UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC
DIRETORIA DE PESQUISA, PÓS-GRADUAÇÃO, INOVAÇÃO E EXTENSÃO - PROPIEX
PROGRAMA DE PÓS-GRADUAÇÃO EM DESENVOLVIMENTO SOCIOECONÔMICO - PPGDS
DOUTORADO EM DESENVOLVIMENTO SOCIOECONÔMICO

LUAN PHILIPPI MACHADO

CIBERSEGURANÇA E DESENVOLVIMENTO SOCIOECONÔMICO DAS CIDADES: MATURIDADE INSTITUCIONAL E REGULAÇÃO NOS MUNICÍPIOS DA REGIÃO DA AMREC

CRICIÚMA
2025

LUAN PHILIPPI MACHADO

CIBERSEGURANÇA E DESENVOLVIMENTO SOCIOECONÔMICO DAS CIDADES: MATURIDADE INSTITUCIONAL E REGULAÇÃO NOS MUNICÍPIOS DA REGIÃO DA AMREC

Tese apresentada ao Programa de Pós-Graduação em Desenvolvimento Socioeconômico da Universidade do Extremo Sul Catarinense - UNESC, como requisito parcial para a obtenção do título de Doutor em Desenvolvimento Socioeconômico.

Orientador: Prof. Dr. Sílvio Parodi Oliveira Camilo
Coorientadora: Profa. Dra. Melissa Watanabe

CRICIÚMA

2025

Dados Internacionais de Catalogação na Publicação

M149i Machado, Luan Philippi.
Cibersegurança e desenvolvimento socioeconômico das cidades : maturidade institucional e regulação nos municípios da região da AMREC / Luan Philippi Machado. - 2025.
205 p. : il.

Tese (Doutorado) - Universidade do Extremo Sul Catarinense, Programa de Pós-Graduação em Desenvolvimento Socioeconômico, Criciúma, 2025.
Orientação: Sílvio Parodi Oliveira Camilo.
Coorientação: Melissa Watanabe.

1. Cibersegurança. 2. Cibernética - Medidas de segurança. 3. Proteção de dados. 4. Capacidade institucional. 5. Sociedade da informação. 6. Segurança da informação. I. Título.

CDD 23. ed. 003.5

Bibliotecária Eliziane de Lucca Alosilla – CRB 14/1101
Biblioteca Central Prof. Eurico Back - UNESC

Luan Philippi Machado

CIBERSEGURANÇA E DESENVOLVIMENTO SOCIOECONÔMICO DAS CIDADES: MATURIDADE INSTITUCIONAL E REGULAÇÃO NOS MUNICÍPIOS DA REGIÃO DA AMREC

Esta tese foi julgada e aprovada para obtenção do Grau de Doutor(a) em Desenvolvimento Socioeconômico no Programa de Pós-Graduação em Desenvolvimento Socioeconômico da Universidade do Extremo Sul Catarinense.

Criciúma, 30 de setembro de 2025.

BANCA EXAMINADORA

Prof. Dr. Sílvio Parodi Oliveira Camilo
(Presidente e Orientador – UNESC)

gov.br Documento assinado digitalmente
MELISSA WATANABE
Data: 14/10/2025 18:15:23-0300
Verifique em https://validar.iti.gov.br

(Coorientadora – UFPR)

Prof. Dr. Vilson Gruber
(Membro – UFSC)

Prof. Dr. Dimas de Oliveira Estevam
(Membro – UNESC)

Prof. Dr. Rogério Antônio Casagrande
(Membro – UNESC)

Prof. Dr. Thiago Rocha Fabris
(Membro – UNESC)

Luan Philippi Machado
(Discente)

Prof. Dr. Dimas de Oliveira Estevam
Coordenador do PPGDS – UNESC

Dedico esta tese aos meus amados avós, Genésio e Olinda, que partiram em 2024. A ausência deles deixou um vazio profundo, mas o amor, a sabedoria e o exemplo que me deixaram continuam vivos em mim. Esta conquista carrega a marca da força que herdei deles. Com toda a saudade e gratidão, esta obra é para vocês.

AGRADECIMENTOS

A Deus, por ser fonte de sabedoria, força e serenidade em todos os momentos dessa jornada. Foi na fé e na espiritualidade que encontrei alento para enfrentar os desafios e coragem para seguir adiante.

À minha família, pelo amor incondicional e por compreenderem, com generosidade, os momentos de ausência. Cada gesto de apoio silencioso e compreensão teve um papel fundamental para que eu pudesse me dedicar a esta caminhada.

Ao Pedro Henrique, pelo companheirismo sensível e respeitoso. Sua capacidade de compreender meus silêncios, apoiar minhas escolhas e caminhar ao meu lado, mesmo nos momentos em que eu precisei me recolher, foi essencial.

Aos meus amigos, que foram abrigo, incentivo e inspiração. Em meio às exigências da vida acadêmica, vocês mantiveram viva a leveza e a esperança, sendo base afetiva para que eu continuasse.

Ao meu orientador, Sílvio Parodi, por sua escuta atenta, orientação segura e generosidade intelectual. Sua confiança no meu trabalho e sua dedicação foram fundamentais para que eu conseguisse avançar com firmeza. À minha coorientadora, Melissa Watanabe, por sua contribuição cuidadosa e precisa ao longo desta trajetória.

Aos docentes do PPGDS, pelo compromisso com a formação acadêmica, pelo conhecimento compartilhado e pelas provocações que me impulsionaram a pensar de forma mais ampla e crítica.

Aos colegas que conheci no PPGDS, pela convivência rica e pelas trocas que transcenderam o espaço acadêmico. A amizade e a colaboração de vocês tornaram essa trajetória mais leve e significativa.

À Professora Gisele Silveira Coelho Lopes, reitora em exercício da UNESC, pela atenção dedicada e incentivo constante à pesquisa e à produção científica. Estendo, em seu nome, minha gratidão a todos os membros da gestão da universidade, pelo compromisso com o desenvolvimento acadêmico.

Ao UNIEDU, programa que, por meio da concessão de bolsa, viabilizou financeiramente o desenvolvimento desta pesquisa. Essa política pública de fomento foi essencial para que este trabalho se concretizasse.

Aos entrevistados que representaram os municípios da AMREC, por dedicarem seu tempo e compartilharem conhecimentos e experiências que deram vida a esta pesquisa. Sem suas contribuições generosas, este estudo não teria sido possível.

À Coordenação do Curso de Ciências Contábeis da UNESC, pela compreensão diante das exigências desta fase e pela sensibilidade em me permitir o afastamento de algumas demandas. Esse apoio foi determinante para minha concentração e dedicação à tese.

À equipe do SEPLAN, setor que tenho a honra de coordenar, pela maturidade e compreensão diante da minha ausência em alguns momentos. A confiança e o suporte de vocês foram essenciais para que eu pudesse conciliar responsabilidades.

A todos que contribuíram para este momento, direta ou indiretamente, meus sinceros agradecimentos. Cada palavra, gesto, incentivo e colaboração deixaram marcas nesta trajetória que agora se concretiza em forma de tese.

“Só existem dois dias no ano que nada pode ser feito. Um se chama ontem e o outro se chama amanhã. Portanto hoje é o dia certo para amar, acreditar, fazer e principalmente viver.” Dalai Lama

RESUMO

MACHADO, Luan Philippi. **Cibersegurança e desenvolvimento socioeconômico das cidades: maturidade institucional e regulação nos municípios da região da AMREC.** 2025. 189f. Tese (Doutorado em Desenvolvimento Socioeconômico). Programa de Pós-Graduação em Desenvolvimento Socioeconômico – PPGDS da Universidade do Extremo Sul Catarinense – UNESC, Criciúma, 2025.

A crescente digitalização das estruturas sociais, econômicas e governamentais tem ampliado a relevância da cibersegurança como pilar estratégico para o desenvolvimento e a proteção de dados. No contexto brasileiro, e especialmente na realidade municipal, observam-se lacunas significativas na maturidade institucional e na adoção de políticas efetivas para gestão da segurança da informação. Essa tese tem como objetivo compreender e propor mecanismos que fortaleçam a governança cibernética municipal, tomando como unidade de análise a região da Associação dos Municípios da Região Carbonífera (AMREC). Para atingir esse objetivo, a pesquisa foi estruturada em quatro estudos complementares. O primeiro realizou uma revisão bibliométrica e sistemática da literatura internacional e nacional, identificando tendências e limitações na produção científica sobre cibersegurança. O segundo conduziu uma análise conceitual aprofundada a partir de clusters temáticos, evidenciando constructos emergentes na interface entre cibersegurança e desenvolvimento. O terceiro adotou um estudo de caso, envolvendo entrevistas semiestruturadas com representantes dos doze municípios da AMREC, de modo a mapear níveis de maturidade, capacidades institucionais e fragilidades locais. O quarto estudo, de caráter propositivo, elaborou diretrizes estratégicas para a construção de um marco legal municipal de cibersegurança, fundamentado nos achados empíricos e teóricos dos estudos anteriores. Os resultados evidenciam que, apesar do avanço normativo em âmbito federal — como o Marco Civil da Internet e a Lei Geral de Proteção de Dados —, a maioria dos municípios pesquisados carece de instrumentos legais, estruturas organizacionais e políticas específicas para proteção digital. A análise aponta ainda que a ausência de integração entre dimensões legais, institucionais, operacionais e epistemológicas compromete a efetividade da governança cibernética local. Como contribuição, a tese apresenta um modelo conceitual e normativo que pode ser replicado por outros municípios brasileiros, promovendo maior alinhamento entre legislações, práticas institucionais e estratégias de proteção de dados.

Palavras-chave: Governança Cibernética. Proteção de dados. Capacidade Institucional. Políticas de Segurança da Informação.

ABSTRACT

MACHADO, Luan Philippi. **Cybersecurity and Socioeconomic Development of Cities: Institutional Maturity and Regulation in the Municipalities of the AMREC Region.** 2025. 189f. Tese (Doutorado em Desenvolvimento Socioeconômico). Programa de Pós-Graduação em Desenvolvimento Socioeconômico – PPGDS da Universidade do Extremo Sul Catarinense – UNESC, Criciúma, 2025.

The growing digitalization of social, economic, and governmental structures has increased the relevance of cybersecurity as a strategic pillar for development and data protection. In the Brazilian context, and particularly at the municipal level, there are significant gaps in institutional maturity and in the adoption of effective policies for information security management. This thesis aims to understand and propose mechanisms to strengthen municipal cyber governance, using as its analyse unit the region of the Association of Municipalities of the Carboniferous Region (AMREC). To achieve this objective, the research was structured into four complementary studies. The first carried out a bibliometric and systematic review of international and national literature, identifying trends and limitations in scientific production on cybersecurity. The second conducted an in-depth conceptual analysis based on thematic clusters, highlighting emerging constructs at the interface between cybersecurity and development. The third adopted a case study approach, involving semi-structured interviews with representatives from the twelve municipalities of AMREC to map levels of maturity, institutional capacities, and local vulnerabilities. The fourth, of a propositional nature, developed strategic guidelines for the construction of a municipal legal framework for cybersecurity, grounded in the empirical and theoretical findings of the previous studies. The results show that, despite regulatory advances at the federal level—such as the Civil Rights Framework for the Internet and the General Data Protection Law—most of the surveyed municipalities lack legal instruments, organizational structures, and specific policies for digital protection. The analysis also indicates that the absence of integration among legal, institutional, operational, and epistemological dimensions undermines the effectiveness of local cyber governance. As a contribution, the thesis presents a conceptual and normative model that can be replicated by other Brazilian municipalities, promoting greater alignment between legislation, institutional practices, and data protection strategies.

Keywords: Cyber Governance. Data Protection. Institutional Capacity. Information Security Policies.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AMREC	Associação dos Municípios da Região Carbonífera
ANATEL	Agência Nacional de Telecomunicações
ANCiber	Agência Nacional de Cibersegurança
ANPD	Autoridade Nacional de Proteção de Dados
BID	Banco Interamericano de Desenvolvimento
BTM DERs	Behind-The-Meter Distributed Energy Resources
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CNCiber	Comitê Nacional de Cibersegurança
CMM	Cybersecurity Capacity Maturity Model
CMMI	Capability Maturity Model Integration
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
CSIRT	Cybersecurity Ventures Report on Cybercrime
CTIRGov	Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo
CyberTEA	Cybersecurity Technical and Economic Approach
DPO	Data Protection Officer
E-Ciber	Estratégia Nacional de Segurança Cibernética
FGV	Fundação Getúlio Vargas
FIESP	Federação das Indústrias do Estado de São Paulo
GDPR	General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados)
GGCiber	Gabinete de Gerenciamento de Cibercrises
GGE	Group of Governmental Experts
IA	Inteligência artificial
IBGE	Instituto Brasileiro de Geografia e Estatística
ICS	Industrial Control Systems (Sistemas de Controle Industrial)
IoT	Internet of Things (Internet das Coisas)
ISO	International Organization for Standardization
LANs	Local Area Network
LGPD	Lei Geral de Proteção de Dados
MP	Ministério Público

NCCIC	National Cybersecurity and Communications Integration Center
NIS2	Network and Information Security
NIST	National Institute of Standards and Technology
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ODS	Objetivos de Desenvolvimento Sustentável
OEA	Organização Dos Estados Americanos
ONU	Organização das Nações Unidas
OT	Operational Technology (Tecnologia Operacional)
PIB	Produto Interno Bruto
PNCiber	Política Nacional de Cibersegurança
PNI	Política Nacional de Inovação
PNP	Política Nacional de Proteção de Dados
PNSI	Política Nacional de Segurança da Informação
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
PSI	Política de Segurança da Informação
SCADA	Supervisory Control and Data Acquisition (Supervisão, Controle e Aquisição de Dados)
SIAFI	Sistema Integrado de Administração Financeira
STJ	Superior Tribunal de Justiça
TCE	Tribunal de Contas do Estado
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TIOM	Theory-dependent Innovative Optimization Model
UIT	União Internacional de Telecomunicações
UNCTAD	United Nations Conference on Trade and Development (Conferência das Nações Unidas sobre Comércio e Desenvolvimento)
USD	United States dollar
VPN	Virtual Private Network (Rede Virtual Privada)
WTO	World Trade Organization (Organização Mundial do Comércio)

SUMÁRIO

1 INTRODUÇÃO

A presente tese trata da cibersegurança como um fator estratégico para o desenvolvimento socioeconômico de cidades, com ênfase na realidade institucional dos municípios da região da AMREC (Associação dos Municípios da Região Carbonífera, em Santa Catarina). A crescente digitalização das estruturas públicas municipais exige não apenas soluções técnicas de proteção digital, mas também uma abordagem articulada que considere aspectos legais, institucionais e sociais. Nesse sentido, o trabalho está estruturado em seis seções principais, que se complementam e convergem para uma proposta normativa aplicável à realidade local.

A Seção 1, apresenta a introdução da pesquisa e estabelece o ponto de partida conceitual e metodológico da tese. Nela, são abordados o contexto da transformação digital nas cidades, os desafios da proteção de dados e os impactos da cibersegurança sobre a governança pública local. A subseção 1.2 delimita o problema e a questão de pesquisa, a subseção 1.3 apresenta os objetivos geral e específicos. A subseção seguinte discute a relevância científica, social e institucional da investigação, destacando a originalidade do recorte analítico e sua contribuição para o campo do desenvolvimento socioeconômico. Ao tratar a cibersegurança como uma dimensão transversal das políticas públicas municipais, essa seção estabelece o fio condutor das demais partes da tese.

A Seção 2 compreende o Estudo I, no qual é realizada uma revisão bibliométrica e sistemática da literatura científica nacional e internacional. O objetivo é mapear tendências, lacunas e limitações no campo da cibersegurança, especialmente no que se refere à sua interface com o desenvolvimento regional e à aplicação em contextos subnacionais. A análise permite compreender os marcos teóricos predominantes, os autores e instituições mais influentes e os recortes temáticos ainda pouco explorados, oferecendo subsídios analíticos para os capítulos seguintes.

Na Seção 3, o Estudo II aprofunda a análise conceitual a partir da identificação de constructos emergentes no cruzamento entre cibersegurança, desenvolvimento urbano, institucionalidade e soberania informacional. Partindo de clusters temáticos como ferramenta metodológica, essa seção organiza categorias analíticas relevantes para diagnósticos institucionais e formulações de políticas públicas. Essa base conceitual sustenta os critérios de análise adotados nos estudos de caso e na proposição normativa.

A Seção 4 apresenta o Estudo III, voltado à investigação empírica sobre o nível de maturidade institucional dos municípios da AMREC no campo da cibersegurança. Por meio de

entrevistas semiestruturadas com representantes das prefeituras, o estudo mapeia capacidades, vulnerabilidades e barreiras para a implementação de políticas de proteção digital. A análise revela assimetrias estruturais entre os municípios, bem como fragilidades na articulação entre os marcos normativos federais e as realidades locais.

Na Seção 5, o Estudo IV desenvolve uma proposta de marco legal municipal para a cibersegurança, construída a partir dos dados empíricos e dos fundamentos teóricos anteriores. A proposta contempla diretrizes estratégicas, princípios normativos e sugestões operacionais que podem orientar a estruturação de políticas públicas de cibersegurança em nível municipal. A seção busca promover uma governança digital mais eficaz, alinhada aos princípios de segurança, soberania e inclusão.

Por fim, a Seção 6 reúne as considerações finais da tese. Nela são discutidas as relações entre os estudos desenvolvidos, as hipóteses teóricas e empíricas, as limitações do trabalho e as recomendações para futuras pesquisas. A seção também reforça as contribuições teóricas, metodológicas e práticas da tese, destacando seu potencial de replicabilidade em outros contextos subnacionais brasileiros.

1.1 CONTEXTUALIZAÇÃO DO TEMA

A transformação digital tem redefinido as estruturas sociais, econômicas e institucionais em todo o mundo. No Brasil, esse fenômeno é particularmente evidente nas esferas públicas, onde a digitalização de serviços e a integração de tecnologias da informação têm se tornado componentes essenciais para a eficiência administrativa e a promoção do desenvolvimento socioeconômico.

A cibersegurança, entendida como o conjunto de práticas, tecnologias e políticas destinadas à proteção de sistemas computacionais e dados contra-ataques cibernéticos, tornou-se um tema estratégico no âmbito da segurança pública. Segundo a Estratégia Nacional de Segurança Cibernética – E-Ciber (Brasil, 2020), a proteção do ambiente digital é essencial para a preservação de direitos fundamentais, da ordem pública e da soberania nacional. À medida que essas instituições se digitalizam, também se tornam alvos mais atrativos para atores maliciosos, evidenciando a necessidade de uma regulação robusta.

Ao longo das últimas décadas, a cibersegurança deixou de ser um tema restrito ao campo técnico da tecnologia da informação e passou a configurar uma agenda estratégica multidisciplinar. Originalmente focada na proteção da confidencialidade, integridade e disponibilidade dos dados (Anderson, 2001), sua evolução acompanha o crescimento da

interdependência entre sistemas digitais, infraestruturas críticas e estruturas sociais. Como demonstra Nissenbaum (2005), a cibersegurança não deve ser reduzida a um conjunto de protocolos técnicos, mas compreendida a partir do conceito de "privacidade contextual", que vincula proteção digital à preservação de valores democráticos e normativos em sociedades conectadas.

Nos estudos desenvolvidos nesta tese, a cibersegurança é tratada como um campo transversal, que articula dimensões técnicas, institucionais e sociopolíticas. O Estudo I revelou que a literatura científica ainda se encontra fragmentada, com predomínio de abordagens técnico-operacionais, enquanto o Estudo II destaca a emergência de constructos como governança de dados, soberania informacional e resiliência digital, especialmente quando situados em contextos urbanos e regionais. Essa abordagem ampliada permite compreender a cibersegurança como um componente essencial da governança pública contemporânea, integrando proteção digital, capacidade institucional e justiça informacional.

Os impactos econômicos desses ataques já são amplamente mensuráveis. De acordo com a Fortinet (2024), apenas em 2023, 81% das organizações globalmente relataram ter sido alvo de pelo menos um ataque de *ransomware*, e o custo aproximado para recuperação total dos dados e sistemas foi de USD 2,6 milhões no ano. No Brasil, o prejuízo econômico estimado com crimes cibernéticos em 2022 foi de aproximadamente USD 10 bilhões, o que posiciona o país entre os mais visados da América Latina (Kaspersky, 2023). Globalmente, a IBM (2023) apontou que o custo médio de um vazamento de dados corporativos alcançou USD 4,45 milhões em 2023, o valor mais alto registrado em 20 anos de medição da empresa.

Casos emblemáticos também reforçam a urgência do tema. Em 2021, o Superior Tribunal de Justiça (STJ) sofreu um ataque *ransomware* que comprometeu totalmente o acesso aos sistemas internos por semanas, exigindo reconstrução e restauração manual de processos (Brasil, 2021). Ainda em 2021, a Colonial Pipeline, responsável por 45% do fornecimento de combustível da costa leste dos Estados Unidos, desembolsou USD 4,4 milhões em resgate para restaurar seus sistemas após um ataque (WEF, 2022).

Nos primeiros meses de 2025, o Brasil registrou um preocupante aumento nos incidentes de cibersegurança. Segundo dados do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov (2025), o número de notificações relativas a ataques — incluindo *phishing*, abuso de e-mail, páginas falsas e vazamento de dados — apresentou crescimento contínuo ao longo do período. Paralelamente, estudo da Check Point Research (2025) indicou um crescimento de 21% nos ataques cibernéticos globais durante o segundo trimestre do ano, enquanto no âmbito nacional foi reportada uma média de quase três mil

ataques por semana por organização, um incremento de 3% em relação a 2024. Esses indicadores reforçam a intensificação das ameaças digitais e a urgência de fortalecer a defesa institucional dos municípios.

No que se refere aos custos financeiros, o Brasil vive uma escalada preocupante. O custo aproximado de violação de dados atingiu R$ 7,19 milhões em 2025, um aumento de 6,5% em relação ao ano anterior, sendo o *phishing* o principal vetor de ataque, associado a prejuízos médios de R$ 7,18 milhões por incidente (IT Fórum, 2025). No caso de *ransomware*, 66% das empresas afetadas no país ainda acabam pagando pelo resgate, com valor médio de R$ 2 milhões, embora se observe uma redução nos valores pagos em comparação a 2024 (Convergência Digital, 2025). Esses dados reforçam a relevância de políticas públicas locais que promovam maturidade institucional, preparação para resposta a incidentes e redução da dependência de resgates financeiros onerosos.

A regulação da cibersegurança enfrenta, contudo, desafios significativos. Entre eles, destaca-se o desequilíbrio informacional entre o setor público e o privado, além da assimetria técnica que dificulta a formulação de políticas eficazes. Nesse sentido, a teoria da regulação proposta por George Stigler (1971) torna-se particularmente útil para análise crítica desse processo. De acordo com o autor, “toda indústria ou ocupação que ganhe substancialmente com a regulação econômica tenderá a usar os recursos disponíveis para obter tal regulação” (Stigler, 1971, p. 3), ou seja, a regulação é frequentemente capturada por interesses privados, que moldam as regras segundo suas conveniências.

Essa lógica se aplica ao campo da cibersegurança. Como demonstrado por Zuboff (2019), empresas que detêm o controle sobre tecnologias digitais e infraestruturas críticas exercem forte influência sobre a formulação de políticas públicas, contribuindo para o que ela denomina como “capitalismo de vigilância”. Segundo a autora, a capacidade dessas corporações de moldar padrões normativos e tecnológicos ameaça à democracia e a autonomia institucional do Estado.

A dependência de soluções proprietárias e a contratação de fornecedores sem critérios técnicos claros contribuem para um cenário de vulnerabilidade institucional. Quando empresas privadas dominam o ecossistema digital de segurança pública, surgem riscos não apenas técnicos, mas também de soberania, uma vez que o controle sobre os dados e sistemas críticos escapa da administração pública. Isso está em consonância com o argumento de Peltzman (1976), que afirma que a regulação pode ser utilizada como mecanismo de redistribuição de benefícios entre grupos organizados, muitas vezes em detrimento do interesse público.

Além disso, a interseção entre cibersegurança e desenvolvimento urbano traz à tona uma nova dimensão da política pública. Cidades com maior maturidade digital e capacidade de resposta a incidentes cibernéticos tendem a atrair investimentos e fomentar ambientes de inovação (OCDE, 2020). Uma governança digital eficaz, que inclui a cibersegurança como pilar, torna-se um ativo econômico. Por outro lado, cidades que negligenciam a proteção cibernética estão mais suscetíveis a crises de confiança institucional, paralisações de serviços essenciais e perda de competitividade.

Como observa Castells (1999), na sociedade em rede, a capacidade de produzir, processar e aplicar informações torna-se determinante para o poder. Essa constatação reforça a importância de políticas públicas que protejam as infraestruturas digitais da segurança pública, enquanto garantem a transparência e a justiça social. Quando falhas em cibersegurança ocorrem, os grupos mais vulneráveis são os primeiros a sofrer seus efeitos, seja pela perda de acesso a serviços essenciais ou pela exposição de dados pessoais.

1.2 PROBLEMA E QUESTÃO DE PESQUISA

A cibersegurança se consolida como elemento central para o desenvolvimento socioeconômico no cenário contemporâneo. A expansão da conectividade, impulsionada pela Internet das Coisas (IoT), inteligência artificial e tecnologias de comunicação de última geração, trouxe novas oportunidades para inovação e melhoria de serviços públicos. Contudo, essa interconexão ampliou amplamente a superfície de ataque dos sistemas digitais, tornando-os mais vulneráveis a incidentes que afetam diretamente a continuidade dos serviços, a integridade das informações e a confiança institucional.

A relação entre cibersegurança e desenvolvimento local é cada vez mais evidente. Cidades capazes de proteger suas infraestruturas digitais e garantir a disponibilidade de serviços críticos são mais atrativas para investimentos, fomentam ecossistemas de inovação e promovem a inclusão digital de maneira sustentável (OCDE, 2020). Essa proteção não é apenas um requisito técnico, mas um ativo estratégico que sustenta a competitividade econômica e a resiliência social.

No Brasil, avanços normativos importantes estabeleceram bases para a governança digital. O Marco Civil da Internet (Lei nº 12.965/2014) definiu princípios para o uso da rede, como neutralidade, proteção de dados e privacidade. Mais recentemente, o Decreto nº 11.856/2023 instituiu a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança, com diretrizes para coordenar ações de proteção no âmbito federal. Em 2025,

o Decreto nº 12.572 instituiu a Política Nacional de Segurança da Informação (PNSI), ampliando o escopo para a proteção de dados e ativos informacionais no setor público.

Esses instrumentos reforçam a importância da cibersegurança como política pública, integrando proteção digital à defesa da soberania nacional e à preservação de direitos fundamentais. Entretanto, sua eficácia depende de implementação coordenada e capilarizada, alcançando não apenas órgãos federais, mas também governos estaduais e municipais. É nesse ponto que surgem os maiores desafios.

A aplicação dessas políticas no nível local exige adaptação às realidades específicas de cada município. Estruturas administrativas distintas, capacidades técnicas limitadas e restrições orçamentárias influenciam diretamente a efetividade das medidas de segurança digital. Sem considerar essas variáveis, normas federais podem permanecer distantes da realidade das cidades e de suas necessidades operacionais.

Assim, a cibersegurança deve ser tratada como um eixo transversal de políticas urbanas, incorporando aspectos técnicos, jurídicos e sociais, para garantir que a transformação digital promova não apenas eficiência, mas também proteção e desenvolvimento sustentável para as comunidades.

Apesar do avanço do marco regulatório federal, sua aplicação no nível municipal é incipiente e fragmentada. A inexistência de marcos legais específicos nas cidades, combinada à ausência de estruturas de governança digital locais, impede a implementação consistente das políticas nacionais. Isso significa que, mesmo com diretrizes robustas em nível central, a execução no campo municipal carece de coordenação, prioridade e recursos.

A produção acadêmica, tanto nacional quanto internacional, tende a se concentrar em abordagens técnico-normativas, priorizando aspectos como criptografia, protocolos de segurança e *compliance* regulatório. Poucos estudos exploram a aplicação da cibersegurança em contextos subnacionais, particularmente em municípios de médio e pequeno porte, onde as capacidades institucionais são limitadas e os riscos são crescentes. Essa ausência de territorialização analítica dificulta a construção de modelos aplicáveis à realidade municipal brasileira.

Outro ponto crítico é a escassez de articulação entre cibersegurança e desenvolvimento socioeconômico. A maioria das pesquisas ainda trata esses campos como esferas dissociadas, negligenciando os efeitos que a proteção digital exerce sobre a confiança institucional, a atratividade para investimentos e a inclusão digital. Assim, a literatura carece de abordagens integradas que articulem segurança da informação, governança local e planejamento urbano. Essa fragmentação teórica reforça a importância de estudos como o

presente, que buscam construir pontes entre campos disciplinares e oferecer contribuições analíticas voltadas à formulação de políticas públicas eficazes e contextualizadas.

Essa lacuna se agrava quando se observa a disparidade de recursos e capacidades entre municípios. Enquanto alguns possuem equipes técnicas qualificadas e investimento contínuo em tecnologia, a maioria opera com estruturas reduzidas, sem setores especializados em segurança da informação. Nesses casos, políticas de cibersegurança tendem a ser reativas, adotadas apenas após incidentes significativos.

Outro problema crítico é a ausência de integração institucional entre municípios e a esfera federal. A centralização de ações no nível nacional, sem a devida descentralização de competências e apoio técnico, compromete a capacidade de resposta local. Isso perpetua a dependência de instâncias superiores e retarda a adoção de medidas preventivas.

O resultado é um cenário em que a vulnerabilidade digital se torna estrutural no nível municipal. Sem protocolos claros, recursos adequados e arcabouço legal próprio, prefeituras permanecem expostas a ataques capazes de comprometer serviços essenciais, gerar prejuízos econômicos e abalar a confiança pública.

Considerando esse cenário, esta tese parte do entendimento de que a cibersegurança, especialmente no contexto municipal, constitui um pilar estratégico para fortalecer a governança digital e ampliar as condições para o desenvolvimento socioeconômico. A pesquisa desenvolve-se integrando análises teóricas e conceituais, diagnósticos empíricos e proposições normativas, com o propósito de gerar um resultado capaz de orientar políticas públicas e práticas institucionais. Nesse sentido, formula-se a seguinte questão de pesquisa: **Quais diretrizes e instrumentos, fundamentados em evidências teóricas, conceituais, empíricas e normativas, podem compor uma proposta integrada para o fortalecimento da cibersegurança municipal e a promoção do desenvolvimento socioeconômico na região da AMREC?** Para responder a essa questão, o estudo propõe-se em apresentar um referencial teórico atualizado, organizar constructos que articulem cibersegurança e desenvolvimento, diagnosticar a realidade institucional dos municípios e, a partir dessas bases, estruturar uma proposta normativa capaz de promover avanços concretos na proteção da informação e na resiliência digital em âmbito local.

1.3 OBJETIVOS DA PESQUISA

A presente pesquisa se estruturou de forma sequencial e integrada, articulando quatro estudos complementares para compreender a cibersegurança como vetor estratégico de

desenvolvimento socioeconômico no contexto municipal. Ao longo da investigação, os objetivos inicialmente propostos foram atingidos de maneira progressiva, resultando em um corpo de evidências que conecta fundamentos teóricos, análises conceituais, diagnósticos empíricos e proposições normativas aplicáveis.

