ReGeo ISSN: 2177-3246

GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO NO EXÉRCITO BRASILEIRO: UMA REVISÃO SISTEMÁTICA DA LITERATURA NO CONTEXTO DA DEFESA CIBERNÉTICA

GOVERNANCE AND INFORMATION SECURITY IN THE BRAZILIAN ARMY: A SYSTEMATIC LITERATURE REVIEW IN THE CONTEXT OF CYBERSECURITY

GOBERNANZA Y SEGURIDAD DE LA INFORMACIÓN EN EL EJÉRCITO BRASILEÑO: UNA REVISIÓN SISTEMÁTICA DE LA LITERATURA EN EL CONTEXTO DE LA CIBERSEGURIDAD

https://doi.org/10.56238/revgeov17n8-188

Data de submissão: 20/07/2026 **Data de publicação:** 20/08/2026

Rômulo Ferreira dos Santos
Instituição: Universidade de Brasília - Brasília
E-mail: romulo.santos@ieee.org
Orcid: https://orcid.org/0009-0001-3588-7583

Anderson Lellis Alves Moura
Instituição: Gabinete do Comandante do Exército - Brasília
E-mail: moura.anderson@gabcmt.eb.mil.br

Jaime de Melo Gama da Silva
Instituição: Universidade de Brasília - Brasília
E-mail: jaime.silva@aluno.unb.br

Marcelo Lopes Pereira Junior
Instituição: Universidade de Brasília - Brasília
E-mail: marcelo.lopes@unb.br
Orcid: https://orcid.org/0000-0001-9058-510X

RESUMO

Este artigo analisa como os marcos teóricos, normativos e metodológicos de governança e segurança da informação influenciam a formulação de políticas nos órgãos de assessoria estratégica do Exército Brasileiro, considerando as especificidades do ambiente militar e os desafios contemporâneos da Defesa Cibernética. Para isso, foi realizada uma Revisão Sistemática da Literatura, orientada pelo protocolo PRISMA 2020, contemplando estudos científicos e documentos institucionais relacionados à governança de TI, segurança da informação, cibersegurança e Defesa. Os resultados indicam que referenciais como COBIT, ISO/IEC 27001, ISO/IEC 27002 e documentos estratégicos nacionais contribuem para estruturar políticas, mecanismos de controle, gestão de riscos e práticas de conformidade. Contudo, a literatura evidencia alinhamento normativo ainda parcial, lacunas de maturidade e dificuldades de operacionalização em ambientes militares. A análise também aponta a necessidade de governança multinível, integração entre dimensões estratégicas, táticas e operacionais, além do equilíbrio entre centralização militar e cooperação multissetorial. Como contribuição, o estudo propõe diretrizes para fortalecer a governança e a segurança da informação no contexto da Defesa Cibernética, com ênfase em alinhamento normativo, *accountability*, gestão de riscos, auditoria, capacitação, integração interagências e proteção de informações sem síveis.

Palavras-chave: Governança. Segurança da Informação. Defesa Cibernética. Exército Brasileiro. Revisão Sistemática da Literatura.

ABSTRACT
This article analyzes how theoretical, normative, and methodological frameworks for governance and information security influence policy formulation within the Brazilian Army's strategic advisory bodies, taking into account the specific characteristics of the military environment and the contemporary challenges of cyber defense. To this end, a Systematic Literature Review was conducted, guided by the PRISMA 2020 protocol, encompassing scientific studies and institutional documents related to IT governance, information security, cybersecurity, and defense. The results indicate that frameworks such as COBIT, ISO/IEC 27001, ISO/IEC 27002, and national strategic documents contribute to structuring policies, control mechanisms, risk management, and compliance practices. However, the literature highlights still partial regulatory alignment, maturity gaps, and difficulties in operationalization within military environments. The analysis also points to the need for multilevel governance, integration between strategic, tactical, and operational dimensions, as well as a balance between military centralization and multisectoral cooperation. As a contribution, the study proposes guidelines to strengthen governance and information security in the context of Cyber Defense, with an emphasis on regulatory alignment, accountability, risk management, auditing, training, interagency integration, and the protection of sensitive information.

Keywords: Governance. Information Security. Cyber Defense. Brazilian Army. Systematic Literature Review.

RESUMEN
Este artículo analiza cómo los marcos teóricos, normativos y metodológicos de gobernanza y seguridad de la información influyen en la formulación de políticas en los órganos asesores estratégicos del Ejército Brasileño, considerando las especificidades del entorno militar y los desafíos contemporáneos de la ciberdefensa. Para ello, se realizó una revisión sistemática de la literatura, guiada por el protocolo PRISMA 2020, que abarcó estudios científicos y documentos institucionales relacionados con la gobernanza de TI, la seguridad de la información, la ciberseguridad y la defensa. Los resultados indican que marcos como COBIT, ISO/IEC 27001, ISO/IEC 27002 y los documentos estratégicos nacionales contribuyen a la estructuración de políticas, mecanismos de control, gestión de riesgos y prácticas de cumplimiento. Sin embargo, la literatura revela una alineación normativa aún parcial, brechas de madurez y dificultades operacionales en entornos militares. El análisis también señala la necesidad de una gobernanza multinivel, la integración entre las dimensiones estratégica, táctica y operacional, y un equilibrio entre la centralización militar y la cooperación multisectorial. Como contribución, el estudio propone directrices para fortalecer la gobernanza y la seguridad de la información en el contexto de la Ciberdefensa, con énfasis en la alineación regulatoria, la rendición de cuentas, la gestión de riesgos, la auditoría, el desarrollo de capacidades, la integración interinstitucional y la protección de información sensible.

Palabras clave: Gobernanza. Seguridad de la Información. Ciberdefensa. Ejército Brasileño. Revisión Sistemática de la Literatura.

1 INTRODUÇÃO

A transformação digital ampliou a dependência das organizações contemporâneas em relação a ativos informacionais, sistemas digitais e infraestruturas tecnológicas. No setor de Defesa, essa dependência assume dimensão estratégica, pois a superioridade informacional, a proteção de dados sensíveis, a continuidade dos sistemas de comando e controle e a resiliência cibernética tornaram-se condições para o planejamento, a condução e o apoio às operações militares. Assim, a segurança da informação deixou de ser apenas uma questão técnica para se consolidar como componente crítico da governança institucional e da capacidade de defesa do Estado.

O reconhecimento do espaço cibernético como domínio estratégico tem levado governos e instituições militares a fortalecer mecanismos de governança voltados à proteção de infraestruturas críticas, à gestão de riscos, à continuidade operacional e à resposta a incidentes. No Brasil, essa preocupação está presente na Política Nacional de Defesa (PND), que reconhece a dimensão cibernética como área relevante para a soberania nacional e para a proteção dos interesses estratégicos do Estado brasileiro (Brasil, 2024a). De modo complementar, a Estratégia Nacional de Defesa (END) estabelece o Setor Cibernético como um dos setores estratégicos de Defesa, destacando a necessidade de desenvolver capacidades de proteção, monitoramento, coordenação e resposta frente a ameaças que possam comprometer a segurança nacional (Brasil, 2024b).

No âmbito da Defesa, a Política Cibernética de Defesa (PCD) define princípios, objetivos e diretrizes para orientar o planejamento e a execução das atividades de Defesa Cibernética, enfatizando a integração entre capacidades humanas, tecnológicas, organizacionais, doutrinárias e normativas (Brasil, 2023). Mais recentemente, a Estratégia Nacional de Cibersegurança, instituída pelo Decreto nº 12.573, de 4 de agosto de 2025, reforçou a necessidade de articulação entre órgãos públicos, setor privado, academia e sociedade, conferindo centralidade à governança, à cooperação institucional e à resiliência do ecossistema cibernético nacional (Brasil, 2025b). No mesmo contexto normativo, o Decreto nº 12.572, de 4 de agosto de 2025, instituiu a Política Nacional de Segurança da Informação e dispôs sobre a governança da segurança da informação no âmbito da administração pública federal, estabelecendo diretrizes voltadas à disponibilidade, integridade, confidencialidade e autenticidade da informação (Brasil, 2025a).

Esses marcos normativos evidenciam que a segurança da informação e a cibersegurança passaram a ocupar posição central na agenda estratégica do Estado brasileiro. No caso do Exército Brasileiro, essa agenda possui relevância particular, uma vez que a Força Terrestre participa da consolidação das capacidades cibernéticas nacionais e atua na formulação, coordenação e implementação de iniciativas institucionais relacionadas à proteção da informação e à Defesa

Cibernética. Nesse processo, os órgãos de assessoria estratégica exercem papel relevante ao subsidiar a tomada de decisão em níveis superiores da administração militar, contribuindo para a elaboração de diretrizes, normas, políticas e mecanismos de governança compatíveis com as necessidades institucionais da Defesa.

Sob a perspectiva teórica, a governança de tecnologia da informação e a governança da segurança da informação evoluíram de uma abordagem predominantemente operacional para um modelo estratégico orientado à geração de valor, à gestão de riscos, à conformidade e ao alinhamento organizacional. Weill e Ross (2004) compreendem a governança de TI como o conjunto de mecanismos que define direitos decisórios e responsabilidades, buscando assegurar comportamentos coerentes com os objetivos organizacionais. Peterson (2004), por sua vez, destaca que a governança de TI deve articular estratégia, estruturas, processos e mecanismos de decisão, de modo que os investimentos tecnológicos contribuam efetivamente para os resultados institucionais.

No campo da segurança da informação, Von Solms e Von Solms (2004) argumentam que a segurança não pode ser tratada apenas como responsabilidade técnica, pois envolve decisões estratégicas, participação da alta administração e integração aos processos de governança corporativa. De forma convergente, De Haes e Van Grembergen (2009) indicam que mecanismos eficazes de governança dependem da combinação entre estruturas organizacionais, processos formais e mecanismos relacionais capazes de promover alinhamento estratégico, controle, responsabilização e gestão adequada dos riscos. Esses fundamentos têm sido operacionalizados por modelos e *frameworks* reconhecidos internacionalmente, como o COBIT, voltado à governança e à gestão da informação e da tecnologia (ISACA, 2019), e as normas da família ISO/IEC 27000, associadas à estruturação de sistemas de gestão da segurança da informação.

Apesar da relevância desses referenciais, ainda há lacunas na compreensão sobre como *frameworks* de governança, normas de segurança da informação e marcos normativos nacionais são apropriados, adaptados e aplicados no processo de formulação de políticas em ambientes militares. A literatura tende a concentrar-se em abordagens técnicas de cibersegurança, em modelos gerais de governança de TI ou em análises amplas da administração pública, sem examinar de forma suficiente a relação entre *frameworks* internacionais, diretrizes nacionais de Defesa, cultura organizacional militar, hierarquia decisória, sigilo institucional e atuação dos órgãos de assessoria estratégica. Essa lacuna é relevante porque a formulação de políticas em organizações militares exige equilíbrio entre conformidade normativa, proteção de informações sensíveis, eficiência administrativa, interoperabilidade, resiliência operacional e preservação da soberania nacional.

Diante desse cenário, este artigo é orientado pela seguinte questão de pesquisa: como os marcos teóricos, normativos e metodológicos de governança e segurança da informação influenciam a formulação de políticas nos órgãos de assessoria estratégica do Exército Brasileiro, considerando as especificidades do ambiente militar e os desafios contemporâneos da Defesa Cibernética?

Com o objetivo de responder a essa questão, o estudo realiza uma revisão sistemática da literatura sobre governança e segurança da informação em contextos militares e de Defesa, analisando políticas, modelos teóricos, *frameworks* de governança e mecanismos institucionais relacionados à atuação dos órgãos de assessoria estratégica do Exército Brasileiro. Busca-se identificar tendências, lacunas e oportunidades de aperfeiçoamento que possam contribuir para o fortalecimento da governança da segurança da informação e da Defesa Cibernética no âmbito militar.

