000), que propõe uma visão mais dinâmica da estratégia. Para esse autor, a estratégia não deve ser entendida apenas como resultado de um planejamento formal, mas também como consequência das experiências, adaptações e decisões que surgem ao longo do tempo. Essa perspectiva amplia a compreensão dos processos estratégicos ao reconhecer que muitas decisões organizacionais são influenciadas por fatores emergentes e por mudanças no ambiente externo.

Senge (1990), por sua vez, destaca a importância da aprendizagem organizacional no desenvolvimento da estratégia. Segundo o autor, organizações capazes de aprender continuamente apresentam maior capacidade de adaptação frente às mudanças do ambiente, favorecendo a inovação e a construção de vantagens competitivas sustentáveis. Nessa perspectiva, o conhecimento passa a ser considerado um recurso estratégico essencial para o sucesso organizacional.

Independentemente das diferentes abordagens teóricas, observa-se que a estratégia organizacional está diretamente relacionada à capacidade de antecipar desafios, identificar oportunidades e direcionar recursos de forma eficiente. Em ambientes caracterizados por rápidas transformações tecnológicas e elevada competitividade, a formulação de estratégias

eficazes torna-se um fator determinante para a sobrevivência e o crescimento das organizações.

Além disso, a formulação estratégica depende cada vez mais da capacidade das organizações de interpretar informações confiáveis e avaliar riscos associados ao ambiente de negócios. Em cenários marcados pela transformação digital, decisões estratégicas passaram a considerar não apenas fatores econômicos e competitivos, mas também aspectos relacionados à segurança da informação, à proteção de dados e à continuidade das operações.

Nesse contexto, a crescente digitalização dos negócios e o aumento dos riscos cibernéticos ampliaram a necessidade de incorporar aspectos relacionados à segurança da informação nos processos de planejamento estratégico. Assim, decisões relacionadas à proteção de dados, à gestão de riscos e à resiliência organizacional passaram a integrar as discussões estratégicas das organizações, demonstrando que a cibersegurança deixou de ser apenas uma questão operacional para assumir relevância no âmbito da gestão estratégica.

Observa-se que, embora os autores apresentem perspectivas distintas sobre estratégia organizacional, suas abordagens não são excludentes, mas complementares. Porter (1985) enfatiza o posicionamento competitivo como fonte de vantagem sustentável, enquanto Mintzberg (2000) destaca a natureza dinâmica e emergente da estratégia diante das mudanças do ambiente organizacional. Por sua vez, Senge (1990) amplia essa compreensão ao defender que a aprendizagem contínua constitui elemento essencial para a adaptação organizacional, ao passo que Bharadwaj et al. (2013) incorporam a transformação digital como componente estratégico capaz de redefinir modelos de negócios e processos decisórios. Em conjunto, essas perspectivas evidenciam que a estratégia organizacional contemporânea exige equilíbrio entre planejamento, adaptação, aprendizagem e inovação tecnológica.

Quadro 3 – Principais abordagens sobre estratégia organizacional

Autor	Visão de Estratégia	Contribuição para a Gestão
Porter (1985)	Estratégia como vantagem competitiva.	Auxilia na diferenciação e posicionamento organizacional.
Mintzberg (2000)	Estratégia como processo emergente e adaptativo.	Destaca a influência das mudanças e da aprendizagem organizacional.
Senge (1990)	Estratégia baseada na aprendizagem organizacional.	Valoriza o conhecimento e a adaptação contínua.
Bharadwaj et al. (2013)	Estratégia digital.	Destaca a integração entre tecnologia, inovação e objetivos organizacionais.

Fonte: Elaborado pelo autor (2026), com base em Porter (1985), Mintzberg (2000), Senge (1990) e Bharadwaj et al. (2013).

A análise comparativa apresentada no Quadro 2 evidencia que a evolução do conceito de estratégia organizacional acompanha as transformações do ambiente competitivo e tecnológico. Enquanto Porter (1985) enfatiza a obtenção de vantagem competitiva por meio do posicionamento estratégico, Mintzberg (2000) demonstra que as estratégias também emergem das adaptações realizadas pelas organizações diante de ambientes dinâmicos. Senge

(1990), por sua vez, amplia essa perspectiva ao destacar a aprendizagem organizacional como elemento essencial para a inovação e a adaptação contínua. Já Bharadwaj et al. (2013) incorporam a dimensão digital ao debate estratégico, evidenciando que a tecnologia deixou de atuar apenas como suporte operacional para assumir papel central na formulação das estratégias organizacionais. Dessa forma, observa-se uma convergência entre os autores quanto à necessidade de integrar capacidades organizacionais, inovação e gestão dos riscos como fatores essenciais para a sustentabilidade e competitividade das organizações contemporâneas.

4.2. Processos decisórios nas organizações

A tomada de decisão constitui uma das atividades mais importantes no contexto organizacional, uma vez que influencia diretamente o desempenho, a competitividade e a capacidade de adaptação das organizações diante das mudanças do ambiente externo. Em termos gerais, decidir envolve selecionar uma alternativa entre diferentes opções disponíveis, considerando objetivos, informações disponíveis, recursos e possíveis consequências.

Entre os principais autores que contribuíram para o estudo dos processos decisórios destaca-se Herbert Simon (1979), que propôs o conceito de racionalidade limitada. Segundo essa perspectiva, os indivíduos não possuem capacidade ilimitada para processar informações e avaliar todas as alternativas possíveis, tomando decisões com base nas informações disponíveis e em suas limitações cognitivas. Dessa forma, as decisões organizacionais nem sempre representam a solução ótima, mas sim alternativas consideradas satisfatórias dentro das circunstâncias existentes.

O processo decisório normalmente envolve diferentes etapas que auxiliam gestores na identificação de problemas, avaliação de alternativas e implementação de soluções. Embora

existam variações entre os modelos apresentados na literatura, observa-se que a maioria dos processos decisórios contempla fases relacionadas à identificação do problema, coleta e análise de informações, geração de alternativas, escolha da melhor opção e acompanhamento dos resultados obtidos.

Nesse contexto, a qualidade das informações disponíveis desempenha papel fundamental na efetividade das decisões organizacionais. Informações precisas, atualizadas e confiáveis contribuem para reduzir incertezas e aumentar a capacidade dos gestores de avaliar riscos e oportunidades. Por outro lado, informações incompletas ou incorretas podem comprometer significativamente os resultados das decisões adotadas.

A confiabilidade das informações utilizadas no processo decisório está diretamente relacionada às práticas de segurança da informação adotadas pela organização. A ocorrência de incidentes cibernéticos, vazamentos de dados ou manipulação indevida de informações pode comprometer a qualidade dos dados disponíveis para análise, influenciando negativamente a tomada de decisão. Dessa forma, a cibersegurança passa a desempenhar papel relevante na preservação da integridade das informações utilizadas pelos gestores.