Dessa forma, os objetivos estão apresentados integrando conhecimento científico, ferramentas analíticas e recomendações concretas para fortalecer a governança digital e a resiliência institucional no nível municipal.

1.3.1 Objetivo Geral

Compreender e propor soluções para o fortalecimento da cibersegurança como fator estratégico de desenvolvimento socioeconômico em municípios, por meio da integração de análise teórica, investigação empírica e proposição normativa aplicável ao contexto regional brasileiro.

1.3.2 Objetivos Específicos

Com base no exposto, têm-se os seguintes objetivos específicos:

a) Mapear tendências, limitações e lacunas da literatura científica sobre cibersegurança em perspectiva internacional, identificando contribuições teóricas e metodológicas relevantes para a construção do campo;

b) Analisar constructos emergentes que relacionem cibersegurança e desenvolvimento, por meio de *clusters* temáticos que orientem investigações e subsidiem diagnósticos aplicados;

c) Diagnosticar o nível de maturidade institucional em cibersegurança das prefeituras da Região da AMREC, identificando vulnerabilidades, capacidades e potenciais de desenvolvimento;

d) Propor um marco legal municipal para cibersegurança, fundamentado em evidências empíricas e alinhado às diretrizes nacionais e internacionais, a fim de orientar políticas públicas e fortalecer a resiliência digital local.

1.4 RELEVÂNCIA, JUSTIFICATIVA E CONTRIBUIÇÃO DA PESQUISA

A cibersegurança se consolidou nas últimas décadas como um campo estratégico para o desenvolvimento socioeconômico, ultrapassando a esfera puramente tecnológica e

tornando-se elemento essencial da governança, da inovação e das políticas públicas (Bada; Nurse, 2019; ENISA, 2023). Em um cenário de digitalização crescente dos serviços públicos e privados, a proteção de ativos informacionais e a resiliência frente a incidentes cibernéticos configuram condições indispensáveis para a competitividade regional e a sustentabilidade das organizações.

Este estudo se insere na linha de pesquisa Trabalho e Organizações do Programa de Pós-Graduação em Desenvolvimento Socioeconômico - PPGDS, que investiga o trabalho no âmbito das organizações e suas implicações no desenvolvimento socioeconômico, abordando práticas e capacidades organizacionais relacionadas aos *stakeholders*, bem como desempenho, dinâmica organizacional, responsabilidade social, inovação, gestão de negócios e cadeias produtivas. A pesquisa contribui para esse escopo ao examinar como a cibersegurança, tratada como política pública transversal, impacta diretamente o desempenho institucional e o relacionamento com atores internos e externos.

A relevância social e política do tema também se expressa em sua conexão direta com os Objetivos de Desenvolvimento Sustentável (ODS). O ODS 9 – Indústria, Inovação e Infraestrutura é contemplado na medida em que a pesquisa propõe estruturas normativas e capacidades institucionais para fortalecer a infraestrutura digital e a inovação. O ODS 11 – Cidades e Comunidades Sustentáveis é atendido ao integrar a cibersegurança como componente da resiliência urbana. O ODS 16 – Paz, Justiça e Instituições Eficazes é abordado ao propor mecanismos que fortalecem a governança local, a integridade institucional e a transparência (ONU, 2015).

Nesse contexto, a tese cumpre seu objetivo geral ao propor uma norma jurídica aplicável ao nível municipal, construída a partir da articulação entre evidências empíricas, fundamentos teóricos e diretrizes legais. Essa proposição normativa se materializa no Estudo IV, que apresenta um modelo de marco legal municipal de cibersegurança adaptado à realidade dos municípios da AMREC, com potencial de replicação em outros contextos subnacionais. Trata-se de uma contribuição prática que integra os elementos investigados nos estudos anteriores, convertendo o diagnóstico analítico em diretrizes jurídicas concretas para fortalecer a governança digital local.

No campo acadêmico, a pesquisa responde à necessidade de aprofundar o debate sobre a cibersegurança em contextos subnacionais brasileiros, área ainda pouco explorada e frequentemente negligenciada na literatura (Morelato *et al.*, 2021). Ao articular dimensões técnicas, jurídicas e sociotécnicas, o estudo atende à demanda por abordagens interdisciplinares defendida por Craigen *et al.* (2014) e De Bruijn e Janssen (2017), demonstrando que a

cibersegurança deve ser compreendida como fenômeno complexo, com impactos diretos no desenvolvimento econômico e social.

A realização desta pesquisa é justificada por lacunas científicas, demandas práticas e alinhamento com agendas de desenvolvimento sustentável. A literatura nacional carece de estudos abrangentes que considerem simultaneamente dimensões técnicas, institucionais e sociais da cibersegurança no contexto municipal. A predominância de análises restritas a aspectos normativos de nível federal ou a soluções técnicas isoladas limita a compreensão do fenômeno em sua totalidade.

O diagnóstico da Região da AMREC revelou vulnerabilidades concretas, como baixa maturidade institucional, ausência de marcos regulatórios específicos e carência de recursos humanos especializados. Essas lacunas afetam diretamente a capacidade das administrações municipais de proteger informações, manter serviços digitais essenciais e promover um ambiente seguro para a inovação e o desenvolvimento econômico.

A vinculação da pesquisa aos ODS 9, 11 e 16 reforça sua pertinência, pois as metas desses objetivos incluem a construção de infraestruturas resilientes, o fortalecimento de cidades seguras e sustentáveis e a promoção de instituições eficazes, transparentes e responsáveis. Ao propor um modelo normativo fundamentado em evidências, o estudo contribui para o alcance dessas metas de forma concreta e mensurável.

A inserção da pesquisa na linha de Trabalho e Organizações se justifica pela análise das capacidades organizacionais e das práticas de gestão pública voltadas à proteção digital, à inovação e à sustentabilidade socioeconômica. Ao compreender a cibersegurança como elemento estratégico da dinâmica organizacional, o estudo amplia a visão sobre sua função no setor público, não apenas como barreira contra-ataques, mas como pilar para o desenvolvimento local e a confiança institucional.

A pesquisa apresenta contribuições relevantes em três dimensões principais: teórica, metodológica e social. No campo teórico, integra conceitos dispersos na literatura, sistematizando constructos emergentes que articulam maturidade institucional, governança de dados, soberania informacional e resiliência digital ao desenvolvimento socioeconômico municipal. Essa sistematização, derivada dos Estudos I e II, estabelece uma base conceitual robusta e replicável.

No âmbito metodológico, inova ao combinar diferentes estratégias de pesquisa de forma articulada: análise bibliométrica e revisão sistemática para mapear a produção científica; análise conceitual para consolidar categorias emergentes; estudo de caso regional para mensurar a maturidade institucional; e proposição normativa fundamentada em evidências para orientar

a implementação de políticas públicas locais. Essa triangulação garante consistência e aplicabilidade aos resultados, exemplificando a integração entre rigor científico e utilidade prática.

A contribuição social materializa-se na elaboração de um marco legal municipal para cibersegurança, desenvolvido no Estudo IV com base no diagnóstico empírico do Estudo III. Esse instrumento normativo propõe diretrizes estratégicas e operacionais que podem ser adaptadas e aplicadas em outros municípios brasileiros, especialmente em contextos de baixa capacidade técnica e carência de recursos.

O estudo também contribui para o fortalecimento da governança pública local, ao recomendar medidas de capacitação contínua de equipes, fomento à cooperação intermunicipal e adoção de práticas de *security by design* em contratações públicas. Tais recomendações dialogam com os princípios da administração pública e com a necessidade de assegurar a continuidade de serviços essenciais diante de riscos digitais.

1.5 INEDITISMO DA TESE

A contribuição teórica da tese se ampara na articulação das três principais correntes analíticas identificadas no Estudo I: a técnico-operacional, a institucionalista e a sociotécnica. Embora cada uma dessas abordagens ofereça insumos valiosos para compreender a complexidade da cibersegurança, o presente trabalho assume a corrente institucionalista como eixo central de sua construção teórica. Essa escolha decorre do entendimento de que, para além de soluções técnicas ou de críticas estruturais, é a capacidade das instituições públicas de formularem, implementarem e sustentarem políticas eficazes que define a resiliência digital em contextos municipais.

A partir dessa perspectiva, a tese propõe uma sistematização inédita de categorias analíticas que orientam a estruturação de um marco legal municipal de cibersegurança. Essas categorias são: (i) os fundamentos e objetivos da política de cibersegurança; (ii) a estrutura institucional de governança cibernética; (iii) a normatização interna e a gestão de riscos; (iv) a capacitação e a cultura organizacional; e (v) os mecanismos de transparência e controle social. Essas dimensões não apenas operam como pilares conceituais, mas também funcionam como vetores analíticos para diagnosticar lacunas institucionais, orientar políticas públicas e promover maior alinhamento entre os princípios regulatórios nacionais e as realidades locais.

O ineditismo teórico da tese reside, portanto, na integração entre uma base institucionalista robusta e categorias normativas aplicáveis ao contexto municipal, superando a

fragmentação que ainda caracteriza a literatura sobre cibersegurança no Brasil. Ao deslocar o foco da mera conformidade técnica para a construção de capacidades institucionais sustentáveis, a tese contribui para o avanço do campo ao oferecer um modelo conceitual replicável e sensível às desigualdades estruturais que afetam os municípios brasileiros. Essa abordagem também permite que a cibersegurança seja compreendida como um eixo transversal de políticas públicas, conectando proteção digital à promoção do desenvolvimento socioeconômico, da justiça informacional e da governança democrática.

A contribuição empírica da tese está ancorada no diagnóstico sobre a maturidade institucional em cibersegurança dos municípios que integram a AMREC. A partir da realização de entrevistas semiestruturadas com representantes das prefeituras, o estudo mapeou os níveis de governança digital, os instrumentos normativos existentes, as práticas operacionais e as percepções sobre riscos cibernéticos no nível local. Esse levantamento permitiu não apenas identificar vulnerabilidades comuns e barreiras estruturais, mas também reconhecer experiências incipientes de regulamentação e práticas colaborativas que podem ser fortalecidas.

Além de preencher uma lacuna na produção científica sobre cibersegurança em contextos subnacionais, os dados coletados possibilitaram a construção de uma matriz analítica de maturidade institucional adaptada à realidade municipal brasileira. Esse instrumento, que agrupa evidências em cinco blocos analíticos — capacidade organizacional, governança normativa, infraestrutura e operação, cooperação intermunicipal e barreiras institucionais —, constitui uma ferramenta empírica replicável para outros territórios. Assim, a tese avança ao transformar um mapeamento qualitativo em base estruturante para a formulação de políticas públicas locais, promovendo um diagnóstico orientado por evidências e sensível às singularidades de municípios de pequeno e médio porte.

A contribuição metodológica da tese reside na construção de um percurso investigativo articulado, que combina múltiplas estratégias analíticas para tratar a cibersegurança como fenômeno complexo e interdisciplinar. No Estudo I, utilizou-se análise bibliométrica e revisão sistemática da literatura para mapear tendências, lacunas e abordagens predominantes sobre o tema em nível internacional e nacional. O Estudo II avançou para uma análise conceitual com base em clusters temáticos, organizando constructos emergentes e categorias analíticas que fundamentam o instrumento de diagnóstico. No Estudo III, foi conduzido um estudo de caso com abordagem qualitativa, envolvendo entrevistas com representantes dos municípios da AMREC, o que permitiu mapear a maturidade institucional em cinco dimensões analíticas. Por fim, o Estudo IV adotou uma abordagem propositiva, estruturando diretrizes estratégicas e um modelo normativo de marco legal municipal a partir

dos achados empíricos e teóricos. A combinação desses métodos resulta em um percurso metodológico integrador e potencialmente replicável em outras regiões.

1.6 ESTRUTURA DOS ESTUDOS

O quadro a seguir apresenta uma visão panorâmica dos quatro estudos que estruturam esta tese, detalhando seus respectivos títulos, objetivos e aspectos metodológicos. Cada estudo foi concebido de forma a contribuir, de maneira complementar, para a compreensão e o fortalecimento da cibersegurança em contextos municipais, com foco na realidade da região da AMREC. A organização em colunas permite visualizar a progressão analítica adotada, que parte da revisão da literatura (Estudo I) e culmina na formulação de uma proposta normativa (Estudo IV).

O Estudo I realiza uma revisão bibliométrica e sistemática da produção científica sobre cibersegurança, utilizando bases internacionais e técnicas reconhecidas, com o objetivo de mapear tendências e lacunas conceituais. Em sequência, o Estudo II aprofunda a análise teórica por meio da identificação de constructos emergentes, utilizando *clusters* temáticos extraídos da literatura como ferramenta metodológica para organizar categorias analíticas com potencial aplicação diagnóstica. Ambos os estudos oferecem a base conceitual e teórica que sustenta a investigação empírica desenvolvida nos estudos posteriores.

O Estudo III adota uma abordagem qualitativa para diagnosticar o nível de maturidade institucional em cibersegurança das prefeituras da AMREC, por meio de entrevistas semiestruturadas. Seus resultados são fundamentais para embasar o Estudo IV, que propõe um marco legal municipal alinhado aos achados empíricos e teóricos da tese. A metodologia de cada estudo foi escolhida para assegurar coerência entre os objetivos propostos e os produtos gerados, evidenciando a integração entre teoria, prática e proposição normativa que caracteriza a presente pesquisa.

Quadro 1 – Framework dos estudos da Tese

Título: Cibersegurança e desenvolvimento socioeconômico das cidades: maturidade institucional e regulação nos municípios da região da AMREC			
Objetivo da Tese: Compreender e propor soluções para o fortalecimento da cibersegurança como fator estratégico de desenvolvimento socioeconômico em municípios, por meio da integração de análise teórica, investigação empírica e proposição normativa aplicável ao contexto regional brasileiro.			
Estudo I	**Estudo II**	**Estudo III**	**Estudo IV**
Título: Tendências e limitações da literatura em cibersegurança: subsídios analíticos para a construção do campo em perspectiva regional	**Título:** Constructos Emergentes em Cibersegurança e Desenvolvimento: Uma Análise Conceitual com Base em Clusters Temáticos	**Título:** Segurança cibernética em instituições públicas locais: estudo de caso na Associação dos Municípios da Região Carbonífera - AMREC	**Título:** Proposição de um marco legal municipal em cibersegurança: diretrizes estratégicas para a região da AMREC a partir da análise de maturidade institucional
Objetivo: Examinar os núcleos temáticos da produção científica sobre cibersegurança, evidenciando limitações conceituais e possibilidades de ampliação dos enfoques existentes.	**Objetivo:** Compreender como normas, instituições e estruturas de governança moldam os caminhos possíveis para o desenvolvimento digital seguro, ancorados na perspecitva institucionalista de cibersegurança.	**Objetivo:** Examinar, com base em evidências empíricas, o nível de maturidade institucional dos municípios da AMREC relacionados à cibersegurança, analisando estruturas existentes, práticas adotadas, limitações operacionais e possibilidades de fortalecimento das capacidades locais.	**Objetivo:** Propor um modelo de legislação municipal em cibersegurança, com base nas evidências empíricas levantadas nos municípios da AMREC.
Aspectos metodológicos: **Tipo:** Revisão de literatura **Técnicas:** Análise bibliométrica (VOSviewer) Revisão sistemática (PRISMA) **Base de dados:** Scopus e Web of Science	**Aspectos metodológicos:** **Tipo:** Estudo conceitual-analítico **Técnicas:** Mapeamento de clusters temáticos Análise qualitativa de conteúdos científicos **Fonte de dados:** Corpus teórico extraído da revisão do Estudo I	**Aspectos metodológicos:** **Tipo:** Estudo de caso qualitativo **Técnicas:** Entrevistas semiestruturadas com representantes dos municípios da AMREC Análise de conteúdo **Instrumento:** Roteiro estruturado com blocos analíticos	**Aspectos metodológicos:** **Tipo:** Estudo propositivo **Técnicas:** Síntese dos achados empíricos e conceituais dos estudos anteriores Construção de diretrizes estratégicas **Produto:** Estrutura de um marco legal municipal em cibersegurança

Fonte: Elaborado pelo autor (2025).

2 ESTUDO I – TENDÊNCIAS E LIMITAÇÕES DA LITERATURA EM CIBERSEGURANÇA: SUBSÍDIOS ANALÍTICOS PARA A CONSTRUÇÃO DO CAMPO EM PERSPECTIVA REGIONAL

2.1 INTRODUÇÃO

A cibersegurança tem se consolidado como uma preocupação central na era digital, impactando diretamente as esferas sociais, econômicas e políticas das nações. No Brasil, o cenário é particularmente alarmante: em 2024, o país registrou mais de 700 milhões de ataques cibernéticos, o que equivale a aproximadamente 1.379 ataques por minuto, posicionando-o como o segundo país mais visado no mundo (CNN Brasil, 2024).

Esses ataques não se limitam ao setor privado. Órgãos governamentais também têm sido alvos frequentes. No primeiro semestre de 2024, os incidentes cibernéticos em sistemas do governo federal dobraram em relação ao ano anterior, totalizando 4,7 mil registros até julho (Mozzelli, 2024). Casos emblemáticos incluem a invasão ao Sistema Integrado de Administração Financeira (SIAFI), que resultou no desvio de aproximadamente R$ 15 milhões (OBlock, 2024).

A população brasileira também sofre diretamente com esses crimes. Uma pesquisa do Instituto DataSenado revelou que 24% dos brasileiros com mais de 16 anos foram vítimas de golpes digitais nos últimos 12 meses, representando mais de 40,85 milhões de pessoas (Senado Federal, 2024). Além disso, o Fórum Brasileiro de Segurança Pública estimou que, entre julho de 2023 e julho de 2024, os prejuízos decorrentes de crimes virtuais e roubos de celulares ultrapassaram R$ 186 bilhões (El País, 2024).

Em nível internacional, a situação é igualmente preocupante. O Fórum Econômico Mundial alertou que nove em cada dez organizações sofreram pelo menos um ataque cibernético em 2024, com perdas globais estimadas em US$ 10,5 trilhões até 2025 (CSIRT, 2024). Casos notórios como o ataque ao governo da Costa Rica em 2022 — que paralisou serviços essenciais e levou à decretação de estado de emergência nacional — demonstram o potencial disruptivo de falhas na segurança digital de instituições públicas.

A resposta a esse cenário tem sido, em parte, normativa. No Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), regulamenta o tratamento de dados pessoais por entes públicos e privados, assegurando direitos fundamentais como liberdade, privacidade e autodeterminação informativa (Brasil, 2018). A LGPD introduz diretrizes que impactam diretamente a formulação de políticas de

cibersegurança, exigindo medidas preventivas e mecanismos de responsabilização.

Em complemento à LGPD, o Decreto nº 11.856/2023 institui a Política Nacional de Cibersegurança (PNCiber), estabelecendo diretrizes estratégicas e criando o Comitê Nacional de Cibersegurança (CNCiber) para coordenar ações entre os entes federativos (Brasil, 2023). O decreto define objetivos como o fortalecimento da atuação diligente no ciberespaço, o estímulo ao desenvolvimento de tecnologias nacionais e a integração entre segurança digital e políticas públicas.

Internacionalmente, a norma ISO/IEC 27001 configura um referencial técnico amplamente adotado para gestão da segurança da informação. Essa norma estabelece um sistema estruturado para garantir a confidencialidade, integridade e disponibilidade dos dados organizacionais, sendo especialmente relevante para instituições públicas que buscam demonstrar conformidade com exigências legais e expectativas sociais em relação à proteção digital (ABNT; ISO 27001, 2022).

Esses marcos reforçam a necessidade de compreender a cibersegurança para além de seus aspectos técnicos. Como argumenta Nissenbaum (2005), a segurança informacional deve ser vista sob a ótica da "privacidade contextual", incorporando valores sociais e estruturais. Zuboff (2019) alerta para os riscos do "capitalismo de vigilância", que coloca em tensão direitos fundamentais diante de práticas extrativas de dados em larga escala. A tese sustenta que a cibersegurança, quando ancorada em princípios democráticos, pode ser um instrumento de fortalecimento institucional e de promoção do desenvolvimento local — especialmente em contextos de vulnerabilidade digital.

No entanto, a literatura científica ainda carece de articulação entre essas abordagens. Apesar da crescente produção acadêmica sobre cibersegurança, observa-se uma fragmentação conceitual, com predominância de enfoques técnico-normativos e ausência de leituras territoriais ou aplicadas a escalas subnacionais. São raros os estudos que conectam a segurança digital à capacidade institucional local, à inclusão informacional e ao desenvolvimento urbano, revelando um campo em expansão, mas ainda carente de fundamentos teóricos consolidados.

Diante desse cenário, a questão de pesquisa que orienta o Estudo I consiste em identificar quais são os principais núcleos temáticos, lacunas conceituais e tendências metodológicas que caracterizam a produção científica sobre cibersegurança, especialmente em sua interface com a governança institucional e o desenvolvimento regional. Nesse contexto, o estudo tem por objetivo examinar os núcleos temáticos da literatura científica sobre o tema, evidenciando limitações conceituais e possibilidades de ampliação dos enfoques existentes.

Para tanto, são mobilizadas duas estratégias metodológicas complementares: análise bibliométrica e revisão sistemática da literatura. Com base nesses métodos, o Estudo I mapeia o estado da arte da produção acadêmica internacional, oferecendo subsídios analíticos para a construção do arcabouço teórico e empírico da tese.

Ao revelar padrões temáticos, autores centrais, marcos conceituais e lacunas analíticas da literatura, este estudo cumpre uma função diagnóstica essencial. Ele fundamenta os estudos seguintes, que se debruçarão sobre a realidade institucional dos municípios da região carbonífera de Santa Catarina e as possibilidades de estruturação de políticas públicas digitais mais inclusivas, seguras e orientadas ao bem comum.

2.2 RECORTE TEÓRICO SOBRE O TEMA

A cibersegurança, enquanto campo conceitual, político e tecnológico, é produto direto da transformação digital das sociedades contemporâneas. Sua emergência decorre da crescente interdependência entre os sistemas computacionais, as infraestruturas críticas e os processos sociais, econômicos e institucionais. Com raízes que remontam ao final da década de 1960, a cibersegurança evoluiu de um campo técnico, voltado à integridade de sistemas computacionais isolados, para uma arena complexa e interdisciplinar, que articula ciência da computação, teoria política, direito, sociologia, relações internacionais e economia institucional.

Inicialmente nas décadas de 1960 e 1970, a segurança da informação concentrou-se em garantir confidencialidade, integridade e disponibilidade de dados em ambientes restritos (Anderson, 2001). Com o surgimento das primeiras redes locais e, sobretudo, da internet comercial nos anos 1990, esse escopo se expandiu para abranger não apenas cadeados lógicos, mas toda a conectividade de sistemas distribuídos, dando ensejo ao conceito de cibersegurança como defendido por Nissenbaum (2005).

Nos primórdios da computação, a preocupação com a segurança dos sistemas restringia-se à proteção de informações em ambientes militares ou científicos. O conceito de segurança da informação, fortemente marcado pelo paradigma da confidencialidade, integridade e disponibilidade (CID), era então estruturado com base na arquitetura de sistemas fechados, cujo controle era centralizado (Anderson, 2001). A partir da década de 1980, com o surgimento das redes locais (LANs) e, mais tarde, da internet, a noção de segurança começa a adquirir contornos mais amplos, incluindo a necessidade de proteger os sistemas frente à interconectividade crescente.

Na década de 1990, o advento da internet comercial e a progressiva informatização de setores públicos e privados impuseram novos desafios à segurança dos sistemas. A noção de "*cybersecurity*" — cibersegurança — passa a consolidar-se como categoria distinta da mera segurança da informação. Segundo Nissenbaum (2005), a transição entre esses dois conceitos não é apenas semântica, mas estrutural: enquanto a segurança da informação se orienta para proteger ativos informacionais dentro de sistemas fechados, a cibersegurança trata da proteção de redes interconectadas, sistemas complexos e infraestruturas críticas, com implicações éticas, sociais e políticas.

Nos anos 2000, a cibersegurança passou a figurar com mais força nas agendas de segurança nacional. O reconhecimento de que as infraestruturas críticas — como energia, telecomunicações, finanças, transporte e saúde — estavam se tornando crescentemente dependentes de redes digitais impulsionou a formulação de estratégias nacionais em países centrais, como os Estados Unidos, Alemanha e Reino Unido. Ao mesmo tempo, começaram a surgir instituições voltadas à ciberdefesa e à formulação de políticas públicas para o setor, como a *National Cybersecurity and Communications Integration Center* (NCCIC) nos EUA e a Agência Europeia para a Segurança das Redes e da Informação (ENISA).

A década de 2010 marca uma inflexão importante no campo da cibersegurança. A massificação dos dispositivos móveis, a explosão dos dados digitais e a difusão de tecnologias como Internet das Coisas (IoT), inteligência artificial e computação em nuvem redefiniram os vetores de risco e ampliaram significativamente a superfície de ataque. Ao mesmo tempo, a digitalização das instituições públicas, das práticas econômicas e dos relacionamentos sociais aprofundou a interdependência entre segurança cibernética e estabilidade social. A cibersegurança passou a ser reconhecida não apenas como um componente da segurança nacional, mas como uma condição de governabilidade, soberania e desenvolvimento.

Conceitualmente, o campo evoluiu em três frentes principais. A corrente técnico-operacional, ancorada em protocolos criptográficos, análise de vulnerabilidades e arquiteturas de rede seguras, fundamenta-se em estudos de Choo (2011) e em *frameworks* como o *NIST Cybersecurity Framework*, que valorizam a defesa proativa de ativos críticos. A corrente institucionalista, conforme analisado por Mishra *et al.* (2022), interpretam a cibersegurança como política pública que exige arranjos multi-níveis de governança, capacitação estatal e cooperação público-privada. Por fim, a abordagem crítica e sociotécnica, ilustrada pelo conceito de “capitalismo de vigilância” de Zuboff (2019), problematiza a captura comercial dos dados e o risco de erosão de liberdades civis, exigindo uma regulação que vá além do *compliance* técnico, para abarcar princípios de justiça informacional.

É nesse contexto que emergem diferentes correntes teóricas para interpretar a cibersegurança. A primeira é a corrente técnico-operacional, oriunda da engenharia e da ciência da computação, que se dedica ao estudo de protocolos de segurança, criptografia, engenharia reversa, arquitetura de redes e vulnerabilidades sistêmicas. Embora essencial, essa abordagem tende a restringir-se à dimensão técnica da proteção, sem considerar os impactos sociais ou institucionais de sua aplicação (Choo, 2011).

Uma segunda corrente é a institucionalista, que compreende a cibersegurança como função do Estado e como resultado da articulação entre normas jurídicas, capacidades organizacionais e cooperação intergovernamental. Essa perspectiva encontra respaldo em autores que defendem a necessidade de políticas públicas integradas de cibersegurança, capazes de alinhar estratégias nacionais, marcos regulatórios e programas de capacitação institucional (Mishra *et al.*, 2022). Aqui, a segurança digital é vista como um bem público cuja provisão depende da coordenação entre diferentes níveis de governo e setores da sociedade.

Em estudo comparativo com sete países (EUA, Canadá, China, Índia, Austrália, Malásia e UE), Mishra *et al.,* (2022) identificam 16 atributos fundamentais para o desenvolvimento de políticas públicas de cibersegurança, destacando a variabilidade na ênfase atribuída a fatores como privacidade, encriptação, proteção de infraestrutura crítica e cooperação internacional. Esses achados demonstram que a formulação de políticas de cibersegurança é altamente dependente do contexto político, institucional e tecnológico de cada país, o que reforça a inadequação de modelos normativos universalizantes. A incorporação desses atributos como categorias analíticas pode qualificar a análise comparativa de estratégias nacionais e regionais, contribuindo para uma compreensão mais robusta da capacidade regulatória dos Estados em ambientes digitais complexos.

A relevância desse estudo reside na sua capacidade de revelar empiricamente como Estados nacionais priorizam dimensões distintas em suas políticas públicas de cibersegurança. Mishra *et al.* (2022) mostram, por exemplo, que países como EUA e Austrália enfatizam defesa de infraestrutura crítica e segurança nacional, enquanto UE e Canadá concentram-se em privacidade e transparência. Essa diversidade revela que modelos normativos importados podem ser disfuncionais se descolados do contexto político-institucional local, o que é particularmente relevante para o caso brasileiro, onde a LGPD e a E-Ciber convivem com baixa capacidade institucional subnacional.

A terceira corrente é crítica e sociotécnica. Ela se fundamenta em uma leitura política da cibersegurança, destacando os riscos de sua apropriação por interesses corporativos ou autoritários. Zuboff (2019), ao tratar do capitalismo de vigilância, argumenta que a

arquitetura digital contemporânea foi construída para extrair, prever e modificar o comportamento humano em larga escala, colocando em xeque os princípios democráticos e os direitos individuais. Essa perspectiva denuncia a assimetria de poder entre empresas de tecnologia, governos e cidadãos, e defende uma regulação que vá além da proteção técnica, promovendo justiça informacional e soberania digital.

Figura 1 – Correntes teóricas sobre estudos de cibersegurança

Fonte: Elaborado pelo autor (2025).

A figura apresentada ilustra, por meio de um triângulo equilátero, a interação entre três abordagens teóricas fundamentais que estruturam o campo da cibersegurança: a técnico-operacional, a institucionalista e a sociotécnica. A disposição em triângulo não é apenas estética, mas conceitual: cada vértice representa uma corrente teórica distinta, e, ao centro, encontra-se a expressão “Políticas Públicas de Cibersegurança”, simbolizando o ponto de convergência e articulação dessas abordagens. A escolha de posicionar o conceito de políticas públicas no centro da figura justifica-se pelo reconhecimento de que nenhuma dessas abordagens, de forma isolada, é suficiente para dar conta da complexidade envolvida na formulação, implementação e avaliação de estratégias de segurança digital em contextos democráticos e tecnologicamente interdependentes.

A corrente técnico-operacional aparece em um dos vértices como base tradicional do campo, sendo centrada na proteção de sistemas, redes e dados. Essa abordagem é responsável por desenvolver ferramentas práticas, como *firewalls*, criptografia e testes de

penetração, e sustenta o funcionamento técnico dos sistemas digitais. Os trabalhos de Anderson (2001), ao tratar da engenharia da segurança, e Choo (2011), ao mapear o cenário de ameaças cibernéticas, fundamentam esse enfoque. A presença dos termos "criptografia", "monitoramento", "vulnerabilidade" e "defesa" abaixo do vértice expressa os principais conceitos operacionais associados à manutenção da integridade e continuidade dos sistemas de informação.

Já a corrente institucionalista enfatiza a importância da organização estatal, da legislação e da governança para o tratamento da cibersegurança. Aqui, as ações dos governos, agências reguladoras e organismos internacionais são cruciais, pois a segurança digital é compreendida como um bem público. Mishra *et al.* (2022), por exemplo, discutem a fragmentação institucional nos países do Sul Global e aponta a necessidade de estruturas coordenadas para uma resposta efetiva às ameaças cibernéticas. Termos como "Estado", "regulação", "coordenação" e "*compliance*" inseridos abaixo deste vértice expressam o campo de atuação dessa abordagem, voltado à criação de estratégias nacionais, marcos legais e estruturas de cooperação.