A relevância do estudo decorre da necessidade de ampliar a compreensão científica sobre a governança da informação em instituições de Defesa, especialmente diante da crescente complexidade do ambiente cibernético e da atualização dos marcos normativos nacionais. Ao articular referenciais clássicos de governança, *frameworks* internacionais, documentos estratégicos de Defesa e normas nacionais recentes sobre segurança da informação e cibersegurança, a pesquisa pretende oferecer subsídios teóricos e práticos para o aprimoramento de políticas institucionais, para o fortalecimento da resiliência organizacional e para o desenvolvimento das Ciências Militares no campo da Defesa Cibernética.

2 METODOLOGIA

2.1 DELINEAMENTO DA PESQUISA

Este estudo caracteriza-se como uma pesquisa de natureza aplicada, com abordagem qualitativa e objetivo exploratório-descritivo, desenvolvida por meio de uma Revisão Sistemática da Literatura (RSL). A adoção desse método justifica-se pela necessidade de identificar, selecionar, avaliar e sintetizar criticamente a produção científica e documental relacionada à governança, à segurança da informação e à defesa cibernética em contextos militares, com ênfase nos órgãos de assessoria estratégica do Exército Brasileiro.

A revisão foi conduzida com base nas recomendações do protocolo PRISMA 2020 (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), com o objetivo de aumentar a transparência, a rastreabilidade e a reprodutibilidade do processo de seleção e análise dos estudos (PAGE *et al*., 2021). Embora o PRISMA tenha sido originalmente desenvolvido para revisões na área da saúde, sua estrutura tem sido amplamente empregada em revisões sistemáticas interdisciplinares,

especialmente quando há necessidade de explicitar critérios de busca, triagem, elegibilidade e inclusão de estudos.

A questão norteadora da pesquisa foi definida nos seguintes termos: Como os marcos teóricos, normativos e metodológicos de governança e segurança da informação influenciam a formulação de políticas nos órgãos de assessoria estratégica do Exército Brasileiro, considerando as especificidades do ambiente militar e os desafios contemporâneos da Defesa Cibernética?

2.2 ESTRATÉGIA DE BUSCA

A estratégia de busca foi estruturada a partir da decomposição da questão de pesquisa em eixos temáticos relacionados ao objeto do estudo, contemplando: governança; governança de tecnologia da informação; governança da segurança da informação; segurança da informação; segurança cibernética; defesa cibernética; políticas públicas; governança militar; Exército Brasileiro; órgãos de assessoria estratégica; e administração pública federal.

As buscas foram realizadas entre os anos de 2006 e 2026, em bases científicas nacionais e internacionais, com o objetivo de recuperar estudos publicados em português e inglês. Foram consultadas as seguintes bases: Scopus, Web of Science, IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Google Scholar e Portal de Periódicos CAPES.

Para ampliar a abrangência da recuperação e reduzir vieses de seleção, foram utilizadas combinações de descritores em português e inglês, associadas por operadores booleanos. As principais expressões de busca foram:

a) "Information Security Governance" AND "Brazilian Army";
b) "Cybersecurity Governance" AND "Military Organizations";
c) "Defense Cyber Policy" AND Governance;
d) "Information Security Policy Development" AND Military;
e) "IT Governance" AND "Information Security" AND Military;
f) "Cyber Defense" AND Governance AND Brazil;
g) "Governança da Segurança da Informação" AND "Exército Brasileiro";
h) "Governança Cibernética" AND Defesa;
i) "Política de Segurança da Informação" AND "Organizações Militares";
j) "Defesa Cibernética" AND Governança AND "Exército Brasileiro";
k) "Governança de TI" AND "Segurança da Informação" AND "Administração Pública".

Além das bases acadêmicas, foram consultados documentos normativos e institucionais de acesso público, considerados relevantes para a compreensão do contexto brasileiro de Defesa, segurança da informação e cibersegurança. Essa inclusão justifica-se pelo fato de o objeto do estudo envolver a formulação de políticas, diretrizes e mecanismos de governança em ambiente militar, campo no qual documentos oficiais exercem papel estruturante na definição de competências, responsabilidades, prioridades estratégicas e parâmetros institucionais.

Entre os documentos consultados, destacam-se: Política Nacional de Defesa (PND); Estratégia Nacional de Defesa (END); Política Cibernética de Defesa (PCD); Estratégia Nacional de Cibersegurança (E-Ciber); Política Nacional de Segurança da Informação; normativos do Ministério da Defesa; e publicações institucionais ostensivas do Exército Brasileiro.

2.3 CRITÉRIOS DE INCLUSÃO E EXCLUSÃO

Foram definidos critérios de elegibilidade com o objetivo de assegurar a pertinência temática, a qualidade mínima e a aderência dos estudos ao problema de pesquisa.

Foram incluídos estudos que atenderam a pelo menos um dos seguintes critérios:

a) abordassem governança, governança de TI, governança da segurança da informação, segurança da informação, segurança cibernética ou defesa cibernética em organizações militares, governamentais ou de Defesa;
b) discutissem desenvolvimento, implementação, avaliação ou aprimoramento de políticas de segurança da informação ou cibersegurança;
c) apresentassem modelos teóricos, *frameworks*, normas ou estruturas de governança aplicáveis ao contexto militar ou à administração pública;
d) analisassem documentos oficiais, políticas públicas, estratégias nacionais ou marcos regulatórios relacionados à segurança da informação, cibersegurança ou defesa cibernética;
e) fossem publicados em periódicos científicos, anais de conferências, livros acadêmicos, relatórios técnicos qualificados ou documentos oficiais de acesso público;
f) estivessem disponíveis integralmente em português ou inglês.

Foram excluídos estudos que:

a) tratassem exclusivamente de aspectos técnicos de segurança, sem relação com governança, formulação de políticas, gestão institucional ou defesa;
b) não apresentassem relação com o setor público, militar, governamental, institucional ou de Defesa;

c) consistissem apenas em resumos, apresentações, materiais promocionais ou documentos sem densidade analítica;
d) estivessem duplicados em mais de uma base de dados;
e) não disponibilizassem texto completo para análise;
f) não apresentassem clareza metodológica mínima ou relação direta com a questão norteadora da revisão;
g) abordassem segurança cibernética em contextos estritamente comerciais, sem possibilidade de transferência conceitual para o campo da governança pública, militar ou de Defesa.

2.4 PROCESSO DE SELEÇÃO DOS ESTUDOS

O processo de seleção foi conduzido em quatro etapas, conforme a lógica do protocolo PRISMA 2020: identificação, triagem, elegibilidade e inclusão. A seleção foi realizada por três pesquisadores, de forma independente nas etapas iniciais de leitura de títulos, resumos e palavras-chave. As divergências quanto à inclusão ou exclusão de estudos foram discutidas coletivamente até a obtenção de consenso.

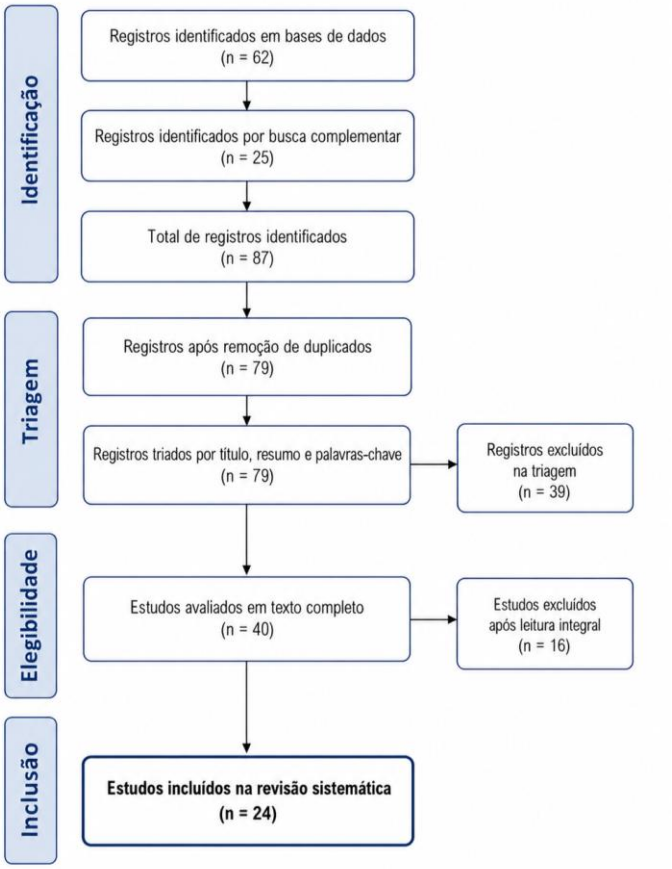
Na etapa de identificação, foram recuperados 87 registros potencialmente relevantes, sendo 62 provenientes das bases científicas consultadas e 25 oriundos de busca complementar em referências dos estudos selecionados, documentos oficiais e publicações institucionais ostensivas.

Na etapa de triagem, foram removidos 8 registros duplicados, resultando em 79 registros únicos. Em seguida, procedeu-se à leitura dos títulos, resumos e palavras-chave, com o objetivo de verificar a aderência preliminar ao tema. Nessa fase, 39 registros foram excluídos por não atenderem aos critérios de inclusão, principalmente por apresentarem foco exclusivamente técnico, ausência de relação com governança ou distanciamento do contexto público, militar ou de Defesa.

Na etapa de elegibilidade, 40 estudos foram avaliados em texto completo. Após leitura integral, 16 estudos foram excluídos por não apresentarem aderência suficiente à questão de pesquisa. As principais razões de exclusão foram: ausência de relação direta com governança ou formulação de políticas; foco predominantemente técnico-operacional; inexistência de conexão com organizações públicas, militares ou de Defesa; fragilidade metodológica; e baixa contribuição para a análise dos marcos teóricos, normativos ou institucionais investigados.

Ao final do processo, 24 estudos foram incluídos no corpus final da Revisão Sistemática da Literatura. O fluxo de seleção dos estudos é apresentado na Figura 1, elaborada conforme o modelo PRISMA 2020, e sintetizado no Quadro 1.

Figura 01 – Fluxograma PRISMA 2020 do processo de seleção dos estudos



Fonte: elaborado pelos autores.

Quadro 1 – Fluxo de seleção dos estudos.

Etapa	Quantidade
Registros identificados em bases de dados	62
Registros identificados por busca complementar	25
Total de registros identificados	87
Registros duplicados removidos	8
Registros após remoção de duplicados	79
Registros triados por título, resumo e palavras-chave	79
Registros excluídos na triagem	39
Artigos avaliados em texto completo	40
Artigos excluídos após leitura integral	16
Estudos incluídos na revisão sistemática	24

Fonte: elaborado pelos autores.

Quadro 2 – Motivos de exclusão dos estudos após leitura integral.

Motivo	Quantidade
Ausência de relação direta com governança ou formulação de políticas	5
Foco exclusivamente técnico-operacional em segurança cibernética	4
Distanciamento do contexto público, militar, governamental ou de Defesa	3
Fragilidade metodológica ou insuficiência analítica	2
Baixa contribuição para a questão norteadora da revisão	2
Total de estudos excluídos após leitura integral	16

Fonte: elaborado pelos autores.

2.5 CRITÉRIOS DE QUALIDADE E RIGOR METODOLÓGICO

Para aumentar o rigor da revisão, os estudos incluídos foram avaliados quanto à pertinência temática, consistência metodológica e contribuição analítica. Essa avaliação não teve caráter eliminatório isolado, mas orientou a seleção final e a interpretação dos achados.