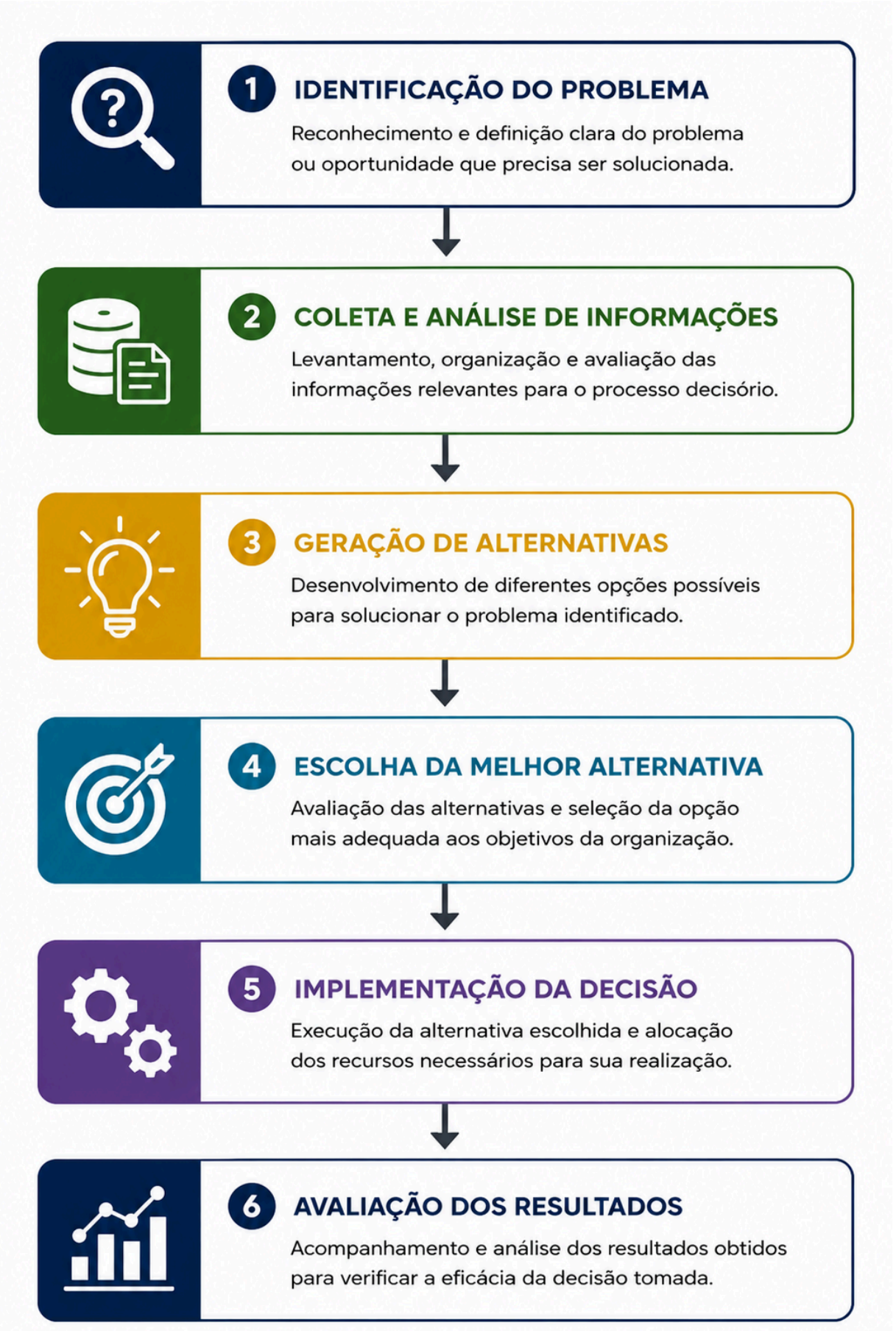
Essa relação entre qualidade das informações, cibersegurança e tomada de decisão também tem sido evidenciada em estudos recentes. Vrhovec e Markelj (2024) demonstram que a efetividade das decisões relacionadas à segurança da informação depende não apenas da disponibilidade de dados confiáveis, mas também do nível de conscientização dos gestores responsáveis pelos processos decisórios. Segundo os autores, fatores como experiência profissional, maturidade organizacional e compreensão dos riscos cibernéticos influenciam diretamente a definição de prioridades estratégicas e a adoção de práticas voltadas ao fortalecimento da postura de segurança das organizações. Esses achados reforçam que a

cibersegurança constitui elemento essencial para subsidiar decisões organizacionais mais seguras e alinhadas aos objetivos estratégicos.

Além dos aspectos informacionais, fatores organizacionais, culturais e tecnológicos também influenciam os processos decisórios. O avanço das tecnologias digitais ampliou o acesso a dados e ferramentas analíticas, permitindo que organizações utilizem informações em tempo real para apoiar decisões estratégicas. Entretanto, essa mesma dependência tecnológica aumenta a relevância de questões relacionadas à segurança da informação e à proteção dos ativos digitais.

Dessa forma, a tomada de decisão deve ser compreendida como um processo contínuo e dinâmico, influenciado por fatores internos e externos à organização. Em ambientes caracterizados por elevada complexidade e incerteza, a capacidade de tomar decisões fundamentadas em informações confiáveis torna-se um diferencial estratégico para organizações que buscam alcançar seus objetivos e manter sua competitividade.

Figura 2 – Etapas do Processo Decisório Organizacional


1
IDENTIFICAÇÃO DO PROBLEMA
Reconhecimento e definição clara do problema ou oportunidade que precisa ser solucionada.
2
COLETA E ANÁLISE DE INFORMAÇÕES
Levantamento, organização e avaliação das informações relevantes para o processo decisório.
3
GERAÇÃO DE ALTERNATIVAS
Desenvolvimento de diferentes opções possíveis para solucionar o problema identificado.
4
ESCOLHA DA MELHOR ALTERNATIVA
Avaliação das alternativas e seleção da opção mais adequada aos objetivos da organização.
5
IMPLEMENTAÇÃO DA DECISÃO
Execução da alternativa escolhida e alocação dos recursos necessários para sua realização.
6
AVALIAÇÃO DOS RESULTADOS
Acompanhamento e análise dos resultados obtidos para verificar a eficácia da decisão tomada.

Fonte: Elaborado pelo autor (2026), com base em Simon (1979).

A Figura 2 apresenta uma representação simplificada do processo decisório organizacional com base nas contribuições de Simon (1979). Observa-se que a tomada de decisão não se restringe ao momento da escolha entre alternativas, mas envolve um conjunto de etapas interdependentes que contribuem para a redução de incertezas e para a melhoria dos resultados organizacionais. Nesse processo, a qualidade das informações utilizadas assume papel central, reforçando a importância da segurança da informação como elemento de suporte às decisões estratégicas. Além disso, a crescente dependência de sistemas digitais torna fundamental a adoção de práticas de cibersegurança capazes de garantir a integridade, a disponibilidade e a confiabilidade dos dados utilizados pelos gestores ao longo de todo o processo decisório.

4.3 Fatores que influenciam a tomada de decisão

A tomada de decisão organizacional é influenciada por diversos fatores que podem impactar tanto a qualidade quanto a efetividade das escolhas realizadas pelos gestores. Esses fatores envolvem aspectos internos e externos à organização, abrangendo elementos relacionados às pessoas, aos recursos disponíveis, ao ambiente competitivo e às condições tecnológicas existentes.

Entre os fatores internos, destaca-se a disponibilidade e a qualidade das informações utilizadas durante o processo decisório. Informações precisas, atualizadas e relevantes contribuem para a redução das incertezas e para a formulação de decisões mais consistentes. Por outro lado, informações incompletas ou imprecisas podem comprometer a avaliação de alternativas e aumentar os riscos associados às decisões organizacionais.

Outro fator relevante refere-se à cultura organizacional. Organizações com culturas voltadas para a inovação, aprendizagem e compartilhamento de conhecimento tendem a apresentar processos decisórios mais participativos e adaptáveis. Em contrapartida, ambientes excessivamente centralizados podem limitar a circulação de informações e reduzir a capacidade de resposta frente às mudanças do ambiente externo.

Os recursos organizacionais também exercem influência significativa sobre as decisões estratégicas. Aspectos financeiros, tecnológicos e humanos podem ampliar ou restringir as alternativas disponíveis para os gestores. Nesse sentido, a disponibilidade de recursos adequados torna-se um elemento importante para a implementação de estratégias e para o alcance dos objetivos organizacionais.

No ambiente externo, fatores econômicos, políticos, sociais, tecnológicos e regulatórios também afetam os processos decisórios. Mudanças na legislação, avanços tecnológicos, transformações no comportamento dos consumidores e alterações nas condições de mercado podem exigir adaptações constantes por parte das organizações.

A evolução tecnológica merece destaque especial devido ao seu impacto crescente sobre a gestão organizacional. Ferramentas de análise de dados, inteligência artificial, sistemas de informação gerencial e plataformas digitais ampliaram significativamente a capacidade de coleta e processamento de informações. Entretanto, a dependência dessas tecnologias também aumentou a exposição a riscos relacionados à segurança da informação e à proteção de dados.

Além dos benefícios associados à inovação tecnológica, as organizações passaram a enfrentar desafios relacionados à proteção de dados estratégicos, à privacidade das informações e à continuidade dos serviços digitais. Como consequência, gestores precisam considerar os

riscos cibernéticos durante a avaliação de alternativas e a definição de estratégias, incorporando aspectos de segurança aos processos de tomada de decisão.

Nesse contexto, a cibersegurança emerge como um fator cada vez mais relevante para a tomada de decisão estratégica. A necessidade de proteger ativos informacionais, garantir a continuidade das operações e atender exigências regulatórias faz com que questões relacionadas à segurança da informação passem a integrar o processo decisório em diferentes níveis organizacionais.

Dessa forma, a tomada de decisão deve ser compreendida como um processo influenciado por múltiplos fatores interdependentes. A capacidade de identificar, analisar e gerenciar esses elementos contribui para decisões mais eficazes, reduzindo riscos e fortalecendo a competitividade organizacional em ambientes caracterizados por elevada complexidade e dinamismo.