A corrente sociotécnica ou crítica, por sua vez, destaca os impactos sociais, éticos e políticos da cibersegurança. Ao considerar os efeitos das tecnologias sobre os direitos, liberdades e estruturas de poder, esta abordagem denuncia práticas de vigilância e a assimetria de poder entre cidadãos e grandes corporações digitais. Zuboff (2019) contribui com a noção de "capitalismo de vigilância", alertando para a instrumentalização dos dados pessoais como insumo para controle comportamental e lucro empresarial. Nissenbaum (2005), por sua vez, problematiza a relação entre segurança e valores democráticos, exigindo a inserção de princípios éticos nas decisões tecnológicas. A presença das palavras "vigilância", "poder", "ética" e "justiça informacional" abaixo do vértice representa os fundamentos desse campo crítico, que visa alertar para os riscos de abordagens meramente técnicas ou burocráticas da cibersegurança.

No plano normativo, a evolução da cibersegurança é influenciada por marcos legais nacionais e transnacionais. O Regulamento Geral de Proteção de Dados da União Europeia (GDPR), em vigor desde 2018, é um marco referencial ao estabelecer princípios como o *privacy by design*, a transparência algorítmica e o direito à autodeterminação informacional. Inspirada nesse modelo, a Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/2018) estabelece diretrizes semelhantes, embora sua implementação ainda enfrente desafios estruturais, especialmente em níveis subnacionais. A Estratégia Nacional de Segurança Cibernética (E-Ciber, 2020) complementa esse arcabouço ao propor diretrizes para governança, cooperação

internacional e capacitação institucional, mas adota um viés predominantemente técnico, com menor ênfase nos aspectos éticos e sociais. Ainda assim, conforme mostram Chander *et al.* (2021), a simples existência de marcos legais como o GDPR ou a LGPD não garante sua efetividade. Em muitos casos, os altos custos de *compliance* e a ausência de estruturas institucionais de *enforcement* comprometem a capacidade real de proteção, especialmente em ambientes públicos ou privados com limitações técnicas e orçamentárias.

Como observam Schubert e Barrett (2024), a existência de marcos regulatórios não garante, por si só, a efetividade da proteção de dados. Muitas dessas normas ainda operam sob uma lógica de *compliance* formalista, sem enfrentar de forma sistemática as assimetrias de poder informacional entre governos, empresas e cidadãos. Para os autores, a governança de dados precisa ser entendida como uma estrutura decisória complexa que define não apenas o que pode ser feito com os dados, mas como essas decisões são tomadas, por quem e com que grau de transparência e responsabilização. Tal compreensão amplia a noção de cibersegurança para além da proteção técnica, incorporando critérios de justiça informacional e *accountability* institucional como pilares de sua efetividade.

Quadro 2– Marcos legais e normativos em cibersegurança

Nome do Marco	**Ano**	**Abrangência**	**Descrição e Objetivo**	**Autores**
Convenção de Budapeste sobre o Cibercrime	2001	Internacional	Primeiro tratado internacional vinculante sobre crimes cibernéticos. Visa harmonizar legislações e fortalecer a cooperação internacional.	Conselho da Europa (2001).
ISO/IEC 27001 – Segurança da Informação	2005*	Internacional	Norma para Sistemas de Gestão de Segurança da Informação (SGSI). Define requisitos para proteção contínua de dados organizacionais. (*atualizada 2022)	ISO (2022).
NIST Cybersecurity Framework	2014	EUA / Global	Modelo baseado em cinco funções (identificar, proteger, detectar, responder e recuperar), usado amplamente por setores públicos e privados.	NIST (2014).
Estratégia da OCDE para Segurança Digital	2015+	Internacional	Diretrizes não vinculantes para promoção de segurança digital, privacidade e resiliência institucional nos países-membros.	OCDE (2015).
GDPR – Regulamento Geral de Proteção de Dados (UE)	2016	União Europeia / Global	Regulamento da UE que estabelece regras sobre privacidade e proteção de dados, inspirando legislações em diversas partes do mundo.	União Europeia (2016).
LGPD – Lei Geral de Proteção de Dados (Brasil)	2018	Nacional	Estabelece princípios e regras para o uso de dados pessoais, com foco na proteção da privacidade e transparência no Brasil.	Brasil (2018).
National Cyber Strategy (EUA)	2018	Nacional (EUA)	Estratégia federal para promover defesa cibernética, segurança de	U.S. Government (2018).

Nome do Marco	Ano	Abrangência	Descrição e Objetivo	Autores
			infraestruturas críticas e inovação tecnológica.	
E-Ciber – Estratégia Nacional de Segurança Cibernética	2020	Nacional (Brasil)	Define diretrizes brasileiras para governança cibernética, capacitação, cooperação internacional e gestão de riscos.	Brasil (2020).
Relatório do GGE da ONU sobre Ciberespaço Responsável	2021	Internacional	Recomendações sobre conduta estatal responsável no uso de TICs, buscando a paz e a estabilidade no ambiente digital.	ONU (2021).
Digital Services Act & Digital Markets Act (UE)	2022	União Europeia	Conjunto de leis para regulação das plataformas digitais, com foco em transparência, responsabilidade e concorrência justa.	Parlamento Europeu (2022).
AI Act – Regulamento Europeu de Inteligência Artificial	2023*	União Europeia	Propõe uma estrutura legal para regular riscos e impactos da IA, incluindo aspectos éticos, segurança cibernética e proteção a direitos fundamentais.	Comissão Europeia (2023).

Fonte: Elaborado pelo autor (2025).

Nos Estados Unidos, estratégias como o *National Cyber Strategy* (2018) e o *Cybersecurity Framework* do NIST (*National Institute of Standards and Technology*) demonstram o esforço em institucionalizar a cibersegurança como política pública transversal. Já em países da América Latina, os marcos legais avançam de forma mais fragmentada, com destaque para o Brasil, que em 2020 publicou a sua Estratégia Nacional de Segurança Cibernética (E-Ciber), visando promover um ambiente digital seguro por meio de medidas como conscientização, capacitação, desenvolvimento tecnológico e cooperação internacional (Brasil, 2020).

No plano institucional, observam-se exemplos contrastantes. A Estônia, pioneira na digitalização governamental, construiu um ecossistema de chaves criptográficas e identidades digitais interoperáveis, o "*e-Residency*", fortalecendo sua soberania informacional. Em contrapartida, em vários países em desenvolvimento, verifica-se lacuna de capacidades técnicas e ausência de marcos legais eficazes, o que compromete a resiliência das infraestruturas críticas e agrava as desigualdades digitais (Hossen *et al*., 2023).

Estudos de caso comparativos ilustram a aplicação desses conceitos. Na Ucrânia, durante o conflito de 2022, ataques cibernéticos a infraestruturas energéticas e de comunicação exigiram respostas técnicas rápidas, mas também mobilizaram mecanismos de cooperação internacional (US-EU *Cybersecurity Task Force*), revelando a interdependência entre capacidade técnica e articulação política. Já em Cingapura, o governo integrou o modelo de *security by design* em projetos de "*Smart Nation*", combinando normas rigorosas de proteção

de dados com certificações obrigatórias para dispositivos IoT, o que reforça a coesão entre abordagem técnica e regulatória.

Para além dos dados e das instituições, a cibersegurança exige atenção aos impactos sociais. A inclusão digital, condição para a justiça informacional, depende de políticas que garantam acesso a ferramentas de proteção e educação digital, conforme demonstrado por Tura e Ojanen (2022) em regiões periféricas da Europa e América Latina. Sem esse olhar social, as medidas de defesa podem aprofundar desigualdades e vulnerabilidades.

A literatura também identifica um conjunto de categorias estruturantes para a análise da cibersegurança. Entre elas, destacam-se:

> i) Infraestruturas críticas: referem-se aos sistemas e serviços cuja interrupção ou comprometimento afeta significativamente a segurança, a saúde, a economia e o bem-estar da população. A proteção dessas infraestruturas contra-ataques cibernéticos é considerada prioridade estratégica (Srivastava *et al.,* 2023);
>
> ii) Governança de dados: diz respeito às normas, processos e estruturas que regulam o uso, a proteção e a circulação dos dados digitais. Essa governança envolve desde questões técnicas, como segurança e interoperabilidade, até questões políticas, como propriedade, controle e acesso (Nissenbaum, 2005). Esse entendimento da governança de dados como um processo técnico-político é ampliado por Schubert e Barrett (2024), que propõem vê-la como a camada decisional que regula "como se decide sobre decisões relacionadas aos dados". Isso implica reconhecer que a proteção de dados não se limita a dispositivos tecnológicos ou marcos legais, mas envolve disputas normativas e éticas sobre quem controla, interpreta e utiliza os dados em ambientes digitais interdependentes. Em contextos urbanos e institucionais, essa perspectiva é especialmente relevante: a ausência de uma governança de dados sólida pode comprometer direitos fundamentais e enfraquecer a confiança institucional, sobretudo quando decisões automatizadas afetam diretamente os cidadãos. Assim, a cibersegurança deve incorporar não apenas instrumentos técnicos de defesa, mas também critérios éticos, participativos e de responsabilidade pública.
>
> iii) Resiliência digital: conceito que designa a capacidade dos sistemas sociais e técnicos de resistir, absorver e se recuperar de incidentes cibernéticos. Vai além da defesa e da prevenção, incorporando a adaptabilidade institucional e a cultura organizacional (Parmentola *et al.,* 2022).

> iv) Soberania informacional: expressão que remete ao direito dos Estados e das comunidades de controlarem seus dados, infraestruturas e fluxos informacionais, em contraposição à dependência de plataformas estrangeiras ou à regulação exógena (Tura; Ojanen, 2022).

Essas categorias operam de forma transversal nas diferentes abordagens teóricas, permitindo articular dimensões técnicas, institucionais e políticas da segurança digital. Elas também servem de base para os estudos que analisam os efeitos da cibersegurança nas dinâmicas de poder, na formulação de políticas públicas e na estruturação das capacidades estatais.

A construção de uma cibersegurança democrática, ética e sustentável requer a articulação de múltiplos atores e escalas. Visvizi e Del Hoyo (2021) defendem a necessidade de modelos de governança multiescalar, nos quais governos locais, nacionais e transnacionais compartilhem responsabilidades e colaborem na formulação de políticas. Isso envolve tanto a harmonização de normas quanto a criação de mecanismos de cooperação operacional.

Do ponto de vista ético, autores como Allam (2021) e Mann *et al.* (2022) argumentam que a cibersegurança deve estar subordinada a valores democráticos, como transparência, participação, justiça e prestação de contas. A adoção de tecnologias de vigilância ou controle comportamental, por exemplo, precisa ser regulada por princípios constitucionais e por instâncias públicas de deliberação. A segurança digital não pode justificar práticas autoritárias nem legitimar o desmonte de garantias civis.

A partir desse percurso teórico e histórico, fica evidente que a cibersegurança constitui um campo em constante reconfiguração, cujas fronteiras se ampliam na medida em que novos riscos, tecnologias e relações sociais são incorporados ao mundo digital. Sua relevância para a estabilidade institucional, a proteção dos direitos e o desenvolvimento tecnológico é inegável, o que torna imprescindível sua consolidação como política pública central nos Estados contemporâneos.

A perspectiva internacional sobre cibersegurança também apresenta importantes variações quanto ao foco, à abrangência e à capacidade de resposta dos Estados. Enquanto países como Alemanha, Reino Unido, Israel, Canadá e Estônia têm consolidado estruturas estatais robustas e marcos normativos avançados, há países em desenvolvimento cuja estrutura normativa permanece incipiente, fragmentada e dependente de diretrizes internacionais. Essa assimetria regula, em parte, o grau de exposição e vulnerabilidade dos sistemas públicos e

privados, e coloca em evidência a necessidade de construção de capacidades nacionais sustentáveis, inclusive nos países periféricos.

Como reforça Mishra *et al.,* (2022), essa fragmentação entre países não decorre apenas da ausência de normas, mas da diversidade de atributos priorizados por cada Estado. Essa heterogeneidade dificulta a interoperabilidade de políticas e compromete a construção de padrões de governança digital comuns, sobretudo no Sul Global, onde há déficits institucionais e técnicos que impedem a plena adoção de *frameworks* abrangentes.

A Organização das Nações Unidas (ONU), a União Internacional de Telecomunicações (UIT), a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e o Fórum Econômico Mundial têm promovido iniciativas de padronização e recomendações voltadas à proteção cibernética e à cooperação internacional. No entanto, os desafios geopolíticos e os interesses econômicos assimétricos dificultam a construção de um regime global uniforme de cibersegurança.

Como demonstram Chander *et al.* (2021), a fragmentação regulatória é um dos principais obstáculos à eficácia da proteção digital, pois as legislações nacionais frequentemente não acompanham a natureza transfronteiriça dos fluxos informacionais e das ameaças cibernéticas. Além disso, os autores alertam para o descompasso entre a legislação formal e a implementação prática dos direitos digitais, fenômeno que chamam de "*privacy enforcement gap*" — distância entre norma e prática. Em países e regiões com baixa capacidade institucional, como ocorre em diversos contextos subnacionais brasileiros, esse descompasso tende a ampliar a vulnerabilidade digital, reproduzindo assimetrias no acesso à proteção informacional e dificultando a consolidação de uma governança eficaz.

Os autores destacam ainda que o "*privacy enforcement gap*" é mais acentuado em contextos de baixa institucionalidade, como ocorre em muitas cidades brasileiras. Essa lacuna se manifesta tanto na ausência de pessoal capacitado quanto na inexistência de estruturas formais para tratamento de dados, auditoria e resposta a incidentes. Assim, a fragmentação não é apenas jurídica, mas operacional.

Nesse contexto, ganha relevância o debate sobre a autonomia regulatória, especialmente em países cuja infraestrutura digital é majoritariamente dependente de soluções desenvolvidas por grandes plataformas globais. A soberania digital passa, portanto, pela capacidade de formulação e aplicação de normas locais, pelo domínio sobre os fluxos de dados e pela possibilidade de fiscalizar e auditar algoritmos e sistemas utilizados por agentes públicos e privados. Para Zuboff (2019), a ausência de regulação eficaz permitiu que as grandes corporações tecnológicas estruturassem suas operações com base em assimetrias de informação

e captura de dados em larga escala, o que reforça a urgência de respostas institucionais mais incisivas.

Nesse cenário, torna-se evidente que os desafios da cibersegurança não podem ser enfrentados apenas com investimentos em infraestrutura ou capacitação técnica. Embora esses elementos sejam essenciais, é a qualidade da governança — entendida como a capacidade de formular, implementar e avaliar políticas públicas eficazes — que determina a efetividade das respostas. Como argumentam Parmentola *et al.* (2022), a resiliência digital depende menos da existência de tecnologias avançadas e mais da capacidade de integrar essas tecnologias a uma cultura organizacional baseada em princípios democráticos e orientada ao bem comum.

A literatura também chama atenção para os riscos do determinismo tecnológico, que pressupõe que o avanço técnico resolve, por si só, os desafios sociais. Autores como Mann *et al.* (2022) e Allam (2021) criticam esse pressuposto, demonstrando que a implantação de soluções de segurança digital pode gerar efeitos adversos quando não acompanhada de planejamento participativo e de salvaguardas jurídicas. Em contextos de baixa institucionalidade, tecnologias de monitoramento, por exemplo, podem ser utilizadas para fins de controle social, repressão política ou discriminação algorítmica.

Por isso, os princípios éticos devem ser incorporados desde o início no ciclo de vida das tecnologias digitais. A abordagem do *privacy by design* propõe que a proteção de dados e da privacidade seja um elemento estrutural no desenvolvimento de sistemas, e não um adendo posterior. Da mesma forma, o conceito de *security by design* enfatiza que a segurança deve estar embutida na arquitetura das soluções, antecipando vulnerabilidades e prevenindo riscos desde a concepção.

Esse debate ético se articula com a necessidade de mecanismos de auditoria algorítmica, transparência nos critérios de decisão automatizada e responsabilização de agentes que violam os direitos digitais. Os marcos regulatórios, nesse sentido, devem prever não apenas a definição de direitos e obrigações, mas também mecanismos de monitoramento, fiscalização e punição em caso de infrações. Como destaca Nissenbaum (2005), a eficácia da regulação depende da coerência entre normas, valores sociais e práticas institucionais.

Ainda dentro da perspectiva ética e normativa, cabe destacar a interseção da cibersegurança com os direitos humanos. O direito à privacidade, à liberdade de expressão e à proteção de dados são frequentemente afetados por práticas de vigilância massiva, monitoramento indevido ou manipulação de informações. Esse debate ganhou relevância com as revelações de Edward Snowden, em 2013, que evidenciaram a existência de sistemas de

espionagem global operados por agências de inteligência, muitas vezes sem o conhecimento ou consentimento dos cidadãos ou mesmo das instituições nacionais.

Essas revelações tiveram um efeito significativo sobre a agenda internacional de cibersegurança, provocando reformas em leis de proteção de dados e incentivando a criação de mecanismos de supervisão e controle democrático sobre atividades cibernéticas sensíveis. O escândalo também impulsionou a adoção de tecnologias de criptografia ponta a ponta, o fortalecimento de mecanismos de anonimato e o debate sobre o uso ético da inteligência artificial em contextos de segurança.

Outra dimensão que a literatura enfatiza é a relação entre cibersegurança e desigualdade. Estudos como os de Tura e Ojanen (2022) mostram que populações marginalizadas ou em territórios periféricos tendem a ter menor acesso a recursos de proteção digital, seja por falta de infraestrutura, capacitação técnica ou capital político. Essa desigualdade de proteção digital contribui para o aprofundamento da exclusão social, cria novas vulnerabilidades e reforça a dependência dessas populações em relação a intermediários tecnológicos, muitas vezes sem transparência ou controle social.

A partir dessa perspectiva, políticas públicas de cibersegurança devem contemplar mecanismos de inclusão digital, formação cidadã, acesso aberto a tecnologias de proteção e redes descentralizadas de resposta a incidentes. Isso significa que a cibersegurança precisa ser tratada como uma política social, voltada não apenas para a proteção de sistemas, mas para a promoção da equidade, da justiça e da cidadania digital.

É nesse contexto que o debate sobre arquitetura institucional adquire centralidade. Estados que desejam promover uma política robusta de cibersegurança precisam articular diferentes órgãos de governo, garantir orçamentos contínuos, estabelecer canais de diálogo com a sociedade civil e manter uma vigilância constante sobre as transformações do ecossistema digital. Como destacam Mishra *et al.* (2022), a capacidade de resposta cibernética não depende exclusivamente de investimentos em tecnologia, mas da maturidade organizacional e da cultura institucional de segurança.

Além disso, a cooperação internacional aparece como um elemento fundamental para a construção de uma governança global de cibersegurança. A crescente interdependência entre sistemas nacionais, a multiplicação de atores transnacionais e a natureza transfronteiriça dos ataques cibernéticos exigem a harmonização de normas, a troca de informações e a construção de confiança entre países. Iniciativas como o Tallinn Manual, a Convenção de Budapeste e o Grupo de Peritos Governamentais da ONU têm buscado estabelecer parâmetros comuns, ainda que as disputas geopolíticas muitas vezes limitem seu alcance.

Em síntese, o campo da cibersegurança é marcado por uma complexa articulação entre fatores técnicos, jurídicos, políticos, econômicos e sociais. Sua evolução histórica reflete tanto os avanços da digitalização quanto as transformações nas estruturas de poder e nos padrões de governança. A consolidação de uma abordagem democrática, eficaz e justa para a cibersegurança exige, portanto, a articulação entre princípios éticos, capacidade institucional, participação cidadã e regulação transparente.

Com base nos fundamentos apresentados, é possível afirmar que a cibersegurança não se limita à proteção de dados ou ao combate a crimes digitais. Trata-se de um campo estratégico para a preservação das democracias, a garantia dos direitos fundamentais e a promoção do desenvolvimento sustentável em um mundo digitalizado. Seu fortalecimento requer políticas públicas transversais, ações coordenadas e uma cultura de segurança orientada por valores republicanos, pluralistas e inclusivos.

Embora *frameworks* como o NIST e normas ISO ofereçam referências valiosas para a construção de políticas de segurança, sua aplicação acrítica pode resultar em ineficiência ou até vulnerabilidade, especialmente quando transplantados para realidades institucionais com menor maturidade. A crítica de autores como Allam (2021) e Mann *et al.* (2022) aponta que a adoção de modelos de governança algorítmica, sem salvaguardas democráticas, pode legitimar vigilância seletiva e aprofundar desigualdades digitais. Mishra *et al*. (2022) mostram empiricamente que países variam amplamente na capacidade de internalizar essas normas. O desafio, portanto, é calibrar padrões internacionais às capacidades locais, respeitando o contexto político, jurídico e social.

A incorporação da cibersegurança como vetor de desenvolvimento exige, portanto, uma abordagem que una infraestrutura tecnológica, arcabouço normativo e estruturas robustas de governança de dados. Como argumentam Schubert e Barrett (2024), a governança de dados precisa estar intrinsecamente vinculada a princípios éticos, mecanismos de responsabilização institucional e modelos de proteção da privacidade individual, sobretudo diante da crescente automatização de decisões que afetam diretamente os cidadãos. Em contextos subnacionais, como os municípios que avançam na digitalização de serviços públicos, essa integração é crítica: sem ela, políticas públicas digitais podem reproduzir assimetrias e vulnerabilidades já existentes, ao invés de mitigá-las.

2.3 PROCEDIMENTOS METODOLÓGICOS

Para o desenvolvimento da pesquisa, adotou-se como procedimento de abordagem o método misto, envolvendo em duas etapas a pesquisa quantitativa e qualitativa. Creswell (2021) descreve que o método misto envolve a coleta de dados em duas etapas, em que o pesquisador coleta os dados quantitativos na primeira fase, analisa os resultados e depois usa os resultados para planejar a (ou se basear na) segunda fase qualitativa. Os resultados quantitativos geralmente informam os tipos de participantes a serem selecionados intencionalmente para a fase qualitativa e os tipos de perguntas que serão solucionadas (Creswell, 2021).

Os métodos qualitativos demonstram uma abordagem de investigação acadêmica, onde os dados são extraídos de textos e imagens, possuem passos singulares de análise dos dados e se valem de diferentes abordagens. A escrita requer, em partes, a educação dos leitores quanto a sua intenção, refletindo o papel do pesquisador, extraindo informações de dados extraídos sob protocolos específicos de coletas (Creswell, 2021).

A análise bibliométrica é uma abordagem quantitativa voltada para a mensuração, mapeamento e interpretação da produção científica em determinado campo de conhecimento. Ela permite identificar tendências temáticas, redes de coautoria, instituições e países mais produtivos, bem como os artigos e autores mais influentes. Trata-se de uma técnica consolidada para estudos exploratórios e diagnósticos da literatura, especialmente útil quando se busca compreender a dinâmica e a evolução de áreas científicas emergentes, como é o caso da cibersegurança em contextos socioeconômicos urbanos.

No presente estudo, a bibliometria foi aplicada com o objetivo de mapear a produção científica recente (2020–2025) relacionada à cibersegurança, desenvolvimento urbano e governança de dados. Foram utilizadas as bases *Scopus* e Web of *Science*, reconhecidas por sua abrangência internacional e rigor técnico. O tratamento dos dados foi realizado por meio do pacote *Bibliometrix* (Aria; Cuccurullo, 2017) em linguagem R, permitindo a extração de indicadores como frequência de palavras-chave, evolução anual de publicações, cocitações, redes de colaboração e análise temática. Os resultados dessa etapa forneceram uma base empírica sólida para orientar a revisão sistemática subsequente e delimitar os principais núcleos de produção científica no tema.

A revisão sistemática da literatura é um procedimento metodológico voltado à identificação, seleção, avaliação e síntese de estudos relevantes sobre um determinado tema, de modo a assegurar transparência, reprodutibilidade e qualidade na coleta e análise das

evidências. Diferente de revisões narrativas, o foco está em reduzir vieses e em seguir um protocolo estruturado para garantir consistência na análise. Neste estudo, a revisão sistemática foi utilizada para aprofundar a compreensão dos marcos conceituais e abordagens teóricas predominantes sobre cibersegurança vinculada ao desenvolvimento socioeconômico, complementando a visão panorâmica oferecida pela análise bibliométrica.

Para condução da revisão, foi adotado um protocolo adaptado das diretrizes PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), com critérios de inclusão e exclusão bem definidos. A triagem foi realizada em três etapas: leitura de título e resumo, avaliação do texto completo e extração das informações centrais por categorias analíticas. A revisão forneceu insumos conceituais fundamentais para o arcabouço teórico da tese e para a formulação das categorias analíticas que orientam os estudos empíricos seguintes.

A escolha das palavras-chave utilizadas na busca não foi apenas técnica, mas estratégica. A intenção foi direcionar o levantamento para estudos que abordem a cibersegurança em sua interface com o desenvolvimento em nível local, privilegiando abordagens que permitissem compreender como políticas, capacidades institucionais e práticas de proteção digital se articulam no contexto de municípios e regiões subnacionais. Essa delimitação reflete o objetivo da tese de propor soluções normativas aplicáveis à realidade institucional dos municípios brasileiros, com base em evidências e conceitos diretamente relacionados à governança pública local e à proteção digital descentralizada.

A seleção dos artigos científicos utilizados na presente análise bibliométrica seguiu critérios sistemáticos, com o objetivo de garantir a relevância temática e a qualidade informacional dos registros.

A estratégia de busca empregada utilizou operadores booleanos aplicados aos campos "título do artigo", "resumo" e "palavras-chave", conforme a seguinte combinação: "*cybersecurity*" OR "*cyber security*" AND "*regulation*" OR "*governance*" AND "*development*". Essa combinação teve por finalidade identificar publicações que abordassem a cibersegurança de forma integrada com aspectos de regulação, governança e desenvolvimento, especialmente no contexto urbano e socioeconômico.

Foram inicialmente recuperados 717 registros, sendo 179 provenientes da base Web of Science e 538 da Scopus. Após a remoção de 266 documentos duplicados (identificados diretamente durante o processo de importação no *software Bibliometrix*), restaram 619 documentos para triagem. A triagem consistiu na aplicação de critérios de exclusão baseados na duplicidade de DOI (n = 73), idioma diferente do inglês (n = 27), tipo documental distinto

de artigo, revisão ou artigo de conferência (n = 191) e ausência ou insuficiência de metadados (n = 16), totalizando 307 exclusões.

Com isso, 312 registros foram considerados elegíveis para análise, sendo processados no ambiente R, por meio do pacote *Bibliometrix*, que oferece suporte às técnicas de análise quantitativa da produção científica (Aria; Cuccurullo, 2017). Adicionalmente, seis registros com elevado número de citações foram incorporados manualmente, após verificação de metadados ausentes nas bases e avaliação de elegibilidade, compondo um total de 318 documentos analisados.

Para assegurar a confiabilidade e a completude dos dados, foi realizada uma avaliação da qualidade dos metadados dos documentos importados, totalizando 318 registros no momento da análise (antes da última exclusão manual). O relatório de qualidade gerado pelo *software* indicou que os principais campos — como título, resumo, autor, afiliação, tipo de documento, idioma, ano de publicação e periódico — apresentaram completude de 100%, sendo classificados como excelentes. Outros campos, como palavras-chave (DE) e palavras-chave adicionais (*Keywords Plus*), apresentaram uma taxa de ausência inferior a 5%, sendo considerados bons. O campo "autor correspondente" (RP), embora com uma taxa de ausência de 11,32%, ainda foi classificado como aceitável.

A aplicação desses critérios metodológicos visou garantir a robustez da base analisada e a validade das inferências obtidas a partir dos indicadores bibliométricos, conforme recomendações da literatura (Donthu *et al.*, 2021).

2.4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

O processo de seleção e preparação dos dados para a análise bibliométrica foi conduzido em conformidade com o modelo PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Ao final do processo de triagem, 318 registros foram considerados adequados e processados no *Bibliometrix*, por meio de conversão e limpeza no formato *.bibtex.*

A base final analisada é composta por 318 documentos publicados no intervalo de 2020 a 2025, refletindo uma amostra representativa da produção científica recente sobre cibersegurança em contextos relacionados ao desenvolvimento, regulação e governança. Esse recorte temporal foi estratégico para compreender as tendências contemporâneas do tema, principalmente considerando a intensificação da digitalização e a maior atenção política e científica às questões de segurança cibernética nos últimos anos.

Figura 2 – Informações gerais sobre os dados

Fonte: Dados da pesquisa (2023).

As publicações analisadas foram extraídas de 245 fontes diferentes, incluindo periódicos e anais de conferência, o que revela uma diversidade significativa de canais de disseminação científica. A dispersão das fontes pode ser interpretada como um indicativo da multidisciplinaridade do tema, que perpassa áreas como ciência da computação, ciências sociais, engenharia, economia e administração — conforme delimitado na filtragem inicial.

O crescimento médio anual da produção científica no período analisado foi de 4,14%, indicando uma tendência de expansão estável, ainda que moderada, do interesse acadêmico pelo tema. Esse crescimento contínuo reflete a consolidação do campo de estudos em cibersegurança, especialmente em sua interface com políticas públicas e desenvolvimento urbano, reforçando sua relevância na agenda científica global (Donthu *et al.*, 2021).

No total, 1.013 autores participaram da produção dos 318 documentos, resultando em uma média de 3,35 coautores por publicação, o que aponta para uma predominância do trabalho colaborativo no campo. O número de autores que publicaram de forma individual foi de 63, ou seja, apenas cerca de 6,2% dos pesquisadores optaram por autoria solo, o que evidencia a natureza coletiva e interdisciplinar das investigações. A taxa de coautoria internacional foi de 9,43%, sugerindo uma colaboração transnacional ainda modesta, embora presente.

No que tange à terminologia utilizada pelos autores, a análise identificou 1.416 palavras-chave fornecidas diretamente nos artigos (*Author's Keywords*), que serão exploradas em seções posteriores por meio de técnicas de coocorrência e análise de rede. Esse alto volume sugere uma ampla variedade de abordagens e subtemas dentro do escopo delimitado, permitindo identificar padrões emergentes e lacunas na literatura científica.

A média de citações por documento foi de 12,59, indicando um impacto científico razoável, ainda mais relevante considerando a baixa média de idade dos documentos, que foi

de 2,18 anos. Esse indicador reflete a atualidade do conjunto analisado e aponta que muitos artigos ainda estão no início de seu ciclo de citação, o que pode resultar em crescimento futuro do impacto. O quadro 3 está apresentado de forma decrescente pelo total de citação por ano.