Foram considerados os seguintes critérios de qualidade:

a) clareza do objetivo e do problema investigado;
b) coerência entre objetivo, método, resultados e conclusões;
c) pertinência do estudo para governança, segurança da informação, cibersegurança ou defesa cibernética;
d) aplicabilidade ao contexto público, militar, governamental ou de Defesa;
e) uso de bases teóricas, normativas ou metodológicas reconhecidas;
f) transparência quanto às fontes, dados ou documentos analisados;
g) contribuição para a compreensão dos marcos de governança, formulação de políticas ou especificidades institucionais do ambiente militar.

Nos documentos oficiais, a avaliação considerou a relevância normativa, a vigência, a relação com o objeto do estudo e a contribuição para a compreensão do ambiente institucional brasileiro de Defesa, segurança da informação e cibersegurança.

2.6 EXTRAÇÃO E ANÁLISE DOS DADOS

Os estudos selecionados foram submetidos à extração sistemática de informações, com base em uma matriz analítica elaborada pelos autores. Foram extraídas as seguintes informações: autoria; ano de publicação; tipo de documento; objetivo do estudo; contexto organizacional; abordagem metodológica; modelo ou *framework* de governança utilizado; normas ou diretrizes mencionadas; mecanismos de segurança da informação; relação com defesa cibernética; principais resultados; limitações apontadas; e contribuições para o contexto militar ou governamental.

Após a extração, os dados foram analisados por meio da Análise Temática, conforme proposta de Braun e Clarke (2006). A aplicação dessa técnica permitiu identificar padrões recorrentes, convergências, divergências e lacunas de conhecimento presentes na literatura. O processo analítico envolveu leitura exploratória dos estudos, codificação inicial dos achados, agrupamento dos códigos em temas, revisão das categorias temáticas e consolidação interpretativa dos resultados.

A análise permitiu organizar os achados em cinco categorias principais:

a) alinhamento das políticas com normas e *frameworks* internacionais;

b) características dos modelos de governança;
c) integração da segurança cibernética às políticas de Defesa;
d) fatores institucionais e organizacionais que influenciam a formulação e a implementação de políticas;
e) marcos teóricos utilizados no desenvolvimento de políticas de governança e segurança da informação.

Essas categorias orientaram a apresentação dos resultados e a discussão crítica do estudo, permitindo relacionar os achados da literatura aos desafios específicos da governança da segurança da informação em ambientes militares e aos órgãos de assessoria estratégica do Exército Brasileiro.

3 RESULTADOS E DISCUSSÃO

Este capítulo apresenta os resultados da revisão sistemática da literatura e, em seguida, discute criticamente os achados à luz da questão de pesquisa. Para evitar sobreposição analítica, os resultados são inicialmente descritos com base nas categorias temáticas extraídas dos 24 estudos incluídos no corpus final da revisão. Na sequência, a discussão interpreta esses achados, destacando suas implicações para a governança da segurança da informação, a formulação de políticas e a Defesa Cibernética no contexto dos órgãos de assessoria estratégica do Exército Brasileiro.

3.1 RESUMO DESCRITIVO DOS ESTUDOS

Os trabalhos analisados (Apêndice 1) empregam predominantemente metodologias qualitativas, incluindo análise documental, com forte ênfase nos contextos institucionais brasileiros e no alinhamento com padrões internacionais. A análise comparativa aborda questões-chave de pesquisa relacionadas ao alinhamento de políticas, estruturas de governança, integração da segurança cibernética nas políticas de defesa e fatores institucionais que influenciam o desenvolvimento de políticas. Esta síntese fornece uma base para identificar as melhores práticas e lacunas nos marcos de governança e segurança da informação relevantes para os órgãos consultivos estratégicos do Exército Brasileiro.

3.2 ANÁLISE CRÍTICA E SÍNTESE

A literatura revela um campo multifacetado e em constante evolução. Vários estudos enfatizam o alinhamento das políticas militares de segurança da informação com os padrões internacionais e a integração de marcos de governança adaptados aos contextos militares (Apêndice 2). No entanto, há

lacunas notáveis na validação empírica abrangente, na coordenação institucional e na implementação prática desses marcos. A pesquisa também destaca desafios relacionados à militarização da governança da segurança cibernética e à necessidade de abordagens adaptativas e sensíveis ao contexto, que considerem tanto a dinâmica do setor público militar quanto a do civil. De modo geral, embora os fundamentos teóricos e as propostas de políticas sejam robustos, a literatura indica a necessidade de maior operacionalização e colaboração intersetorial para fortalecer a eficácia da governança.

3.3 REVISÃO TEMÁTICA DA LITERATURA

A literatura revela vários temas convergentes (Apêndice 3). Entre eles, destacam-se o alinhamento das políticas militares de segurança da informação com as normas internacionais, a aplicação e integração de marcos de governança, como o COBIT e as normas ISO, e a evolução do papel da segurança cibernética nas estratégias de defesa nacional. Além disso, as influências institucionais e organizacionais na formulação de políticas, a militarização da governança da segurança cibernética e os desafios da cooperação multissetorial destacam o ambiente complexo que molda as práticas de governança. Esses temas, em conjunto, ressaltam a interação dinâmica entre teoria, política e prática na governança da segurança da informação no setor militar e público do Brasil.

3.4 REVISÃO CRONOLÓGICA DA LITERATURA

A literatura revela um aprofundamento progressivo dos marcos teóricos, das implementações práticas e das análises institucionais ao longo do tempo (Apêndice 4). As pesquisas iniciais enfatizavam conceitos fundamentais de governança de TI e políticas de segurança da informação em organizações públicas, evoluindo para abordar desafios específicos do âmbito militar e a integração da segurança cibernética. Estudos recentes concentram-se cada vez mais em estratégias nacionais de segurança cibernética, cooperação multissetorial e a militarização da governança cibernética no Brasil, destacando tensões institucionais, alinhamento estratégico com padrões internacionais e o papel da inovação tecnológica. Esta síntese cronológica captura a evolução desde os marcos fundamentais de governança até o desenvolvimento de políticas estratégicas contemporâneas e os desafios de governança nos domínios da segurança cibernética militar e pública.

3.5 CONSENSO E DIVERGÊNCIAS ENTRE OS ESTUDOS

A literatura analisada revela um amplo consenso sobre o papel fundamental de alinhar as políticas de segurança da informação e de governança às normas internacionais, particularmente nos contextos militar e do setor público (Apêndice 5). Muitos estudos enfatizam a necessidade de estruturas

integradas e abordagens estratégicas para aumentar a resiliência institucional e a eficiência operacional. No entanto, surgem divergências quanto à maturidade da implementação das políticas, ao grau de militarização na governança da segurança cibernética e à integração das estruturas de governança civis e militares. Essas diferenças geralmente decorrem de fatores contextuais, como o escopo organizacional, os desafios específicos do setor e as diferentes abordagens metodológicas.

3.6 RESULTADOS

A análise dos 24 estudos incluídos revelou um conjunto de contribuições concentradas em cinco eixos principais: alinhamento normativo; maturidade e operacionalização da governança; estruturas de governança multinível; relações entre centralização militar e cooperação multissetorial; e mecanismos de auditoria, rastreabilidade e gestão de riscos.

De modo geral, os estudos analisados indicam que a governança da segurança da informação em organizações militares e públicas tem sido fortemente influenciada por normas, *frameworks* e políticas institucionais. Entre os referenciais mais recorrentes, destacam-se a família ISO/IEC 27000, o COBIT, modelos de maturidade, diretrizes de governança pública e documentos estratégicos relacionados à segurança cibernética e à Defesa. Esses referenciais são mobilizados tanto para estruturar processos de gestão da segurança da informação quanto para apoiar a formulação, avaliação e aperfeiçoamento de políticas institucionais.

Os estudos também evidenciam que a segurança da informação tem deixado de ser tratada apenas como um domínio técnico-operacional, passando a ser compreendida como dimensão estratégica da governança. Essa mudança é relevante no ambiente militar, no qual a proteção de ativos informacionais, a gestão de riscos cibernéticos, a continuidade operacional, a classificação da informação e a resiliência institucional possuem relação direta com a capacidade de comando e controle, com a proteção de infraestruturas críticas e com a soberania nacional.

A síntese dos resultados permitiu agrupar os principais achados em cinco categorias analíticas, conforme apresentado no Quadro 3.

Quadro 3 – Síntese dos principais achados da revisão sistemática.

Categoria analítica	Síntese dos achados nos 24 estudos
Alinhamento normativo parcial	Os estudos indicam esforço de alinhamento das políticas de segurança da informação com normas e *frameworks* internacionais, especialmente ISO/IEC 27001, ISO/IEC 27002, COBIT e referenciais de governança pública. Contudo, esse alinhamento aparece de forma parcial, com lacunas de atualização normativa, aderência prática e adaptação ao contexto militar.
Lacunas de maturidade e operacionalização	Parte significativa da literatura aponta dificuldades para transformar políticas, diretrizes e modelos de governança em práticas institucionais efetivas. As principais lacunas envolvem maturidade organizacional, monitoramento de conformidade, capacitação, integração entre níveis decisórios e mensuração de resultados.

Necessidade de governança multinível	Os estudos destacam que a governança da segurança da informação exige articulação entre níveis estratégico, tático e operacional. Em ambientes militares, essa articulação é condicionada por hierarquia, doutrina, sigilo, interoperabilidade e integração com políticas de Defesa Cibernética.
Tensão entre centralização militar e cooperação multissetorial	A literatura reconhece a importância da coordenação centralizada em temas sensíveis de Defesa, mas também aponta a necessidade de cooperação com atores civis, órgãos governamentais, setor privado e academia. Essa tensão exige equilíbrio entre segurança, sigilo, legitimidade, transparência e colaboração institucional.
Auditoria, rastreabilidade e gestão de riscos	Os estudos convergem quanto à importância de mecanismos formais de controle, auditoria, rastreabilidade, responsabilização e gestão de riscos. Esses mecanismos são apontados para aumentar a confiabilidade das políticas, avaliar maturidade e fortalecer a resiliência institucional.

Fonte: elaborado pelos autores

3.6.1 Alinhamento normativo parcial

O primeiro achado relevante refere-se ao alinhamento parcial das políticas e práticas de governança da segurança da informação com normas e *frameworks* reconhecidos internacionalmente. Estudos que analisam a aplicação de referenciais como ISO/IEC 27001, ISO/IEC 27002 e COBIT indicam que esses modelos contribuem para estruturar controles, processos de gestão, mecanismos de responsabilização e práticas de conformidade.

No entanto, a literatura também aponta que o simples reconhecimento desses referenciais não garante sua implementação efetiva. Em organizações militares e públicas, a adoção de normas internacionais tende a exigir adaptações ao contexto institucional, jurídico, doutrinário e operacional. No caso militar, essa adaptação envolve considerar requisitos específicos de sigilo, cadeia de comando, classificação da informação, continuidade das operações e proteção de dados sensíveis.

Assim, o resultado central não é a ausência de referenciais normativos, mas a existência de uma lacuna entre o alinhamento formal e a operacionalização efetiva desses instrumentos. Essa constatação reforça a necessidade de políticas que integrem normas internacionais, marcos nacionais de Defesa e especificidades organizacionais do Exército Brasileiro.

3.6.2 Lacunas de maturidade e operacionalização

O segundo achado diz respeito às lacunas de maturidade da governança da segurança da informação. Os estudos analisados indicam que muitas organizações públicas e militares possuem políticas, normas e estruturas formais, mas enfrentam dificuldades para implementar práticas contínuas de avaliação, monitoramento e melhoria.