Tabela 2 – Principais fatores que influenciam a tomada de decisão organizacional

Categoria	**Fator**	**Possível impacto**	**Relação com a cibersegurança**
Interno	Qualidade das informações	Redução de incertezas e melhoria das decisões	Garantia da integridade e confiabilidade dos dados utilizados pelos gestores

Interno	Cultura organizacional	Influência sobre comportamento e processos decisórios	Promoção de uma cultura voltada à proteção das informações
Interno	Recursos disponíveis	Determinação das alternativas viáveis	Investimentos em infraestrutura e mecanismos de segurança
Externo	Ambiente econômico	Impacto sobre investimentos e estratégias	Influência na priorização de recursos destinados à proteção digital
Externo	Regulamentação	Necessidade de adequação legal e operacional	Atendimento à LGPD e demais normas relacionadas à segurança da informação
Externo	Tecnologia	Ampliação das capacidades e dos riscos organizacionais	Aumento da exposição a vulnerabilidades e ameaças digitais

Estratégic o	Cibersegurança	Proteção de ativos e suporte à continuidade dos negócios	Elemento central para gestão de riscos e apoio à tomada de decisão

Fonte: Elaborado pelo autor (2026), com base em Simon (1979), Porter (1985) e literatura sobre gestão estratégica.

A Tabela 2 evidencia que a tomada de decisão organizacional resulta da interação entre fatores internos e externos que influenciam diretamente as escolhas estratégicas. Observa-se que aspectos relacionados à informação, cultura organizacional, recursos disponíveis e ambiente competitivo exercem papel relevante na definição das estratégias adotadas pelas organizações. Além disso, a crescente digitalização dos processos organizacionais amplia a importância da cibersegurança como elemento de suporte à gestão de riscos, à proteção dos ativos informacionais e à continuidade dos negócios, reforçando sua influência sobre os processos decisórios contemporâneos. Nesse contexto, organizações que incorporam práticas estruturadas de segurança da informação tendem a desenvolver processos decisórios mais seguros, resilientes e alinhados aos desafios do ambiente digital.

5. Cibersegurança e Estratégia Organizacional

A crescente digitalização das organizações tem provocado transformações significativas na forma como estratégias são formuladas e implementadas. Nesse contexto, a cibersegurança passa a desempenhar um papel central, deixando de ser apenas uma função técnica para se consolidar como um elemento estratégico capaz de influenciar diretamente a tomada de decisão organizacional.

O aumento da dependência de sistemas digitais, aliado à intensificação de ameaças cibernéticas, tem exigido das organizações uma postura mais proativa na gestão de riscos. Dessa forma, a segurança da informação passa a integrar o processo estratégico, influenciando decisões relacionadas à continuidade dos negócios, à proteção de ativos e à conformidade com normas e regulamentações.

Além disso, a incorporação da cibersegurança na estratégia organizacional está diretamente associada à necessidade de garantir vantagem competitiva em um ambiente marcado pela incerteza e pela complexidade. Organizações que conseguem alinhar suas práticas de segurança à sua estratégia tendem a apresentar maior resiliência e capacidade de adaptação frente a cenários adversos.

De acordo com estudos recentes, a integração entre tecnologia, gestão de riscos e estratégia organizacional tem se tornado um fator crítico para o desempenho sustentável das organizações (Bharadwaj et al., 2013). Nesse sentido, a cibersegurança passa a ser compreendida como um componente essencial da governança corporativa, influenciando não apenas a proteção de dados, mas também a qualidade das decisões estratégicas.

Além dos aspectos relacionados à proteção de informações e sistemas, a cibersegurança influencia diretamente a capacidade das organizações de responder a mudanças do ambiente externo e de tomar decisões em cenários de elevada incerteza. A crescente sofisticação das ameaças digitais faz com que gestores considerem os riscos cibernéticos não apenas como problemas operacionais, mas como fatores estratégicos capazes de impactar investimentos, reputação, continuidade operacional e desempenho organizacional. Dessa forma, a integração da cibersegurança aos processos de gestão contribui para decisões mais fundamentadas, alinhadas aos objetivos organizacionais e às exigências de um ambiente cada vez mais digitalizado.

Dessa forma, este capítulo tem como objetivo analisar a relação entre cibersegurança e estratégia organizacional, abordando seus impactos na gestão estratégica, nos processos decisórios e na construção de organizações mais seguras e resilientes. Para isso, serão discutidos aspectos relacionados aos riscos cibernéticos, à governança, à conformidade regulatória e à continuidade dos negócios.

5.1. Impactos da cibersegurança na gestão estratégica

A influência da cibersegurança na gestão estratégica pode ser observada em diferentes dimensões organizacionais, especialmente naquelas relacionadas à gestão de riscos, à proteção de ativos informacionais e à continuidade das operações. Em um ambiente caracterizado pela crescente dependência de tecnologias digitais, decisões relacionadas à segurança da informação passaram a integrar o processo estratégico das organizações, influenciando diretamente sua capacidade de adaptação e competitividade.

Estudos recentes reforçam essa perspectiva ao demonstrar que organizações que incorporam a cibersegurança às decisões estratégicas apresentam maior capacidade de adaptação frente aos

riscos digitais, fortalecem sua governança e ampliam sua resiliência organizacional. Além disso, a literatura contemporânea destaca que a integração entre estratégia corporativa e gestão da cibersegurança passou a representar importante fator de competitividade em ambientes caracterizados pela transformação digital e pela crescente complexidade tecnológica.

Historicamente, a segurança da informação era tratada como uma responsabilidade predominantemente técnica, concentrada nos setores de tecnologia da informação. Entretanto, a ampliação das ameaças cibernéticas e o aumento da relevância dos dados para as atividades organizacionais contribuíram para uma mudança de perspectiva, elevando a cibersegurança à condição de tema estratégico.

Nesse contexto, a gestão estratégica passou a considerar os riscos cibernéticos como fatores capazes de influenciar objetivos organizacionais, investimentos, planejamento e processos decisórios. A possibilidade de interrupções operacionais, vazamentos de informações e prejuízos financeiros faz com que a proteção dos ativos digitais seja incorporada ao planejamento organizacional de longo prazo.

Segundo Bharadwaj et al. (2013), a estratégia digital tornou-se elemento fundamental para a competitividade das organizações, exigindo alinhamento entre tecnologia, objetivos estratégicos e capacidade de adaptação. Nesse cenário, a cibersegurança desempenha papel essencial ao fornecer mecanismos de proteção que sustentam a implementação de estratégias digitais e reduzem vulnerabilidades capazes de comprometer o desempenho organizacional.

Além da mitigação de riscos, a cibersegurança também pode contribuir para a geração de valor organizacional. Organizações que demonstram elevado nível de maturidade em segurança da informação tendem a fortalecer a confiança de clientes, parceiros comerciais e

investidores, criando condições favoráveis para a manutenção de relacionamentos duradouros e para o fortalecimento de sua reputação institucional. Em um ambiente cada vez mais orientado por dados, a confiança passa a representar um ativo estratégico, capaz de influenciar a competitividade, a atração de investimentos e a sustentabilidade organizacional no longo prazo.

No contexto brasileiro, a relevância da cibersegurança tem se intensificado em razão do aumento da digitalização dos serviços e da crescente exposição das organizações a ameaças cibernéticas. Relatórios recentes de empresas especializadas em segurança digital indicam que o Brasil figura entre os países mais visados por ataques cibernéticos na América Latina, especialmente em setores como serviços financeiros, administração pública, saúde e comércio eletrônico. Esse cenário reforça a necessidade de que organizações brasileiras incorporem a gestão dos riscos cibernéticos aos seus processos estratégicos, buscando fortalecer a proteção de dados, a continuidade operacional e a capacidade de resposta a incidentes.

Dados divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e por relatórios de empresas especializadas em segurança digital demonstram que o número de incidentes cibernéticos reportados no país permanece elevado, afetando organizações de diferentes portes e setores econômicos. Esse contexto evidencia que a cibersegurança deixou de representar apenas uma preocupação operacional, passando a influenciar decisões relacionadas a investimentos, governança, conformidade regulatória e continuidade dos negócios no ambiente organizacional brasileiro.