Quadro 3 – Impacto local dos autores

Autor	Título	TC	TCpY
Bolbot V (2023) Banda O (2023)	Pesquisa sobre risco, segurança e confiabilidade de navios autônomos: uma revisão bibliométrica	47	15,667
Chen Y (2024)	Controle distribuído seguro para resposta à demanda em sistemas de energia contra-ataques cibernéticos enganosos com padrões arbitrários	27	13,500
Alzoubi Y (2022)	Atributos que impactam o desenvolvimento de políticas de segurança cibernética: evidências de sete nações	52	13,000
Ahmad I (2022)	Uma nova arquitetura descentralizada de blockchain para a preservação da privacidade e segurança de dados contra-ataques cibernéticos na área da saúde	51	12,750
Chen Y (2022)	O Desenvolvimento e as Questões da Energia-TIC: Uma Revisão da Literatura com Perspectivas Econômicas e Gerenciais	31	7,750
Abbas H (2022)	Nexo entre governo eletrônico, segurança cibernética e corrupção no serviço público (PSS) sustentabilidade em economias asiáticas usando algoritmos de efeito fixo e floresta aleatória	23	5,750
Badal F (2023)	Evolução da microrrede para a rede inteligente: desafios técnicos, soluções atuais e escopos futuros	17	5,667
Bygrave L (2022)	Segurança por Design: Aspirações e Realidades em um Contexto Regulatório	15	3,750
Alzoubi Y (2024)	Tendências de pesquisa em aprendizado profundo e aprendizado de máquina para segurança de computação em nuvem	7	3,500
Ahmad I (2024)	Uma abordagem multiperspectiva baseada em dados para descoberta de conhecimento em segurança cibernética por meio de modelagem de tópicos	6	3,000
Abbas H (2022)	Impacto das medidas de segurança cibernética na melhoria da governança institucional e na digitalização para uma saúde sustentável	12	3,000
Badal F (2021)	Uma nova unidade de mitigação de intrusão para sistemas de energia interconectados em regulação de frequência para melhorar a segurança cibernética	8	1,600
Abdullah A (2022)	Antecedentes da implementação da segurança cibernética: um estudo sobre a preparação cibernética das empresas sociais do Reino Unido	6	1,500
Bolbot V (2025) Banda O (2025)	Avaliação de risco de segurança cibernética de um motor marítimo de combustível duplo em um navio de navegação interior	1	1,000
Bygrave L (2025)	O surgimento da legislação de cibersegurança da UE: uma história de limões, angústia, turfe, surf e caixas cinzentas	1	1,000
Zhou X (2023)	O impacto dos mecanismos regulatórios no comportamento de divulgação de vulnerabilidades durante testes de segurança cibernética de crowdsourcing	1	0,333
TC: Total de citação TCpY: Total de citação por ano			

Fonte: Dados da pesquisa (2025).

A análise do impacto local dos autores evidencia a presença de contribuições relevantes para a interface entre cibersegurança, regulação e desenvolvimento, temática central deste estudo. Dentre os autores com maior destaque, observa-se o trabalho de Bolbot (2023), que apresenta uma revisão bibliométrica sobre riscos e segurança aplicados à navegação

autônoma. Embora o foco da autora seja o setor marítimo, a discussão sobre sistemas críticos autônomos e a necessidade de governança compartilhada entre Estado, indústria e academia é inteiramente aplicável ao contexto urbano digitalizado, sobretudo quando se considera a infraestrutura das chamadas cidades inteligentes. Em sua publicação mais recente, Bolbot (2025) também analisa riscos cibernéticos em motores de combustíveis duplos, utilizando métodos de engenharia de confiabilidade que podem ser transpostos para análise de riscos em infraestruturas urbanas críticas, como redes de energia ou mobilidade conectada.

Outro destaque é Chen, com três artigos analisados. Em um de seus trabalhos, publicado em 2022, o autor realiza uma revisão ampla sobre tecnologias digitais aplicadas à economia de energia verde, estabelecendo conexões entre digitalização, sustentabilidade e políticas públicas. A partir dessa análise, é possível inferir a relevância da cibersegurança como elemento facilitador — e por vezes limitador — do progresso sustentável em áreas urbanas. Em outro estudo, Chen (2024) propõe mecanismos seguros de resposta à demanda em sistemas energéticos, com enfoque na mitigação de ataques cibernéticos, o que reforça a importância da proteção de redes energéticas inteligentes, essenciais para o funcionamento de cidades modernas. A interseção entre segurança cibernética e infraestrutura energética também é abordada por Ahmad (2022), cuja pesquisa propõe uma arquitetura baseada em blockchain para garantir a privacidade de dados no setor de saúde — solução que tem potencial de aplicação em sistemas urbanos digitalizados, como saúde pública conectada, ampliando a confiança e a eficiência dos serviços.

A contribuição de Alzoubi (2022), por sua vez, é particularmente relevante para este estudo ao investigar, de forma comparativa, atributos comuns entre políticas de cibersegurança de diferentes países. O modelo de política proposto pelo autor permite refletir sobre elementos estruturantes que devem ser considerados por governos municipais ao integrar a cibersegurança em suas agendas de desenvolvimento urbano. Complementarmente, Alzoubi também explora tendências de segurança em ambientes de computação em nuvem com uso de inteligência artificial, contribuindo para o entendimento de como soluções tecnológicas avançadas podem ser aplicadas na gestão segura de dados urbanos. A perspectiva política e institucional também é explorada por Abbas, que examina a relação entre governo eletrônico, corrupção e cibersegurança na oferta de serviços públicos, destacando a influência da maturidade institucional na eficácia das iniciativas digitais — aspecto fundamental quando se discute desenvolvimento socioeconômico urbano mediado por tecnologias.

Badal (2023), por sua vez, explora soluções técnicas para a proteção de sistemas energéticos interconectados e a transição de *microgrids* para *smart grids*, temas diretamente

associados à resiliência de cidades inteligentes. Tais contribuições são essenciais para pensar modelos de desenvolvimento urbano que dependam de sistemas energéticos distribuídos e seguros. No campo jurídico e regulatório, destacam-se as publicações de Bygrave (2022), que aborda criticamente o conceito de "*security by design*" em políticas públicas e analisa o desenvolvimento da legislação europeia de cibersegurança. Sua reflexão sobre o equilíbrio entre proteção, liberdades civis e interesses corporativos é de grande valor para cidades que buscam estruturar marcos normativos próprios sobre segurança digital. Abdullah (2022), por sua vez, contribui com uma análise dos fatores organizacionais e individuais que influenciam a implementação de políticas de cibersegurança em empresas sociais, podendo ser aplicada no contexto de organizações públicas locais, como prefeituras e empresas mistas urbanas.

Zhou (2023) oferece abordagens baseadas em aprendizado de máquina para detecção de ameaças cibernéticas em sistemas de saúde e biológicos, áreas sensíveis no planejamento urbano digital. Embora alguns de seus estudos ainda não tenham recebido citações, a aplicação de métodos computacionais avançados para mitigação de riscos em setores críticos reforça a pertinência de suas contribuições dentro do escopo desta tese. Em conjunto, os autores analisados demonstram não apenas um elevado desempenho acadêmico, mas também uma significativa convergência entre cibersegurança, infraestrutura crítica, políticas públicas e desenvolvimento sustentável — pilares que sustentam a proposta teórica aqui desenvolvida. O quadro 4 apresenta em forma decrescente os trabalhos pela citação proporcional entre os anos de publicação.

Quadro 4 – Documentos locais mais citados

Autor/Periódico	Título	TC	TCY	NTC
Sharifi A (2024) Cities	Cidades inteligentes e objetivos de desenvolvimento sustentável (ODS): uma revisão sistemática da literatura sobre cobenefícios e compensações	112	56,00	22,40
Nishant R (2020) Int J Inf Manage	Inteligência artificial para a sustentabilidade: desafios, oportunidades e uma agenda de pesquisa	616	102,6	14,61
Dhirani L (2023) Sensors J Korean Inst Commun Inf Sci	Dilemas éticos e questões de privacidade em tecnologias emergentes: uma revisão	133	44,33	11,01
Hossen M (2025) Pak J Life Soc Sci	Revelando o impacto da governança eletrônica na transformação do Bangladesh digital para o inteligente	5	5,00	8,17
Hui H (2020) Appl Energy	Internet das Coisas baseada em rede 5G para resposta à demanda em redes inteligentes: uma pesquisa sobre o potencial de aplicação	313	52,17	7,42
Asif M (2024) J Clean Prod	Digitalização para edifícios sustentáveis: tecnologias, aplicações, potencial e desafios	37	18,50	7,40
Martinho A (2021) Transp Ver	Questões éticas em foco na indústria de veículos autônomos	92	18,40	7,21
Tettey F (2024) Biomedical Mater Devices	Uma revisão de dispositivos biomédicos: classificação, diretrizes regulatórias, fatores humanos, software como dispositivo médico e segurança cibernética	35	17,50	7,00

Autor/Periódico	Título	TC	TCY	NTC
Srivastava A (2025) Ieee Trans Power Syst	DERs atrás do medidor do sistema de distribuição: estimativa, quantificação de incerteza e controle	4	4,00	6,53
Camilleri M (2024) Expert Syst	Governança da inteligência artificial: considerações éticas e implicações para a responsabilidade social	29	14,50	5,80
Yang S (2024) Ieee Trans Power Syst	Controle distribuído seguro para resposta à demanda em sistemas de energia contra-ataques cibernéticos enganosos com padrões arbitrários	27	13,50	5,40
Wu J (2023) Ieee Open J Comput Soc	Crimes financeiros no metaverso habilitado pela Web3: taxonomia, contramedidas e oportunidades	64	21,33	5,30
Xia L (2023) Sustainable Cities Soc	Um exame completo das aplicações de cidades inteligentes: explorando desafios e soluções ao longo do ciclo de vida, com ênfase na proteção da privacidade dos cidadãos	64	21,33	5,30
El-Sayegh S (2020) Arch Civ Mech Eng	Uma revisão crítica da impressão 3D na construção: benefícios, desafios e riscos	217	36,17	5,15
Said D (2023) Ieee Eng Manage Ver	Uma Pesquisa sobre Tecnologias de Informação e Comunicação na Gestão Moderna da Demanda para Redes Inteligentes: Desafios, Soluções e Oportunidades	57	19,00	4,72
Mishra A (2022) Comput Secur	Atributos que impactam o desenvolvimento de políticas de segurança cibernética: evidências de sete nações	52	13,00	3,81
TC: Total de citação TCY: Total de citação por ano NTC: Normalized TC				

Fonte: Dados da pesquisa (2025).

A análise dos documentos mais citados localmente revela contribuições significativas para o entendimento da interseção entre cibersegurança e desenvolvimento socioeconômico urbano. Sharifi *et al.* (2024) discutem como as tecnologias das cidades inteligentes enfrentam desafios significativos de privacidade, segurança cibernética e ética no uso da Inteligência Artificial (IA), destacando a necessidade de governança robusta para atingir os Objetivos de Desenvolvimento Sustentável (ODS). O estudo organiza as evidências empíricas disponíveis a partir de uma estrutura de co-benefícios e trade-offs, evidenciando que a adoção de tecnologias urbanas inteligentes não se dá de maneira uniforme ou isenta de contradições. A análise inclui temas como energia limpa, inclusão social, gestão de resíduos e mobilidade urbana, vinculando-os ao ciclo de vida de soluções tecnológicas aplicadas ao espaço urbano.

Além dos aspectos socioambientais, o trabalho insere, de forma crítica, o papel das infraestruturas digitais e dos sistemas de dados como elementos que tanto habilitam quanto restringem o cumprimento dos ODS em contextos urbanos. A ausência de diretrizes específicas de proteção de dados e o déficit de governança digital aparecem como obstáculos recorrentes nas experiências avaliadas, apontando para a necessidade de estruturas regulatórias alinhadas à transformação tecnológica das cidades.

Em complemento, Xia *et al.* (2023) reforçam a relevância da segurança digital em infraestruturas críticas das cidades inteligentes, apontando vulnerabilidades em sistemas baseados em IA e IoT, exigindo políticas públicas claras e eficazes. O estudo conduz uma revisão aprofundada das aplicações de cidades inteligentes ao longo de seu ciclo de vida, com ênfase na proteção da privacidade dos cidadãos. A pesquisa estrutura os desafios enfrentados desde o planejamento até a operação de soluções digitais urbanas, considerando aspectos técnicos, legais e sociais. Com base em casos práticos de cidades como Barcelona e Toronto, o artigo propõe o modelo TIOM (*Theory-dependent Innovative Optimization Model*), que equilibra eficiência operacional, sustentabilidade e governança dos dados.

Um dos destaques do trabalho está na constatação de que a ausência de governança integrada de cibersegurança compromete não apenas a privacidade individual, mas a funcionalidade dos sistemas inteligentes como um todo. A discussão sobre ambientes híbridos, onde algoritmos de IA operam dados sensíveis sem supervisão clara, ressalta a urgência de políticas que garantam transparência, auditabilidade e proteção digital nos espaços urbanos conectados.

A conexão entre tecnologias emergentes e sustentabilidade também é abordada por Hui (2020), que analisa o papel da IoT em redes inteligentes de energia (*smart grids*), propondo medidas avançadas de segurança para garantir sua integridade e continuidade operacional. O artigo de Hui (2020), apresenta uma revisão sobre o potencial do 5G e da Internet das Coisas (IoT) no suporte a respostas à demanda em redes elétricas inteligentes. A proposta se concentra em como as novas arquiteturas de comunicação de baixa latência e alta confiabilidade podem viabilizar o controle dinâmico de cargas e dispositivos. O estudo aponta para a necessidade de um arcabouço de segurança que suporte o tráfego intenso de dados e impeça ataques cibernéticos a sistemas críticos.

Entre os desafios destacados estão a ausência de padronização, o risco de vazamentos de dados e a vulnerabilidade dos dispositivos de borda. Os autores propõem que a segurança digital deve estar integrada desde a concepção das redes energéticas inteligentes, incluindo protocolos de autenticação, redundância de dados e controle descentralizado. A infraestrutura energética urbana é apresentada como um campo onde a conectividade e a segurança digital são mutuamente condicionantes.

Em Nishant *et al.* (2020), a proposta é construir uma agenda teórica de pesquisa sobre o uso da inteligência artificial para a sustentabilidade. O artigo opera em escala analítica ampla, considerando aspectos ambientais, sociais e econômicos a partir de diferentes domínios disciplinares. São identificados desafios como a opacidade algorítmica, a pegada ambiental dos

centros de dados, o viés nos sistemas de tomada de decisão e as lacunas regulatórias. A abordagem é conceitual, mas ancorada em exemplos práticos, como o uso de IA em gestão hídrica e planejamento de transportes.

Os autores argumentam que a incorporação ética da inteligência artificial passa por construir estruturas de governança adaptativas, baseadas em justiça algorítmica, responsabilidade institucional e proteção contra falhas sistêmicas. Essa abordagem exige redesenhar as instituições responsáveis pelo controle social das tecnologias digitais, ampliando a perspectiva de risco para incluir impactos sociais, ambientais e éticos das decisões automatizadas.

O trabalho de Dhirani *et al.* (2023) contribui para a discussão crítica sobre ética e privacidade em tecnologias emergentes. Por meio de uma revisão sistemática, os autores discutem os dilemas contemporâneos associados à expansão de tecnologias como veículos autônomos, inteligência artificial, computação em nuvem e sistemas industriais inteligentes. A análise parte de princípios éticos clássicos — como autonomia, justiça e beneficência —, mas os reinterpreta à luz de ambientes tecnológicos dinâmicos e altamente integrados.

A contribuição metodológica do artigo reside em sua sistematização de ameaças ético-regulatórias em ambientes digitalizados, demonstrando que a ausência de padrões internacionais e a fragmentação normativa ampliam as vulnerabilidades sociais e técnicas desses sistemas. Entre os riscos destacados estão a vigilância em massa, a manipulação algorítmica e a ausência de responsabilização legal por decisões automatizadas — elementos que afetam diretamente o espaço urbano digital.

Em uma abordagem de contexto nacional, Hossen *et al.* (2025) investigam o processo de transição de Bangladesh para uma sociedade digital e, posteriormente, para uma sociedade inteligente. O estudo, que tem média de 5 citações por ano, sistematiza iniciativas públicas de e-governança e as relaciona à prestação de serviços, à educação digital e à inclusão de comunidades rurais. Com base em fontes institucionais e acadêmicas, o artigo traça os principais marcos do plano “Digital Bangladesh”, destacando os quatro pilares que sustentam a transformação: governo inteligente, economia inteligente, sociedade inteligente e cidadão inteligente.

A análise revela que, apesar dos avanços em conectividade e serviços digitais, persistem gargalos estruturais relacionados à segurança da informação, à governança de dados e à exclusão digital. O estudo evidencia que políticas públicas de digitalização, quando desarticuladas de estratégias sólidas de proteção cibernética, geram assimetrias e novos riscos

sociais. A ausência de estruturas resilientes de segurança digital surge como uma ameaça à confiança institucional e à inclusão equitativa na sociedade digital.

Asif *et al.* (2024) sistematizam o papel da digitalização na sustentabilidade de edificações ao longo de seu ciclo de vida. O artigo analisa 13 tecnologias digitais — incluindo BIM, IoT, inteligência artificial e blockchain — e seus impactos em termos de eficiência energética, automação e integração de sistemas prediais. A abordagem é centrada na relação entre inovação tecnológica e descarbonização do setor da construção civil.

Um dos destaques do estudo é a ênfase na cibersegurança como requisito técnico e institucional para o funcionamento confiável de edifícios inteligentes. Os autores apontam que, em um ambiente construído cada vez mais conectado, a ausência de proteção contra invasões e falhas digitais compromete o desempenho e a resiliência dos sistemas urbanos. A segurança cibernética é tratada como infraestrutura de suporte para a inteligência predial.

O estudo de Martinho *et al.* (2021), examina os principais dilemas éticos enfrentados pela indústria de veículos autônomos, a partir da triangulação entre literatura científica e relatórios técnicos de empresas autorizadas a operar na Califórnia. A análise revela que, embora a academia dedique atenção a dilemas morais abstratos (como o "problema do bonde"), a indústria se concentra em soluções técnicas e operacionais, com destaque para a segurança funcional e a cibersegurança como preocupações dominantes.

A pesquisa mapeia a ênfase em estratégias de mitigação de risco, como redundância sensorial, controle remoto e algoritmos de segurança baseados em regras rígidas. Ao mesmo tempo, evidencia a lacuna na transparência e na responsabilidade legal em casos de falha sistêmica. A análise posiciona a cibersegurança não como um aspecto isolado, mas como uma condição técnica para a viabilidade social e institucional da mobilidade automatizada, onde a confiança pública depende da robustez e auditabilidade dos sistemas digitais.

Tettey *et al.* (2024) fornecem uma revisão abrangente sobre dispositivos biomédicos, incluindo diretrizes regulatórias e considerações de cibersegurança, com 35 citações totais e uma média anual de 17,50 citações. A pesquisa é relevante para a proteção de dados sensíveis em ambientes urbanos digitalizados, pois, discutem o uso de materiais biomédicos em segurança, destacando como dispositivos inteligentes e conectados exigem estratégias robustas de *cybersecurity* para proteção contra-ataques que poderiam comprometer dados sensíveis.

No campo da energia, Srivastava *et al.* (2025) e Yang *et al.* (2024), propõem um modelo de controle distribuído seguro para recursos energéticos atrás do medidor (BTM DERs), como baterias residenciais e sistemas fotovoltaicos. Os artigos se destacam por aplicar uma

arquitetura de controle resiliente a cenários com ataques cibernéticos de engano com padrões arbitrários.

A contribuição dos trabalhos reside na demonstração de que soluções matemáticas e computacionais podem assegurar a confiabilidade de sistemas energéticos urbanos descentralizados em contextos hostis. A proposta de Srivastava *et al.* (2025) amplia a compreensão da cibersegurança em redes urbanas para além da prevenção, incorporando elementos de autonomia e tolerância a falhas, fundamentais à continuidade dos serviços públicos críticos.

O estudo de Camilleri (2024), avalia o impacto de sistemas especialistas (expert systems) no aprimoramento da cibersegurança, evidenciando sua eficácia em prever e mitigar ataques por meio de abordagens analíticas avançadas. A revisão integra marcos normativos internacionais, como o *AI Act* europeu, e iniciativas privadas de autorregulação ética, propondo um modelo conceitual de governança baseado em cinco eixos: explicabilidade, justiça, *accountability*, privacidade e segurança. O autor argumenta que a regulação da IA precisa ser responsiva e multissetorial, envolvendo governos, empresas e sociedade civil.

A segurança cibernética aparece nesse modelo como um dos pilares da robustez dos sistemas, articulada à necessidade de construir confiança nos ambientes digitais e de garantir o uso responsável de algoritmos em contextos públicos e privados. O trabalho contribui para consolidar uma base normativa e institucional para a discussão sobre governança digital urbana, em que a IA ocupa papel central nos serviços públicos inteligentes.

Com 64 citações e média anual de 21,33, Wu *et al.* (2023) analisa crimes financeiros no metaverso habilitado por tecnologias Web3, oferecendo uma taxonomia de ataques, fraudes e falhas de segurança comuns nesse ecossistema. O estudo cobre tópicos como lavagem de dinheiro, manipulação de mercado, falhas em contratos inteligentes e ausência de identidades confiáveis nas transações entre avatares. A abordagem combina mapeamento técnico com propostas de mecanismos de regulação adaptativa e rastreabilidade digital.

Ao discutir a arquitetura descentralizada das plataformas do metaverso, o artigo mostra que a ausência de um núcleo regulador aumenta a complexidade dos sistemas de controle e monitoramento. A proposta de contramedidas baseadas em mineração comportamental, inteligência artificial e blockchain oferece soluções que transcendem o metaverso e se aplicam também a contextos urbanos que adotam tecnologias descentralizadas como parte de suas infraestruturas digitais.

El-Sayegh (2020) realiza uma revisão crítica sobre o uso da impressão 3D na construção civil. A pesquisa mapeia os benefícios — como redução de resíduos, velocidade de

execução e eficiência de materiais — ao lado dos desafios técnicos e regulatórios que limitam sua aplicação. Um diferencial do trabalho está na ênfase dada aos riscos, incluindo vulnerabilidades cibernéticas nos processos automatizados e integrados digitalmente.

A análise destaca que o uso de impressão 3D em canteiros automatizados envolve sensores, robôs e *softwares* de modelagem que operam sob dependência de redes de dados — o que expõe os sistemas a ataques digitais com consequências estruturais. Essa dimensão, muitas vezes negligenciada em abordagens entusiastas da Indústria 4.0, evidencia que a segurança cibernética é uma exigência não apenas funcional, mas também física, à medida que dados e matéria se tornam indissociáveis na cadeia produtiva da construção urbana.

O estudo de Said (2023) apresenta uma revisão sistemática sobre o papel das tecnologias da informação e comunicação (ICTs) na modernização da gestão do lado da demanda (*Demand Side Management* – DSM) em redes elétricas inteligentes. A pesquisa sistematiza as soluções técnicas mais promissoras para aprimorar a eficiência energética em sistemas urbanos e industriais, como redes de medição avançada, big data, inteligência artificial e blockchain, com ênfase nas ameaças e vulnerabilidades cibernéticas que acompanham essa transformação digital.

A análise destaca que a adoção de arquiteturas de controle descentralizadas e de comunidades energéticas *peer-to-peer* exige uma base tecnológica segura, capaz de proteger os fluxos de dados, garantir autenticidade nas transações energéticas e manter a resiliência das redes contra falhas e ataques externos. Os riscos mais citados incluem ataques de injeção de dados falsos, interrupções por negação de serviço e falhas nos mecanismos de autenticação em dispositivos distribuídos, como medidores inteligentes e sensores de carga.

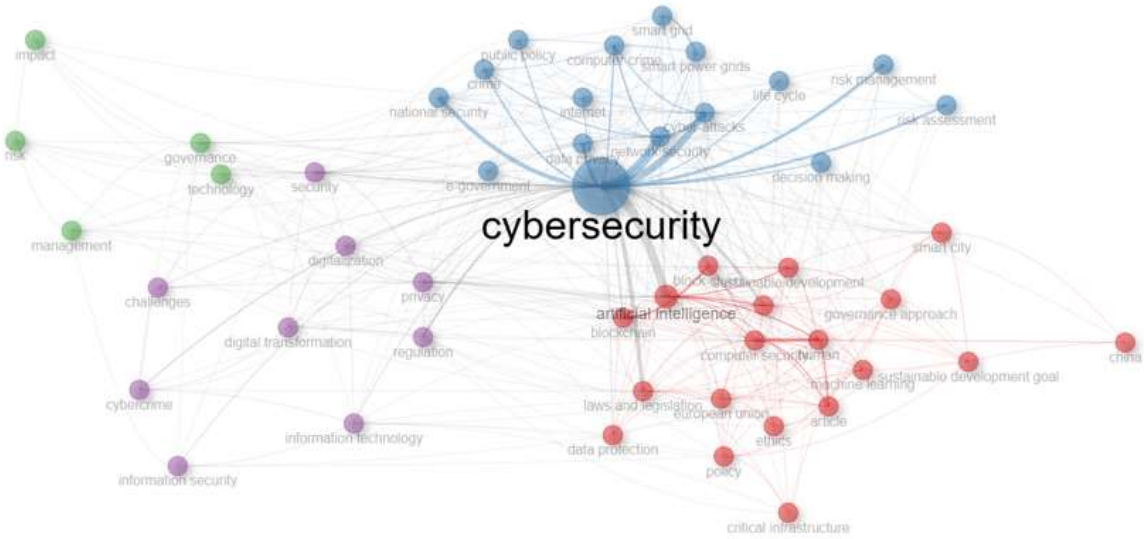
Mishra *et al.* (2022), realizam uma análise comparativa das políticas de cibersegurança em sete países, identificando 14 atributos comuns que moldam a construção das políticas nacionais. A análise revela diferentes graus de maturidade e foco, com destaque para a ênfase norte-americana em identidade digital e crimes cibernéticos, o protagonismo europeu em privacidade e proteção de dados, e a preocupação asiática com redes e infraestruturas críticas.

O estudo oferece um modelo integrador que pode orientar a formulação de políticas em diferentes níveis de governo, especialmente em contextos urbanos onde a interdependência entre setores públicos, privados e cidadãos demanda abordagens multissetoriais. A padronização de atributos técnicos e legais permite construir ambientes digitais mais seguros, resilientes e coerentes com as necessidades socioeconômicas das cidades contemporâneas.

A análise detalhada dos atributos e das políticas associadas em cada país fornece insights valiosos para a formulação de estratégias de cibersegurança adaptadas às realidades locais. No contexto do desenvolvimento socioeconômico de cidades, compreender essas variações é essencial para implementar políticas eficazes que considerem tanto as ameaças cibernéticas quanto as necessidades específicas das comunidades urbanas. Além disso, o estudo destaca a importância de uma abordagem proativa e colaborativa na elaboração de políticas de cibersegurança, envolvendo governos, setor privado e sociedade civil. Essa perspectiva é particularmente pertinente para cidades que buscam integrar tecnologias digitais em sua infraestrutura, garantindo que a segurança cibernética seja incorporada desde o planejamento até a implementação de soluções urbanas inteligentes.

A estrutura conceitual da literatura sobre *cybersecurity* revela um campo denso, multidisciplinar e em rápida expansão, com pontos de convergência entre tecnologia, ética, governança e segurança estratégica. O papel central da *cybersecurity* como hub conceitual evidencia sua transversalidade, enquanto a fragmentação em *clusters* indica especializações temáticas voltadas a setores específicos (infraestrutura, cidades inteligentes, privacidade, etc.).

Figura 3 – Estrutura conceitual de coocorrências de palavras-chaves



Fonte: Dados da pesquisa (2025), imagem gerada por meio do *software bibliometrix*.

A Figura 3 corresponde à rede de coocorrência de palavras-chave (Keywords Plus), representando a estrutura conceitual dos artigos analisados na base bibliométrica.

No centro da rede está o termo "*cybersecurity*", que aparece como o nó mais influente e conectado, funcionando como eixo articulador entre diferentes áreas temáticas. Ao redor desse núcleo, observam-se cinco *clusters* de palavras-chave, identificáveis pelas diferentes cores dos nós, cada um representando um conjunto de temas correlacionados.

O *cluster* vermelho, situado à direita, concentra termos associados a "*smart cities*", "*artificial intelligence*", "*sustainable development goals*", "*e-governance*" e "*data protection*". Esse agrupamento sinaliza uma forte convergência entre cibersegurança, planejamento urbano inteligente e tecnologias emergentes. O destaque para termos como "*governance approach*" e "*ethics*" indica tanto o foco em abordagens institucionais quanto em casos nacionais específicos. Essa configuração é particularmente relevante para o presente estudo, pois demonstra como o discurso sobre cibersegurança está interligado à transformação digital de cidades e à regulação ética e funcional de tecnologias baseadas em dados. A alta pontuação de *PageRank* de termos como *artificial intelligence* (0.052) e *computer security* (0.032) revela a centralidade desses conceitos no avanço científico e técnico do campo.

No *cluster* azul, à esquerda, concentram-se temas ligados à infraestrutura crítica e à gestão de riscos, como "*risk assessment*", "*decision-making*", "*internet*", "*computer science*", "*national security*" e "*smart power grids*". Este agrupamento reforça a centralidade da segurança cibernética em sistemas técnicos complexos, principalmente nos setores energético e de infraestrutura urbana. Essa articulação é essencial para o entendimento da cibersegurança como elemento estratégico do desenvolvimento urbano resiliente e sustentável.

Esse *cluster* expressa o núcleo da literatura especializada sobre ameaças cibernéticas, concentrando estudos sobre ataques, respostas, avaliação de riscos e implicações para segurança nacional. A presença de termos como *public policy* e *decision making* indica o crescente diálogo entre tecnologia e formulação de políticas públicas.

O *cluster* roxo, mais abaixo e ao centro, agrupa termos como "*privacy*", "*digitalization", "regulation", "information technology"* e *"cybercrime*". Esse conjunto reflete preocupações com a proteção de dados, os desafios regulatórios e os impactos sociais das transformações digitais. A presença simultânea de termos técnicos e normativos evidencia que o debate sobre cibersegurança é tanto tecnológico quanto jurídico e ético, aspecto crucial quando se pensa em políticas públicas urbanas baseadas em dados.

Também é neste *cluster* que emergem preocupações com a regulação e a transformação digital no âmbito empresarial, institucional e social. Esse conjunto expressa uma abordagem integradora que busca conciliar eficiência tecnológica com garantias legais e éticas, considerando as transformações induzidas pela adoção em larga escala de tecnologias digitais.

O *cluster* verde, à esquerda superior, foca em palavras como "*governance*", "*management", "technology", "risk*" e "*impact*", refletindo uma perspectiva organizacional e estratégica da cibersegurança. Esse agrupamento sugere a importância de abordagens de gestão

de risco e governança adaptativa, aplicáveis tanto à administração pública quanto à gestão de serviços urbanos mediados por tecnologia.

Este grupo enfatiza os efeitos da digitalização sobre as estruturas de gestão e políticas institucionais. Apesar de valores mais baixos de *PageRank*, os termos deste *cluster* apontam para um eixo complementar de análise: como gerir riscos e impactos da transformação digital, além da necessidade de desenvolver modelos de gestão adaptativos em ambientes altamente dinâmicos.

Alguns termos periféricos, porém relevantes, como *"policy", "critical infrastructure" e "laws and legislation"*, conectam diferentes *clusters* e funcionam como pontes conceituais entre os domínios técnico, político e normativo. A existência dessas conexões demonstra a natureza interdisciplinar e sistêmica do campo analisado, reforçando a necessidade de abordagens integradas para a formulação de políticas de cibersegurança em contextos urbanos.