Entre os problemas recorrentes identificados na literatura, destacam-se: baixa integração entre áreas técnicas e decisórias; ausência de métricas consolidadas de maturidade; dificuldade de mensuração da efetividade das políticas; limitações na disseminação de normas aos níveis

operacionais; necessidade de capacitação contínua; e desafios na atualização de controles diante da rápida evolução das ameaças cibernéticas.

Essas lacunas demonstram que a governança da segurança da informação não depende apenas da existência de documentos normativos. Ela exige mecanismos institucionais permanentes, capazes de conectar políticas, processos, pessoas, tecnologias, auditoria e gestão de riscos.

3.6.3 Necessidade de governança multinível

O terceiro achado refere-se à necessidade de governança multinível. Os estudos analisados convergem ao indicar que a segurança da informação e a defesa cibernética não podem ser conduzidas exclusivamente por estruturas técnicas ou por instâncias estratégicas isoladas. Ao contrário, exigem articulação entre níveis estratégico, tático e operacional.

No nível estratégico, a governança define diretrizes, prioridades, responsabilidades e alinhamento com os objetivos institucionais da Defesa. No nível tático, essas diretrizes são convertidas em processos, programas, planos de ação e mecanismos de coordenação. No nível operacional, materializam-se em controles, procedimentos, capacitação, resposta a incidentes, classificação da informação e proteção de ativos informacionais.

Em organizações militares, essa governança multinível assume complexidade adicional devido à hierarquia, à doutrina, à necessidade de sigilo, à interoperabilidade entre organizações e à relação entre segurança da informação, inteligência, comando e controle e Defesa Cibernética. Nesse contexto, os órgãos de assessoria estratégica assumem papel relevante ao subsidiar decisões de alto nível e articular referenciais normativos, técnicos e institucionais.

3.6.4 Tensão entre centralização militar e cooperação multissetorial

O quarto achado envolve a tensão entre a centralização típica das estruturas militares e a necessidade de cooperação multissetorial na governança cibernética. A literatura reconhece que temas de Defesa, segurança da informação e cibersegurança exigem coordenação, controle e preservação de informações sensíveis. Por essa razão, a centralização decisória pode ser funcional para garantir unidade de comando, coerência institucional e proteção de ativos estratégicos.

Entretanto, os estudos também apontam que a segurança cibernética contemporânea ultrapassa os limites das organizações militares. A proteção do espaço cibernético envolve infraestruturas críticas, redes governamentais, setor privado, academia, indústria de Defesa, organizações internacionais e sociedade civil. Dessa forma, a governança eficaz requer mecanismos de cooperação, compartilhamento de informações, interoperabilidade e coordenação interinstitucional.

O desafio identificado na literatura é equilibrar centralização e cooperação. No contexto militar, esse equilíbrio deve preservar sigilo, soberania, segurança operacional e cadeia de comando, sem comprometer a capacidade de colaboração com outros atores relevantes para a segurança cibernética nacional.

3.6.5 Auditoria, rastreabilidade e gestão de riscos

O quinto achado refere-se à importância dos mecanismos de auditoria, rastreabilidade e gestão de riscos. Os estudos analisados indicam que políticas de segurança da informação tendem a ser mais efetivas quando acompanhadas de processos de controle, indicadores de desempenho, avaliação de maturidade, responsabilização e revisão periódica.

A rastreabilidade é apontada como elemento para conectar decisões estratégicas, normas internas, controles implementados, incidentes registrados e medidas corretivas. Em ambientes militares, esse aspecto é relevante porque a segurança da informação envolve ativos sensíveis, diferentes níveis de classificação, responsabilidades hierárquicas e necessidade de resposta coordenada a ameaças.

A gestão de riscos, por sua vez, aparece como eixo integrador entre governança, segurança da informação e Defesa Cibernética. Ao permitir a identificação, análise, tratamento e monitoramento de ameaças, vulnerabilidades e impactos, ela contribui para orientar prioridades institucionais e alocar recursos de modo mais racional.

3.7 DISCUSSÃO

Os resultados evidenciam que a governança da segurança da informação no contexto da Defesa não pode ser compreendida apenas como aplicação de normas técnicas ou adoção de frameworks internacionais. Embora referenciais como ISO/IEC 27001, ISO/IEC 27002 e COBIT sejam relevantes, sua efetividade depende da capacidade institucional de adaptá-los às especificidades do ambiente militar.

Essa constatação é importante porque organizações militares operam sob condições distintas daquelas observadas em organizações civis. A formulação de políticas nesse ambiente envolve requisitos de sigilo, hierarquia, doutrina, interoperabilidade, prontidão operacional, classificação da informação, preservação da soberania e continuidade das funções críticas. Portanto, a governança da segurança da informação precisa conciliar conformidade normativa com efetividade operacional.

A primeira implicação dos achados é que o alinhamento normativo deve ser entendido como ponto de partida, e não como resultado. A simples menção a normas internacionais ou a documentos

estratégicos nacionais não assegura maturidade de governança. Para que o alinhamento seja efetivo, é necessário traduzi-lo em estruturas decisórias, processos documentados, responsabilidades definidas, mecanismos de controle, indicadores de desempenho e ciclos de melhoria contínua.

A segunda implicação refere-se à necessidade de maior maturidade institucional. A literatura analisada demonstra que há uma lacuna recorrente entre a formulação das políticas e sua operacionalização. Essa lacuna pode comprometer a capacidade de resposta institucional, especialmente em cenários de ameaças cibernéticas dinâmicas e persistentes. Em consequência, políticas de segurança da informação devem ser acompanhadas de mecanismos de implementação, capacitação, auditoria e avaliação periódica.

A terceira implicação diz respeito ao papel dos órgãos de assessoria estratégica. Esses órgãos ocupam posição relevante porque atuam na interface entre formulação de políticas, apoio à decisão, coordenação institucional e alinhamento estratégico. No contexto do Exército Brasileiro, sua atuação pode contribuir para transformar referenciais normativos e teóricos em diretrizes aplicáveis, conectando a alta administração militar às necessidades técnicas, operacionais e doutrinárias da segurança da informação e da Defesa Cibernética.

A quarta implicação envolve a governança multinível. Os estudos analisados sugerem que a segurança da informação deve ser governada de forma integrada, articulando níveis estratégico, tático e operacional. Essa articulação reduz o risco de fragmentação, melhora a coordenação entre setores, aumenta a rastreabilidade das decisões e favorece o alinhamento entre políticas institucionais e controles efetivamente implementados.

A quinta implicação refere-se à tensão entre centralização e cooperação. A centralização possui valor no ambiente militar, sobretudo pela necessidade de preservar unidade de comando, sigilo e segurança operacional. Contudo, a natureza interdependente do espaço cibernético exige cooperação com outros órgãos públicos, setor privado, academia e estruturas de governança nacional. Assim, o desafio não consiste em substituir a centralização por modelos abertos, mas em construir mecanismos de cooperação controlada, institucionalmente seguros e compatíveis com os interesses da Defesa.

Por fim, os resultados reforçam a importância de auditoria, rastreabilidade e gestão de riscos como elementos estruturantes da governança. Esses mecanismos permitem verificar se as políticas foram efetivamente implementadas, se os controles são adequados, se os riscos estão sendo monitorados e se há capacidade institucional para responder a incidentes. No ambiente militar, tais mecanismos também contribuem para preservar a confiabilidade das informações, a responsabilização decisória e a continuidade das atividades críticas.

4 DIRETRIZES PARA O FORTALECIMENTO DA GOVERNANÇA E DA SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA DEFESA CIBERNÉTICA

A revisão sistemática da literatura evidenciou que a governança da segurança da informação em ambientes militares exige a articulação entre marcos normativos, estruturas decisórias, mecanismos de controle, gestão de riscos, cultura organizacional e cooperação institucional. Os achados apontam que, embora existam referenciais consolidados no campo da governança de TI, da segurança da informação e da cibersegurança, sua aplicação ao contexto militar requer adaptações específicas, considerando aspectos como hierarquia, sigilo, cadeia de comando, interoperabilidade, proteção de informações sensíveis e preservação da soberania nacional.

Com base nos resultados da revisão, são propostas sete diretrizes para o fortalecimento da governança e da segurança da informação no contexto da Defesa Cibernética. Essas diretrizes não possuem caráter prescritivo absoluto, mas oferecem um conjunto de orientações sistematizadas para apoiar a formulação, o aperfeiçoamento e a avaliação de políticas institucionais em órgãos de assessoria estratégica e demais estruturas relacionadas à segurança da informação e à Defesa Cibernética.

4.1 ALINHAMENTO NORMATIVO

A primeira diretriz consiste em promover o alinhamento sistemático das políticas institucionais de segurança da informação e Defesa Cibernética aos principais marcos normativos nacionais e referenciais internacionais aplicáveis. Esse alinhamento deve considerar a Política Nacional de Defesa, a Estratégia Nacional de Defesa, a Política Cibernética de Defesa, a Estratégia Nacional de Cibersegurança vigente, a Política Nacional de Segurança da Informação, bem como, *frameworks* reconhecidos, como COBIT e ISO/IEC 27001/27002.

O alinhamento normativo não deve limitar-se à incorporação formal de conceitos ou à simples referência a documentos estratégicos. É necessário que as diretrizes institucionais sejam traduzidas em processos, responsabilidades, controles, indicadores e mecanismos de acompanhamento. No ambiente militar, esse processo deve considerar as especificidades da organização, especialmente no que se refere à cadeia de comando, à classificação da informação, à continuidade operacional, à proteção de ativos críticos e à integração com capacidades de Defesa Cibernética.

Essa diretriz contribui para reduzir fragmentações normativas, aumentar a coerência institucional e fortalecer a compatibilidade entre políticas internas, exigências legais, boas práticas internacionais e objetivos estratégicos de Defesa.

4.2 GOVERNANÇA E *ACCOUNTABILITY*

A segunda diretriz refere-se à necessidade de fortalecer estruturas de governança com definição clara de papéis, responsabilidades, instâncias decisórias e mecanismos de prestação de contas. A literatura analisada demonstra que políticas de segurança da informação tendem a apresentar menor efetividade quando não há clareza sobre quem decide, quem executa, quem monitora e quem responde pelos resultados.

No contexto militar, a governança deve respeitar a hierarquia, mas também precisa assegurar transparência interna, rastreabilidade decisória e coordenação entre áreas estratégicas, técnicas, jurídicas, administrativas e operacionais. Para isso, recomenda-se a formalização de comitês, grupos de trabalho ou instâncias equivalentes responsáveis por acompanhar a implementação das políticas, avaliar riscos, propor atualizações normativas e subsidiar a alta administração.

A *accountability*, nesse contexto, deve ser compreendida como capacidade institucional de demonstrar conformidade, justificar decisões, registrar responsabilidades e avaliar resultados, sem comprometer informações sensíveis ou aspectos protegidos por sigilo. Assim, a governança da segurança da informação deve equilibrar controle, responsabilização e proteção institucional.

4.3 GESTÃO DE RISCOS

A terceira diretriz consiste em institucionalizar processos periódicos de identificação, análise, avaliação, tratamento e monitoramento de riscos cibernéticos e informacionais. Os achados da revisão indicam que a gestão de riscos é um elemento estruturante da governança, pois permite orientar prioridades, alocar recursos, definir controles e antecipar vulnerabilidades que possam comprometer a missão institucional.

No contexto da Defesa Cibernética, a gestão de riscos deve abranger ameaças técnicas, organizacionais, humanas, normativas e operacionais. Isso inclui riscos associados à confidencialidade, integridade, disponibilidade e autenticidade da informação, bem como riscos relacionados à interoperabilidade, continuidade de serviços críticos, exposição de informações sensíveis, dependência tecnológica e resposta a incidentes.