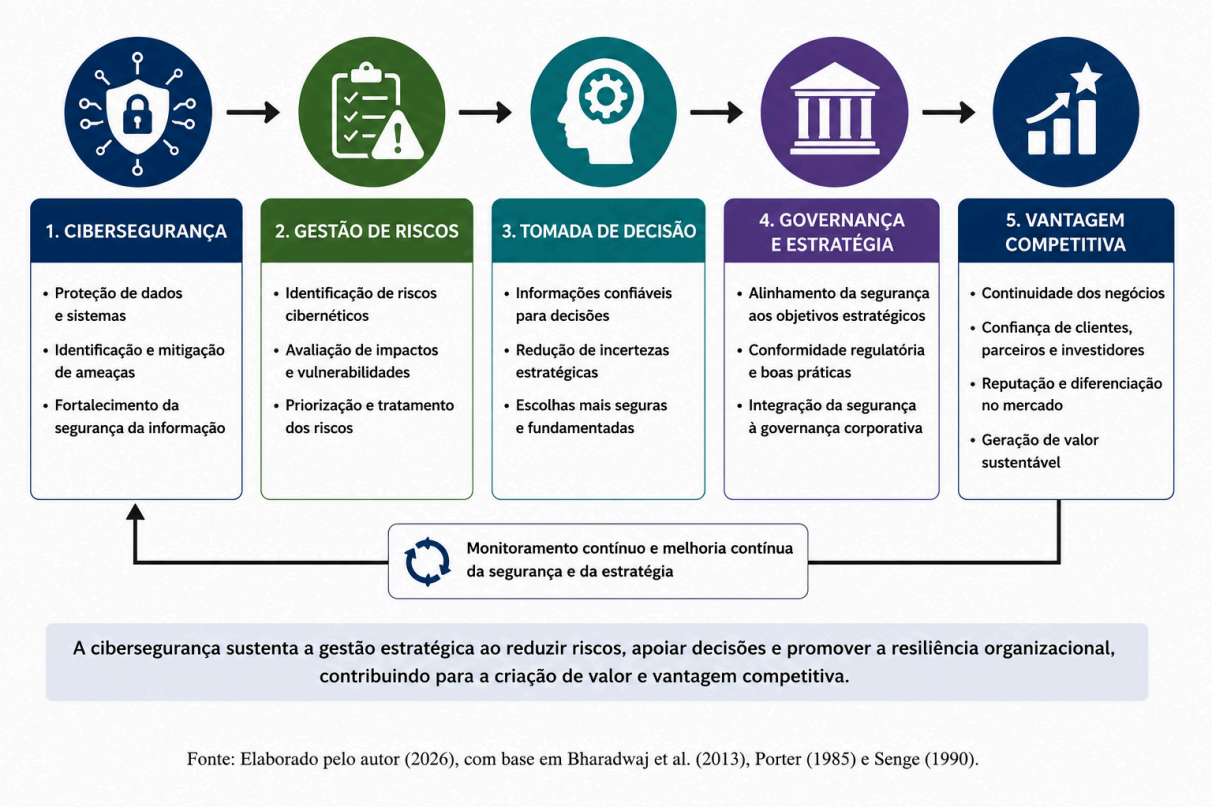
Outro aspecto relevante refere-se à conformidade regulatória. A implementação de normas e legislações relacionadas à proteção de dados, como a Lei Geral de Proteção de Dados (LGPD), ampliou a necessidade de adoção de práticas estruturadas de segurança da

informação. Dessa forma, a cibersegurança passou a representar não apenas um mecanismo de proteção, mas também um requisito para a conformidade legal e para a redução de riscos jurídicos e reputacionais.

Além dos benefícios associados à proteção dos ativos informacionais, a incorporação da cibersegurança à gestão estratégica influencia diretamente a qualidade dos processos decisórios. Organizações que possuem estruturas consolidadas de segurança da informação tendem a dispor de informações mais confiáveis para subsidiar decisões relacionadas a investimentos, inovação, expansão de mercado e gestão de riscos. Nesse sentido, a cibersegurança não atua apenas como mecanismo de proteção, mas como elemento de suporte à formulação de estratégias organizacionais mais consistentes e alinhadas aos objetivos de longo prazo.

Observa-se, portanto, que a cibersegurança ultrapassa os limites operacionais e assume papel estratégico nas organizações contemporâneas. Sua integração aos processos de gestão contribui para decisões mais seguras, maior capacidade de resposta a incidentes, fortalecimento da governança e construção de vantagens competitivas sustentáveis em ambientes digitais cada vez mais complexos.

Figura 3 – Relação entre Cibersegurança e Gestão Estratégica



Fonte: Elaborado pelo autor (2026), com base em Bharadwaj et al. (2013), Porter (1985) e Senge (1990).

A Figura 3 demonstra que a cibersegurança exerce influência direta sobre diferentes dimensões da gestão estratégica. Observa-se que a proteção de dados e sistemas contribui para a gestão de riscos organizacionais, fornecendo informações mais confiáveis para os processos decisórios. Esse alinhamento favorece a governança corporativa, fortalece a conformidade regulatória e amplia a capacidade de adaptação das organizações frente às mudanças do ambiente externo. Como resultado, a integração entre cibersegurança e estratégia pode contribuir para a construção de vantagens competitivas sustentáveis e para a geração de valor no longo prazo.

A literatura analisada demonstra convergência quanto ao reconhecimento da cibersegurança como elemento estratégico para as organizações contemporâneas. Entretanto, observa-se diferença de enfoque entre os autores. Enquanto relatórios institucionais e normas internacionais enfatizam aspectos relacionados à conformidade, continuidade dos negócios e

mitigação de riscos, estudos da área de Administração Estratégica destacam a incorporação da cibersegurança aos processos de formulação estratégica e de geração de vantagem competitiva. Essa complementaridade evidencia que a proteção dos ativos informacionais deixou de representar apenas uma função operacional, passando a integrar as decisões relacionadas ao posicionamento organizacional, à inovação e à sustentabilidade empresarial.

5.2. Riscos cibernéticos e decisões organizacionais

Os riscos cibernéticos passaram a ocupar posição de destaque entre os fatores que influenciam a tomada de decisão nas organizações contemporâneas. A crescente dependência de tecnologias digitais, associada ao aumento da frequência e da sofisticação dos ataques cibernéticos, exige que gestores considerem aspectos relacionados à segurança da informação durante a formulação e implementação de estratégias organizacionais.

Pesquisas recentes reforçam essa compreensão ao demonstrar que os riscos cibernéticos devem ser tratados como riscos organizacionais complexos, capazes de influenciar decisões estratégicas, operacionais e financeiras. Dacorogna e Kratz (2023) destacam que a gestão dos riscos cibernéticos evoluiu para além da identificação de vulnerabilidades tecnológicas, passando a incorporar mecanismos de avaliação contínua, resiliência organizacional e apoio à tomada de decisão em ambientes marcados por elevada incerteza.

De modo geral, os riscos cibernéticos podem ser compreendidos como eventos capazes de comprometer a confidencialidade, a integridade ou a disponibilidade das informações e dos sistemas organizacionais. Esses riscos abrangem desde ataques direcionados a infraestruturas críticas até incidentes relacionados a falhas humanas, vulnerabilidades tecnológicas e acessos não autorizados.

A presença desses riscos influencia diretamente os processos decisórios ao introduzir elementos de incerteza que podem afetar o alcance dos objetivos organizacionais. Nesse contexto, gestores precisam avaliar constantemente os possíveis impactos financeiros, operacionais, jurídicos e reputacionais associados às ameaças digitais, incorporando tais fatores ao planejamento estratégico e à gestão de riscos.

Além disso, a possibilidade de interrupções operacionais decorrentes de incidentes cibernéticos faz com que organizações adotem decisões voltadas ao fortalecimento de sua resiliência. Investimentos em infraestrutura tecnológica, treinamento de colaboradores, monitoramento contínuo e planos de resposta a incidentes passaram a integrar a agenda estratégica de diversas organizações. Essa realidade evidencia que a gestão dos riscos cibernéticos não se limita à prevenção de ataques, mas também envolve a capacidade de preparação, resposta e recuperação frente a eventos que possam comprometer a continuidade dos negócios.

Outro aspecto relevante refere-se à influência dos riscos cibernéticos sobre decisões relacionadas à inovação e à transformação digital. Embora novas tecnologias proporcionem ganhos de eficiência e competitividade, sua implementação também pode ampliar a exposição a vulnerabilidades. Dessa forma, gestores precisam equilibrar oportunidades de inovação com a necessidade de proteção dos ativos informacionais.

Além dos impactos operacionais e tecnológicos, os riscos cibernéticos também influenciam a priorização de recursos e investimentos organizacionais. Em muitos casos, gestores precisam decidir entre ampliar iniciativas de inovação, expansão de mercado ou fortalecimento dos mecanismos de segurança. Essa necessidade de balancear oportunidades de crescimento e proteção dos ativos informacionais evidencia que a gestão dos riscos cibernéticos está

diretamente relacionada à alocação estratégica de recursos e à definição das prioridades organizacionais. Assim, a cibersegurança passa a influenciar não apenas decisões relacionadas à tecnologia, mas também escolhas que afetam o desempenho e a sustentabilidade das organizações no longo prazo.

A conformidade regulatória também exerce influência significativa sobre as decisões organizacionais. A existência de legislações relacionadas à proteção de dados e à segurança da informação, como a Lei Geral de Proteção de Dados (LGPD), exige que organizações adotem medidas adequadas de proteção, influenciando investimentos, processos internos e mecanismos de governança.

Nesse cenário, observa-se que a gestão dos riscos cibernéticos tornou-se parte integrante da tomada de decisão estratégica. Organizações que conseguem identificar, avaliar e mitigar adequadamente esses riscos tendem a apresentar maior capacidade de adaptação, continuidade operacional e sustentabilidade em ambientes cada vez mais dependentes da tecnologia.