Em síntese, a rede de coocorrência de palavras-chave revela uma estrutura conceitual multifacetada, onde a cibersegurança ocupa posição central e se conecta a temas como infraestrutura crítica, cidades inteligentes, proteção de dados, regulação, inteligência artificial e governança urbana. Essa configuração conceitual corrobora a premissa da tese de que a cibersegurança é um componente estruturante do desenvolvimento socioeconômico de cidades, demandando estratégias articuladas entre tecnologia, política pública e cidadania digital.

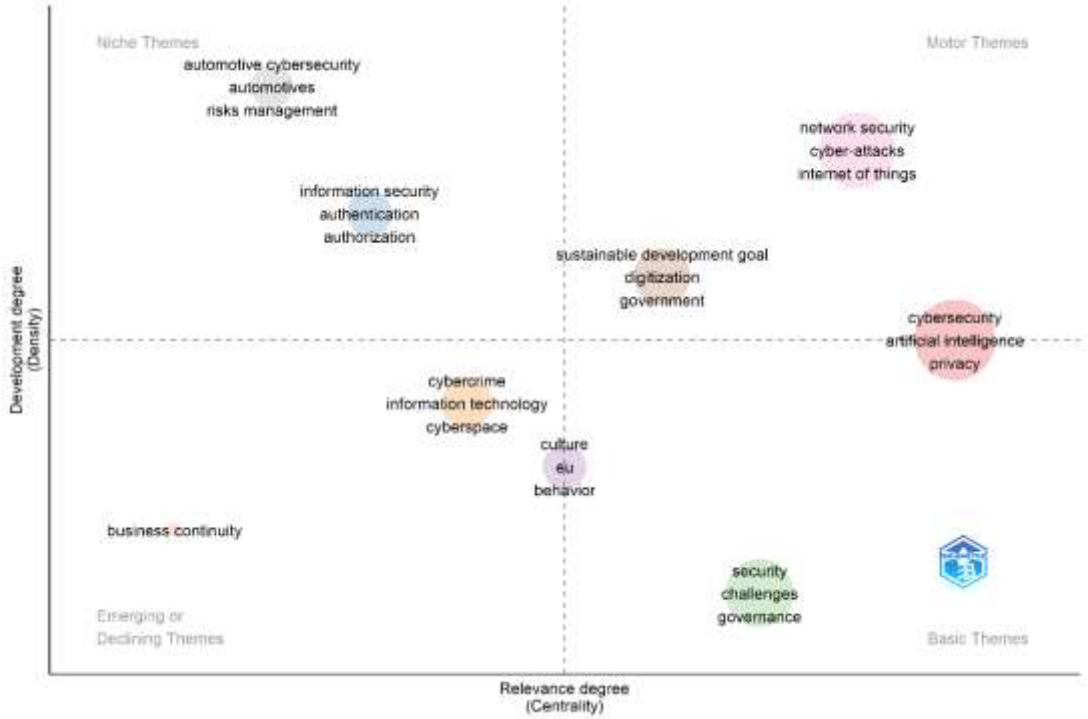
A análise da estrutura conceitual a partir da coocorrência de bigramas extraídos dos resumos dos 318 documentos permitiu a identificação de temas recorrentes, articulados conceitualmente ao redor do eixo central da cibersegurança. Para tanto, foi empregada a técnica de análise de redes semânticas com base em bigramas (N-gramas compostos por duas palavras), extraídos do campo abstract dos artigos. A visualização gerada utilizou o algoritmo de clusterização Louvain, com normalização por associação, sendo considerada a ocorrência mínima de uma conexão por termo. O resultado foi uma rede composta por 50 nós agrupados em cinco grandes comunidades temáticas, evidenciando a diversidade e a convergência das abordagens no campo investigado.

A Figura 4 apresenta o mapa temático gerado com base na coocorrência de termos que, permite compreender a organização dos temas que compõem o campo da cibersegurança no contexto do desenvolvimento socioeconômico. A análise considera dois eixos principais: o grau de desenvolvimento (densidade) e o grau de relevância (centralidade) de cada tema. A

partir dessa classificação, os tópicos são distribuídos em quatro quadrantes, oferecendo uma perspectiva estratégica sobre o posicionamento dos conceitos mais debatidos na literatura.

O mapa temático proporciona uma representação gráfica das tendências e áreas prioritárias de pesquisa relacionadas a um tema específico. Este tipo de análise classifica os temas de pesquisa em quatro quadrantes principais, baseados em seu grau de desenvolvimento (densidade) e sua relevância (centralidade), permitindo identificar os temas emergentes, nichos, básicos e motores do campo de estudo (Aria; Cuccurullo, 2017).

Figura 4 – Estrutura conceitual com base nos resumos



Fonte: Dados da pesquisa (2025), imagem gerada por meio do *software bibliometrix*.

No quadrante superior direito, correspondente aos temas motores, destacam-se expressões como *cybersecurity*, *network security*, *cyber-attacks*, *internet of things*, *privacy* e *artificial intelligence*. Esses termos representam o núcleo da produção científica atual, indicando um forte interesse da comunidade acadêmica e técnica em questões ligadas à proteção de sistemas conectados, especialmente em um contexto de digitalização e hiperconectividade. Esses temas se mostram especialmente relevantes para esta pesquisa, na medida em que configuram os pilares tecnológicos que sustentam as transformações digitais nas cidades.

Corroborando com tais resultados, estudos recentes destacam o papel da integração de tecnologias avançadas como IA e blockchain na proteção e mitigação de riscos cibernéticos em redes inteligentes, infraestrutura crítica e sistemas urbanos (Mustafa *et al.,* 2024; Yu *et al.,*

2024). A segurança associada à privacidade emerge fortemente devido à crescente preocupação com o tratamento ético e seguro dos dados, especialmente em contextos de IoT e cidades inteligentes (Xia *et al.*, 2023).

No quadrante inferior direito, encontram-se os temas básicos, como *security*, *challenges* e *governance*. Apesar de apresentarem menor densidade, esses temas possuem alta centralidade, o que sugere que funcionam como fundamentos conceituais e estruturantes do campo, mas ainda carecem de desenvolvimento mais aprofundado. A presença de *governance*, em especial, sinaliza uma oportunidade para este estudo explorar o papel das políticas de cibersegurança como instrumentos de promoção do desenvolvimento socioeconômico nas cidades.

Ramadhan *et al.* (2024), por exemplo, destacam a necessidade urgente de governança robusta em segurança cibernética, com a proposta de colaboração entre governos, organizações internacionais e atores não estatais para estabelecer uma governança estável e efetiva contra ameaças cibernéticas.

O quadrante superior esquerdo, por sua vez, reúne os temas de nicho, como *automotive cybersecurity, risk management, authentication* e *authorization*. São tópicos com alta densidade, ou seja, tecnicamente bem desenvolvidos, mas com menor conexão com o núcleo temático da área. Isso sugere especializações que podem ser valiosas para contextos específicos, como a mobilidade urbana inteligente e a segurança de infraestruturas críticas, mas que não são o foco principal deste estudo.

Os temas de nicho compreendem temas considerados específicos, altamente desenvolvidos, mas com relevância ainda limitada ao contexto geral da *cybersecurity*. Temas como segurança cibernética automotiva, gestão de riscos e segurança da informação relacionada à autenticação e autorização, representam frentes emergentes, mas ainda pouco interligadas ao corpo principal de pesquisa sobre *cybersecurity*.

Estudos como os de Armellin *et al.* (2024) e Roberts *et al.* (2023) enfatizam a necessidade de abordagens regulatórias e padronizações, particularmente em setores como o automotivo e industrial, onde a cibersegurança deve garantir a integridade operacional e proteger infraestruturas estratégicas.

No extremo oposto, no quadrante inferior esquerdo, localizam-se os temas emergentes ou em declínio, como *business continuity, cybercrime, information technology* e *cyberspace*. Esses tópicos apresentam baixo grau de desenvolvimento e centralidade, o que pode indicar tanto um estágio inicial de exploração quanto uma possível perda de interesse recente na literatura. Ainda assim, a presença de *cybercrime* e *cyberspace* aponta para

potenciais articulações futuras com políticas públicas de segurança cibernética em ambientes urbanos.

Finalmente, no centro do gráfico, encontram-se temas como *sustainable development goal*, *digitization*, *government*, *culture* e *behavior*, que ocupam uma posição intermediária entre densidade e centralidade. Esses temas são particularmente significativos para esta pesquisa, pois indicam uma interseção ainda em consolidação entre cibersegurança e desenvolvimento socioeconômico. A inclusão de termos como *government* e *sustainable development goal* aponta para uma crescente atenção da literatura à articulação entre políticas públicas, transformação digital e segurança, constituindo uma base promissora para aprofundar o estudo da cibersegurança no contexto das cidades.

Khairi e Petlach (2023) por exemplo, ao avaliarem o impacto da pandemia de Covid-19 sobre a digitalização dos países da União Europeia, destacam como a digitalização está intrinsecamente ligada à eficácia governamental e segurança nacional, promovendo um vínculo entre digitalização acelerada e segurança aprimorada através de políticas públicas eficientes

Al-Besher e Kumar (2025) também exploram o potencial da inteligência artificial para melhorar serviços governamentais eletrônicos, destacando os desafios como privacidade e proteção de dados pessoais, que devem ser abordados por modelos regulatórios específicos e tecnologias avançadas de segurança como IA e IoT.

Em termos estratégicos, o mapa confirma que os temas motores se concentram na articulação entre segurança da informação, proteção de dados e objetivos globais de desenvolvimento, sustentando a tese de que a cibersegurança não é apenas um problema técnico, mas uma questão essencial de governança urbana e desenvolvimento socioeconômico. Já os temas básicos reforçam o papel das tecnologias emergentes e das estruturas institucionais como vetores para a transformação digital das cidades, ainda em construção teórica.

A partir da análise dos agrupamentos temáticos e das redes semânticas mapeadas, observa-se uma concentração significativa de estudos orientados à normatização e operacionalização da segurança cibernética, especialmente em ambientes regulados por estruturas institucionais robustas. Embora esse enfoque tenha contribuído para consolidar a cibersegurança como objeto legítimo da agenda política e acadêmica, ele permanece fortemente ancorado em lógicas técnicas e gerenciais. Como destacam Margetts e Dorobantu (2019), a governança digital, quando estruturada apenas sob critérios de eficiência e controle, tende a negligenciar os processos de participação democrática e os impactos redistributivos das políticas tecnológicas. Nesse contexto, faz-se necessário aprofundar a análise sobre como os

núcleos temáticos identificados se alinham – ou não – com os pressupostos teóricos que orientam esta pesquisa, especialmente no que se refere à articulação entre segurança digital e desenvolvimento territorial. A seção a seguir explora essa discussão.

2.5 CONSIDERAÇÕES FINAIS

O Estudo I teve como propósito examinar os núcleos temáticos da produção científica sobre cibersegurança, identificando suas abordagens predominantes, lacunas analíticas e potencialidades conceituais. A partir da articulação entre análise bibliométrica e revisão sistemática da literatura, buscou-se construir um diagnóstico interpretativo do campo, contribuindo para a definição do arcabouço teórico e empírico da tese.

Os resultados evidenciam que a cibersegurança ainda é tratada majoritariamente sob uma perspectiva técnico-normativa, voltada ao controle de riscos, conformidade regulatória e proteção de ativos informacionais. Essa abordagem, identificada como corrente técnico-operacional, domina os principais *clusters* mapeados, com termos *como risk, framework, management* e *compliance*. Ela é instrumentalizada por marcos como a ISO/IEC 27001, o NIST *Framework* e modelos de gestão de segurança centrados na continuidade de negócios e mitigação de vulnerabilidades. Embora essa corrente seja indispensável para estabelecer padrões mínimos de proteção, sua hegemonia contribui para uma visão reducionista da cibersegurança, descolada de seus impactos sociais e políticos.

Paralelamente, a literatura apresenta uma segunda vertente que denominamos corrente institucionalista, centrada na análise de políticas públicas, marcos legais e capacidades organizacionais. Essa abordagem é representada por estudos que discutem a evolução da GDPR, a implementação da LGPD, a emergência de políticas nacionais como a PNCiber e o papel das instituições na regulação do ambiente digital. Embora mais sensível ao papel do Estado e das normas, essa linha ainda opera frequentemente em chave normativa, com foco na eficácia de modelos regulatórios e na adesão a boas práticas internacionais — nem sempre ajustadas às realidades locais. Os estudos institucionalistas também tendem a negligenciar aspectos territoriais, democráticos e de justiça informacional, limitando sua capacidade crítica.

Essa corrente é particularmente relevante para este estudo porque permite compreender a cibersegurança como uma dimensão do fortalecimento institucional e da governança pública, em especial no nível subnacional. Autores como Dunn Cavelty (2007), Nye (2010) e Müller (2019) argumentam que a cibersegurança não deve ser analisada apenas como um conjunto de medidas técnicas, mas como um arranjo político e institucional que

envolve capacidades estatais, sistemas regulatórios, cooperação federativa e cultura organizacional. Em contextos como o brasileiro, marcados por assimetrias federativas e desigualdade de capacidades institucionais entre municípios, a abordagem institucionalista permite identificar como políticas de cibersegurança são formuladas, implementadas ou negligenciadas em diferentes escalas. Além disso, ela contribui para a análise das tensões entre marcos legais nacionais, como a LGPD e o Decreto nº 11.856/2023, e a capacidade efetiva de atores locais em cumprir, adaptar ou mesmo compreender essas normas.

A terceira corrente teórica, ainda minoritária, mas emergente, é a sociotécnica. Essa abordagem parte da premissa de que a cibersegurança é inseparável das estruturas sociais, políticas e econômicas em que se insere. Aqui, destacam-se autores como Nissenbaum (2005), que propõe a "privacidade contextual" como um critério normativo situado, e Zuboff (2019), cuja crítica ao capitalismo de vigilância evidencia a assimetria de poder informacional entre plataformas digitais e cidadãos. Essa linha de análise permite entender a cibersegurança não apenas como defesa contra riscos, mas como um campo de disputa por valores públicos, direitos coletivos e soberania informacional — sobretudo em contextos periféricos.

A partir da análise dos dados, constata-se que há uma concentração geográfica significativa na produção científica sobre o tema, com hegemonia de países do Norte Global e baixa representação de autores e instituições do Sul Global. Essa assimetria epistemológica revela uma importante lacuna: o campo carece de abordagens que problematizem a cibersegurança a partir de contextos regionais, subnacionais e desigualdades estruturais. Os estudos sobre cidades pequenas, municípios com baixa capacidade institucional e territórios economicamente dependentes — como os analisados nos próximos capítulos da tese — são praticamente inexistentes na literatura dominante.

Além disso, a análise dos *clusters* temáticos e das palavras-chave mostra que o conceito de "governança" tem sido apropriado de maneira ambígua. Por vezes, ele aparece associado à governança corporativa e à regulação algorítmica, sem conexão com processos democráticos, participativos ou descentralizados. Essa limitação compromete a compreensão da cibersegurança como um bem público e a articulação de políticas digitais com estratégias de desenvolvimento sustentável. Por isso, este estudo reafirma a importância de recuperar dimensões políticas, éticas e territoriais no debate sobre segurança digital.

A revisão sistemática complementou essa leitura ao identificar a escassez de estudos empíricos que relacionem a segurança digital à formulação de políticas públicas em escala local. A ausência de abordagens multiescalares e a pouca atenção às capacidades institucionais de municípios, especialmente em contextos de transição econômica e tecnológica,

reforçam a relevância do recorte adotado nesta tese. Os poucos estudos que avançam nessa direção permanecem dispersos e ainda carecem de sistematização teórica.

Dessa forma, o Estudo I cumpre uma função estratégica no projeto de pesquisa. Ao mapear os eixos estruturantes da literatura e identificar os limites das abordagens predominantes, oferece uma base sólida para a formulação do arcabouço analítico da tese. Ele fundamenta a escolha por uma perspectiva integrada, que reconhece a cibersegurança como fenômeno multidimensional, articulando tecnologia, instituições e sociedade.

Esse diagnóstico inicial também justifica a adoção de uma abordagem empírica situada, nos Estudos II e III, voltada à análise da segurança cibernética em municípios da região carbonífera de Santa Catarina. O próximo capítulo investigará o estágio atual das práticas de proteção digital em administrações locais, identificando capacidades institucionais, padrões normativos e eventuais assimetrias. A partir dessa leitura do território, será possível discutir estratégias e propor mecanismos assecuratórios que articulem segurança digital e desenvolvimento regional de forma inclusiva e sustentável.

Por fim, os resultados deste capítulo reforçam que pensar a cibersegurança a partir de um olhar crítico e territorialmente sensível é não apenas necessário, mas urgente. Em um contexto marcado pela expansão de infraestruturas digitais, pelo aprofundamento da vigilância informacional e pela fragilidade institucional de governos locais, a segurança digital deve ser compreendida como uma política pública estruturante. Apenas assim será possível assegurar não só proteção técnica, mas também justiça informacional, soberania digital e equidade territorial.

A partir deste diagnóstico teórico, o Estudo II se propõe a aprofundar os constructos conceituais que emergiram na análise, enquanto o Estudo III buscará examinar empiricamente como tais conceitos se manifestam e são operacionalizados nas práticas de gestão pública em nível local, especialmente na região carbonífera de Santa Catarina.

3 ESTUDO II – CONSTRUCTOS EMERGENTES EM CIBERSEGURANÇA E DESENVOLVIMENTO: UMA ANÁLISE CONCEITUAL COM BASE EM CLUSTERS TEMÁTICOS

3.1 INTRODUÇÃO

O avanço das tecnologias digitais e a crescente interconectividade das sociedades têm impulsionado a formulação de políticas públicas mais robustas voltadas à cibersegurança. No contexto urbano, onde a digitalização dos serviços e das infraestruturas é cada vez mais intensa, a governança cibernética emerge como elemento central para assegurar um desenvolvimento socioeconômico equilibrado, seguro e sustentável. A complexidade dessa temática exige abordagens que extrapolem os aspectos técnicos, aprofundando-se nos domínios institucionais, normativos e organizacionais que moldam as respostas públicas e privadas aos riscos cibernéticos. Este segundo estudo se apoia nos achados do Estudo I e prepara o terreno conceitual para as análises empíricas que serão desenvolvidas no Estudo III, promovendo, assim, um encadeamento progressivo da reflexão teórica à aplicação prática.

O Estudo I desta tese mapeou os principais temas e tendências da literatura científica sobre cibersegurança, por meio de uma revisão bibliométrica e sistemática. Entre os resultados, destacaram-se agrupamentos temáticos que evidenciam a emergência de um debate institucionalista sobre a governança da cibersegurança. Esses agrupamentos revelam uma preocupação crescente com questões normativas, regulatórias e organizacionais, particularmente no que se refere ao papel do Estado, das instituições multilaterais e dos marcos legais na promoção de um ambiente digital seguro e favorável ao desenvolvimento.

A análise de parte dos documentos mais representativos reforça a presença de abordagens críticas e estruturais, com foco em temas como soberania digital, justiça informacional, políticas públicas cibernéticas e regulação tecnológica. Tais tópicos remetem à vertente institucionalista da ciência política e da sociologia organizacional, que enfatiza a análise dos arranjos formais e informais que condicionam a atuação dos diversos atores no espaço cibernético. Este Estudo II, portanto, constitui um aprofundamento conceitual e analítico desse recorte.

Com base nesse direcionamento, a questão de pesquisa que orienta o Estudo II é: de que forma os constructos normativos, institucionais e organizacionais identificados na literatura estruturam uma compreensão ampliada da cibersegurança urbana, capaz de integrar

governança digital, soberania informacional e desenvolvimento socioeconômico em contextos locais?

Ao adotar a perspectiva institucionalista, o presente estudo busca compreender como normas, instituições e estruturas de governança moldam os caminhos possíveis para o desenvolvimento digital seguro. A literatura indica que, em contextos urbanos, a cibersegurança deve ser entendida não apenas como um conjunto de soluções técnicas, mas como parte de um ecossistema regido por leis, políticas públicas, práticas organizacionais e valores socioculturais que definem o que é aceitável, desejável ou proibido no ciberespaço (Akdemir; Law, 2021; Kostopoulos *et al.,* 2020).

A centralidade de uma abordagem normativa se torna evidente diante dos desafios enfrentados por cidades que buscam conciliar inovação tecnológica e inclusão social. A cibersegurança institucionalizada atua como um pilar de confiança digital, sendo condição fundamental para a implementação eficaz de políticas públicas digitais, iniciativas de governo eletrônico e serviços urbanos inteligentes. Nesse contexto, a regulação e a governança são entendidas como elementos habilitadores do desenvolvimento (Oliveira *et al*., 2020; Taddeo; Floridi, 2018).

Além disso, o crescimento das ameaças cibernéticas impacta de maneira desigual diferentes grupos sociais e territórios, exigindo que as respostas institucionais sejam sensíveis às assimetrias de poder e às vulnerabilidades específicas de comunidades urbanas. Isso implica reconhecer as interdependências entre segurança digital, justiça social, proteção de dados e direitos humanos. A literatura recente destaca a importância de políticas de cibersegurança que sejam democráticas, inclusivas e orientadas por valores éticos (Martin, 2021; Shackelford *et al.,* 2020).

Este estudo se ancora na análise qualitativa dos documentos mais representativos dos agrupamentos temáticos identificados, adotando como base metodológica a análise de conteúdo e o mapeamento conceitual. Ao explorar os constructos centrais emergentes, busca-se identificar os eixos estruturantes de uma abordagem institucionalista da cibersegurança urbana voltada ao desenvolvimento. Entre os constructos analisados, destacam-se: governança digital, soberania informacional, normatividade cibernética e infraestrutura crítica urbana.

A fundamentação teórica deste estudo está ancorada nas evidências conceituais e estruturais identificadas no Estudo I, com ênfase nos agrupamentos temáticos e nos documentos representativos selecionados para análise qualitativa. Esses elementos oferecem um arcabouço sobre os principais constructos relacionados à institucionalização da cibersegurança, especialmente no que se refere às dimensões normativas, organizacionais e políticas do

fenômeno. Para aprofundar esse referencial, foram mobilizados artigos científicos que dialogam diretamente com os tópicos emergentes desses agrupamentos, permitindo a construção de uma base teórica sólida, diversificada e integrada.

Este esforço analítico visa não apenas descrever os constructos emergentes, mas também interpretá-los à luz dos Objetivos de Desenvolvimento Sustentável (ODS), da literatura sobre cidades inteligentes e das exigências contemporâneas de resiliência urbana. Assim, a cibersegurança é abordada como uma dimensão transversal da governança urbana, articulando segurança, equidade, inovação e sustentabilidade em uma perspectiva sistêmica e interdependente (Calzada, 2020; Dunn Cavelty, 2019).

Nesse sentido, este Estudo II assume uma função estratégica ao aprofundar os aspectos qualitativos e normativos, contribuindo para a consolidação de um constructo teórico sobre a cibersegurança em escala urbana. Ao fazê-lo, busca também preencher lacunas identificadas na literatura, ao propor uma abordagem integrativa da cibersegurança urbana.

Dessa forma, o estudo amplia a investigação iniciada no Estudo I, concentrando-se nos aspectos normativos e institucionais que emergem como elementos estruturantes da governança em cibersegurança. Ao examinar qualitativamente os principais constructos conceituais identificados, busca-se aprofundar a compreensão teórica sobre como essas categorias contribuem para o fortalecimento de políticas públicas digitais alinhadas aos objetivos de desenvolvimento urbano.

Trata-se, portanto, de um estudo de natureza exploratória e analítica, que se dedica ao mapeamento e à interpretação crítica de conceitos centrais à institucionalização da cibersegurança em contextos urbanos. Ao iluminar os caminhos normativos e organizacionais destacados na literatura, pretende-se oferecer subsídios conceituais aos estudos empíricos subsequentes, consolidando uma base teórica que articule cibersegurança, governança e desenvolvimento socioeconômico em um mesmo campo de análise.

3.2 RECORTE TEÓRICO SOBRE O TEMA

A cibersegurança, em sua evolução histórica e conceitual, passou a integrar as agendas institucionais e políticas de modo mais incisivo nas últimas décadas, consolidando-se como um campo que transcende os aspectos técnicos e se insere nas discussões sobre governança, cidadania e desenvolvimento. O advento de tecnologias digitais, particularmente em ambientes urbanos, impulsionou novas formas de articulação entre sistemas informacionais,

instituições públicas e estruturas normativas, exigindo abordagens analíticas que integrem os elementos técnicos à sua dimensão institucional e normativa (Khatoun; Zeadally, 2017).

A fundamentação teórica deste Estudo II apoia-se nos resultados obtidos no Estudo I, especialmente nos agrupamentos temáticos que evidenciaram o protagonismo de uma perspectiva institucionalista na literatura acerca da cibersegurança. Esses agrupamentos indicaram a centralidade de constructos voltados à governança digital, soberania informacional, regulação de dados e segurança cibernética em níveis subnacionais. A partir dessa base, este estudo adota a vertente institucionalista como eixo analítico, aprofundando seus fundamentos a partir da literatura científica contemporânea que trata da normatização da cibersegurança e da ação institucional nos territórios urbanos.

No campo da governança digital, autores como Calzada (2020) defendem que a institucionalização da cibersegurança em ambientes urbanos deve considerar os contextos territoriais, os arranjos de cidadania digital e as formas de engajamento cívico, de modo a evitar que a infraestrutura tecnológica reforce desigualdades existentes. A partir da noção de "cidadania algorítmica", o autor argumenta que a governança das cidades inteligentes requer não apenas segurança digital, mas também mecanismos de transparência, participação e controle democrático sobre os fluxos de dados.

Nesse mesmo sentido, Dunn Cavelty (2019) sustenta que a cibersegurança deve ser compreendida como um processo político e social, e não meramente técnico. A autora critica a tendência de securitização excessiva dos discursos institucionais sobre riscos digitais, apontando para a necessidade de construção de mecanismos de governança baseados em normas claras, princípios éticos e deliberação pública. Em sua análise, a segurança cibernética eficaz depende da existência de instituições resilientes e da inclusão de múltiplos atores na definição das prioridades de proteção digital.

Ainda dentro dessa perspectiva, Shackelford, Russell e Kuehn (2020) destacam o papel da cooperação institucional multissetorial na consolidação de uma governança cibernética sustentável. Para os autores, os desafios da segurança digital em ambientes urbanos exigem estratégias coordenadas entre governo, setor privado, sociedade civil e academia, de modo a construir um ecossistema normativo capaz de responder de forma democrática e eficaz às ameaças emergentes. O conceito de "ciberpaz", defendido pelos autores, articula segurança, direitos humanos e desenvolvimento local, sendo especialmente relevante para contextos municipais.

A dimensão institucional da cibersegurança também é explorada por Formosa, Wilson e Richards (2021), que propõem um arcabouço principialista para orientar decisões em

ambientes digitais complexos. O modelo apresentado pelos autores baseia-se em cinco princípios: beneficência, não maleficência, autonomia, justiça e explicabilidade, sendo adaptado de *frameworks* bioéticos e aplicável à governança de riscos cibernéticos em políticas públicas. Tal abordagem oferece um suporte conceitual relevante para a formulação de políticas de cibersegurança que busquem equilíbrio entre proteção e direitos individuais.

Por sua vez, Akdemir e Law (2021) analisam como a governança da cibersegurança em cidades inteligentes está cada vez mais associada à regulação de fluxos de dados, vigilância algorítmica e tensões entre privacidade e segurança pública. Os autores apontam que os arcabouços legais e institucionais precisam ser constantemente atualizados para lidar com os novos riscos impostos por tecnologias emergentes, como inteligência artificial e internet das coisas, exigindo estruturas estatais mais adaptáveis e responsivas.

A relação entre segurança digital e políticas públicas é também discutida por Oliveira, Figueiredo e Nascimento (2020), que examinam a capacidade institucional dos municípios brasileiros em implementar ações de cibersegurança. Os autores identificam desafios estruturais como a ausência de legislação local, a baixa especialização técnica e a fragmentação normativa entre diferentes esferas de governo, indicando que a maturidade institucional é um fator determinante para a eficácia das políticas cibernéticas em nível local.

A proteção de dados pessoais, enquanto dimensão central da cibersegurança, é tratada por Martin (2021) a partir de uma perspectiva de justiça informacional. O autor argumenta que a cibersegurança deve ser orientada por princípios de equidade, transparência e inclusão, sendo incompatível com modelos de governança baseados em opacidade e controle assimétrico da informação. Essa abordagem reforça a necessidade de políticas públicas comprometidas com a proteção de direitos fundamentais no ambiente digital.

Taddeo e Floridi (2018) defendem que tecnologias digitais, incluindo soluções de segurança cibernética, devem ser desenhadas e implementadas com base em valores éticos e orientações públicas. Para os autores, a inteligência artificial e os sistemas autônomos, quando aplicados à cibersegurança, devem respeitar princípios de proporcionalidade, responsabilidade e supervisão humana, de modo a garantir que a inovação tecnológica não comprometa os direitos dos cidadãos e a legitimidade das instituições democráticas.

A institucionalização da cibersegurança, tal como apresentada nas obras de Akdemir e Law (2021), não se limita à formalização de normas, mas envolve a internalização de práticas, valores e rotinas organizacionais que configuram a cultura institucional da segurança digital. Os autores enfatizam que a governança eficaz depende de mecanismos de responsabilização, monitoramento e participação ativa de múltiplos stakeholders,

especialmente em ambientes urbanos onde a interdependência entre sistemas críticos e infraestrutura digital é mais evidente.

Khatoun e Zeadally (2017) contribuem ao discutir a integração entre segurança e privacidade no contexto de cidades inteligentes. Em sua análise, a segurança cibernética deve ser planejada desde o design dos sistemas urbanos, incorporando requisitos como anonimização de dados, autenticação robusta, controle de acesso e criptografia. Essa visão reforça a ideia de que a cibersegurança não é uma camada adicional, mas parte integrante da arquitetura institucional e tecnológica das cidades contemporâneas.

A partir dos estudos de Dunn Cavelty (2019) e Calzada (2020), percebe-se a articulação entre os elementos técnicos, normativos e organizacionais da cibersegurança por meio de um modelo tridimensional. Esse modelo conceitual permite visualizar que uma política pública de cibersegurança eficaz requer o equilíbrio entre os três domínios — técnico (Khatoun; Zeadally, 2017), institucional (Akdemir; Law, 2021; Dunn Cavelty, 2019; Oliveira *et al.*, 2020; Shackelford *et al.*, 2020) e normativo (Formosa *et al.*, 2021; Martin, 2021; Taddeo; Floridi, 2018) —, sendo que a ausência de qualquer um deles compromete a resiliência do sistema como um todo. Isso é particularmente relevante em contextos municipais, onde é comum a concentração de esforços apenas na dimensão técnica, em detrimento de marcos regulatórios e capacidades institucionais.

Com base nesse arcabouço, torna-se possível interpretar os resultados do Estudo I de maneira mais estruturada. Os agrupamentos temáticos identificados apontam para a emergência de constructos conceituais que articulam justamente essas três dimensões, com destaque para categorias como soberania digital, proteção de dados, estrutura normativa e governança compartilhada. Ao aprofundar esses constructos, o Estudo II propõe contribuir para uma abordagem conceitual integrativa, voltada à compreensão da cibersegurança enquanto vetor de desenvolvimento urbano.