Recomenda-se que a avaliação de riscos seja realizada de forma recorrente, documentada e integrada ao ciclo de planejamento institucional. Além disso, os resultados dessas avaliações devem subsidiar a formulação de políticas, a priorização de investimentos, a capacitação de pessoal e a definição de medidas de prevenção, detecção, resposta e recuperação.

4.4 MATURIDADE E AUDITORIA

A quarta diretriz propõe a adoção de modelos de maturidade e mecanismos de auditoria para avaliar a evolução da governança da segurança da informação. A literatura analisada aponta que muitas organizações possuem políticas e normas formalmente instituídas, mas enfrentam dificuldades para mensurar sua implementação, efetividade e aderência às boas práticas.

A adoção de modelos de maturidade permite verificar o estágio de desenvolvimento da governança, identificar lacunas, estabelecer metas de evolução e comparar resultados ao longo do tempo. Esses modelos podem considerar dimensões como liderança, processos, controles, gestão de riscos, capacitação, cultura organizacional, resposta a incidentes, conformidade normativa e melhoria contínua.

A auditoria, por sua vez, deve ser compreendida como mecanismo de verificação, aprendizado e aperfeiçoamento institucional. Em ambientes militares, os processos de auditoria devem observar requisitos de sigilo, segurança operacional e classificação da informação, mas sem deixar de assegurar rastreabilidade, conformidade e responsabilização. Essa diretriz contribui para reduzir a distância entre políticas formalmente aprovadas e práticas efetivamente implementadas.

4.5 CAPACITAÇÃO E CULTURA ORGANIZACIONAL

A quinta diretriz consiste em fortalecer a capacitação continuada e a cultura organizacional em segurança da informação, Defesa Cibernética e proteção de dados. Os estudos analisados indicam que a efetividade da governança não depende apenas de normas, tecnologias ou estruturas formais, mas também do comportamento dos usuários, da compreensão das responsabilidades individuais e coletivas e do engajamento da liderança.

No ambiente militar, a cultura de segurança deve estar integrada aos processos de formação, aperfeiçoamento, especialização e capacitação continuada. Essa formação deve contemplar tanto aspectos técnicos quanto dimensões estratégicas, jurídicas, éticas e operacionais da segurança da informação. É necessário que militares e servidores compreendam a importância da proteção de dados, da classificação da informação, da prevenção de incidentes, do uso adequado de sistemas e da observância das políticas institucionais.

A alta administração possui papel decisivo nesse processo, pois a cultura de segurança tende a ser mais efetiva quando apoiada por liderança, comunicação clara, exemplos institucionais e mecanismos consistentes de orientação e responsabilização.

4.6 INTEGRAÇÃO CIVIL-MILITAR E INTERAGÊNCIAS

A sexta diretriz trata da necessidade de ampliar a cooperação civil-militar e interagências, preservando o sigilo, a soberania e a segurança institucional. A revisão demonstrou que a governança cibernética contemporânea ultrapassa os limites das organizações militares, envolvendo órgãos públicos, setor privado, academia, indústria de Defesa, centros de pesquisa e entidades responsáveis por infraestruturas críticas.

Essa integração é necessária porque as ameaças cibernéticas são dinâmicas, transversais e interdependentes. Incidentes ocorridos em redes civis podem afetar estruturas governamentais e militares, assim como vulnerabilidades em infraestruturas críticas podem comprometer a segurança nacional. Dessa forma, a cooperação institucional contribui para ampliar capacidades de prevenção, detecção, resposta e recuperação.

Entretanto, no contexto da Defesa, essa cooperação deve ocorrer de forma controlada, formalizada e compatível com os requisitos de segurança. Recomenda-se o estabelecimento de protocolos de compartilhamento de informações, canais seguros de coordenação, exercícios conjuntos, mecanismos de interoperabilidade e acordos institucionais que preservem informações sensíveis e respeitem as competências de cada ator envolvido.

4.7 PROTEÇÃO DE INFORMAÇÕES SENSÍVEIS

A sétima diretriz refere-se à proteção de informações sensíveis, com ênfase na confidencialidade, classificação da informação, segurança operacional e preservação dos interesses estratégicos da Defesa. Em organizações militares, a segurança da informação possui relação direta com a proteção da missão, da cadeia de comando, das capacidades operacionais e dos ativos críticos.

A proteção de informações sensíveis deve envolver políticas claras de classificação, tratamento, armazenamento, transmissão, compartilhamento, retenção e descarte de dados e documentos. Deve também contemplar controles de acesso, segregação de funções, monitoramento de uso, criptografia, registro de eventos, gestão de identidades e mecanismos de resposta a incidentes.

Essa diretriz é relevante diante da crescente digitalização dos processos administrativos, estratégicos e operacionais. Quanto maior a dependência de sistemas digitais, maior a necessidade de assegurar que informações classificadas, estratégicas ou institucionalmente sensíveis sejam protegidas contra acesso indevido, vazamento, alteração, destruição ou uso não autorizado.

4.8 SÍNTESE DAS DIRETRIZES PROPOSTAS

As diretrizes propostas indicam que o fortalecimento da governança e da segurança da informação no contexto da Defesa Cibernética depende de uma abordagem integrada, multinível e adaptada às especificidades do ambiente militar. O alinhamento normativo fornece a base de conformidade; a governança e a *accountability* definem responsabilidades; a gestão de riscos orienta prioridades; a maturidade e a auditoria permitem avaliar a evolução institucional; a capacitação fortalece a cultura de segurança; a integração civil-militar amplia a cooperação; e a proteção de informações sensíveis preserva a segurança operacional e os interesses estratégicos da Defesa.

Dessa forma, a principal contribuição das diretrizes está em articular referenciais teóricos, normativos e práticos em uma estrutura aplicável ao aprimoramento de políticas institucionais. No caso dos órgãos de assessoria estratégica do Exército Brasileiro, essas diretrizes podem subsidiar a formulação de recomendações, a revisão de normativos, a avaliação de maturidade, a priorização de riscos e o fortalecimento da governança da segurança da informação em apoio à Defesa Cibernética.

5 CONSIDERAÇÕES FINAIS

Este artigo teve como objetivo analisar como os marcos teóricos, normativos e metodológicos de governança e segurança da informação influenciam a formulação de políticas nos órgãos de assessoria estratégica do Exército Brasileiro, considerando as especificidades do ambiente militar e os desafios contemporâneos da Defesa Cibernética. Para isso, foi realizada uma Revisão Sistemática da Literatura, orientada pelo protocolo PRISMA 2020, com a finalidade de identificar tendências, lacunas e contribuições relacionadas à governança da segurança da informação em contextos militares, governamentais e de Defesa.

A revisão revelou que os marcos de governança e segurança da informação exercem influência significativa sobre a formulação de políticas institucionais, especialmente ao oferecerem estruturas conceituais, critérios de conformidade, mecanismos de controle e práticas de gestão de riscos. Referenciais como COBIT, ISO/IEC 27001 e ISO/IEC 27002, quando articulados a documentos estratégicos nacionais, como a Política Nacional de Defesa, a Estratégia Nacional de Defesa, a Política Cibernética de Defesa, a Estratégia Nacional de Cibersegurança vigente e a Política Nacional de Segurança da Informação, fornecem bases relevantes para orientar políticas de segurança da informação e Defesa Cibernética. Contudo, os achados indicam que esse alinhamento ainda ocorre de forma parcial, exigindo maior adaptação às especificidades do ambiente militar.

A resposta à questão de pesquisa evidencia que a formulação de políticas de governança e segurança da informação nos órgãos de assessoria estratégica do Exército Brasileiro não depende

apenas da adoção formal de normas e frameworks. Ela exige a capacidade institucional de traduzir esses referenciais em diretrizes aplicáveis, responsabilidades definidas, processos documentados, mecanismos de auditoria, práticas de gestão de riscos e instrumentos de monitoramento contínuo. No contexto militar, essa tradução deve considerar fatores como hierarquia, cadeia de comando, sigilo, classificação da informação, interoperabilidade, cultura organizacional, continuidade operacional e proteção de ativos estratégicos.

Os resultados também demonstraram que a governança da segurança da informação deve ser compreendida como uma função estratégica e multinível. Isso significa que sua efetividade depende da articulação entre decisões estratégicas, coordenação tática e execução operacional. No caso dos órgãos de assessoria estratégica, essa função assume especial relevância, pois essas estruturas atuam como elo entre a alta administração militar, os marcos normativos nacionais, os referenciais internacionais de governança e as necessidades práticas de proteção da informação e de fortalecimento da Defesa Cibernética.

Como contribuição científica, o artigo sistematiza a literatura sobre governança e segurança da informação em contextos militares e evidencia cinco achados centrais: o alinhamento normativo parcial; as lacunas de maturidade e operacionalização; a necessidade de governança multinível; a tensão entre centralização militar e cooperação multissetorial; e a importância de mecanismos de auditoria, rastreabilidade e gestão de riscos. Esses achados contribuem para o campo das Ciências Militares ao demonstrar que a Defesa Cibernética não depende apenas de capacidades tecnológicas, mas também de estruturas robustas de governança, coordenação institucional e formulação qualificada de políticas.

Com base nesses resultados, foram propostas sete diretrizes para o fortalecimento da governança e da segurança da informação no contexto da Defesa Cibernética: alinhamento normativo; governança e accountability; gestão de riscos; maturidade e auditoria; capacitação e cultura organizacional; integração civil-militar e interagências; e proteção de informações sensíveis. Essas diretrizes oferecem uma estrutura orientadora para apoiar a revisão de políticas institucionais, a definição de responsabilidades, o aperfeiçoamento dos mecanismos de controle, a avaliação de maturidade e a proteção de informações estratégicas em ambientes militares.

Apesar das contribuições apresentadas, o estudo possui limitações. A primeira refere-se à natureza da revisão sistemática, baseada em literatura científica e documentos institucionais de acesso público, o que restringe a análise a fontes ostensivas. A segunda limitação está relacionada à escassez de estudos empíricos específicos sobre os órgãos de assessoria estratégica do Exército Brasileiro, o que dificulta a avaliação direta da implementação das políticas nesse contexto. A terceira limitação

decorre da heterogeneidade dos estudos analisados, que utilizam diferentes abordagens metodológicas, níveis de profundidade e contextos organizacionais, exigindo cautela na generalização dos achados.

Como agenda de pesquisas futuras, recomenda-se o desenvolvimento de estudos empíricos sobre a implementação da governança da segurança da informação em organizações militares, especialmente em órgãos de assessoramento estratégico e estruturas relacionadas à Defesa Cibernética. Também são recomendadas pesquisas sobre modelos de maturidade aplicáveis ao contexto militar, indicadores de efetividade de políticas de segurança da informação, mecanismos de auditoria e rastreabilidade, integração civil-militar em governança cibernética e impactos da cultura organizacional na adoção de boas práticas de segurança. Estudos comparativos entre instituições militares nacionais e internacionais também podem contribuir para identificar padrões, lacunas e boas práticas transferíveis ao contexto brasileiro.

Conclui-se que a governança da segurança da informação, no contexto militar, deve equilibrar efetividade operacional, conformidade normativa, resiliência cibernética, proteção de informações sensíveis e coordenação institucional. Esse equilíbrio é importante para que políticas de segurança da informação e Defesa Cibernética deixem de ser apenas instrumentos formais e passem a constituir capacidades institucionais efetivas, capazes de fortalecer a soberania nacional, a continuidade das operações, a proteção de ativos estratégicos e o desenvolvimento das Ciências Militares diante dos desafios do ambiente cibernético contemporâneo.

REFERÊNCIAS

A STRATEGY for cybersecurity governance in Brazil. Zenodo, 2025. DOI: https://doi.org/10.5281/zenodo.16270003.