Tabela 3 – Impactos dos riscos cibernéticos sobre as decisões organizacionais

Tipo de risco	Possíveis consequências	Impacto na tomada de decisão
Vazamento de dados	Exposição de informações sensíveis	Reforço de investimentos em proteção de dados
Ransomware	Paralisação de operações	Priorização de continuidade dos negócios

Phishing	Comprometimento de credenciais	Fortalecimento de treinamentos e controles internos
Falhas em sistemas	Interrupções operacionais	Revisão de infraestrutura tecnológica
Descumprimento regulatório	Multas e sanções legais	Aumento das ações de conformidade
Ataques à reputação digital	Perda de confiança de stakeholders	Revisão de estratégias de comunicação e governança
Vulnerabilidades em terceiros	Comprometimento da cadeia de suprimentos	Reavaliação de fornecedores e parceiros estratégicos

Fonte: Elaborado pelo autor (2026), com base na literatura sobre gestão de riscos cibernéticos.

A Tabela 3 demonstra que os riscos cibernéticos podem afetar diferentes áreas organizacionais e influenciar diretamente os processos decisórios. Observa-se que os impactos associados a incidentes de segurança vão além dos aspectos tecnológicos, alcançando dimensões financeiras, operacionais, jurídicas e reputacionais. Essa realidade reforça a necessidade de incorporar a gestão dos riscos cibernéticos ao planejamento estratégico, permitindo decisões mais alinhadas aos objetivos organizacionais e à sustentabilidade dos negócios. Além disso, a diversidade dos riscos apresentados evidencia que a cibersegurança deve ser tratada de forma

integrada à governança corporativa, à gestão de riscos e aos processos de tomada de decisão, fortalecendo a capacidade das organizações de responder a ameaças e manter sua competitividade em ambientes digitais.

5.3 Integração entre segurança da informação e estratégia

A crescente relevância da cibersegurança no ambiente organizacional ampliou sua integração com práticas de governança corporativa, conformidade regulatória e continuidade dos negócios. Em um cenário caracterizado pela intensificação dos riscos digitais, as organizações passaram a reconhecer que a proteção das informações não deve ser tratada apenas como uma responsabilidade técnica, mas como um elemento essencial para a sustentabilidade organizacional.

Nesse contexto, a integração entre segurança da informação e estratégia organizacional ocorre quando os objetivos relacionados à proteção dos ativos informacionais passam a ser considerados durante a formulação e implementação das estratégias corporativas. Em vez de atuar de forma isolada, a segurança da informação passa a apoiar decisões relacionadas à inovação, expansão de mercado, transformação digital e gestão de riscos. Essa integração favorece maior alinhamento entre tecnologia e objetivos organizacionais, contribuindo para decisões mais consistentes e para a criação de valor sustentável no longo prazo.

A governança corporativa desempenha papel fundamental nesse contexto ao estabelecer mecanismos de controle, monitoramento e direcionamento estratégico. Quando integrada à cibersegurança, a governança contribui para o alinhamento entre objetivos organizacionais e práticas de proteção da informação, favorecendo uma gestão mais eficiente dos riscos e fortalecendo os processos de tomada de decisão.

Além disso, a conformidade regulatória tornou-se um aspecto cada vez mais relevante para as organizações. A criação de legislações voltadas à proteção de dados e à segurança da informação, como a Lei Geral de Proteção de Dados (LGPD), ampliou a necessidade de implementação de políticas, procedimentos e controles capazes de garantir o tratamento adequado das informações. Nesse sentido, a conformidade não deve ser compreendida apenas como uma obrigação legal, mas também como um mecanismo capaz de fortalecer a confiança de clientes, parceiros e investidores.

Outro aspecto importante refere-se à continuidade dos negócios. A ocorrência de incidentes cibernéticos pode comprometer operações críticas, gerar interrupções significativas e provocar impactos financeiros e reputacionais. Dessa forma, as organizações têm investido em estratégias de resiliência, incluindo planos de contingência, recuperação de desastres e mecanismos de resposta a incidentes, visando minimizar os efeitos de possíveis eventos adversos. A integração entre segurança da informação e continuidade dos negócios permite que as organizações desenvolvam maior capacidade de antecipação e resposta frente a cenários de crise, fortalecendo sua estabilidade operacional e sua capacidade de adaptação em ambientes altamente dinâmicos.

Além dos aspectos relacionados à proteção e à conformidade, a integração entre segurança da informação e estratégia organizacional contribui para que as organizações desenvolvam uma visão mais preventiva dos riscos. Essa abordagem permite antecipar vulnerabilidades, fortalecer mecanismos de controle e aumentar a capacidade de resposta frente a ameaças digitais. Como consequência, a segurança da informação passa a atuar como elemento de suporte à competitividade organizacional e à sustentabilidade dos negócios.

A integração entre governança, conformidade, continuidade dos negócios e segurança da informação contribui para uma abordagem mais abrangente da cibersegurança. Em vez de atuar apenas de forma reativa, as organizações passam a desenvolver capacidades preventivas e estratégicas, fortalecendo sua capacidade de adaptação frente aos desafios do ambiente digital.

Dessa forma, observa-se que a cibersegurança exerce influência significativa sobre a governança organizacional, os processos de conformidade e as estratégias de continuidade dos negócios. Essa integração favorece decisões mais seguras, reduz vulnerabilidades e contribui para a construção de organizações mais resilientes e preparadas para enfrentar os desafios associados à transformação digital.

5.4 Governança, Compliance e Cibersegurança

A governança corporativa desempenha papel fundamental na definição de diretrizes, controles e práticas que orientam a gestão das organizações, garantindo transparência, responsabilidade e alinhamento entre os interesses dos diferentes stakeholders. Em um ambiente caracterizado pela crescente digitalização dos processos organizacionais, a cibersegurança passou a integrar as discussões relacionadas à governança, assumindo posição estratégica na proteção dos ativos informacionais e na gestão dos riscos corporativos.

Essa perspectiva é corroborada por estudos recentes que apontam a crescente necessidade de incorporar a governança da cibersegurança aos processos decisórios da alta administração. Modi, Kuzminykh e Ghita (2023) destacam que conselhos de administração e executivos ainda enfrentam dificuldades para traduzir riscos cibernéticos em informações estratégicas capazes de subsidiar decisões organizacionais, evidenciando a necessidade de modelos de governança que aproximem aspectos técnicos das prioridades estratégicas da organização.

A integração entre governança e cibersegurança está diretamente relacionada à necessidade de estabelecer políticas, procedimentos e mecanismos de controle capazes de assegurar a proteção das informações e a continuidade das operações. Nesse contexto, a segurança da informação deixa de ser uma responsabilidade exclusiva das áreas técnicas e passa a envolver a alta administração, que assume papel relevante na definição de diretrizes estratégicas, na supervisão dos riscos cibernéticos e na promoção de uma cultura organizacional voltada à segurança.

Além da governança, o conceito de compliance ganhou destaque como instrumento essencial para garantir a conformidade das organizações com normas, leis e regulamentos aplicáveis. No contexto da cibersegurança, o compliance está diretamente associado à adoção de medidas que assegurem a proteção de dados, a privacidade das informações e o cumprimento das exigências regulatórias. A Lei Geral de Proteção de Dados (LGPD), por exemplo, ampliou a necessidade de implementação de controles e práticas capazes de garantir o tratamento adequado das informações pessoais.

De acordo com o Institute of Internal Auditors (IIA, 2018), uma estrutura de governança eficaz deve incorporar a gestão de riscos como parte integrante dos processos organizacionais. Essa abordagem inclui os riscos cibernéticos, que passaram a representar uma das principais ameaças à continuidade dos negócios e à sustentabilidade organizacional. Dessa forma, a integração entre governança, compliance e gestão de riscos contribui para decisões mais seguras e alinhadas aos objetivos estratégicos da organização.

Outro aspecto relevante refere-se à adoção de frameworks e padrões internacionais voltados à segurança da informação. Modelos como a ISO/IEC 27001 oferecem diretrizes para a implementação de sistemas de gestão da segurança da informação, contribuindo para a

estruturação de processos, definição de responsabilidades e fortalecimento dos mecanismos de controle. A utilização dessas boas práticas auxilia as organizações na identificação de vulnerabilidades, na mitigação de riscos e na promoção da conformidade regulatória. Além disso, a adoção de frameworks reconhecidos internacionalmente favorece a padronização dos processos de segurança, amplia a maturidade organizacional e fortalece a capacidade de tomada de decisão baseada em práticas estruturadas de gestão de riscos.