A conexão entre cibersegurança e desenvolvimento sustentável é reforçada por Shackelford, Russell e Kuehn (2020), que argumentam que a governança digital deve ser considerada um dos pilares dos Objetivos de Desenvolvimento Sustentável (ODS), em especial aqueles voltados à inovação, à infraestrutura resiliente e à governança eficaz. Os autores advogam por políticas de cibersegurança que respeitem os direitos humanos, promovam inclusão e estejam alinhadas a estratégias mais amplas de desenvolvimento territorial.

Essa perspectiva ganha relevância em contextos marcados por disparidades institucionais, como o brasileiro. Oliveira, Figueiredo e Nascimento (2020) demonstram que, mesmo diante de diretrizes federais consolidadas, a implementação de políticas de

cibersegurança nos municípios depende de fatores como capital humano qualificado, recursos orçamentários e cultura organizacional orientada à proteção digital. O estudo dos autores revela que a ausência de legislações locais e a baixa articulação interinstitucional são entraves significativos para a consolidação de uma política cibernética eficaz nos entes subnacionais.

Nesse contexto, torna-se necessário repensar os mecanismos de transferência de capacidades e os modelos de cooperação intergovernamental. A literatura internacional aponta para iniciativas exitosas de construção colaborativa de estratégias de cibersegurança envolvendo municípios, universidades, empresas de tecnologia e organizações da sociedade civil (Akdemir; Law, 2021; Shackelford *et al.*, 2020). Esses modelos pressupõem a existência de um marco normativo claro, instrumentos de coordenação horizontal e instâncias de deliberação pública que assegurem legitimidade às políticas implementadas.

Além disso, o avanço das tecnologias de inteligência artificial (IA) impõe novos desafios à governança da cibersegurança. Taddeo e Floridi (2018) alertam para os riscos éticos associados ao uso indiscriminado de algoritmos em decisões públicas automatizadas, especialmente em áreas sensíveis como segurança, vigilância e justiça criminal. Para os autores, a governança da IA deve estar ancorada em princípios como explicabilidade, auditabilidade e supervisão humana contínua, de modo a evitar a opacidade algorítmica e a erosão de direitos fundamentais.

O quadro abaixo sintetiza os principais princípios éticos aplicáveis à cibersegurança, conforme discutidos por Formosa, Wilson e Richards (2021).

Quadro 5 - Princípios éticos para a governança da cibersegurança

Princípio	**Descrição**
Beneficência	As ações devem promover benefícios aos usuários e à sociedade.
Não maleficência	Evitar danos desnecessários aos usuários e ao sistema social.
Autonomia	Garantir o direito dos indivíduos ao controle sobre seus próprios dados.
Justiça	Tratar todos os usuários com equidade, sem discriminação.
Explicabilidade	Tornar compreensíveis os processos e decisões de segurança digital.

Fonte: Adaptado de Formosa, Wilson e Richards (2021).

Esses princípios reforçam a necessidade de uma abordagem ética e responsável da cibersegurança, especialmente em políticas públicas urbanas. Sua aplicação exige não apenas dispositivos legais, mas também capacidade institucional para traduzir os princípios em normas operacionais e práticas administrativas coerentes.

Ao observar a integração da cibersegurança no cotidiano urbano, percebe-se que sua presença vai além da esfera técnica, exigindo que os marcos institucionais e normativos acompanhem a complexidade das interações sociais mediadas por tecnologias digitais. A

governança da cibersegurança, portanto, deve ser compreendida como parte do arranjo institucional que configura as capacidades de ação do Estado frente aos desafios emergentes da sociedade em rede. Essa perspectiva é particularmente importante quando se considera a multiplicidade de atores envolvidos na gestão da segurança digital, incluindo agências públicas, fornecedores de tecnologia, cidadãos e organismos internacionais.

Martin (2021) reforça essa leitura ao argumentar que a justiça informacional deve ocupar posição central na formulação de políticas de cibersegurança. Para o autor, não se trata apenas de proteger infraestruturas críticas ou dados pessoais, mas de assegurar que os direitos informacionais sejam distribuídos de forma equitativa, com atenção às vulnerabilidades estruturais que afetam determinadas populações e territórios. Isso implica uma abordagem sensível ao contexto social, capaz de identificar e mitigar desigualdades no acesso, uso e proteção de informações digitais.

Nesse sentido, a institucionalização da cibersegurança também precisa considerar os processos de aprendizagem institucional e difusão de normas. Oliveira, Figueiredo e Nascimento (2020) destacam que a adoção de políticas públicas nessa área está fortemente condicionada pela capacidade dos governos locais de interpretar e internalizar marcos legais como a LGPD. Tal internalização depende da existência de mecanismos de governança local, como comitês de proteção de dados, planos de segurança da informação e processos contínuos de formação de servidores públicos.

Adicionalmente, a literatura aponta para a necessidade de adaptação normativa contínua frente ao dinamismo das ameaças cibernéticas. Como demonstram Akdemir e Law (2021), os ciclos de inovação tecnológica nas cidades inteligentes frequentemente superam os tempos institucionais de resposta, criando zonas de indeterminação regulatória onde a proteção dos direitos e a eficiência operacional entram em tensão. Essa lacuna entre inovação e regulação reforça o papel do Estado como mediador das transformações tecnológicas, devendo agir tanto como promotor da inovação quanto como garantidor de direitos fundamentais.

Essa mediação institucional demanda uma abordagem integrada, em que segurança, desenvolvimento e cidadania estejam articulados. Calzada (2020) propõe que as políticas públicas urbanas incorporem uma concepção ampliada de cidadania digital, que vá além do acesso à tecnologia e inclua a proteção contra abusos informacionais, a possibilidade de participação em decisões sobre dados e o direito à desconexão. Tais elementos são cruciais para que a digitalização urbana seja compatível com os valores democráticos e os objetivos de equidade social.

Outro ponto relevante diz respeito à fragmentação normativa frequentemente observada entre diferentes níveis de governo. Shackelford, Russell e Kuehn (2020) argumentam que a ausência de coordenação entre políticas federais, estaduais e municipais cria inconsistências que comprometem a eficácia das medidas de segurança cibernética. Em resposta, os autores defendem a institucionalização de redes colaborativas de governança, que permitam o compartilhamento de boas práticas, a definição conjunta de prioridades e a construção de uma arquitetura normativa coerente.

A construção dessa arquitetura normativa exige, ainda, atenção à legitimidade das políticas implementadas. Formosa, Wilson e Richards (2021) sugerem que a aceitação social das práticas de cibersegurança está condicionada à percepção de justiça, transparência e responsabilidade institucional. Quando os cidadãos não compreendem os critérios utilizados para decisões automatizadas ou políticas de vigilância, há risco de desconfiança generalizada e resistência às iniciativas públicas. Por isso, os autores propõem que a explicabilidade e a prestação de contas sejam pilares normativos da governança digital.

Essa exigência de transparência e participação ressoa com a crítica de Dunn Cavelty (2019) ao modelo de securitização tecnocrática que domina parte das políticas de cibersegurança. Para a autora, a ênfase exclusiva em ameaças e soluções técnicas tende a excluir o debate público e a concentrar o poder decisório em instâncias opacas. Uma abordagem institucionalista crítica, por outro lado, exige que os processos de decisão sejam abertos, negociados e orientados por critérios normativos claros, em consonância com os princípios democráticos.

No contexto brasileiro, essas discussões ganham especial relevância diante da diversidade de capacidades institucionais e da desigualdade na distribuição de recursos entre os entes federativos. Estudos como o de Oliveira, Figueiredo e Nascimento (2020) revelam que muitos municípios operam sem estrutura mínima de segurança da informação, sendo frequentemente dependentes de soluções externas e contratos com fornecedores que não consideram critérios de soberania e controle local. Essa dependência estrutural fragiliza a autonomia institucional e dificulta a criação de estratégias sustentáveis de cibersegurança.

Como resposta a esses desafios, autores como Taddeo e Floridi (2018) advogam por um modelo de governança digital baseado em responsabilidade distribuída, onde diferentes atores compartilham deveres normativos e operacionais conforme suas competências. Essa proposta está alinhada à noção de governança colaborativa, que busca romper com o modelo hierárquico de comando e controle e construir redes de coprodução de políticas públicas mais sensíveis às especificidades locais.

Ao consolidar essas contribuições teóricas, torna-se evidente que a cibersegurança, quando pensada como política pública urbana, deve ser entendida como um processo institucional em permanente construção. Isso envolve tanto a adaptação de normas quanto o fortalecimento de capacidades estatais e o engajamento da sociedade civil. A literatura analisada neste Estudo II fornece uma base sólida para interpretar os constructos identificados no Estudo I, reforçando a importância de uma abordagem integrativa e crítica que articule segurança, equidade e desenvolvimento no espaço urbano digital.

Em síntese, os conceitos de governança digital, soberania informacional, justiça informacional e infraestrutura crítica constituem os pilares analíticos deste estudo. Esses eixos servirão como lentes teóricas para a interpretação dos dados e articulação dos resultados, com vistas à formulação de diretrizes integradas para políticas públicas de cibersegurança urbana.

3.3 PROCEDIMENTOS METODOLÓGICOS

Com base na análise temática empreendida no Estudo I, este segundo estudo propõe-se a aprofundar os constructos conceituais, orientando-se por uma leitura crítica das inter-relações normativas e institucionais que moldam a governança cibernética no contexto urbano.

Este Estudo II adotou uma abordagem qualitativa e exploratória, com o objetivo de aprofundar a análise dos constructos conceituais identificados no Estudo I a partir da revisão bibliométrica e sistemática. Enquanto o primeiro estudo mapeou o panorama temático da produção científica sobre cibersegurança e desenvolvimento, esta etapa buscou compreender em profundidade os sentidos, tensões e inter-relações entre os conceitos emergentes, com ênfase na análise crítica das dimensões normativas e institucionais que estruturam a governança cibernética local.

A seleção dos documentos analisados partiu dos *clusters* temáticos previamente identificados no primeiro estudo, com ênfase nos agrupamentos que abordavam a governança da cibersegurança, a regulação normativa e as estruturas institucionais vinculadas ao desenvolvimento urbano. Foram selecionados os artigos mais representativos desses agrupamentos, considerando sua centralidade, frequência de citação e alinhamento com os eixos analíticos deste estudo. A amostra final compreendeu um conjunto de publicações internacionais e nacionais, totalizando doze documentos principais.

A estratégia metodológica adotada está alinhada ao objetivo central da tese de compreender a cibersegurança como vetor de desenvolvimento urbano. Para tanto, utilizou-se

a análise de conteúdo de abordagem temática (Bardin, 2011), combinada ao mapeamento conceitual guiado pelas categorias teóricas previamente sistematizadas no Estudo I. Essa estratégia permitiu a identificação de núcleos de sentido e categorias emergentes, articulando elementos conceituais que revelam os tensionamentos presentes na institucionalização da cibersegurança urbana.

O processo de análise foi conduzido manualmente, em ciclos iterativos de leitura e categorização, nos quais os documentos foram submetidos a codificação aberta, com posterior agregação em categorias temáticas. Foram utilizados quadros-síntese para sistematizar os constructos identificados, além de diagramas de relação para representar visualmente os vínculos conceituais entre os elementos. Este procedimento permitiu consolidar um modelo analítico próprio, alinhado à proposta teórica da tese.

O rigor metodológico foi assegurado por meio da triangulação entre a literatura científica, os dados da revisão sistemática do Estudo I e as inferências interpretativas realizadas ao longo da análise. Buscou-se garantir coerência interna entre os referenciais teóricos mobilizados, os objetivos da pesquisa e os achados da análise qualitativa. A opção por uma metodologia interpretativa foi orientada pela natureza exploratória da investigação, que visa compreender como os discursos sobre cibersegurança se articulam em torno de constructos políticos, normativos e institucionais.

A delimitação da unidade de análise neste estudo foi o discurso científico contido nos textos selecionados, entendido como produto e reflexo das práticas institucionais e dos marcos normativos em disputa no campo da cibersegurança. Tal escolha metodológica viabilizou a conexão entre arcabouços teóricos e evidências empíricas, promovendo uma análise crítica que transcende a mera descrição documental, contribuindo para a construção de um referencial analítico aplicável às políticas públicas de segurança digital em contextos urbanos.

Com isso, a seção de análise dos resultados, que se apresenta a seguir, tem por objetivo sistematizar os principais constructos emergentes dos documentos selecionados, organizando-os em eixos temáticos que expressam diferentes dimensões da institucionalização da cibersegurança urbana voltada ao desenvolvimento socioeconômico.

3.4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Os resultados obtidos foram interpretados à luz dos referenciais teóricos discutidos, com o objetivo de avaliar a aderência dos discursos científicos aos modelos institucionais de

governança cibernética. Essa análise buscou não apenas identificar categorias emergentes, mas também confrontar as evidências com os desafios enfrentados por municípios brasileiros em termos de capacidade institucional e normatividade digital.

3.4.1 Núcleos temáticos e oportunidades de análise

Esta subseção propõe uma leitura crítica de dois agrupamentos temáticos identificados na etapa bibliométrica do Estudo I, que se mostram diretamente conectados ao campo da segurança cibernética e da governança digital. Ancorados em termos como *cybersecurity, risk, network* e *framework*, esses núcleos demonstram forte adesão a um enfoque institucionalista, no qual se destacam a construção de normas, estruturas regulatórias e protocolos de cooperação entre agentes estatais e privados. Embora esse referencial represente um avanço em relação ao tecnicismo puro, como indicam Gomes (2000) e Neves (2010), ele ainda se distancia de uma abordagem territorializada da cibersegurança, pouco explorando os efeitos sociais, políticos e espaciais das estratégias de proteção digital.

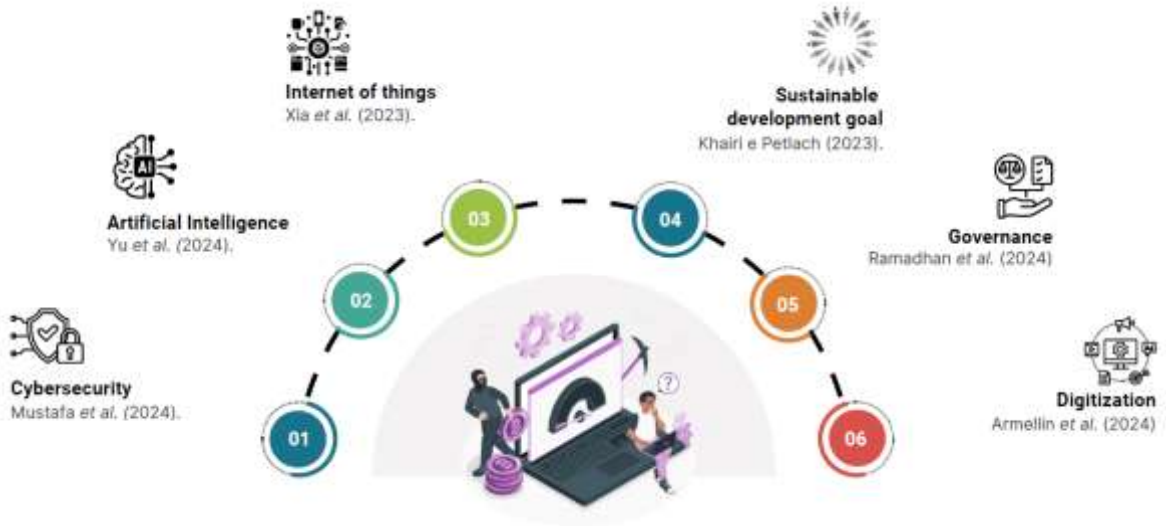
Dois dos agrupamentos temáticos resultantes da análise bibliométrica se conectam diretamente aos objetivos desta pesquisa, ao concentrarem estudos estruturados sobre *cybersecurity, risk, network* e *framework*. Tais agrupamentos refletem o predomínio de produções alinhadas com a tradição institucionalista da cibersegurança, voltada à normatização da proteção digital e à construção de arranjos formais de governança. Embora essa abordagem represente um avanço em relação à perspectiva estritamente técnica, ao incorporar dimensões organizacionais, jurídicas e de articulação entre níveis de governo, ela ainda demonstra limitações ao negligenciar a mediação socioterritorial dos riscos e das políticas de segurança nos contextos locais.

O enfoque institucionalista, como demonstrado por Mishra *et al.* (2022), enfatiza a criação de estratégias nacionais, marcos legais e estruturas administrativas que permitam a coordenação de ações entre diferentes atores estatais e privados. A literatura analisada nesse agrupamento apresenta forte incidência de estudos preocupados com a capacidade de conformidade regulatória, a implantação de políticas públicas setoriais e a avaliação de riscos associados à infraestrutura crítica. Essa perspectiva se revela útil na identificação de lacunas institucionais e na proposição de modelos de resposta coordenada, mas tende a reproduzir, em parte, a racionalidade técnica do enfoque tecno-operacional ao assumir que o fortalecimento institucional se resume à elaboração de normas, indicadores e procedimentos formais.

Como apontam Chander *et al.* (2021), a existência de arcabouços regulatórios, como o GDPR europeu ou a LGPD brasileira, não garante, por si só, a efetividade da proteção digital. A fragmentação institucional, sobretudo em contextos subnacionais, gera lacunas de implementação que aprofundam o descompasso entre norma e prática. A tese de Mishra *et al.* (2022) reforça essa constatação ao demonstrar empiricamente que os atributos de uma política de cibersegurança eficaz variam conforme a capacidade regulatória e a maturidade institucional de cada país ou região, sendo inadequado o transplante de modelos normativos padronizados para realidades onde o Estado atua com limitações estruturais.

Nesse sentido, os agrupamentos analisados revelam que, embora haja uma incorporação relevante de categorias institucionais — como *compliance*, políticas públicas, governança e cooperação intergovernamental —, a literatura ainda carece de abordagens que articulem essas dimensões à estrutura social e territorial onde tais políticas se realizam. A própria Estratégia Nacional de Segurança Cibernética (Brasil, 2020), embora formulada sob inspiração institucionalista, apresenta forte orientação técnica, com baixa inserção dos aspectos socioculturais e políticos no processo decisório. A consequência é a formulação de políticas cuja efetividade depende da existência de capacidades organizacionais e culturais que não estão igualmente distribuídas entre os entes federativos.

Figura 5 – Núcleos temáticos



Fonte: Elaborado pelo autor (2025).

Ao criticar esse descolamento entre aparato normativo e realidade institucional, Schubert e Barrett (2024) reforçam que a governança de dados deve ser compreendida como um processo decisório estruturado por dinâmicas de poder, e não apenas como um sistema

regulado por normas. Sua efetividade depende da presença de mecanismos de responsabilização, da transparência das decisões e da capacidade dos atores locais em exercer controle sobre os fluxos e usos dos dados. No entanto, como indicam os achados desta pesquisa, poucos estudos abordam diretamente essas questões quando analisam os efeitos institucionais da cibersegurança no plano municipal ou regional.

A limitação mais evidente da perspectiva institucionalista, tal como operacionalizada nos estudos dos agrupamentos analisados, é a sua tendência a interpretar a segurança digital como uma função organizacional a ser aprimorada por meio de boas práticas, regulação e cooperação. Essa abordagem, embora mais abrangente do que o enfoque tecno-operacional, ainda opera a partir de um modelo racionalizador de políticas públicas, que subestima os conflitos normativos, os interesses econômicos em disputa e a desigual distribuição das capacidades institucionais. A fragmentação da governança e a assimetria de acesso à proteção digital, sobretudo em territórios periféricos, seguem como pontos pouco explorados nesse corpo teórico.

A crítica à insuficiência do enfoque tecno-operacional já foi destacada por Zuboff (2019), ao mostrar como a estrutura técnica dos sistemas digitais foi desenhada para consolidar assimetrias de informação, vigilância e controle. Esse alerta é fundamental para compreender que a segurança cibernética não se limita à eficácia dos mecanismos de defesa, mas está intrinsecamente relacionada à justiça informacional e à autonomia dos sujeitos e das instituições. O risco de se manter uma racionalidade puramente funcionalista está na naturalização de práticas de vigilância e centralização decisória, o que compromete o próprio ideal de governança democrática no campo digital.

O debate sobre soberania digital, discutido por Tura e Ojanen (2022), reforça a necessidade de contextualização das políticas de segurança, uma vez que o controle sobre dados e infraestrutura tecnológica está cada vez mais concentrado em grandes corporações transnacionais. Nessa lógica, a adesão a *frameworks* institucionais globalmente validados pode representar mais uma forma de alinhamento normativo do que um exercício real de autonomia regulatória. Os efeitos dessa dinâmica são particularmente evidentes em países e regiões com baixa capacidade institucional, onde o discurso sobre segurança se desvincula das práticas locais e das prioridades coletivas.

A crítica à universalização das abordagens institucionais torna-se ainda mais evidente quando se observa a escassez de estudos empíricos voltados à implementação de políticas de cibersegurança em escalas locais, como municípios e consórcios regionais. A literatura analisada nos agrupamentos concentra-se majoritariamente em experiências nacionais

ou supranacionais, com ênfase em países do eixo Europa–EUA, onde estruturas institucionais consolidadas, sistemas jurídicos robustos e ampla capacidade técnica permitem a formulação e aplicação de políticas de segurança mais sofisticadas. No entanto, conforme destacado por Mishra *et al.* (2022), esse padrão dificulta a compreensão dos desafios enfrentados por governos locais em contextos marcados por assimetrias técnicas, baixa institucionalidade e dependência de tecnologias exógenas.

Essa limitação é particularmente relevante para o caso brasileiro, em que a maioria dos municípios ainda opera com estruturas administrativas enxutas, ausência de equipes especializadas em segurança da informação e restrições orçamentárias significativas. Apesar da existência de marcos regulatórios como a LGPD e a E-Ciber, os municípios encontram dificuldades concretas para implementar políticas de proteção de dados, realizar auditorias, desenvolver planos de resposta a incidentes e estabelecer protocolos mínimos de cibersegurança. Essa situação agrava o que Chander *et al.* (2021) denominam de "*privacy enforcement gap*", isto é, o descompasso entre o texto normativo e sua aplicação efetiva, fenômeno intensificado nas periferias institucionais do sistema federativo.

A baixa incidência de estudos voltados às realidades subnacionais também implica a invisibilização de experiências relevantes de inovação e adaptação local. Como apontam Schubert e Barrett (2024), a governança de dados deve ser analisada como um processo que se concretiza nas decisões cotidianas de atores públicos e privados, em múltiplas escalas, e não apenas em diretrizes macroestruturais. Ignorar as dinâmicas locais de apropriação e resistência pode resultar em políticas que, embora formalmente consistentes, se revelam desfuncionais em contextos onde os instrumentos técnicos e os recursos institucionais necessários simplesmente não estão presentes.

Por outro lado, as regiões periféricas também enfrentam maior exposição a práticas de vigilância comercial e dependência de plataformas tecnológicas que operam sob lógicas algorítmicas opacas, conforme advertido por Zuboff (2019). A ausência de políticas locais de governança da informação, somada à limitada autonomia sobre os fluxos de dados, reforça a vulnerabilidade digital de populações já excluídas por outras dimensões do desenvolvimento. Nesse sentido, a cibersegurança, ao ser pensada exclusivamente sob a ótica da proteção normativa, desconsidera os efeitos estruturais que sua ausência ou aplicação seletiva produz sobre o território.

Os próprios princípios que orientam o conceito de soberania digital, como formulados por Tura e Ojanen (2022), tornam-se inviáveis em contextos onde o poder decisório sobre os sistemas digitais escapa ao controle dos governos locais. A concentração de decisões

técnicas em esferas superiores ou em empresas privadas, associada à carência de capacitação e investimento público, limita a possibilidade de construção de políticas de segurança enraizadas nas necessidades dos territórios. A ausência de indicadores sensíveis às realidades locais e de métricas que capturem os efeitos sociais da cibersegurança reforça essa lacuna analítica.

A lacuna de pesquisas voltadas às escalas locais também compromete a produção de conhecimento capaz de subsidiar políticas públicas mais equitativas. A centralidade das cidades e regiões como agentes de inovação e transformação digital tem sido amplamente reconhecida por organismos internacionais como a OCDE (2020), mas ainda carece de atenção sistemática na literatura de cibersegurança. Em vez disso, observa-se uma concentração de esforços em casos paradigmáticos — como Estônia, Alemanha ou Canadá — que, embora importantes, não refletem a diversidade de desafios enfrentados por municípios em países em desenvolvimento.

Embora o termo *governance* surja com frequência na literatura científica sobre cibersegurança, sua aplicação majoritária se restringe a contextos organizacionais voltados à gestão de riscos, conformidade normativa e eficiência operacional. Na maioria dos estudos analisados, a governança aparece atrelada aos conceitos de *management* e *compliance*, sem conexão explícita com estratégias mais amplas de desenvolvimento regional ou com modelos de políticas públicas que incorporem participação social e diversidade territorial (Mishra *et al*., 2022; Chander *et al*., 2021). A ênfase recai, sobretudo, na capacidade institucional de implementar estruturas formais de controle e auditoria, com foco na segurança de infraestruturas críticas e na conformidade com marcos legais como o GDPR ou a LGPD.

Essa limitação conceitual indica uma compreensão restrita do papel da governança digital, desassociada das dinâmicas socioterritoriais e das potencialidades transformadoras da segurança cibernética em escala local. Como indicam Schubert e Barrett (2024), a governança de dados envolve disputas sobre quem define os critérios de uso, quem exerce controle sobre os fluxos informacionais e com que grau de responsabilização esses processos são mediados. No entanto, essas dimensões políticas e estruturais da governança raramente são abordadas nas produções centradas no campo da segurança cibernética, o que contribui para a naturalização de práticas tecnocráticas e pouco transparentes.

Nesse cenário, reforça-se a hipótese central desta tese: o potencial da cibersegurança como elemento indutor do desenvolvimento urbano e regional ainda é subteorizado. A produção científica tende a privilegiar a segurança como um fim em si mesmo, descolada das agendas de inclusão digital, justiça informacional e fortalecimento institucional de territórios periféricos. A ausência de articulação entre governança da informação e

estratégias de desenvolvimento compromete a capacidade de utilizar a cibersegurança como instrumento de promoção de cidades mais seguras, resilientes e equitativas, sobretudo em regiões fora do eixo geopolítico dominante da Europa e América do Norte.

3.4.2 Dimensões Teóricas e Alinhamento com o Instrumento de Diagnóstico

A continuidade da análise dos núcleos temáticos identificados no Estudo I exige uma articulação direta com as dimensões teóricas mobilizadas, de modo a consolidar um quadro interpretativo sobre a institucionalização da cibersegurança no nível subnacional. Essa subseção tem por objetivo explicitar como os referenciais analíticos foram operacionalizados em domínios específicos do diagnóstico institucional, e de que forma dialogam com a literatura contemporânea sobre cibersegurança e desenvolvimento urbano.

A primeira dimensão — capacidade institucional e organizacional — está ancorada nas formulações clássicas de Hall e Taylor (1996), que associam a efetividade das políticas públicas à existência de estruturas estáveis, previsíveis e capacitadas. No campo da cibersegurança, essa perspectiva é reforçada por Oliveira, Figueiredo e Nascimento (2020), ao apontarem que a ausência de estruturas mínimas nos municípios brasileiros compromete a viabilidade de estratégias sustentáveis no setor.

A literatura enfatiza que a fragilidade institucional local não pode ser corrigida apenas por normas externas ou por transferência de tecnologia. Como observam Dunn Cavelty (2019) e Cravo (2023), é necessário reconhecer os limites estruturais e o papel central dos agentes públicos na construção cotidiana da política, ainda que em contextos de escassez e informalidade institucional.

Nesse sentido, o instrumento de diagnóstico não apenas quantifica a presença de estruturas formais, mas busca captar o grau de consolidação institucional, empregando uma escala de maturidade que reflete o processo evolutivo das práticas administrativas. A inspiração metodológica para isso vem do *Cybersecurity Capability Maturity Model* (C2M2) e do NIST *Framework*, adaptados para a realidade municipal brasileira.

Esse eixo dialoga com os argumentos de Hall e Taylor (1996) sobre a importância das instituições na conformação das ações dos atores públicos, destacando a relevância da profissionalização e da estabilidade institucional para o fortalecimento da governança digital.

A segunda dimensão — governança digital e normatização local — remete a debates sobre a construção de marcos legais coerentes com os desafios do ambiente digital. Autores como Akdemir e Law (2021) e Formosa, Wilson e Richards (2021) alertam para a

necessidade de normas que sejam, simultaneamente, tecnicamente eficazes e democraticamente legitimadas.

No plano municipal, como mostram estudos analisados no Estudo I, a normatização tende a ser incipiente, com forte dependência de diretrizes federais e escassa capacidade interpretativa por parte dos gestores locais. Por isso, o questionário busca aferir não apenas a existência de normas, mas sua adequação, aplicabilidade e origem, distinguindo entre iniciativas autônomas e aquelas meramente reativas.

Como apontam Cravo (2023) e Akdemir e Law (2021), a governança digital pressupõe um arcabouço normativo claro, adaptado às especificidades do ambiente cibernético, sendo essencial à construção de ambientes urbanos seguros e transparentes.

A terceira dimensão — infraestrutura tecnológica e práticas de segurança — está fortemente conectada aos conceitos de captura operacional discutidos por Stigler (1971), Posner (1974) e retomados por Torres (2012). Essa noção refere-se à naturalização de soluções técnicas padronizadas que, em vez de resolver os problemas locais, acabam por reforçar assimetrias e dependência de fornecedores externos.

Essa crítica aparece com força na literatura sociotécnica, como em Zuboff (2019) e Nissenbaum (2005), que denunciam a mercantilização das soluções digitais e a invisibilização dos interesses públicos na formulação de sistemas de segurança. O diagnóstico local, nesse campo, busca revelar não apenas a existência de rotinas técnicas, mas o grau de autonomia e de adaptação local dessas práticas.

Taddeo e Floridi (2018) argumentam que a maturidade tecnológica das instituições públicas está diretamente associada à sua capacidade de enfrentar riscos sistêmicos, o que demanda rotinas operacionais consistentes, padrões mínimos de segurança e gestão proativa da infraestrutura crítica.

A quarta dimensão — cooperação intermunicipal e suporte regional — parte da premissa de que a governança da cibersegurança não pode ser pensada exclusivamente em termos locais. Como defendem Shackelford, Russell e Kuehn (2020), a construção de um ecossistema de cibersegurança exige articulação multiescalar, cooperação horizontal e redes de suporte técnico entre municípios.

Esse ponto é especialmente relevante para regiões como a AMREC, onde há forte tradição de consórcios e atuação intermunicipal. O questionário, portanto, investiga não só a existência de parcerias formais, mas também a percepção dos gestores sobre a utilidade e efetividade desses arranjos.

A literatura institucionalista contemporânea, como a de Calzada (2020), enfatiza a governança colaborativa e a construção de redes territoriais como estratégias de compensação para déficits técnicos e organizacionais em escalas locais.

A quinta dimensão — barreiras institucionais e percepções dos agentes públicos — incorpora elementos da teoria da implementação desviada, conforme formulada por Lipsky (2010), e das críticas contemporâneas à fragmentação normativa, como exposto por Cravo (2023). Aqui, busca-se entender a política "em ação", ou seja, como os servidores interpretam, adaptam ou ignoram as diretrizes formais no cotidiano da gestão pública.