AFLAKHAH, E.; SOEWITO, B. Assessing information security using COBIT 2019 and ISO 27001:2013. Journal of System and Management Sciences, 2024. DOI: https://doi.org/10.33168/jsms.2024.0308.

BALDISSERA, T. A. et al. Segurança da informação em organizações militares do Exército Brasileiro sob a ótica da norma NBR ISO/IEC 27002:2022. 2024. DOI: https://doi.org/10.29327/5545702.1-6.

BRASIL. Decreto nº 12.572, de 4 de agosto de 2025. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal. Diário Oficial da União: seção 1, Brasília, DF, 5 ago. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12572.htm.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. Diário Oficial da União: seção 1, Brasília, DF, 5 ago. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm.

BRASIL. Ministério da Defesa. Política Cibernética de Defesa. Brasília, DF: Ministério da Defesa, 2023.

BRASIL. Ministério da Defesa. Política Nacional de Defesa e Estratégia Nacional de Defesa. Brasília, DF: Ministério da Defesa, 2024. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/publicacoes-politica-e-estrategia-nacional-de-defesa/2024-pnd-end.pdf.

BRAUN, Virginia; CLARKE, Victoria. Using thematic analysis in psychology. Qualitative Research in Psychology, London, v. 3, n. 2, p. 77-101, 2006. DOI: https://doi.org/10.1191/1478088706qp063oa.

BRITO, R. V. L. et al. Panorama das políticas de defesa e segurança cibernéticas no Brasil. 2024. DOI: https://doi.org/10.51359/1808-8708.2023.261927.

CARVALHO, M. S. Diretrizes para aplicação de governança de TI nos órgãos públicos federais brasileiros usando o framework COBIT. 2006.

CIBERSEGURANÇA no Brasil: uma análise da estratégia nacional. Zenodo, 2025. DOI: https://doi.org/10.5281/zenodo.16105451.

CINTIENE, S. M. M. Capability-based planning in tackling complex threats. Zenodo, 2025. DOI: https://doi.org/10.5281/zenodo.15725549.

CUNHA, M. S.; NETO, J. S. Comitês de governança de tecnologia da informação na administração pública federal brasileira: fatores críticos de sucesso. Revista do Serviço Público, Brasília, DF, v. 65, n. 3, 2014. DOI: https://doi.org/10.21874/RSP.V65I3.629.

CUNHA, V. C.; FARIA, A. M. M.; MARINS, J. A. O. IESGO como guia estratégico para impulsionar a governança de TI em instituições públicas brasileiras. Caderno Pedagógico, v. 21, n. 13, 2024. DOI: https://doi.org/10.54033/cadpedv21n13-330.

DE HAES, S.; VAN GREMBERGEN, W. Enterprise governance of information technology. New York: Springer, 2009.

GOLDONI, L. R. F.; RODRIGUES, K. F.; MEDEIROS, B. P. Qual é o futuro da governança de cibersegurança no Brasil? Cadernos Gestão Pública e Cidadania, 2024. DOI: https://doi.org/10.12660/cgpc.v29.90972. Disponível em: https://doi.org/10.12660/cgpc.v29.90972.

HENDRY, H. et al. Integrating COBIT 2019 and ISO/IEC 27001 for strengthening IT governance and information security. 2025. DOI: https://doi.org/10.64803/cessmuds.v1.40.

ISACA. COBIT 2019 Framework: governance and management objectives. Schaumburg: ISACA, 2019.

JÚNIOR, A. W. M. T. The Brazilian Army's concept of transformation: technology and military change. Revista Brasileira de Estudos de Defesa, v. 9, n. 1, 2022. DOI: https://doi.org/10.26792/rbed.v9n1.2022.75209.

LOBATO, L. C. La política brasileña de ciberseguridad como estrategia de liderazgo regional. URVIO: Revista Latinoamericana de Estudios de Seguridad, n. 20, p. 16-30, 2017. DOI: https://doi.org/10.17141/URVIO.20.2017.2576.

MACIEL, T.; ZANIBONI, J. Examining the perspective of public policies in cyber defense area: the Brazilian case. Revista da Escola de Guerra Naval. DOI: https://doi.org/10.21544/2359-3075.29210.

MANJEZI, Z.; BOTHA, R. A. From concept to practice: untangling the direct-control cycle. 2019. DOI: https://doi.org/10.1145/3357419.3357427.

MARTINS, A. K. et al. O papel das Forças Armadas no desenvolvimento, manutenção e defesa de infraestruturas críticas no Brasil. Zenodo, 2023. DOI: https://doi.org/10.5281/zenodo.8421425.

MARTINS, J.; SANTOS, H.; NUNES, P.; SILVA, R. J. Framework de gestão de segurança da informação para organizações militares orientada pelos principais vetores de ataque. 2014. DOI: https://doi.org/10.18803/CAPSI.V12.%P.

NODEHI, S. et al. A contingency view of CISO-board interactions in information security governance. 2024. DOI: https://doi.org/10.5220/0013743700004000.

OLIVEIRA, R. J. de. Notes on the militarization of Brazilian cybersecurity: current state of affairs and perspectives on the near future. Brasiliana: Journal for Brazilian Studies, v. 10, n. 2, 2022. DOI: https://doi.org/10.25160/bjbs.v10i2.128390.

ORDING, L. G.; GAO, S.; CHEN, W. The influence of inputs in the information security policy development: an institutional perspective. Transforming Government: People, Process and Policy, v. 16, n. 4, p. 418-435, 2022. DOI: https://doi.org/10.1108/TG-03-2022-0030.

PAGE, M. J. et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ, v. 372, n. 71, 2021. DOI: https://doi.org/10.1136/bmj.n71.

PETERSON, R. Crafting information technology governance. Information Systems Management, 2004.

REIS, A. L. N.; NETO, J. S. Fatores críticos de sucesso na implantação da governança da tecnologia da informação na administração pública federal. Revista do Serviço Público, v. 70, n. 4, 2019. DOI: https://doi.org/10.21874/RSP.V70I4.3495.

RODRIGUES, K. F. O sigilo nas Forças Armadas brasileiras: normas e procedimentos para classificar informações com base na segurança do Estado e da sociedade. Revista Direito GV, v. 20, 2024. DOI: https://doi.org/10.1590/2317-6172202415.

SANTOS, R. F. et al. Modelo de gestão da informação aplicado ao Exército Brasileiro. Revista Políticas Públicas & Cidades, v. 13, n. 2, 2024. DOI: https://doi.org/10.23900/2359-1552v13n2-9-2024.

SCHINAGL, S.; SHAHIM, A. What do we know about information security governance? From the basement to the boardroom: towards digital security governance. Information & Computer Security, 2020. DOI: https://doi.org/10.1108/ICS-02-2019-0033.

SOININEN, J. Cybersecurity governance in information technology: a review of what has been done and what is next. 2021. DOI: https://doi.org/10.1007/978-981-19-0898-9_22.

SOLMS, R. von; THOMSON, K.; MANINJWA, P. M. Information security governance control through comprehensive policy architectures. 2011. DOI: https://doi.org/10.1109/ISSA.2011.6027522.

SOUZA, J. A.; SEIXAS, R. J. S.; FRAGOSO, M. D. Reflexões do direito administrativo e da teoria do ciclo de políticas públicas aplicadas às operações de inteligência da ABIN. Diké, v. 23, n. 27, p. 33-68, 2024. DOI: https://doi.org/10.36113/dike.27.2024.4570.

TOAZA, G.; MONTENEGRO, C.; SALAZAR, C. Designing an I&T governance system in the context of strategic public sector based on COBIT 2019 framework: case study in a developing country. 2022. DOI: https://doi.org/10.1145/3564858.3564920.

VIANNA, E. W.; FERNANDES, J. H. C. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos. 2015.

VON SOLMS, B.; VON SOLMS, R. From information security to corporate governance. Computers & Security, 2004.

WEILL, P.; ROSS, J. W. IT governance: how top performers manage IT decision rights for superior results. Boston: Harvard Business School Press, 2004.

APÊNDICE 1: RESUMO DESCRITIVO DOS ESTUDOS

Quadro 4 – Resumo descritivo dos estudos.

Estudo	Alinhamento das políticas com as normas	Características do quadro de governança	Integração da segurança cibernética na defesa	Desafios e facilitadores institucionais	Enquadramentos teóricos no desenvolvimento de políticas
(Baldissera et al., 2024)	Aderência parcial à norma ISO/IEC 27002:2022, com lacunas nos controles tecnológicos	Normas militares abrangentes, mas desatualizadas em alguns aspectos	Governança de segurança cibernética parcialmente integrada, necessita de fortalecimento	Lacunas legislativas e necessidade de atualizações contínuas	Enfatiza as normas internacionais como base para as políticas
(Santos et al., 2024)	Foco na gestão estruturada da informação, alinhada aos objetivos organizacionais	Modelo enfatiza o mapeamento de processos e a governança de dados	A segurança cibernética como parte da gestão do fluxo de informações	Preferência organizacional por abordagens estruturadas	Utiliza teorias de gestão da informação para a concepção do modelo
(Silva, 2026)	Em conformidade com as normas internacionais e os requisitos regulatórios	Governança programática que integra risco e continuidade	A segurança cibernética incluída como componente central da governança	Enfatiza a auditabilidade e a escalabilidade	Estrutura conceitual para a integração de políticas
(Cunha et al., 2024)	Comparado com as melhores práticas de governança do setor público	Ferramenta estratégica para avaliar a maturidade da governança	Foco na maturidade da governança em segurança cibernética	Identifica lacunas e promove a melhoria contínua	Utiliza ferramentas estratégicas de avaliação da governança
(Toaza et al., 2022)	Aplicação do COBIT 2019 no contexto do setor público militar	Sistema de governança projetado para as especificidades do setor público	Governança de segurança cibernética integrada por meio do COBIT	Consideração dos fatores contextuais dos países em desenvolvimento	Abordagem de projeto de governança baseada em um quadro de referência
(Reis & Neto, 2019)	Fatores de sucesso alinhados às políticas da administração pública federal	Identifica fatores críticos de sucesso para a governança de TI	Governança de segurança cibernética vinculada ao apoio da alta administração	Destaca a importância da liderança e da comunicação	Identificação empírica dos fatores de sucesso da governança
(Vianna & Fernandes, 2015)	Políticas de segurança da informação alinhadas ao ambiente cibernético federal	Governança estratificada em níveis operacional, tático e estratégico	Gestão da segurança cibernética detalhada em todos os níveis de governança	Desafios na gestão de atores distribuídos e diversos	Estrutura prática de estratificação da governança
(Souza et al., 2024)	Teoria do ciclo de políticas públicas aplicada à governança da inteligência	Ciclo de inteligência vinculado à governança administrativa	Governança da segurança cibernética vinculada às operações de inteligência	Opacidade institucional e questões de prestação de contas	Combina o direito administrativo e a teoria do ciclo de políticas
(Rodrigues, 2023)	Classificação de segurança alinhada às normas de sigilo de Estado	Governança centrada nos processos de classificação de informações	Governança da segurança cibernética implícita nos	Desafios relacionados ao poder discricionário e	Análise do marco jurídico e regulatório