Além dos benefícios relacionados à proteção dos ativos informacionais, a integração entre governança, compliance e cibersegurança fortalece a confiança de clientes, investidores e parceiros comerciais. Organizações que demonstram maturidade em segurança da informação tendem a apresentar maior credibilidade institucional e melhor capacidade de adaptação frente às exigências de um ambiente cada vez mais regulado e dependente da tecnologia.

Dessa forma, observa-se que a governança e o compliance desempenham papel essencial na consolidação da cibersegurança como elemento estratégico nas organizações. Ao integrar esses aspectos à gestão organizacional, as empresas tornam-se mais preparadas para enfrentar desafios relacionados à segurança da informação, fortalecer sua resiliência e sustentar decisões alinhadas aos objetivos de longo prazo.

5.5 LGPD e Risco Estratégico nas Organizações

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), conhecida como LGPD, representa um marco regulatório no tratamento de dados pessoais no Brasil, estabelecendo diretrizes que impactam diretamente a forma como as organizações coletam, armazenam, processam e utilizam informações. Nesse contexto, a proteção de dados deixa de ser apenas uma exigência legal e passa a assumir caráter estratégico, influenciando decisões relacionadas à gestão, inovação e competitividade organizacional.

A LGPD impõe às organizações a responsabilidade de adotar medidas técnicas e administrativas capazes de garantir a segurança das informações pessoais, reduzindo riscos relacionados a vazamentos, acessos indevidos, perdas de dados e utilização inadequada de informações. O descumprimento dessas normas pode resultar em sanções administrativas, multas financeiras, restrições operacionais e impactos negativos sobre a reputação institucional.

Dessa forma, o risco associado à proteção de dados passa a integrar o conjunto de riscos estratégicos das organizações. A necessidade de conformidade com a legislação exige que decisões relacionadas à tecnologia, processos internos, armazenamento de dados e desenvolvimento de serviços digitais sejam tomadas de forma mais criteriosa, considerando não apenas aspectos operacionais, mas também implicações legais, financeiras e reputacionais.

De acordo com a Lei nº 13.709/2018 (Brasil, 2018), as organizações devem implementar práticas de governança e segurança da informação capazes de assegurar a proteção dos dados pessoais, incluindo políticas internas, controles de acesso, mecanismos de monitoramento e procedimentos para tratamento de incidentes. Essas exigências reforçam a importância da integração entre cibersegurança, compliance e estratégia organizacional.

Além dos aspectos regulatórios, a LGPD influencia diretamente a tomada de decisão estratégica ao exigir maior transparência, responsabilidade e prestação de contas no tratamento das informações. Decisões relacionadas à inovação tecnológica, transformação digital e expansão de serviços passam a considerar os riscos associados à privacidade e à proteção de dados, influenciando tanto a velocidade quanto a direção das estratégias organizacionais. Nesse contexto, a conformidade com a LGPD deixa de representar apenas

uma obrigação legal e passa a atuar como fator de suporte à gestão estratégica, contribuindo para decisões mais seguras, redução de riscos e fortalecimento da confiança dos stakeholders.

Outro aspecto relevante refere-se à confiança dos stakeholders. Em um ambiente cada vez mais orientado por dados, organizações que demonstram compromisso com a proteção das informações tendem a fortalecer sua credibilidade perante clientes, investidores, parceiros e órgãos reguladores. Dessa forma, a conformidade com a LGPD pode contribuir não apenas para a redução de riscos, mas também para a construção de vantagens competitivas e fortalecimento da imagem institucional.

Assim, a LGPD consolida a proteção de dados como um fator estratégico para as organizações contemporâneas, exigindo uma postura mais estruturada e integrada na gestão dos riscos digitais. Compreender essa relação é fundamental para o desenvolvimento de estratégias capazes de equilibrar inovação, segurança, conformidade regulatória e geração de valor em um ambiente cada vez mais dependente da informação.

Quadro 4 – Impactos Estratégicos da LGPD nas Organizações

Dimensão	**Impacto Organizacional**
Jurídica	Redução do risco de sanções e penalidades regulatórias.
Operacional	Fortalecimento dos controles internos e da proteção de dados.
Estratégica	Maior suporte à tomada de decisão e à gestão de riscos.

Reputacional	Aumento da confiança de clientes, parceiros e demais stakeholders.
Competitiva	Fortalecimento da imagem institucional e diferenciação no mercado.

Fonte: Elaborado pelo autor (2026).

O Quadro 3 evidencia que os impactos da LGPD ultrapassam a dimensão jurídica e alcançam aspectos operacionais, estratégicos, reputacionais e competitivos. Observa-se que a conformidade com a legislação contribui não apenas para a redução de riscos regulatórios, mas também para o fortalecimento da governança, da confiança dos stakeholders e da qualidade dos processos decisórios. Além disso, a adequação às exigências da LGPD favorece a construção de uma cultura organizacional orientada à proteção de dados, ampliando a capacidade das organizações de atuar de forma segura, transparente e sustentável em ambientes digitais. Dessa forma, a proteção de dados passa a representar um elemento estratégico para a sustentabilidade organizacional.

5.6 Continuidade de Negócios e Resiliência Organizacional

A continuidade de negócios e a resiliência organizacional têm se tornado aspectos centrais na gestão estratégica das organizações, especialmente em um cenário caracterizado por riscos crescentes, transformação digital e elevada dependência de sistemas de informação. Nesse contexto, a cibersegurança assume papel fundamental, uma vez que incidentes cibernéticos podem comprometer operações críticas, impactando diretamente a capacidade das organizações de manter suas atividades e alcançar seus objetivos estratégicos.

A continuidade de negócios refere-se à capacidade de uma organização de manter suas operações essenciais mesmo diante de eventos adversos, como falhas tecnológicas, desastres naturais, erros humanos ou ataques cibernéticos. Para isso, torna-se necessário o desenvolvimento de planos estruturados que contemplem ações de prevenção, resposta e recuperação de incidentes, garantindo a minimização dos impactos e a rápida retomada das atividades organizacionais.

Nesse sentido, a cibersegurança está diretamente relacionada à continuidade operacional, pois a proteção dos sistemas e dados é essencial para evitar interrupções nos processos organizacionais. A ausência de medidas adequadas de segurança pode resultar em paralisações significativas, perda de informações estratégicas, comprometimento da confiança dos clientes e prejuízos financeiros capazes de afetar a sustentabilidade da organização.

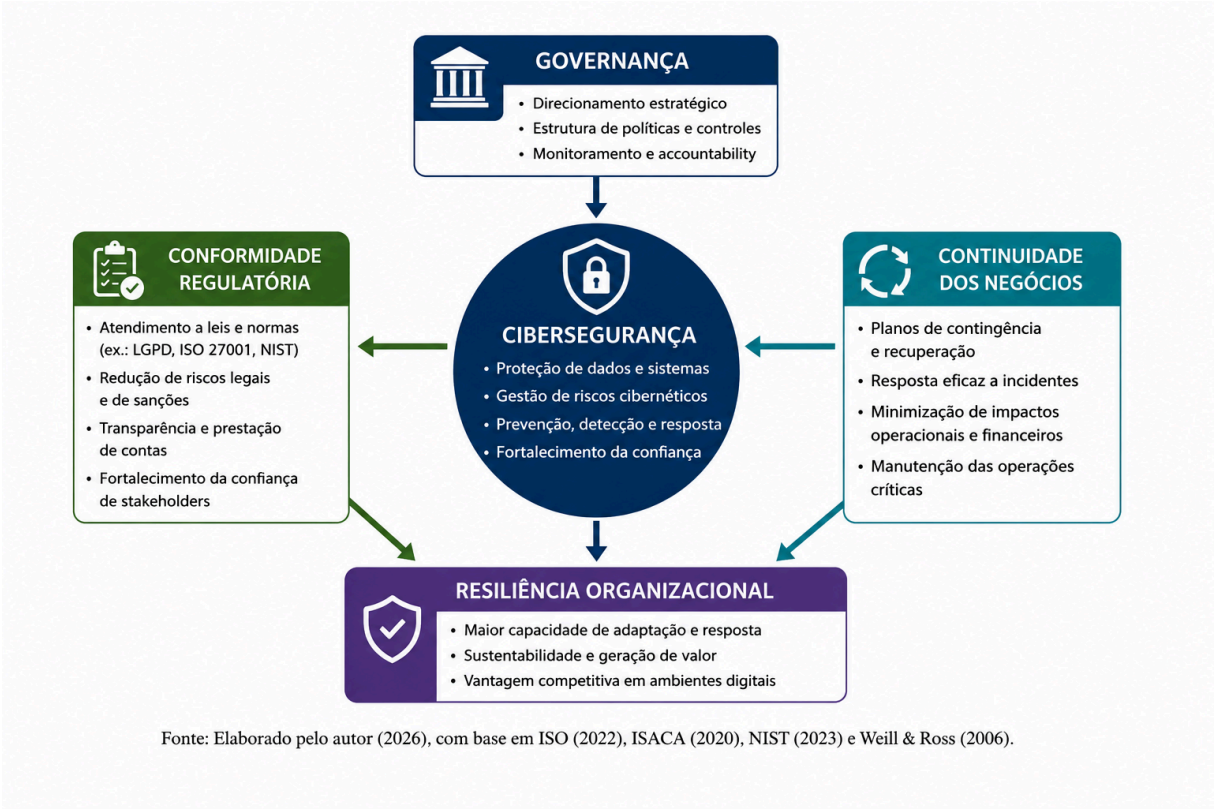
De acordo com a ISO 22301 (2019), norma internacional voltada à gestão da continuidade de negócios, as organizações devem implementar sistemas que permitam identificar riscos, avaliar impactos e estabelecer estratégias para garantir a resiliência frente a eventos disruptivos. Essa abordagem reforça a importância de integrar a cibersegurança aos planos de continuidade, considerando os riscos digitais como parte relevante do ambiente organizacional contemporâneo.