Essa abordagem permite revelar as zonas cinzentas entre norma e prática, entre prescrição e improviso, fornecendo uma base empírica para compreender os limites reais da governança digital em contextos periféricos. A coleta de percepções é, portanto, estratégica para captar não apenas gargalos técnicos, mas as disputas, resistências e criatividades institucionais envolvidas na implementação da cibersegurança.

As resistências institucionais descritas por Lipsky (2010) e os obstáculos normativos destacados por Martin (2021) revelam que, para além das capacidades formais, a forma como os agentes públicos percebem e priorizam a cibersegurança influencia diretamente a efetividade das políticas digitais.

Ao alinhar essas dimensões ao quadro teórico da tese, constata-se uma forte coerência entre os referenciais utilizados e as práticas investigadas. A literatura analisada fornece categorias analíticas para compreender a cibersegurança como um processo institucionalizado, tensionado por assimetrias federativas, disputas normativas e condições estruturais desiguais.

O instrumento de diagnóstico, nesse sentido, atua como mediador entre a teoria e a realidade empírica, permitindo avaliar a aplicabilidade dos referenciais teóricos em contextos concretos. Ele revela como conceitos como capacidade estatal, governança multiescalar e justiça informacional se materializam — ou não — na prática institucional cotidiana dos municípios.

Além disso, o cruzamento entre as respostas dos questionários, os documentos institucionais e os marcos legais vigentes permite mapear áreas de convergência e de dissonância, indicando tanto boas práticas quanto lacunas regulatórias. Essa triangulação de dados reforça a perspectiva crítica da tese, que busca ir além da conformidade normativa e explorar os limites e possibilidades da cibersegurança como vetor de desenvolvimento.

A dimensão territorial, ausente em grande parte da literatura dominante, é recolocada no centro do debate por meio da análise da capacidade dos municípios em interpretar

e implementar políticas de segurança digital segundo suas especificidades. Como apontam os estudos mais recentes, como os de Al-Besher e Kumar (2025), o localismo é fundamental para uma governança responsiva e adaptada à realidade socioeconômica.

A articulação entre os núcleos temáticos analisados e os referenciais teóricos adotados reforça a consistência metodológica do Estudo II e demonstra o potencial analítico da abordagem escolhida para compreender os desafios da governança cibernética em contextos locais. Ao integrar marcos normativos, práticas organizacionais e percepções institucionais, a tese oferece uma leitura crítica e abrangente da cibersegurança no nível subnacional.

Assim, os eixos discutidos evidenciam que a institucionalização da cibersegurança ultrapassa os limites da regulação formal, exigindo articulações multiescalares, engajamento intersetorial e compromisso com a equidade digital. Esses achados não apenas reforçam os desafios enfrentados pelas gestões locais, como também apontam caminhos para políticas mais eficazes e adaptadas às realidades urbanas contemporâneas.

3.5 CONSIDERAÇÕES FINAIS

As análises empreendidas ao longo do Estudo II permitiram consolidar uma interpretação aprofundada dos constructos conceituais mais relevantes relacionados à cibersegurança em contextos urbanos, com especial atenção às dimensões normativas e institucionais. A partir da base teórica estruturada no Estudo I, foi possível avançar para uma leitura crítica dos elementos que configuram os principais eixos da governança digital no nível subnacional.

Este estudo demonstrou que a literatura científica recente reconhece a cibersegurança como uma dimensão fundamental do desenvolvimento socioeconômico, articulando temas como soberania informacional, justiça digital, proteção de dados e resiliência institucional. Contudo, também evidenciou-se uma lacuna no tocante à aplicação desses referenciais no âmbito local, onde as capacidades institucionais são limitadas e os marcos regulatórios ainda carecem de consolidação.

A análise qualitativa realizada destacou que, apesar da diversidade de abordagens teóricas, há uma convergência em torno da importância de estruturas organizacionais estáveis, de uma normatização adequada ao contexto digital e de práticas colaborativas que transcendem os limites administrativos locais. Esses elementos formam o núcleo conceitual sobre o qual se pode sustentar políticas públicas de cibersegurança com potencial transformador.

Foram identificados cinco eixos principais a partir da literatura analisada: (i) capacidade institucional e organizacional; (ii) governança digital e normatização local; (iii) infraestrutura tecnológica e práticas de segurança; (iv) cooperação intermunicipal e suporte regional; e (v) barreiras institucionais e percepções dos agentes públicos. Esses eixos servem como categorias analíticas para interpretar a presença e a ausência de políticas estruturadas nos territórios.

O Estudo II também reafirma o papel da institucionalização como vetor estratégico da segurança digital. Conforme a vertente institucionalista mobilizada, o desenvolvimento da cibersegurança depende não apenas de tecnologia, mas de marcos legais eficazes, capacidade de coordenação e valores compartilhados entre os agentes públicos. A literatura sustenta que a eficácia das políticas está vinculada à sua capacidade de se enraizar nas rotinas organizacionais e de se articular com múltiplos níveis de governo.

As análises indicam que políticas públicas de cibersegurança efetivas exigem não apenas investimentos técnicos, mas um ecossistema normativo e organizacional. Esse ecossistema deve incluir regulação clara, órgãos de coordenação, mecanismos de monitoramento e estratégias de formação continuada. Em especial, a capacidade de promover ações intermunicipais e construir redes colaborativas aparece como um diferencial estratégico para territórios com baixa densidade estatal.

A literatura também denuncia a existência de zonas cinzentas entre o que é normatizado e o que é efetivamente implementado. A distância entre a prescrição legal e a prática cotidiana das organizações públicas revela limitações que vão além dos recursos financeiros ou tecnológicos, alcançando a cultura organizacional, a burocracia e a priorização política do tema.

Este estudo reforça a necessidade de abordagens sistêmicas, que tratem a cibersegurança como um campo transversal às políticas urbanas. A articulação com temas como mobilidade, educação, saúde e governança digital exige que os referenciais analíticos avancem para além dos limites setoriais, integrando segurança digital como parte das estratégias de desenvolvimento local sustentável.

A metodologia qualitativa adotada permitiu apreender nuances e complexidades que não seriam acessíveis por abordagens quantitativas ou apenas bibliométricas. A análise de conteúdo e o mapeamento conceitual, combinados à seleção crítica de documentos, favoreceram a construção de uma base teórica consolidada e crítica.

Os resultados do Estudo II fornecem elementos para pensar a cibersegurança não apenas como uma política defensiva, mas como uma agenda propositiva de transformação

institucional. Governar a cibersegurança é, em última instância, governar o futuro digital das cidades, suas infraestruturas e sua capacidade de garantir direitos em ambientes cada vez mais mediados por tecnologia.

Por meio dos constructos sistematizados, foi possível compreender que o desenvolvimento da cibersegurança em contextos urbanos envolve disputas por autonomia, padrões de regulação, controle da infraestrutura e a própria concepção de privacidade e justiça informacional. Assim, o estudo contribui para ampliar o campo analítico da segurança digital em direção a uma agenda de justiça territorial e equidade digital.

Além disso, a análise crítica das dimensões institucionais e normativas proporciona um olhar mais profundo sobre as condições reais de implementação das políticas públicas, permitindo avançar da mera prescrição legal para a análise das práticas, interpretações e resistências que moldam o cotidiano institucional.

Nesse sentido, o Estudo II cumpre sua função estratégica dentro da tese: consolidar um marco conceitual que aprofunda os achados do Estudo I e oferece ferramentas teóricas para leituras empíricas mais qualificadas sobre a cibersegurança como política pública. Embora não antecipe resultados de aplicações práticas, oferece um referencial robusto para análises futuras.

Conclui-se, portanto, que os constructos analisados neste estudo devem ser compreendidos como componentes centrais de uma política de cibersegurança voltada para o fortalecimento da capacidade estatal, a proteção dos direitos digitais e o estímulo ao desenvolvimento urbano seguro, inclusivo e resiliente.

Os eixos e constructos sistematizados aqui servirão de base analítica para o Estudo III, que testará empiricamente a aderência e aplicabilidade dessas categorias nos contextos institucionais dos municípios que compõem a AMREC. Tal transição permitirá verificar em campo as potencialidades e os limites das abordagens aqui discutidas.

4 ESTUDO III – SEGURANÇA CIBERNÉTICA EM INSTITUIÇÕES PÚBLICAS LOCAIS: ESTUDO DE CASO NA ASSOCIAÇÃO DOS MUNICÍPIOS DA REGIÃO CARBONÍFERA - AMREC

4.1 INTRODUÇÃO

Nos últimos anos, o crescimento tecnológico tem trazido evoluções significativas, e a segurança cibernética acompanha essa tendência. Inicialmente, as medidas de proteção focavam em vírus e *malwares* básicos, porém, os ataques cibernéticos se tornaram mais complexos, exigindo soluções avançadas, como *firewalls* e antivírus sofisticados. Com o avanço da tecnologia, surgiram novas ameaças, demandando adaptações na segurança cibernética para proteger dados em ambientes complexos e em desenvolvimento.

O presente estudo dá continuidade ao percurso analítico iniciado nos estudos anteriores, com especial atenção à materialização dos constructos identificados nos níveis local e subnacional. Busca-se, assim, verificar como os marcos normativos, as estruturas institucionais e os princípios de governança digital mapeados conceitualmente são interpretados e implementados nos territórios analisados.

Segundo Sen (2011), o desenvolvimento tem como objetivo principal a construção do bem-estar coletivo, sendo as liberdades substantivas elementos essenciais desse processo. É necessário que o Estado promova programas e ações para alcançar esses objetivos e concretizar o bem-estar coletivo e as liberdades substantivas.

Para promover o desenvolvimento econômico e social, de forma sustentável, os doze municípios que compreendem a Associação dos Municípios da Região Carbonífera – AMREC, uniram-se na intenção de promover o desenvolvimento da região de forma assistida e sustentável. O Plano de Desenvolvimento Socioeconômico da AMREC é fruto de um processo colaborativo e democrático envolvendo moradores, representantes da sociedade civil, setor produtivo e governo municipal.

Para a elaboração das metas de trabalho, o plano foi elaborado com objetivos, que devem ser alcançados dentro do período proposto para sua execução, que são: identificar as desigualdades socioeconômicas dos municípios-região; construir uma Visão de Futuro compartilhada e um projeto de desenvolvimento sustentável de longo prazo para os municípios-região; identificar as possibilidades para ampliar a atratividade dos municípios-região no que diz respeito aos investimentos fomentados, dessa forma, o seu desenvolvimento econômico e social; reconhecer as potencialidades dos municípios-região, identificando os *clusters*

existentes e prospectar novas redes para o ecossistema municipal; identificar os eixos e vetores estratégicos para o desenvolvimento sustentável dos municípios-região; identificar um portfólio de projetos estruturantes para serem utilizados no desenvolvimento dos municípios-região; propor formas de convergência e integração entre instituições privadas e públicas a fim de gerar benefícios econômicos e sociais para os municípios-região; sugerir a alocação dos recursos públicos nos municípios-região para aumentar a capacidade de captação de recursos externos.

Dentre as etapas de execução, o plano contou com a contribuição das mais diversas entidades que compreendem os municípios, para que pudesse atrair diferentes perspectivas e anseios que amparassem a proposição de ações para o desenvolvimento da região. A segurança foi então citada em diversas etapas de coleta de dados entre os municípios, algumas contribuições trouxeram: a segurança do futuro precisa estar aliada às ferramentas tecnológicas como o uso de drones, por exemplo; proporcionar o desenvolvimento com mais segurança; e, ampliar a segurança econômica.

Logo, com as contribuições propostas, as metas foram estabelecidas visando atender as demandas que surgiam, de acordo com cada eixo em específico. No conjunto de ações, voltadas à segurança, proposições como: constituir um observatório de segurança pública na região carbonífera para orientar a população no âmbito coletivo e, analisar a possibilidade de uso intensivo das tecnologias para ampliar a segurança pública, trouxeram a discussão de como a segurança pública pode e deve ser otimizada, visando a relação com a Tecnologia da Informação e Comunicação (TIC) em benefícios dos municípios, para assim estimular e garantir o desenvolvimento social e econômico sustentável.

Assim, visando o contexto que os municípios estão inseridos e a necessidade de identificar como a TIC aliada a políticas públicas podem fomentar e garantir o desenvolvimento dos municípios, o estudo visa responder a seguinte questão de pesquisa: como se encontram os estágios de segurança cibernética das instituições de segurança pública dos municípios que fazem parte da Associação dos Municípios da Região Carbonífera?

A importância da segurança cibernética na era digital crescente justifica o estudo. Com a dependência cada vez maior da tecnologia, é fundamental proteger as informações e dados pessoais contra ameaças virtuais. O objetivo é compreender melhor os riscos e vulnerabilidades presentes no mundo virtual, bem como as melhores práticas de segurança cibernética para preveni-los ou mitigá-los. O estudo pode fornecer insights sobre práticas já adotadas em diferentes instituições para garantir a segurança cibernética, bem como os desafios éticos e legais associados ao uso dessas soluções nas políticas públicas.

4.2 CONTEXTO BRASILEIRO DA CIBERSEGURANÇA: RECORTE SOBRE OS INSTRUMENTOS REGULATÓRIOS

A crescente digitalização dos serviços públicos, das interações sociais e da atividade econômica no Brasil tem impulsionado a relevância estratégica da cibersegurança como campo normativo, técnico e institucional. Nos últimos vinte anos, o país presenciou um avanço gradual, porém ainda fragmentado, na construção de um arcabouço regulatório voltado à proteção do espaço cibernético e à promoção de práticas seguras de governança digital. Esse movimento, embora estimulado inicialmente por reações pontuais a incidentes de segurança e pressões internacionais, tem se estruturado, sobretudo a partir da última década, em políticas nacionais e instrumentos legais com pretensão sistêmica.

A presente seção tem como objetivo analisar o desenvolvimento normativo da cibersegurança no Brasil, enfatizando seus principais marcos legais e estratégias públicas. Além de mapear essa trajetória, a seção discute os desafios e lacunas regulatórias que persistem, sobretudo no que se refere à capacidade de coordenação federativa e à maturidade institucional nos níveis subnacionais. O foco analítico recai sobre a inter-relação entre os dispositivos legais e estratégias governamentais, destacando suas implicações para a formulação de políticas locais e regionais de cibersegurança.

4.2.1 Política e Estratégia Nacional de Cibersegurança no Brasil

A emergência da cibersegurança como eixo estruturante das políticas públicas no Brasil deve ser compreendida no contexto das profundas transformações provocadas pela digitalização dos serviços, a ampliação do uso da internet nas relações sociais e econômicas e a crescente interdependência entre os sistemas tecnológicos e o funcionamento do Estado. Esse cenário tornou o Brasil um dos países mais afetados por incidentes cibernéticos na América Latina, impulsionando o debate sobre a formulação de uma política nacional robusta e coordenada de segurança cibernética (IDB; OEA, 2020).

A construção da política nacional de cibersegurança no Brasil foi historicamente marcada por reações dispersas a problemas emergentes. Até a década de 2010, o país não contava com uma estratégia coordenada para lidar com ameaças cibernéticas, sendo as ações mais voltadas à segurança da informação em órgãos públicos e às demandas pontuais por tipificação penal de condutas ilícitas na internet. O desenvolvimento normativo sobre cibersegurança, nesse período, teve um caráter reativo, surgindo como resposta a eventos de

alta repercussão, como no caso da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que tipificou penalmente crimes informáticos após o vazamento de dados de celebridades. A promulgação dessa norma ilustra um primeiro esforço legislativo para enfrentar as ameaças digitais, ainda que de forma fragmentada e desconectada de um projeto estratégico mais amplo (Belli *et al.*, 2023; Cravo, 2023).

Em 2014, o país aprovou a Lei nº 12.965, o Marco Civil da Internet, que introduziu um novo paradigma ao estabelecer os direitos e deveres no uso da internet no Brasil, trazendo princípios como neutralidade de rede, privacidade e proteção de dados como eixos centrais da regulação digital. Embora o foco do Marco Civil fosse mais amplo que a cibersegurança em sentido estrito, ele estabeleceu bases fundamentais para a posterior formulação de políticas de proteção da informação e infraestrutura crítica, articulando aspectos de governança e segurança. A consolidação da cibersegurança como política de Estado, no entanto, apenas se formalizou com o Decreto nº 9.637/2018, que instituiu a Política Nacional de Segurança da Informação (PNSI). Essa política ampliou o escopo de atuação do governo federal ao reconhecer a cibersegurança como dimensão estratégica da segurança nacional, ao lado da defesa cibernética e da proteção de dados sensíveis. O decreto também delineou diretrizes para a criação de estratégias modulares, culminando na elaboração da Estratégia Nacional de Segurança Cibernética (E-Ciber).

Publicada por meio do Decreto nº 10.222/2020, a E-Ciber consolidou o primeiro plano estratégico de cibersegurança do Brasil com abrangência nacional. Estruturada em dez objetivos estratégicos, a estratégia propôs eixos de ação voltados ao fortalecimento da governança, proteção das infraestruturas críticas, desenvolvimento da cultura de segurança, capacitação de pessoal e promoção da cooperação internacional. Como observam Azambuja e Neto (2020), a E-Ciber introduziu mecanismos de cooperação multissetorial e destacou a importância da articulação federativa – um dos principais desafios da implementação da estratégia. A E-Ciber dialoga diretamente com o *Cybersecurity Capacity Maturity Model* (CMM) desenvolvido pela Universidade de Oxford, sendo inclusive referenciada na Revisão de Capacidade de Cibersegurança no Brasil, conduzida pela OEA e pelo Centro de Oxford (OEA; Oxford, 2020). A análise dessa revisão indica que o Brasil apresentou avanços significativos em dimensões como “estratégia nacional” e “capacidade institucional de resposta”, mas manteve fragilidades relevantes nas áreas de educação cibernética, engajamento da sociedade civil e, sobretudo, na articulação entre os níveis de governo.

Paralelamente à E-Ciber, a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) entrou em vigor e se tornou um pilar normativo complementar, ao estabelecer

obrigações para tratamento de dados pessoais e incidentes de segurança da informação. A LGPD ampliou o papel regulador do Estado ao instituir a Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar, orientar e aplicar sanções em casos de descumprimento. A conexão entre cibersegurança e proteção de dados é particularmente destacada por autores como Ribeiro (2023), que argumenta que o tratamento seguro da informação é uma condição para o exercício da soberania digital.

A ausência de uma instância central de regulação da cibersegurança foi uma das lacunas mais criticadas tanto por organismos internacionais quanto por pesquisadores nacionais (Cravo, 2023; PNCiber, 2023b). Essa crítica motivou a elaboração da proposta da Política Nacional de Cibersegurança (PNCiber), discutida publicamente em 2023. A proposta visa unificar e racionalizar o arcabouço regulatório, criando uma arquitetura institucional ancorada em três elementos fundamentais: a Agência Nacional de Cibersegurança (ANCiber), o Comitê Nacional de Cibersegurança (CNCiber) e o Gabinete de Gerenciamento de Cibercrises (GGCiber). A estrutura inspira-se no modelo europeu da NIS2, que promove a atuação de um ente regulador com funções técnicas, normativas e fiscalizatórias centralizadas (PNCiber, 2023a).

O texto do anteprojeto da PNCiber foi debatido amplamente em audiência pública com participação de representantes do Senado Federal, ANPD, FIESP, Polícia Federal, FGV e demais atores relevantes (PNCiber, 2023c). A proposta de agência reguladora também reflete uma adaptação institucional ao que Cravo (2023) denomina de “regulação distribuída com centralidade estratégica”, ou seja, um modelo que preserva a atuação setorializada, mas que institui um centro unificado de normatização, coordenação e fiscalização. Nesse sentido, o Brasil busca superar a fragmentação institucional que marca a atuação dos múltiplos CSIRTs existentes no país, promovendo mecanismos de resposta coordenada a incidentes e políticas públicas baseadas em evidências.

Em 2023, com o Decreto nº 11.856, a PNCiber foi oficializada como política permanente de Estado, consolidando a trajetória iniciada com a E-Ciber e ampliando o esforço de institucionalização da governança cibernética no Brasil. Embora ainda fortemente concentrada na esfera federal, a política sinaliza um avanço importante na tentativa de construir um sistema nacional de segurança cibernética integrado. Outros marcos normativos, como as Resoluções do Banco Central (nº 4.893/2021) e da ANATEL (nº 740/2020), também se somam a esse ecossistema regulatório, impondo obrigações específicas para instituições financeiras e empresas de telecomunicações no que tange à gestão de riscos, notificação de incidentes e nomeação de responsáveis técnicos.

Esse arcabouço se apoia, ainda, em normas técnicas internacionais adaptadas ao contexto brasileiro, como a ABNT NBR ISO/IEC 27001, voltada à gestão da segurança da informação; a ISO/IEC 27014, que trata da governança; e a mais recente ISO/IEC 27032:2023, que orienta práticas seguras para a internet. Conforme destaca a ANBIMA (2021), essas normas funcionam como referenciais de maturidade e estruturação de políticas internas, sendo amplamente adotadas tanto no setor público quanto no setor privado.

A trajetória normativa da cibersegurança no Brasil, portanto, revela um movimento de transição institucional que parte de normas reativas e fragmentadas em direção a um modelo de governança mais coordenado, integrado e tecnicamente orientado. A consolidação da PNCiber e da ANCiber poderá representar não apenas um avanço regulatório, mas também uma inflexão na capacidade estatal de proteger o espaço cibernético como infraestrutura vital para o desenvolvimento soberano, a continuidade de serviços públicos essenciais e a proteção dos direitos fundamentais no ambiente digital.

4.2.2 Normas Setoriais, Referenciais Técnicos e Desafios da Maturidade Institucional

A consolidação do campo da cibersegurança no Brasil ultrapassa a construção de políticas nacionais de caráter geral. Nos últimos anos, a regulação tem se expandido para além da esfera federal executiva, com o surgimento de normativas específicas em setores estratégicos da economia, bem como a adoção crescente de referenciais técnicos internacionais como guias para a estruturação de programas e práticas de segurança digital em instituições públicas e privadas.

Entre os setores regulados, destaca-se o sistema financeiro, onde a preocupação com a resiliência cibernética tem impulsionado a edição de normas de elevado rigor. A Resolução nº 4.893/2021, do Banco Central do Brasil, por exemplo, obriga instituições financeiras a estabelecerem um plano de cibersegurança, com definição clara de papéis, realização de testes periódicos e notificação obrigatória de incidentes relevantes. Essa normativa é complementada pela Instrução Normativa BCB nº 85/2021, que detalha os procedimentos operacionais e os prazos para o cumprimento das exigências. A motivação para tais diretrizes decorre da crescente interdependência digital dos sistemas bancários e do histórico de tentativas de ataques a grandes instituições financeiras.

No setor de telecomunicações, a Resolução nº 740/2020 da ANATEL define critérios mínimos de segurança da informação para as prestadoras de serviços, com foco em infraestrutura crítica e continuidade operacional. Essas obrigações estão alinhadas à percepção,

também presente na Estratégia Nacional de Cibersegurança (E-Ciber), de que as redes de comunicação são vetores prioritários de defesa no espaço cibernético. A atuação das agências reguladoras evidencia a tendência de especialização normativa, na qual riscos e especificidades setoriais passam a demandar regulação própria, muitas vezes inspirada em parâmetros internacionais.

Além das normas jurídicas, o ecossistema de cibersegurança brasileiro tem incorporado progressivamente padrões técnicos reconhecidos internacionalmente, como os estabelecidos pelas normas ISO/IEC. A ABNT NBR ISO/IEC 27001, em vigor desde 2006 no Brasil, estabelece requisitos para sistemas de gestão da segurança da informação, sendo amplamente utilizada por instituições públicas e privadas como referência para auditorias e certificações. Já a ISO/IEC 27014 orienta práticas de governança da segurança da informação, enquanto a ISO/IEC 27032:2023, em sua versão mais recente, trata da segurança na internet, com ênfase em proteção contra *malwares*, vulnerabilidades de redes e privacidade online.

Esses padrões, embora voluntários, têm influenciado diretamente os manuais e guias setoriais produzidos por entidades como a ANBIMA, que em 2021 publicou a terceira edição do seu Guia de Cibersegurança. Esse documento orienta instituições do mercado financeiro a desenvolverem programas estruturados de proteção, com base nos pilares de avaliação de riscos, governança, resposta a incidentes e capacitação contínua. A convergência entre padrões técnicos internacionais e guias locais reforça o papel da normatização privada como um eixo complementar ao aparato jurídico estatal.

Paralelamente à proliferação de normas e padrões, autores como Azambuja e Neto (2020) têm destacado um desafio estrutural latente: a baixa maturidade institucional em cibersegurança no âmbito da administração pública. Estudos empíricos com base em modelos de maturidade demonstram que muitos órgãos federais ainda operam sem processos formalizados de gestão de riscos, resposta a incidentes ou capacitação de pessoal. Essa constatação é reforçada por pesquisas internacionais, como o estudo de Ribeiro (2023), que identificou também na Europa significativa disparidade de maturidade entre grandes centros urbanos e regiões periféricas.

O Brasil tem avançado em algumas iniciativas para endereçar esse problema, como a adoção de modelos de avaliação da maturidade cibernética, a exemplo daquele proposto por Azambuja e Neto, que define domínios como governança, controle de acesso, continuidade de serviços e gestão de vulnerabilidades. Instrumentos dessa natureza têm servido de base para diagnósticos institucionais, planejamento de capacidades e implementação de políticas de segurança adaptadas à realidade de cada organização.

Apesar do esforço normativo e técnico, ainda persiste um cenário de fragmentação regulatória. Como apontam Belli *et al.* (2023), há sobreposição de competências entre agências, ausência de coordenação federativa robusta e uma escassez de mecanismos obrigatórios de articulação entre políticas setoriais e estratégias nacionais. Essa fragmentação gera incerteza regulatória, dificulta o monitoramento de incidentes e limita a eficácia das ações em contextos locais, especialmente em municípios de médio e pequeno porte.

A distância entre o arcabouço regulatório federal e a realidade dos entes subnacionais se acentua quando se considera a ausência de uma política estruturada de avaliação da maturidade cibernética nas esferas estadual e municipal. Como evidenciado na Revisão da Capacidade de Cibersegurança conduzida pelo GCSCC em parceria com a OEA, os governos subnacionais brasileiros enfrentam restrições severas relacionadas à infraestrutura, qualificação técnica e cultura institucional de segurança da informação. O documento destaca a inexistência de mecanismos de coordenação que permitam mensurar ou induzir o desenvolvimento de capacidades em segurança cibernética nos diferentes níveis de governo, o que compromete a efetividade da governança federativa no setor (OEA; Oxford, 2020).

Essa assimetria torna-se ainda mais crítica frente à crescente dependência digital dos serviços públicos locais e à fragmentação das respostas institucionais a incidentes cibernéticos. A análise da OEA aponta que, apesar de existirem iniciativas setoriais avançadas, como no setor financeiro, a maioria dos municípios e órgãos públicos estaduais ainda opera em estágios embrionários do modelo de maturidade cibernética. As respostas a incidentes, quando ocorrem, são frequentemente ad hoc, sem protocolos padronizados, indicadores de desempenho ou integração com os CSIRTs nacionais. Tais fragilidades evidenciam a necessidade de uma estrutura articulada que promova a interoperabilidade normativa e técnica entre os entes federativos, bem como a institucionalização de capacidades locais por meio de instrumentos diagnósticos, apoio técnico e financiamento estratégico (OEA; Oxford, 2020).

A análise de Cravo (2023) corrobora esse diagnóstico ao argumentar que a Estratégia Nacional de Segurança Cibernética vigente, embora formalmente instituída, ainda carece de densidade material para se configurar como uma política pública efetiva. A autora destaca que o Decreto nº 10.222/2020, que criou a E-Ciber, não estabelece obrigações concretas, métricas de desempenho nem mecanismos vinculantes de articulação federativa, o que limita seu alcance e dificulta a adaptação das diretrizes às realidades subnacionais. Tal fragilidade é ainda mais acentuada pelo fato de a governança da cibersegurança no Brasil permanecer excessivamente concentrada no âmbito federal, sem canais institucionais permanentes de apoio técnico, financeiro e regulatório aos estados e municípios.

Além disso, a autora aponta a ausência de um marco legal específico para a segurança cibernética como um dos principais entraves à institucionalização do tema no país. Em sua proposta, Cravo (2023) defende a criação de uma Autoridade Nacional de Segurança Cibernética, dotada de competências normativas e fiscalizatórias, com capacidade para atuar de forma articulada com as agências setoriais e os entes federados. Essa estrutura permitiria um modelo de regulação coordenada, inspirado nas melhores práticas internacionais, como o modelo europeu da NIS2, ao mesmo tempo em que seria adaptado à realidade federativa brasileira. Nesse cenário, os municípios e consórcios intermunicipais, como a AMREC, poderiam se tornar unidades estratégicas para a implementação descentralizada de políticas de cibersegurança, recebendo suporte técnico e recursos regulados por diretrizes nacionais.

O Relatório de Cibersegurança 2020, publicado pelo BID e pela OEA, oferece evidências robustas sobre os baixos níveis médios de maturidade cibernética nos países da América Latina e Caribe, apontando que a maioria das estratégias nacionais carece de coordenação multissetorial, mecanismos de avaliação de impacto e integração com os níveis subnacionais de governo. O relatório enfatiza a urgência de desenvolver estruturas federativas capazes de sustentar a implementação das estratégias em nível local, sobretudo em contextos municipais que, como o brasileiro, enfrentam restrições severas em termos de orçamento, infraestrutura técnica e quadros funcionais especializados (BID; OEA, 2020).

Um dos principais gargalos identificados pelo relatório é a escassez de profissionais qualificados em cibersegurança, estimada em cerca de 600 mil postos não preenchidos na região. No caso brasileiro, essa carência compromete a adoção de boas práticas em segurança digital nos municípios, uma vez que a maioria das iniciativas depende da atuação direta de equipes reduzidas e, muitas vezes, sem formação específica na área. Adicionalmente, o documento destaca que a divulgação responsável de incidentes e a cooperação internacional ainda são limitadas, o que dificulta o compartilhamento de informações estratégicas entre entes federados e setores críticos. Nesse contexto, iniciativas regionais de cooperação, como o CSIRT Américas e os programas de capacitação em parceria com a Europa, são apresentados como caminhos promissores para elevar o nível de maturidade institucional em ambientes subnacionais e descentralizados (BID; OEA, 2020).

Uma contribuição recente ao debate sobre eficiência de investimentos em cibersegurança vem do conceito de segmentação da informação, conforme analisado por Gordon, Loeb e Zhou (2021). Os autores argumentam que a segmentação lógica e funcional de sistemas de informação permite não apenas limitar o alcance de incidentes, mas também aplicar uma alocação diferenciada de recursos com base em análises custo-benefício por segmento de

risco. Em termos práticos, a adoção de modelos como o Gordon-Loeb Model, ajustados para múltiplos segmentos informacionais, permite a otimização do investimento em segurança de acordo com a vulnerabilidade, valor e função da informação armazenada em cada subsetor organizacional. Essa abordagem, pouco difundida entre municípios brasileiros, poderia representar um avanço significativo para realidades com recursos limitados, como as que serão analisadas no estudo empírico com os municípios da AMREC.