			controles de classificação	lacunas de transparência	
(Sarmento & Rocha, 2025)	Alinha-se aos modelos internacionais de agências de defesa cibernética	Propõe uma estrutura organizacional para a agência de defesa cibernética	Governança da segurança cibernética centralizada na nova agência	Desafios jurídicos, tecnológicos e operacionais	Elaboração de políticas baseada em análises comparativas
(Sousa et al., 2025)	Estrutura nacional alinhada às regulamentações internacionais	Priorização de medidas de segurança por meio do método AHP	Governança de segurança cibernética integrada à estrutura nacional	Enfatiza a tomada de decisões e a alocação de recursos	Utiliza o processo hierárquico analítico para a priorização de políticas
(Goldoni et al., 2024)	A política nacional apresenta documentos abrangentes, mas desconexos	Estrutura de governança analisada quanto à coerência e maturidade	Governança de segurança cibernética fragmentada e em evolução	Maturidade da implementação e lacunas nas ferramentas políticas	Análise de políticas com foco na estrutura de governança
(Brito et al., 2024)	Mapeamento das políticas de defesa e segurança cibernética com sua evolução histórica	Identificação dos desafios de governança no setor de defesa cibernética	A relação entre a governança da segurança cibernética e a evolução da política de defesa	Déficits de recursos e desafios de complexidade	Análise de políticas com métodos mistos
(Martins et al., 2023)	Políticas alinhadas à proteção de infraestruturas críticas nacionais	Funções de governança das Forças Armadas na defesa de infraestruturas	Governança da segurança cibernética integrada às infraestruturas críticas	Coordenação institucional entre os setores de defesa	Análise exploratória de documentos
(Cintiene, 2025)	Planejamento baseado em capacidades alinhado às necessidades estratégicas de defesa	Governança focada na coordenação interagências	Governança da segurança cibernética como parte da resposta a ameaças complexas	Desafios de coordenação política e institucional	Teoria do planejamento baseado em capacidades
(Júnior, 2022)	Conceito de transformação parcialmente alinhado com os objetivos de modernização	A governança reflete tendências de determinismo tecnológico	A governança da segurança cibernética está incluída em projetos específicos	Limitações conceituais na compreensão da transformação	Estudo de caso com análise documental
(Ording et al., 2022	Fatores que influenciam a elaboração de políticas sob pressões institucionais	O desenvolvimento da governança moldado pelo contexto organizacional	A governança da segurança cibernética influenciada pela legitimidade e pelas normas	A teoria institucional destaca fatores contextuais	A perspectiva da teoria institucional sobre os fatores que influenciam as políticas
(Aflakhah & Soewito, 2024)	COBIT 2019 e ISO 27001 utilizados para a avaliação da governança	Maturidade da governança avaliada com lacunas identificadas	Maturidade da governança em cibersegurança abaixo dos níveis almejados	Necessidade de melhorias abrangentes enfatizada	Integração de estruturas para a avaliação da governança
(Martins et al., 2014)	A doutrina militar limita ou promove a aplicação de controles de segurança	Estrutura de governança orientada para vetores de ataque militar	Governança de segurança cibernética focada na proteção de	Desafios na integração entre doutrina e controles	Desenvolvimento de uma estrutura baseada no contexto militar

			informações militares		
(Hendry et al., 2025)	A integração do COBIT 2019 e da ISO/IEC 27001 melhora o alinhamento	A estrutura de governança fortalece os vínculos estratégicos e operacionais	A governança da segurança cibernética é aprimorada por meio da síntese da estrutura	A validação por especialistas confirma os benefícios operacionais	Desenvolvimento e validação da estrutura integrada
(Meyer, 2022)	Crítica à militarização da governança da segurança cibernética	A governança concebida como um domínio militarizado	A governança da segurança cibernética dominada por perspectivas militares	Apelos por um envolvimento social mais amplo	Revisão crítica da literatura
(Soininen, 2021)	Análise dos principais marcos de governança em segurança cibernética	Análise dos fundamentos teóricos da governança	Avaliação das limitações dos marcos de governança em segurança cibernética	Sugestão de novos marcos para pesquisas futuras	Revisão teórica e crítica dos marcos
(Nodehi et al., 2024)	As interações entre o CISO e o conselho variam de acordo com o contexto organizacional	Governança caracterizada por estratégias adaptativas e contingentes	Governança de segurança cibernética moldada por dinâmicas relacionais	Enfatiza abordagens de governança sensíveis ao contexto	Teoria da contingência aplicada à governança
(Schinagl & Shahim, 2020)	Transição da segurança isolada para a governança digital estratégica	Revisão da literatura sobre governança para avaliar o impacto da digitalização	A governança da segurança cibernética está evoluindo para um enfoque na resiliência	Destaca tensões e lacunas nas abordagens atuais	Revisão da literatura conceitual

Fonte: elaborado pelos autores.

APÊNDICE 2: ANÁLISE CRÍTICA E SÍNTESE

Quadro 5 – Análise crítica e síntese.

Aspecto	Pontos fortes	Pontos fracos
Alinhamento com normas internacionais	Vários estudos demonstram esforços para alinhar as políticas de segurança da informação do Exército Brasileiro com estruturas internacionais, como a ISO/IEC 27002:2022 e o COBIT 2019, proporcionando estruturas de controle abrangentes e atualizadas que reforçam a postura de segurança e a confiança das partes interessadas (Toaza et al., 2022). Esse alinhamento facilita a comparação com as melhores práticas globais e apoia a modernização institucional.	Apesar de fazer referência a normas internacionais, alguns regulamentos militares apresentam lacunas, particularmente em controles tecnológicos e normas legadas, indicando adesão parcial e a necessidade de atualizações contínuas (Baldissera et al., 2024). A literatura também aponta para uma falta de clareza sobre o grau de maturidade e o *status* de implementação desses alinhamentos dentro dos órgãos consultivos militares (Goldoni et al., 2024).
Estruturas teóricas e modelos de desenvolvimento de políticas	A literatura apresenta diversos modelos teóricos, incluindo perspectivas da teoria institucional sobre os fatores que influenciam as políticas e abordagens contingentes à tomada de decisões de governança, que enriquecem a compreensão da formulação de políticas em contextos militares (Nodehi et al., 2024). Estruturas como a PPGSI oferecem arquiteturas de governança estruturadas e	Muitas estruturas permanecem conceituais ou em estágios iniciais de validação, com evidências empíricas limitadas sobre sua eficácia no ambiente de assessoria estratégica do Exército Brasileiro (Hendry et al., 2025). Há também uma tendência ao determinismo tecnológico em alguns conceitos de transformação militar, o que pode levar a

	escaláveis que integram gestão de riscos e conformidade (Silva, 2026).	ignorar fatores organizacionais e culturais mais amplos (Júnior, 2022).
Fatores institucionais e organizacionais	Pesquisas destacam o papel das pressões institucionais, dos comportamentos voltados para a busca de legitimidade e da cultura organizacional na definição da governança da segurança da informação, enfatizando a importância de estratégias de governança adaptativas, adaptadas aos contextos organizacionais militares (Nodehi et al., 2024). Estudos também destacam a influência do apoio administrativo de alto nível e do alinhamento estratégico na implementação bem-sucedida da governança (Reis & Neto, 2019) (Cunha & Neto, 2014).	Os desafios institucionais incluem estruturas de governança fragmentadas, coordenação interagências limitada e a militarização da governança da segurança cibernética, o que pode dificultar o desenvolvimento de políticas inclusivas e eficazes (Oliveira, 2021). A literatura revela tensões entre as abordagens militar e civil, complicando a coerência da governança.
Integração da governança de cibersegurança nas políticas mais amplas de defesa	A governança de cibersegurança do Exército Brasileiro é cada vez mais reconhecida como parte integrante das estratégias de defesa nacional, com iniciativas voltadas para a gestão cibernética conjunta e a interoperabilidade entre as Forças Armadas (Sarmento & Rocha, 2025) (Cintiene, 2025). Estratégias nacionais como o E-Ciber fornecem uma estrutura baseada em princípios que promove a coordenação, a integração de conhecimento e a capacitação.	Apesar das estruturas estratégicas, a integração prática permanece desigual, com lacunas persistentes na coordenação operacional e na coerência de políticas entre os setores militar e público (Goldoni et al., 2024). A abordagem militarizada da governança da cibersegurança pode limitar um engajamento social mais amplo e a cooperação multissetorial (Meyer, 2022).
Rigor metodológico e validação empírica	Alguns estudos empregam metodologias qualitativas robustas, incluindo grupos focais, etnografia e métodos Delphi, para captar percepções detalhadas sobre práticas de governança e fatores críticos de sucesso (Santos et al., 2024) (Reis & Neto, 2019) (Cunha & Neto, 2014). Estudos de caso que aplicam as normas COBIT e ISO fornecem avaliações práticas da maturidade da governança (Toaza et al., 2022) (Aflakhah & Soewito, 2024).	De modo geral, a pesquisa empírica específica sobre os órgãos de assessoria estratégica do Exército Brasileiro é limitada, com muitos estudos baseando-se em dados secundários ou em análises conceituais (Júnior, 2022). Há escassez de avaliações longitudinais ou quantitativas que meçam o impacto das estruturas de governança nos resultados de segurança (Hendry et al., 2025).
Implementação de políticas e desafios operacionais	A literatura reconhece a complexidade de traduzir políticas de governança em controles operacionais eficazes, destacando questões como a divulgação de políticas, a medição da conformidade e o ciclo de controle direto na governança da segurança da informação (Manjezi & Botha, 2019). A estratificação da gestão da segurança cibernética em níveis operacionais, táticos e estratégicos reflete uma compreensão da complexidade da governança (Vianna & Fernandes, 2015).	Os desafios de implementação incluem a divulgação insuficiente das políticas para os níveis operacionais, dificuldades no monitoramento da conformidade e a necessidade de capacitação contínua (Solms et al., 2011). O cenário de ameaças em constante evolução e as rápidas mudanças tecnológicas exigem mecanismos de governança ágeis que ainda não foram plenamente concretizados (Schinagl et al., 2021).
Relações civis-militares e dinâmicas de governança	Estudos reconhecem a interação contínua entre atores civis e militares na governança da segurança cibernética no Brasil, o que contribui para a segurança estratégica e a defesa, mas também gera tensões de governança. A literatura sugere a cooperação multissetorial para uma governança eficaz e o desenvolvimento de políticas.	A militarização da governança da segurança cibernética pode criar barreiras a um envolvimento social mais amplo e limitar a transparência, afetando potencialmente a legitimidade e a adaptabilidade das políticas (Meyer, 2022) (Oliveira, 2021). A literatura apela por mecanismos aprimorados para equilibrar os imperativos militares com os princípios da governança democrática (Rodrigues, 2023).

Fonte: elaborado pelos autores.

APÊNDICE 3: REVISÃO TEMÁTICA DA LITERATURA

Quadro 6 – Revisão temática da literatura.