Além dos aspectos operacionais, a continuidade de negócios também influencia a tomada de decisão estratégica. Organizações que possuem estruturas robustas de gestão de riscos e planos de resposta a incidentes tendem a tomar decisões com maior segurança e previsibilidade, reduzindo os impactos associados a eventos inesperados. Dessa forma, a resiliência organizacional passa a representar não apenas uma capacidade de recuperação, mas também uma vantagem estratégica em ambientes marcados pela incerteza.

A resiliência organizacional envolve ainda a capacidade de adaptação e aprendizado frente a mudanças e crises. Organizações resilientes não apenas conseguem superar eventos adversos, mas também utilizam essas experiências para aprimorar processos, fortalecer mecanismos de controle e desenvolver maior capacidade de resposta frente a novos desafios. Nesse contexto, a gestão dos riscos cibernéticos contribui para a construção de uma cultura organizacional mais preparada para enfrentar ameaças e aproveitar oportunidades de melhoria. Além disso, a capacidade de aprender com incidentes e incorporar esse conhecimento aos processos organizacionais fortalece a tomada de decisão estratégica, permitindo respostas mais rápidas e eficazes diante de cenários de incerteza.

Dessa forma, a continuidade de negócios e a resiliência organizacional estão diretamente relacionadas à eficácia das práticas de cibersegurança adotadas pelas organizações. Ao integrar esses elementos à estratégia organizacional, as empresas tornam-se mais preparadas para enfrentar desafios, proteger seus ativos, sustentar a continuidade operacional e manter sua competitividade em um ambiente cada vez mais complexo e dependente da tecnologia.

Figura 4 – Integração entre Governança, Cibersegurança, Conformidade e Continuidade dos Negócios



Fonte: Elaborado pelo autor (2026), com base em ISO (2022), ISACA (2020), NIST (2023) e Weill & Ross (2006).

A Figura 4 demonstra que a cibersegurança atua como elemento integrador entre governança, conformidade regulatória e continuidade dos negócios. Observa-se que essas dimensões não operam de forma isolada, mas se complementam na construção da resiliência organizacional. Dessa forma, organizações que desenvolvem práticas estruturadas de segurança da informação tendem a apresentar maior capacidade de adaptação, melhor gestão de riscos e maior sustentabilidade em ambientes caracterizados por elevada complexidade tecnológica.

5.7 Síntese Analítica dos Achados da Revisão

A análise integrada da literatura evidencia que a cibersegurança passou por uma significativa evolução conceitual nas últimas décadas, deixando de ser compreendida apenas como um conjunto de mecanismos técnicos de proteção da informação para assumir papel estratégico na gestão organizacional. Os estudos analisados convergem

ao reconhecer que a crescente dependência das tecnologias digitais ampliou a exposição das organizações a riscos cibernéticos, tornando indispensável a incorporação da segurança da informação aos processos de planejamento e tomada de decisão.

Embora exista consenso quanto à importância da cibersegurança para a sustentabilidade das organizações, a literatura não apresenta uniformidade quanto ao seu posicionamento na estrutura organizacional. Parte dos estudos e normas internacionais enfatiza a cibersegurança como função de governança, vinculada à gestão de riscos, à conformidade regulatória e ao nível estratégico das organizações. Por outro lado, ainda são encontrados trabalhos que a tratam predominantemente como atividade operacional, concentrada na área de Tecnologia da Informação. Essa diferença de abordagem evidencia que o processo de consolidação da cibersegurança como tema estratégico ainda está em evolução, especialmente em organizações que se encontram em diferentes níveis de maturidade digital.

Observou-se que autores da Administração Estratégica enfatizam a necessidade de integrar a gestão dos riscos ao processo decisório, enquanto estudos específicos de cibersegurança direcionam maior atenção à proteção dos ativos informacionais, à continuidade dos negócios e à conformidade regulatória. Embora essas perspectivas possuam enfoques distintos, verificou-se forte complementaridade entre elas, indicando que a efetividade da gestão organizacional depende da articulação entre capacidades estratégicas, governança, inovação tecnológica e mecanismos de proteção digital.

Outro aspecto evidenciado pela revisão refere-se à crescente aproximação entre cibersegurança, governança corporativa e gestão de riscos. A literatura demonstra que organizações com estruturas de governança mais consolidadas tendem a incorporar a gestão dos riscos cibernéticos de forma mais sistemática aos processos decisórios, favorecendo maior capacidade de resposta a incidentes, redução de vulnerabilidades e fortalecimento da resiliência organizacional.

Também se verificou que a produção científica recente ainda apresenta espaço para aprofundar investigações acerca da influência da cibersegurança sobre as decisões estratégicas propriamente ditas. Grande parte dos estudos concentra-se em aspectos tecnológicos, normativos ou operacionais, enquanto permanecem relativamente limitadas as pesquisas que analisam a interação entre cibersegurança, formulação estratégica, comportamento dos gestores e geração de vantagem competitiva, especialmente no contexto das organizações brasileiras.

Dessa forma, os achados desta revisão permitem compreender que a cibersegurança deve ser interpretada como elemento transversal à gestão organizacional, influenciando não apenas a proteção dos ativos digitais, mas também a qualidade das decisões estratégicas, a sustentabilidade dos negócios e a capacidade das organizações de responder às constantes transformações do ambiente competitivo e tecnológico. Assim, a revisão realizada permitiu responder ao problema de pesquisa ao evidenciar que a cibersegurança influencia a tomada de decisão estratégica por meio da gestão de riscos, da governança corporativa, da proteção dos ativos informacionais e do fortalecimento da resiliência organizacional.

6. Considerações Finais

O presente estudo teve como objetivo analisar de que forma a cibersegurança influencia a tomada de decisão estratégica em organizações brasileiras, considerando o contexto da transformação digital e o aumento dos riscos associados ao ambiente tecnológico. A partir da revisão da literatura, foi possível compreender que a cibersegurança deixou de ser uma questão exclusivamente técnica, passando a ocupar uma posição estratégica nas organizações e influenciando diretamente processos relacionados à gestão, governança e tomada de decisão.

Os resultados evidenciam que a crescente dependência de sistemas digitais e a ampliação das ameaças cibernéticas têm impactado significativamente os processos decisórios, exigindo das organizações uma abordagem mais integrada entre gestão de riscos, governança corporativa e planejamento estratégico. Nesse contexto, a cibersegurança influencia decisões relacionadas à alocação de recursos, adoção de tecnologias, proteção de dados, conformidade regulatória e definição de diretrizes organizacionais.

Além disso, observou-se que a incorporação da cibersegurança à estratégia organizacional contribui para a mitigação de riscos, o fortalecimento da governança e a garantia da continuidade dos negócios. Aspectos como compliance regulatório, especialmente no que se refere à Lei Geral de Proteção de Dados (LGPD), e a implementação de práticas estruturadas de segurança da informação destacam-se como fatores essenciais para a sustentabilidade organizacional e para a construção de ambientes corporativos mais seguros e resilientes.

Outro ponto relevante refere-se à necessidade de desenvolvimento de uma cultura organizacional voltada à segurança da informação, envolvendo todos os níveis da organização na proteção dos ativos informacionais. Essa abordagem reforça a importância de integrar a

cibersegurança aos processos estratégicos, promovendo maior capacidade de adaptação frente às constantes mudanças e desafios do ambiente digital.

Do ponto de vista teórico, o estudo contribui para a aproximação entre os campos da cibersegurança e da gestão estratégica, evidenciando a necessidade de abordagens interdisciplinares para compreender os impactos dos riscos digitais sobre as organizações contemporâneas. Sob a perspectiva prática, os resultados podem auxiliar gestores e organizações na formulação de estratégias mais seguras, alinhadas às exigências regulatórias e aos desafios decorrentes da transformação digital.

Como limitação, destaca-se o fato de a pesquisa ter sido baseada exclusivamente em revisão bibliográfica, não contemplando análise empírica. Dessa forma, sugere-se que estudos futuros explorem pesquisas de campo, estudos de caso ou abordagens quantitativas capazes de aprofundar a compreensão da relação entre cibersegurança, gestão de riscos e tomada de decisão estratégica em diferentes contextos organizacionais.

Do ponto de vista gerencial, os achados desta pesquisa reforçam que a incorporação da cibersegurança aos processos de planejamento estratégico pode contribuir para decisões organizacionais mais seguras, maior capacidade de prevenção de riscos, fortalecimento da governança corporativa e ampliação da resiliência organizacional. Para gestores brasileiros, especialmente em organizações que enfrentam crescente digitalização de seus processos, a integração entre segurança da informação, gestão de riscos e estratégia representa importante instrumento para apoiar decisões relacionadas à alocação de recursos, conformidade regulatória, continuidade dos negócios e proteção da reputação institucional.

Como possibilidades para pesquisas futuras, recomenda-se a realização de estudos empíricos envolvendo organizações brasileiras de diferentes setores econômicos, bem como pesquisas

com gestores e executivos responsáveis por decisões estratégicas relacionadas à cibersegurança. Também se mostram promissoras investigações comparativas entre organizações com diferentes níveis de maturidade em governança digital e gestão de riscos cibernéticos, contribuindo para ampliar as evidências sobre a influência da cibersegurança na formulação de estratégias organizacionais.

Conclui-se, portanto, que o objetivo proposto foi alcançado e que a questão de pesquisa foi respondida ao demonstrar que a cibersegurança exerce influência significativa sobre a tomada de decisão estratégica nas organizações. Mais do que um mecanismo de proteção tecnológica, a cibersegurança consolidou-se como um elemento estratégico capaz de apoiar a gestão de riscos, fortalecer a governança, garantir a continuidade dos negócios e contribuir para a construção de organizações mais resilientes, competitivas e preparadas para os desafios da transformação digital.

7. Referências

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). *Digital business strategy: Toward a next generation of insights*. *MIS Quarterly, 37*(2), 471–482.

Brasil. (2018). *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União.

Cybersecurity Ventures. (2023). *Cybercrime damages to hit $10.5 trillion annually by 2025*. https://cybersecurityventures.com

Dacorogna, M., & Kratz, M. (2023). *Managing cyber risk, a science in the making*. arXiv. https://doi.org/10.48550/arXiv.2303.12939

Gil, A. C. (2019). *Métodos e técnicas de pesquisa social* (7ª ed.). Atlas.

IBM Security. (2024). *Cost of a data breach report 2024*. IBM Corporation. https://www.ibm.com/reports/data-breach

Institute of Internal Auditors. (2018). *International Professional Practices Framework (IPPF).* The Institute of Internal Auditors.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements.* ISO.

International Organization for Standardization. (2019). *ISO 22301: Security and resilience — Business continuity management systems — Requirements.* ISO.

International Organization for Standardization. (2022). *ISO 22301:2022 Security and resilience — Business continuity management systems — Requirements.* ISO.

ISACA. (2020). *COBIT 2019 Framework: Governance and Management Objectives.* ISACA.

Mintzberg, H. (2000). *Safári de estratégia: Um roteiro pela selva do planejamento estratégico.* Bookman.

Modi, A., Kuzminykh, I., & Ghita, B. (2023). *Data driven approaches to cybersecurity governance for board decision-making: A systematic review*. arXiv. https://doi.org/10.48550/arXiv.2311.17578

National Institute of Standards and Technology. (2023). *Cybersecurity framework (CSF) 2.0.* U.S. Department of Commerce.

Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance.* Free Press.

Senge, P. M. (1990). *The fifth discipline: The art and practice of the learning organization.* Doubleday.

Simon, H. A. (1979). Rational decision making in business organizations. *American Economic Review, 69*(4), 493–513.

Vrhovec, S., & Markelj, B. (2024). *We need to aim at the top: Factors associated with cybersecurity awareness of cyber and information security decision-makers*. arXiv. https://doi.org/10.48550/arXiv.2404.04725

Weill, P., & Ross, J. W. (2006). *IT governance: How top performers manage IT decision rights for superior results.* Harvard Business School Press.

World Economic Forum. (2023). *Global risks report 2023.* World Economic Forum.

8. Glossário

Cibersegurança: Conjunto de práticas, tecnologias e processos voltados à proteção de sistemas, redes e dados contra acessos não autorizados, ataques e danos no ambiente digital.

Segurança da Informação: Área responsável pela proteção das informações, garantindo sua confidencialidade, integridade e disponibilidade, independentemente do meio em que estejam armazenadas ou transmitidas.

Confidencialidade: Princípio da segurança da informação que assegura que os dados sejam acessados apenas por indivíduos autorizados.

Integridade: Garantia de que as informações permanecem corretas, completas e não foram alteradas de forma indevida.

Disponibilidade: Princípio que assegura que as informações e sistemas estejam acessíveis sempre que necessário.

Tomada de Decisão Estratégica: Processo de escolha que envolve decisões de longo prazo, com impacto significativo na direção e no desempenho da organização.

Gestão de Riscos: Processo de identificação, análise e controle de riscos que podem afetar os objetivos organizacionais.

Governança Corporativa: Conjunto de práticas e mecanismos que orientam a gestão organizacional, garantindo transparência, responsabilidade e alinhamento entre stakeholders.

Compliance: Conjunto de ações destinadas a garantir que a organização esteja em conformidade com leis, normas e regulamentos aplicáveis.

LGPD (Lei Geral de Proteção de Dados): Legislação brasileira que regula o tratamento de dados pessoais, estabelecendo direitos e deveres para organizações e indivíduos.

Riscos Cibernéticos: Possibilidade de ocorrência de eventos adversos relacionados à segurança digital, como ataques, invasões ou vazamento de dados.

Continuidade de Negócios: Capacidade da organização de manter suas operações essenciais mesmo diante de eventos adversos.

Resiliência Organizacional: Capacidade da organização de se adaptar, responder e se recuperar de situações de crise ou mudanças no ambiente.

Transformação Digital: Processo de integração de tecnologias digitais nas atividades organizacionais, alterando a forma como as empresas operam e geram valor.

Estratégia Organizacional: Conjunto de decisões e ações que definem a direção da organização e sua forma de atuação no ambiente competitivo.

Stakeholders: Indivíduos, grupos ou organizações que possuem interesse direto ou indireto nas atividades, decisões e resultados de uma organização, podendo influenciar ou ser influenciados por suas ações.

9. Apêndice

Este apêndice apresenta a relação entre o problema de pesquisa, os objetivos propostos e os principais temas desenvolvidos ao longo do trabalho, evidenciando a lógica utilizada na construção da investigação.

O problema de pesquisa consistiu em compreender de que forma a cibersegurança influencia a tomada de decisão estratégica em organizações brasileiras, considerando o contexto da transformação digital e o aumento dos riscos associados ao ambiente tecnológico.

Para responder a essa questão, foi estabelecido como objetivo geral analisar a influência da cibersegurança sobre a tomada de decisão estratégica nas organizações, analisando seus impactos sobre a gestão de riscos, a governança corporativa, a conformidade regulatória e a continuidade dos negócios.

O desenvolvimento do estudo foi estruturado em três eixos centrais. O primeiro eixo abordou os fundamentos teóricos da cibersegurança e da segurança da informação, apresentando conceitos essenciais, evolução das ameaças digitais e a importância da proteção dos ativos informacionais no contexto organizacional.

O segundo eixo concentrou-se na análise da gestão estratégica e dos processos de tomada de decisão, explorando conceitos relacionados à formulação de estratégias, gestão

organizacional, vantagem competitiva e fatores que influenciam o processo decisório nas organizações contemporâneas.

O terceiro eixo promoveu a integração entre os temas centrais da pesquisa, discutindo os impactos da cibersegurança na gestão estratégica, os riscos cibernéticos, a governança corporativa, o compliance, a Lei Geral de Proteção de Dados (LGPD), a continuidade dos negócios e a resiliência organizacional. Esse eixo permitiu compreender como a cibersegurança ultrapassa a dimensão técnica e passa a atuar como elemento estratégico para a sustentabilidade e competitividade das organizações.

A estrutura adotada possibilitou uma análise integrada da literatura, permitindo identificar relações entre cibersegurança e tomada de decisão estratégica e evidenciar a importância da incorporação da segurança da informação aos processos de gestão organizacional. Dessa forma, buscou-se garantir alinhamento entre o problema de pesquisa, os objetivos definidos e os resultados apresentados nas considerações finais.