Tema	Aparece em	Descrição do tema
Alinhamento das políticas de segurança da informação das Forças Armadas brasileiras com as normas internacionais	15/24 artigos	A pesquisa destaca a adesão parcial das políticas de segurança da informação do Exército Brasileiro a normas internacionais como a ISO/IEC 27002, com lacunas identificadas nos controles tecnológicos e normas desatualizadas (Aflakhah & Soewito, 2024) (Carvalho, 2006).
Integração e aplicação de estruturas de governança (COBIT, ISO e outras)	13/24 artigos	Vários estudos se concentram na aplicação de estruturas de governança, como COBIT 2019 e ISO/IEC 27001/27002, em instituições militares e públicas federais, enfatizando a harmonização e a síntese para fortalecer o alinhamento estratégico, a gestão de riscos e a conformidade. Estruturas são propostas e validadas por meio de estudos de caso, análises de especialistas e modelos integrados para melhorar a governança e a coordenação da segurança (Toaza et al., 2022) (Hendry et al., 2025).
Governança da Cibersegurança e Estratégia de Defesa Nacional	12/24 artigos	A Estratégia Nacional de Cibersegurança (E-Ciber) e as políticas de defesa relacionadas representam um foco central, com pesquisas que analisam a evolução da governança da cibersegurança no Brasil, os desafios estratégicos e os esforços de institucionalização. Esses trabalhos destacam o impacto da pandemia nas superfícies de ameaça, a militarização da cibersegurança e a necessidade de respostas multissetoriais coordenadas e alinhadas às prioridades de defesa nacional (Goldoni et al., 2024) (Meyer, 2022).
Influências institucionais e organizacionais no desenvolvimento de políticas	10/24 artigos	Estudos que aplicam a teoria institucional destacam o papel significativo do contexto organizacional, das pressões institucionais e da legitimidade na definição do desenvolvimento de políticas de segurança da informação. Contribuições de autoridades superiores, crenças das partes interessadas e estratégias de governança adaptativa são consideradas cruciais para a formulação e implementação eficazes de políticas nos setores militar e público (Ording et al., 2022) (Nodehi et al., 2024) (Schinagl et al., 2021).
Relações entre os setores civil e militar e a colaboração na governança da segurança cibernética	7/24 artigos	A pesquisa aborda a relação entre atores civis e militares na governança da segurança cibernética no Brasil, apontando para uma interação contínua por meio de pesquisas e debates estratégicos que contribuem para avanços na governança. Persistem desafios na integração de visões organizacionais conjuntas para a interoperabilidade em operações de informação (Manjezi & Botha, 2019).
Processos de elaboração de políticas e marcos teóricos	6/24 artigos	A literatura explora os fundamentos teóricos que orientam os ciclos de políticas, tais como o Ciclo de Inteligência e a Teoria das Políticas Públicas, aplicados à inteligência militar e à elaboração de políticas de segurança da informação. Esses marcos facilitam a compreensão dos desafios processuais e de prestação de contas dentro de órgãos consultivos estratégicos (Souza et al., 2024) (Solms et al., 2011).
Desafios na implementação e aplicação de políticas de segurança da informação	6/24 artigos	Entre os obstáculos comuns estão a legislação obsoleta, a falta de divulgação das políticas no nível operacional, as deficiências de coordenação e os obstáculos político-institucionais que afetam a aplicação das políticas. Estudos sugerem que lacunas em maturidade e preparação dificultam a execução eficaz de medidas de governança em contextos militares (Vianna & Fernandes, 2015) (Schinagl et al., 2021) (Manjezi & Botha, 2019).

Papel dos Comitês de Governança da Segurança da Informação e da Liderança	5/24 artigos	Destaca-se a importância do apoio da alta administração, da comunicação estratégica e dos comitês de governança, especialmente no que diz respeito aos seus papéis na tomada de decisões e na supervisão de políticas. Os fatores críticos de sucesso identificados destacam a necessidade de envolvimento contínuo da liderança e das partes interessadas na administração pública federal (Reis & Neto, 2019) (Cunha & Neto, 2014) (Nodehi et al., 2024).
Inovação tecnológica e integração na defesa cibernética	4/24 artigos	Estudos destacam a inovação tecnológica e a gestão conjunta do setor cibernético como elementos para a integração das Operações de Informação no Brasil, com recomendações para a unificação das estruturas cibernéticas a fim de aprimorar a interoperabilidade entre as Forças Armadas (Júnior, 2022).
A política de segurança cibernética como componente da liderança regional e da estratégia internacional	3/24 artigos	Alguns trabalhos analisam a política de segurança cibernética do Brasil como parte de sua estratégia de *soft power* e liderança regional no Sul Global, destacando benefícios e incoerências que afetam a projeção de segurança internacional do país (Lobato, 2017).
Teoria da Governança da Segurança da Informação e Direções Futuras	3/24 artigos	As análises da literatura sobre governança da segurança da informação apontam para a necessidade de ampliar os marcos teóricos para além das abordagens tradicionais, sugerindo que a governança da segurança digital é um domínio em evolução que requer modelos de governança contingentes e adaptativos (Soininen, 2021) (Schinagl & Shahim, 2020).

Fonte: elaborado pelos autores.

APÊNDICE 4: REVISÃO CRONOLÓGICA DA LITERATURA

Quadro 7 – Revisão cronológica da literatura.

Período	Área de pesquisa	Descrição
2006–2014	Fundamentos da Governança de TI e Estruturas de Segurança da Informação Militar	A pesquisa inicial concentrou-se no estabelecimento de estruturas de governança para TI e segurança da informação em organizações públicas e militares, destacando lacunas na divulgação de políticas e nos mecanismos de controle. Os estudos propuseram estruturas para a gestão da segurança da informação em contextos militares e diretrizes para a aplicação de estruturas de governança de TI em órgãos públicos federais brasileiros.
2015–2019	Identificação dos fatores críticos de sucesso e dos desafios de governança na segurança do setor público	A pesquisa explorou os fatores críticos de sucesso para a implementação da governança de TI na administração pública federal, com ênfase no envolvimento da liderança e no alinhamento com os objetivos de negócios. Os estudos também examinaram os desafios da gestão das operações de segurança cibernética, incluindo as funções dos gestores de segurança e a integração da governança de segurança às estratégias organizacionais mais amplas nas instituições públicas.
2020–2022	Estratégias emergentes de segurança cibernética e perspectivas teóricas no Brasil	Este período marcou a publicação da Estratégia Nacional de Segurança Cibernética do Brasil e a análise de suas implicações. As pesquisas abordaram o panorama em evolução da governança da segurança cibernética, a militarização dos esforços nessa área e a aplicação de estruturas internacionais, como o COBIT, na governança de TI do setor público. As investigações teóricas sobre as limitações da governança da segurança da informação e o papel das forças institucionais no desenvolvimento de políticas ganharam destaque.
2023–2025	Integração avançada, desenvolvimento de políticas estratégicas e cooperação multissetorial	Estudos recentes se concentram na integração de estruturas de governança, como o COBIT e as normas ISO, na institucionalização de agendas de segurança cibernética e na abordagem da complexa relação entre os setores civil e militar na governança da segurança cibernética. A pesquisa enfatiza funções de consultoria estratégica, inovação em operações de defesa cibernética e a necessidade de modelos de políticas adaptáveis para aprimorar as capacidades de defesa nacional e alinhá-las às normas internacionais. As investigações também destacam os

		desafios da coerência das políticas, da maturidade da governança e do desenvolvimento de agências nacionais de defesa cibernética.

Fonte: elaborado pelos autores.

APÊNDICE 5: CONSENSO E DIVERGÊNCIAS ENTRE OS ESTUDOS

Quadro 8 – Consenso e divergências entre os estudos.

Critério de comparação	Estudos em concordância	Estudos em divergência	Possíveis explicações
Alinhamento com normas internacionais	Os estudos geralmente concordam que a adesão a estruturas internacionais como a ISO/IEC 27002 e o COBIT aprimora a governança da segurança da informação; os setores militar e público brasileiros demonstram conformidade parcial e buscam melhorias por meio dessas normas (Aflakhah & Soewito, 2024) (Hendry et al., 2025).	Alguns estudos destacam lacunas na conformidade e a necessidade de atualizações na legislação e nas políticas militares, indicando adesão parcial ou inconsistente (Baldissera et al., 2024) (Goldoni et al., 2024).	As diferenças surgem devido à inércia institucional, aos sistemas legados ou a atrasos nas atualizações legislativas entre agências militares e civis, afetando os níveis de conformidade.
Integração e concepção de estruturas	Vários artigos defendem modelos de governança integrada que combinam gestão de riscos, conformidade e alinhamento estratégico (por exemplo, a estrutura PPGSI, IGSF) para organizações complexas (Silva, 2026) (Hendry et al., 2025) (Toaza et al., 2022). A importância de uma governança programática e adaptável é enfatizada.	Existe divergência quanto ao grau em que essas estruturas são adotadas ou operacionalizadas em órgãos consultivos militares em comparação com o setor público civil, com algumas organizações ainda dependendo de modelos fragmentados ou normativos (Martins et al., 2014) (Toaza et al., 2022).	As variações podem ser devidas à complexidade organizacional, aos diferentes ambientes operacionais e à natureza evolutiva das ameaças à segurança cibernética, que exigem estruturas personalizadas.
Relações de governança entre os setores civil e militar	Há consenso quanto à necessidade de cooperação entre os setores civil e militar para aprimorar a governança da segurança cibernética, reconhecendo os benefícios mútuos e os desafios comuns.	No entanto, alguns estudos criticam a centralização da militarização da governança da segurança cibernética no Brasil, o que pode limitar um engajamento social mais amplo e a colaboração multissetorial (Meyer, 2022) (Oliveira, 2021).	A divergência reflete tensões entre paradigmas de segurança que priorizam o controle militar e aqueles que defendem uma governança inclusiva envolvendo a sociedade civil e outras partes interessadas.
Desafios no desenvolvimento de políticas e fatores institucionais	Os autores concordam que as pressões institucionais, as expectativas das partes interessadas e a cultura organizacional influenciam significativamente o desenvolvimento de políticas e o sucesso de sua implementação (Ording et al., 2022) (Nodehi et al., 2024) (Schinagl et al., 2021).	A necessidade de apoio da alta administração e alinhamento com os objetivos de negócios é amplamente enfatizada. Discordâncias surgem quanto à eficácia percebida das políticas existentes, com alguns relatórios destacando baixos níveis de maturidade e lacunas na implementação, especialmente em contextos do setor público (Aflakhah & Soewito, 2024) (Goldoni et al., 2024) (Reis & Neto, 2019).	As diferenças podem ser atribuídas a variações na capacidade institucional, na disponibilidade de recursos e no panorama político-institucional que afeta a maturidade da governança.

Estratégia de segurança cibernética e integração com a defesa nacional	Os estudos concordam quanto à crescente relevância da segurança cibernética nas estratégias de defesa nacional e nos esforços de modernização do Exército Brasileiro, com ênfase na inovação tecnológica e nas operações conjuntas.	Existem visões divergentes sobre a coerência estratégica e o planejamento de longo prazo das políticas de defesa cibernética, com alguns apontando a falta de uma política nacional coesa e iniciativas fragmentadas (Meyer, 2022) (Goldoni et al., 2024).	As disparidades decorrem de cenários de ameaças em evolução, da complexidade burocrática e dos desafios de articular políticas públicas de longo prazo em um ambiente de segurança dinâmico.
O papel das normas e dos modelos na governança	Há consenso quanto à utilidade de normas como a ISO 27001, o COBIT 2019 e os modelos do NIST na estruturação de processos e controles de governança (Toaza et al., 2022) (Aflakhah & Soewito, 2024) (Hendry et al., 2025).	No entanto, alguns destacam dificuldades na aplicação prática e no controle eficaz das políticas de segurança em todos os níveis organizacionais, indicando lacunas entre a teoria e a prática (Solms et al., 2011) (Manjezi & Botha, 2019) (Ording et al., 2022).	Essa divergência pode refletir desafios na operacionalização de estruturas dentro de organizações complexas e hierárquicas, bem como no equilíbrio entre diretrizes estratégicas e realidades operacionais.
Maturidade e implementação da governança de segurança da informação	Vários estudos revelam que muitas instituições, incluindo os setores militar e público federal, ainda não alcançaram os níveis de maturidade desejados em governança de segurança, indicando espaço para crescimento (Reis & Neto, 2019) (Aflakhah & Soewito, 2024) (Goldoni et al., 2024).	Por outro lado, algumas estruturas e programas demonstram progresso e propõem ações estratégicas para melhoria, sinalizando trajetórias de desenvolvimento positivas (Cunha et al., 2024) (Hendry et al., 2025) (Nodehi et al., 2024).	As discrepâncias podem ser explicadas por diferenças no compromisso institucional, na alocação de recursos e nos modelos específicos de governança empregados.

Fonte: elaborado pelos autores.