Um dos principais entraves à difusão de práticas avançadas de segurança cibernética nos contextos subnacionais é a dificuldade de planejamento técnico e econômico de ações coordenadas de proteção digital. Essa lacuna é diretamente enfrentada pela proposta metodológica do *CyberTEA – Cybersecurity Technical and Economic Approach*, desenvolvida por Franco, Granville e Stiller (2023), que propõe uma abordagem em cinco fases integradas para apoiar o processo decisório em segurança digital. Voltado especialmente para pequenas e médias organizações, o modelo permite mapear ameaças, dimensionar custos, identificar prioridades e definir arquiteturas técnicas com base na lógica de retorno sobre investimento. Embora desenvolvido para aplicação em ambientes empresariais, o CyberTEA possui alto potencial de adaptação para prefeituras municipais e consórcios intermunicipais, oferecendo uma alternativa pragmática ao desafio da ausência de expertise interna nos entes locais.

Complementando a discussão sobre maturidade institucional, Xu *et al.* (2019) introduzem uma perspectiva estratégica baseada na teoria das opções reais, que considera o valor da flexibilidade na tomada de decisão sobre investimentos em segurança digital. Os autores diferenciam investimentos proativos (voltados ao crescimento futuro e à mitigação preventiva) dos investimentos reativos (motivados por incidentes passados), demonstrando empiricamente que o alinhamento entre estratégia de segurança e momento do investimento influencia diretamente o desempenho organizacional. Em contextos institucionais com baixa capacidade de previsão e gestão de riscos — como é o caso de muitos municípios brasileiros — essa distinção adquire centralidade. A aplicação de modelos como esse poderia auxiliar gestores públicos a definir se o momento é de antecipação ou resposta, promovendo uma lógica mais racional e eficaz de alocação de recursos limitados em cibersegurança.

Portanto, os desafios da cibersegurança no Brasil não são exclusivamente técnicos ou normativos, mas fundamentalmente institucionais e federativos. A superação dessas barreiras exigirá a integração das estratégias nacionais às políticas setoriais e à realidade dos entes subnacionais, com a construção de um modelo coordenado, tecnicamente orientado e financeiramente viável, capaz de induzir a maturidade cibernética em todos os níveis da federação.

4.2.3 Regulação e seus limites no contexto local

A formulação de políticas públicas de cibersegurança no Brasil segue, historicamente, uma lógica fortemente centralizada, ancorada em marcos legais de origem federal, como a Lei Geral de Proteção de Dados (LGPD), o Decreto nº 10.222/2020 (que instituiu a Estratégia Nacional de Segurança Cibernética – E-Ciber), o Decreto nº 11.856/2023 (que estabelece a Política Nacional de Cibersegurança – PNCiber) e o Decreto nº 12.572/2025 (que instituiu a Política Nacional de Segurança da Informação). Embora esses instrumentos representem avanços significativos no plano normativo, seus efeitos sobre os entes subnacionais — especialmente os municípios — têm sido limitados por obstáculos estruturais e pela ausência de mecanismos de indução regulatória. Como observa Cravo (2023), há uma fragmentação profunda entre o que é proposto como estratégia nacional e aquilo que os governos locais têm capacidade real de implementar.

Essa desconexão entre norma e prática pode ser interpretada à luz da teoria econômica da regulação formulada por George Stigler (1971), da Escola de Chicago. Em oposição à abordagem normativa que concebe a regulação como ferramenta de correção de falhas de mercado, Stigler propôs uma visão realista, segundo a qual a regulação frequentemente emerge da pressão de grupos organizados que instrumentalizam o Estado para fins privados. O autor argumenta que agentes reguladores — públicos ou autônomos — são suscetíveis à influência das indústrias que deveriam fiscalizar, criando situações em que o marco regulatório favorece os próprios regulados.

Essa proposição foi aprofundada por Richard Posner (1974), que sugere que as agências não falham por deficiência administrativa, mas por operarem com incentivos distorcidos, e por Sam Peltzman (1976), que destaca a multiplicidade de interesses que disputam a orientação da regulação. No Brasil, essas ideias foram retomadas por autores como Luz Neto (2016) e Torres (2012), que evidenciam como, mesmo com estruturas autônomas, os órgãos reguladores seguem vulneráveis à captura — especialmente em contextos de baixa capacitação técnica, assimetria informacional e dependência econômica.

No contexto brasileiro, marcado por profundas desigualdades federativas, a regulação no plano municipal é particularmente frágil. Embora a Constituição de 1988 tenha conferido autonomia administrativa e normativa aos municípios, essa autonomia colide com limitações estruturais severas: escassez de servidores qualificados, ausência de áreas técnicas especializadas, dependência financeira da União e pouca institucionalização de processos

estratégicos. O paradoxo é evidente: cabe aos municípios operacionalizar políticas de alta complexidade, como as que envolvem proteção de dados, sistemas digitais e cibersegurança, mas com recursos humanos, técnicos e normativos insuficientes.

Na prática, a regulação que emana da esfera federal tende a ser internalizada de forma fragmentada ou meramente simbólica pelos entes subnacionais. Muitos municípios replicam modelos prontos — decretos, portarias ou estruturas organizacionais — apenas para demonstrar conformidade, sem consolidar internamente as capacidades necessárias à efetivação dessas normas. Esse fenômeno é identificado na literatura como "conformidade simbólica" ou "implementação formal-desviada" (Lipsky, 2010; Torres, 2012), em que a forma é cumprida, mas o conteúdo e a finalidade da regulação permanecem esvaziados.

Além disso, o cenário de fragilidade institucional abre espaço para novas formas de captura regulatória, não necessariamente via *lobby* direto de grandes grupos econômicos — como previam os modelos clássicos —, mas por meio de dependência técnica e contratual. Em muitos casos, fornecedores privados de *software* e infraestrutura tecnológica tornam-se os responsáveis de fato pela definição e aplicação de padrões de cibersegurança no âmbito municipal. Sem capacidade de supervisão, auditoria ou elaboração normativa própria, os municípios tornam-se reféns desses contratos, instaurando o que se pode denominar captura operacional da regulação local. A regulação, assim, é terceirizada, mas sem os dispositivos públicos de controle e transparência.

Mesmo diante de marcos legais obrigatórios, como a LGPD, verifica-se que a maioria dos municípios brasileiros não dispõe de estruturas organizacionais para implementar rotinas mínimas de proteção de dados, controle de acesso, resposta a incidentes ou capacitação interna. A vulnerabilidade é dupla: os sistemas informacionais tornam-se alvos fáceis de ataques, e a administração pública local perde a autonomia sobre seu próprio ambiente digital.

A ausência de um ente federativo nacional com atribuição clara de coordenação e indução da maturidade cibernética nos municípios agrava o cenário. A PNCiber prevê a criação do Comitê Nacional de Cibersegurança (CNCiber), mas não explicita mecanismos para fomentar capacidades nos entes subnacionais. Não há diretrizes técnicas, incentivos fiscais ou linhas de financiamento vinculadas à implementação de políticas municipais. Como consequência, perpetuam-se a dependência de soluções de mercado, a desigualdade de maturidade entre os municípios e a desconexão entre regulação e prática.

Essa constatação reforça que os limites da regulação no plano local não derivam exclusivamente da ausência de marcos legais, mas da impossibilidade material de transformar norma em política pública eficaz. Como aponta Torres (2012), a efetividade regulatória exige

mais que prescrição normativa: pressupõe capacidade de planejamento, financiamento, fiscalização, participação social e articulação entre os níveis de governo — fatores ausentes ou precários em boa parte dos municípios brasileiros.

Diante desse cenário, o papel de associações intermunicipais e consórcios públicos, como a AMREC, adquire centralidade estratégica. Ao promover compartilhamento de expertise, padronização de processos e construção coletiva de soluções, essas estruturas cooperativas podem funcionar como vetores de indução regulatória, compensando parcialmente as limitações locais e aproximando os municípios das diretrizes nacionais. A análise do caso da AMREC, a seguir, oferecerá uma visão empírica dessas dinâmicas.

4.3 PROCEDIMENTOS METODOLÓGICOS

Este terceiro estudo da tese tem por objetivo realizar uma investigação qualitativa, com caráter descritivo e exploratório, sobre a institucionalização da cibersegurança em nível local, tomando como campo empírico os doze municípios que compõem a Associação dos Municípios da Região Carbonífera (AMREC), no sul de Santa Catarina. A proposta metodológica visa operacionalizar os constructos teóricos identificados no Estudo II, os quais derivam de uma revisão sistemática da literatura e de um mapeamento conceitual dos principais eixos da governança da cibersegurança municipal.

A abordagem adotada neste estudo é de natureza qualitativa, com ênfase na análise institucional e na interpretação das práticas, normas e estruturas organizacionais que sustentam a atuação municipal frente aos desafios da cibersegurança. Parte-se do entendimento de que a cibersegurança não se limita a dimensões técnicas, mas envolve uma complexa rede de fatores normativos, culturais, políticos e organizacionais. Por essa razão, optou-se pela utilização de entrevistas estruturadas como principal técnica de coleta de dados.

O instrumento de pesquisa foi elaborado com base nos achados do Estudo II e nos referenciais teóricos nele sistematizados, especialmente aqueles relacionados à capacidade institucional (Hall; Taylor, 1996), normatividade digital (Cravo, 2023; Akdemir; Law, 2021), infraestrutura crítica (Taddeo; Floridi, 2018), governança colaborativa (Calzada, 2020; Shackelford *et al.*, 2020) e justiça informacional (Dunn Cavelty, 2019; Martin, 2021). Esses referenciais fundamentaram a criação de cinco blocos temáticos de investigação.

O primeiro bloco, denominado "Capacidade institucional e organizacional", busca compreender como os municípios organizam internamente suas estruturas de tecnologia da informação, com foco na qualificação de equipes, definição de atribuições e existência de

rotinas institucionais. A intenção é captar o grau de estabilidade e racionalização da burocracia local, conforme argumentam Hall e Taylor (1996).

O segundo bloco, "Governança digital e normatização local", trata da presença de políticas públicas, marcos legais e instrumentos normativos locais relacionados à cibersegurança. Esta dimensão é crucial para avaliar o grau de institucionalização da agenda no âmbito subnacional, em consonância com a literatura que defende uma abordagem crítica e democrática da governança digital (Akdemir; Law, 2021; Cravo, 2023).

O terceiro bloco temático, "Infraestrutura tecnológica e práticas operacionais", investiga os procedimentos técnicos e as condições materiais que sustentam a proteção de dados e sistemas, considerando aspectos como autonomia tecnológica, resposta a incidentes e rotinas de manutenção. Referenciais como Zuboff (2019), Nissenbaum (2005) e Taddeo e Floridi (2018) balizam essa dimensão.

O quarto bloco, "Cooperação intermunicipal e redes colaborativas", objetiva mapear se há práticas de governança compartilhada e integração territorial entre os municípios da região. Essa dimensão é inspirada na literatura que discute o papel das redes e do ecossistema colaborativo para o enfrentamento de ameaças cibernéticas (Calzada, 2020; Shackelford *et al.*, 2020).

O quinto bloco, "Barreiras institucionais e percepções", explora as resistências, dificuldades e compreensões subjetivas dos agentes públicos sobre os temas da cibersegurança. Essa dimensão considera o papel da cultura organizacional e da burocracia de nível de rua (Lipsky, 2010) como fatores condicionantes das práticas institucionais.

O instrumento de pesquisa foi aplicado por meio de entrevistas estruturadas com perguntas abertas. Os respondentes foram os servidores municipais diretamente envolvidos com a gestão da tecnologia da informação e/ou com a aplicação de políticas de segurança da informação. O critério de seleção priorizou gestores com poder de decisão ou conhecimento técnico-operacional da realidade local. As entrevistas foram realizadas no mês de julho de 2025, com duração média de 40 a 60 minutos cada.

A análise dos dados foi conduzida com base na técnica de análise de conteúdo, em sua vertente categorial, conforme proposto por Bardin (2011). As respostas foram organizadas em categorias previamente definidas com base nos blocos temáticos do instrumento, e posteriormente trianguladas com a literatura de apoio do Estudo II. Essa estratégia analítica buscou identificar padrões, lacunas, contradições e boas práticas presentes nas realidades municipais investigadas.

Os dados empíricos foram interpretados à luz do modelo analítico construído na fundamentação teórica do Estudo II, permitindo avaliar o grau de aderência entre os constructos conceituais e as práticas institucionais verificadas nos municípios. Além disso, buscou-se respeitar a lógica interna de cada município, reconhecendo especificidades contextuais, capacidades diferenciadas e trajetórias institucionais singulares.

Como etapa complementar, os achados do Estudo III serão posteriormente sistematizados para subsidiar a construção de um plano de diretrizes voltado ao fortalecimento da governança da cibersegurança municipal, no intuito de oferecer contribuições práticas e aplicáveis à realidade dos municípios da AMREC. Ressalta-se, contudo, que este produto derivado será desenvolvido em momento posterior, respeitando os limites analíticos deste estudo.

As entrevistas foram realizadas ao longo do mês de julho de 2025 e contaram com a participação de representantes de nove municípios pertencentes à região de estudo. Os respondentes ocupavam diferentes posições técnicas e estratégicas nas estruturas administrativas locais, entre elas: gerente de tecnologia da informação, diretor de planejamento e estratégia, instrutor de informática, diretor de TI, secretário de administração e planejamento, chefe de TI, analista de sistemas, chefe de informática, secretária de administração e assessor jurídico de gabinete. Essa diversidade funcional enriqueceu a coleta ao possibilitar a observação do tema da cibersegurança sob múltiplas perspectivas institucionais, técnicas e jurídicas. Em um dos municípios, a entrevista foi conduzida com dois profissionais da área, o que ampliou a densidade das respostas e permitiu confrontar percepções internas sobre a estrutura organizacional.

Três municípios da região não participaram da etapa de entrevistas, são eles Balneário Rincão, Forquilhinha e Nova Veneza. Um deles alegou não possuir um departamento voltado para segurança de dados e, por esse motivo, optou por não integrar a amostra. Os outros dois municípios inicialmente agendaram a entrevista, mas não compareceram no horário marcado e tampouco responderam às duas tentativas de reagendamento posteriores. A ausência dessas respostas não compromete a robustez da análise, mas deve ser considerada como uma limitação metodológica da pesquisa. Ainda assim, o conjunto de entrevistas obtido representa uma amostra significativa e diversificada do território analisado, suficiente para identificar padrões regionais, barreiras comuns e possibilidades de avanço em relação à institucionalização da cibersegurança na gestão pública municipal.

4.4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Criada em 1961, a AMREC é composta por doze municípios do sul catarinense: Balneário Rincão, Cocal do Sul, Criciúma, Forquilhinha, Içara, Lauro Müller, Morro da Fumaça, Nova Veneza, Orleans, Siderópolis, Treviso e Urussanga. Sua finalidade institucional é fomentar o desenvolvimento regional por meio da cooperação entre os entes consorciados, com atuação em diversas áreas, como infraestrutura, saúde, meio ambiente e tecnologia. Embora a AMREC possua câmaras técnicas voltadas à gestão da informação e tecnologia, a temática da cibersegurança ainda não está institucionalizada como pauta estratégica transversal, tampouco há estruturas consolidadas para proteção digital no conjunto dos municípios.

Para compreender as assimetrias institucionais observadas nos níveis de maturidade em cibersegurança, é necessário considerar o contexto socioeconômico dos municípios investigados. O quadro a seguir apresenta informações demográficas, econômicas e históricas dos doze municípios que compõem a Região da AMREC, incluindo projeções populacionais para 2025, Produto Interno Bruto (PIB) per capita referente ao ano de 2021 e respectivas datas de emancipação política. Esses dados contribuem para contextualizar a capacidade administrativa e os recursos disponíveis em cada localidade, fatores que impactam diretamente na estruturação de políticas públicas, incluindo aquelas voltadas à proteção digital e à governança cibernética.

Quadro 6 – Características dos municípios da AMREC

Município	**População 2025**	**PIB per capita 2021**	**Emancipação**
Balneário Rincão	17.697	R$ 22.440,07	03/10/2003
Cocal do Sul	18.106	R$ 52.196,27	26/09/1991
Criciúma	227.438	R$ 45.871,13	04/11/1925
Forquilhinha	34.771	R$ 44.327,22	26/04/1989
Içara	63.489	R$ 60.654,48	20/12/1961
Lauro Muller	14.628	R$ 27.226,41	20/01/1957
Morro da Fumaça	19.490	R$ 50.954,44	20/05/1962
Nova Veneza	14.004	R$ 69.255,25	21/06/1958
Orleans	24.686	R$ 51.296,22	30/08/1913
Siderópolis	14.156	R$ 47.931,80	19/12/1958
Treviso	3.920	R$ 58.025,97	08/07/1995
Urussanga	21.464	R$ 50.731,67	06/10/1900

Fonte: Elaborado pelo autor (2025).

A análise do quadro permite observar que há considerável heterogeneidade entre os municípios no que se refere ao porte populacional, ao desempenho econômico e ao grau de consolidação institucional, refletido, em parte, pelo tempo de emancipação. Municípios como Criciúma, Içara e Urussanga, com maior densidade populacional e histórico administrativo mais

consolidado, tendem a possuir estruturas administrativas mais consolidadas, ainda que isso não se traduza automaticamente em maturidade cibernética. Por outro lado, cidades como Treviso e Lauro Muller, com menor população e PIB per capita mais modesto, enfrentam desafios adicionais para implementar políticas de cibersegurança de forma estruturada. Essa diversidade reforça a importância de propostas normativas sensíveis às realidades locais, que considerem não apenas os aspectos técnicos, mas também as limitações socioeconômicas e históricas de cada município.

A perspectiva estratégica adotada pelo Plano de Desenvolvimento Regional da AMREC para o decênio 2021-2030 revela uma preocupação crescente com a integração digital e a modernização da gestão pública como pilares do desenvolvimento regional. Em seu eixo de "Inovação e Governança", o plano destaca a importância da transformação digital dos serviços públicos e da estruturação de redes colaborativas intermunicipais como mecanismos essenciais para o aumento da eficiência administrativa e da transparência institucional. Embora o documento ainda não detalhe ações específicas voltadas à cibersegurança, ele reconhece a necessidade de aprimoramento das infraestruturas digitais e da proteção de dados como elementos centrais para a promoção da cidadania digital, da sustentabilidade administrativa e da confiança social nas instituições públicas. Essa diretriz estratégica estabelece um terreno fértil para a inserção da cibersegurança como política transversal, sobretudo diante da crescente digitalização dos serviços municipais e da interoperabilidade de sistemas entre entes consorciados, o que exige padrões mínimos de segurança da informação e capacidades institucionais partilhadas. A incorporação da agenda da cibersegurança ao plano de desenvolvimento pode, assim, representar uma oportunidade de integração entre políticas territoriais de inovação e estratégias nacionais de proteção digital, promovendo uma governança mais resiliente e conectada às demandas contemporâneas da sociedade digital.

4.4.1 Cibersegurança em Municípios do Sul Catarinense: o Caso da AMREC

A realidade institucional dos municípios brasileiros frente à agenda da cibersegurança é marcada por assimetrias profundas. A ausência de estrutura normativa local, a carência de equipes técnicas especializadas e a fragmentação dos sistemas de informação colocam os municípios em uma posição de elevada vulnerabilidade digital. A análise preliminar da legislação municipal e dos portais institucionais revela uma ausência quase generalizada de normas locais voltadas à segurança da informação, proteção de dados ou governança digital. Poucos municípios da AMREC possuem legislação específica sobre o tema, e mesmo entre

esses, a efetivação de políticas concretas é limitada ou inexistente. Em sua maioria, os órgãos públicos locais operam sem planos de contingência digital, sem protocolos formais de resposta a incidentes e sem estrutura organizacional que abrigue funções como encarregado de dados, analista de risco ou auditor de segurança.

Essa lacuna normativa e institucional torna os municípios da AMREC especialmente suscetíveis àquilo que a literatura tem denominado de captura operacional: a dependência direta de fornecedores privados de tecnologia da informação para a gestão e segurança dos sistemas públicos digitais. Empresas terceirizadas assumem o papel de configuradoras, mantenedoras e até de responsáveis pela integridade de bases de dados e sistemas essenciais — como contabilidade, folha de pagamento, arrecadação tributária e sistemas de saúde — sem que haja controle efetivo por parte do poder público local. Esse arranjo intensifica a assimetria técnica entre contratante e contratado e transfere, de forma implícita, o poder normativo para fora da esfera estatal.

A ausência de políticas municipais de cibersegurança e de marcos regulatórios voltados à proteção de dados, como evidenciado no levantamento feito nos municípios da AMREC, não pode ser interpretada apenas como omissão normativa. Trata-se de um reflexo das limitações estruturais que historicamente afetam a capacidade regulatória dos entes locais. Entre os principais obstáculos está a inexistência de diretrizes técnicas nacionais específicas voltadas aos municípios, o que deixa as gestões locais sem parâmetros adaptados à sua realidade para implementar ações efetivas de governança digital. A LGPD, por exemplo, estabelece obrigações genéricas válidas para todo o setor público, mas não é acompanhada de planos de implementação, recursos vinculados ou modelos de maturidade para entes subnacionais. Essa lacuna normativa gera insegurança jurídica, inibe a inovação institucional e amplia a dependência de consultorias externas ou soluções improvisadas.

Além disso, os municípios de pequeno e médio porte enfrentam uma estrutura administrativa reduzida, escassez de recursos financeiros e carência de quadros técnicos especializados em tecnologia da informação e segurança da informação. A rotatividade de servidores, a ausência de formação continuada e a sobreposição de funções dificultam a institucionalização de práticas complexas como a gestão de riscos digitais ou o desenvolvimento de políticas de proteção de dados. Soma-se a isso um fator frequentemente negligenciado: a resistência política ou burocrática à internalização de normas federais que impõem novos deveres sem oferecer suporte técnico ou orçamentário correspondente. Nesse contexto, a conformidade com legislações como a LGPD tende a ser simbólica, refletida em portarias e comissões formais, mas desvinculada de uma estrutura capaz de garantir efetividade

prática. Tal cenário reforça a importância de iniciativas intermunicipais que promovam padronização, compartilhamento de soluções e apoio técnico estruturado.

Adicionalmente, a ausência de estruturas consorciadas de governança digital regional — como núcleos intermunicipais de cibersegurança, comitês regionais de proteção de dados ou estratégias compartilhadas de TIC — evidencia a inexistência de uma política coletiva e articulada no âmbito da AMREC. Embora haja experiências de cooperação em outras áreas, como consórcios de saúde ou saneamento, a cibersegurança ainda é tratada como responsabilidade residual, muitas vezes vinculada apenas ao suporte técnico ou à gestão da infraestrutura de rede.

O contexto regional também reflete os desafios apontados pela literatura especializada sobre maturidade cibernética em ambientes subnacionais. Segundo o Relatório de Capacidade de Cibersegurança da OEA e da Universidade de Oxford (2020), o Brasil apresenta avanços importantes no plano nacional, mas mantém níveis baixos de maturidade nas dimensões de planejamento local, educação em segurança digital e integração intergovernamental. A realidade dos municípios da AMREC ilustra essas lacunas: falta capacitação, faltam sistemas integrados de alerta e resposta, e falta sobretudo uma visão estratégica de cibersegurança como política pública essencial à prestação de serviços e à proteção dos direitos fundamentais.

Apesar do reconhecimento crescente da importância da cibersegurança no plano federal e da formulação de diretrizes estratégicas, como a E-Ciber e a PNCiber, a realidade normativa local dos municípios da AMREC ainda é marcada por certa assimetria e escassez regulatória. A análise documental realizada a partir da base do site LeisMunicipais.com.br, por meio de busca específica pela palavra-chave "segurança", identificou que nenhum dos doze municípios da AMREC apresenta, até o momento, legislação municipal voltada especificamente à proteção de dados e à segurança da informação, porém, alguns já apresentam normas voltadas à regulamentação da LGPD. As ocorrências localizadas referem-se, em sua maioria, à segurança pública em sentido amplo (iluminação, vigilância, patrulhamento urbano), sem articulação com políticas de proteção digital ou governança de dados.

Embora o panorama estadual ainda revele grande heterogeneidade, diversos municípios catarinenses têm avançado na formulação de normativas locais sobre proteção de dados e segurança da informação. Iniciativas como a promulgação de decretos municipais para aplicação da LGPD, a criação de comissões especializadas, a instituição de políticas de segurança digital e a elaboração de programas de governança e transparência demonstram que, em alguns contextos, os governos locais têm buscado internalizar os princípios da regulação

federal com maior proatividade. Municípios como Blumenau, Lages, Brusque, Chapecó e São Bento do Sul já contam com dispositivos normativos que sinalizam uma preocupação institucional com a conformidade à LGPD e com a segurança da informação em ambiente público. Ainda que em estágios distintos de maturidade, essas experiências reforçam que a regulação local é possível quando há alinhamento estratégico, capacidade administrativa e articulação técnica. Nesse sentido, analisar a realidade dos municípios da AMREC permite compreender se e como essa tendência de normatização local também se manifesta na região carbonífera, considerando suas especificidades institucionais, nível de cooperação consorciada e estágio de desenvolvimento digital.

Contudo, é importante destacar que a AMREC, por sua estrutura institucional consolidada e pela tradição de cooperação entre os municípios, apresenta potencial para se tornar um polo de governança cibernética regional. A criação de uma câmara técnica específica para segurança da informação, a instituição de uma política regional de proteção de dados e a adoção de marcos de maturidade cibernética compartilhados poderiam representar um salto qualitativo significativo para os municípios consorciados. Nesse sentido, experiências já consolidadas em outras regiões do país, como consórcios intermunicipais de tecnologia e redes regionais de proteção de dados, podem servir como referência para a construção de soluções adaptadas à realidade da AMREC.

A seção empírica a ser apresentada na próxima etapa desta tese buscará aprofundar esse diagnóstico, por meio de uma investigação aplicada aos municípios da AMREC. Serão exploradas as dimensões de governança institucional, normatização local, dependência tecnológica e capacitação técnica, com base em modelos de maturidade cibernética validados na literatura. O objetivo é compreender como esses municípios lidam com os desafios da cibersegurança e que caminhos podem ser construídos para fortalecer sua capacidade de ação diante das crescentes ameaças do ambiente digital.

Quadro 7 – Leis municipais voltadas à segurança em Balneário Rincão

Documento/Lei	**Data**	**Tema da Lei**	**Assunto e relação com o tema**
Lei Orgânica do Município	05/07/1990	Organização Administrativa/Poder Público	Define a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão. Inclui incentivo ao desenvolvimento tecnológico.
Lei Complementar nº 50	2024	Estrutura Administrativa	Define a estrutura organizacional do Poder Executivo, incluindo a criação da Divisão de Tecnologia da Informação.
Plano Municipal de Educação (PME)	2015	Educação	Define metas e diretrizes para a educação municipal, incluindo o uso de TICs e laboratórios de informática nas escolas.

Fonte: Elaborado pelo autor (2025).

Em Balneário Rincão, embora não haja legislação municipal específica voltada à proteção de dados ou à cibersegurança, algumas normativas vigentes apresentam elementos que podem servir de base institucional para a construção futura de políticas nessa área. A Lei Orgânica do Município (1990) estabelece diretrizes gerais sobre organização administrativa e inovação tecnológica, mas não menciona diretamente temas como governança digital, segurança da informação ou proteção de dados. Já a Lei Complementar nº 50 (2024), que trata da estrutura administrativa do Poder Executivo, inclui a criação de uma Divisão de Tecnologia da Informação (TI), o que representa uma oportunidade concreta para o desenvolvimento de ações de gestão de riscos, maturidade digital e políticas de cibersegurança. Além disso, o Plano Municipal de Educação (2015) incentiva o uso de tecnologias e TICs nas escolas, mas não incorpora orientações sobre cultura de segurança digital, capacitação em proteção de dados ou protocolos de segurança da informação no ambiente educacional. Esses marcos demonstram que, apesar da ausência de normativas diretamente vinculadas à cibersegurança, o município possui estruturas institucionais que podem ser fortalecidas e articuladas para a formulação de políticas públicas alinhadas às diretrizes da LGPD e da Política Nacional de Cibersegurança.

Quadro 8 – Leis municipais voltadas à segurança em Cocal do Sul

Documento/Lei	**Data**	**Tema da Lei**	**Assunto e relação com o tema**
Lei Orgânica do Município	05/07/1990	Organização Administrativa / Poder Público	Estabelece a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão. Inclui políticas de desenvolvimento urbano e rural, assistência social e meio ambiente.
Lei Complementar nº 146 (Plano Diretor Participativo)	18/12/2023	Planejamento Urbano e Desenvolvimento Sustentável	Institui o Plano Diretor Participativo, estabelecendo diretrizes para o desenvolvimento sustentável do meio ambiente urbano e rural, incluindo políticas de mobilidade urbana, iluminação pública e desenvolvimento socioeconômico.
Lei Ordinária nº 784	2007	Estrutura Administrativa do Poder Legislativo	Dispõe sobre a estrutura administrativa e organizacional do Poder Legislativo do Município de Cocal do Sul, estabelecendo cargos e funções.
Lei Ordinária nº 1221	2014	Educação / Plano de Cargos e Carreiras	Institui o plano de cargos, carreira e remuneração do magistério público municipal, estabelecendo diretrizes para os profissionais da educação.

Fonte: Elaborado pelo autor (2025).

No município de Cocal do Sul, a análise das normativas municipais revela a ausência de legislações diretamente voltadas à cibersegurança, proteção de dados ou regulamentação da LGPD. A Lei Orgânica do Município (1990) estabelece diretrizes gerais sobre organização administrativa, desenvolvimento urbano e assistência social, mas não

contempla dispositivos específicos sobre governança digital ou segurança da informação. Da mesma forma, a Lei Complementar nº 146/2023, que institui o Plano Diretor Participativo, menciona o uso de tecnologias no contexto urbano e de desenvolvimento sustentável, mas não incorpora dispositivos relacionados à proteção de dados ou à gestão de riscos digitais. Além disso, a Lei Ordinária nº 784/2007, que trata da estrutura administrativa do Poder Legislativo, e a Lei Ordinária nº 1221/2014, que estabelece o plano de cargos e carreira do magistério, também não abordam o uso de tecnologias, segurança digital ou cultura de proteção da informação. Esse panorama indica que, embora haja dispositivos normativos estruturantes no município, não há internalização da agenda de cibersegurança nos marcos legais existentes. As oportunidades de avanço residem na possibilidade de inserir diretrizes de proteção de dados e segurança da informação nas políticas urbanas, nos processos legislativos e no ambiente educacional, alinhando Cocal do Sul às exigências da legislação nacional e às boas práticas de governança digital.

Quadro 9 – Leis municipais voltadas à segurança em Criciúma

Documento/Lei	**Data**	**Tema da Lei**	**Assunto e relação com o tema**
Lei Orgânica do Município	05/07/1990	Organização Administrativa / Poder Público	Estabelece a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Lei Complementar nº 511	09/12/2022	Estrutura Administrativa do Poder Executivo	Dispõe sobre a organização e a estrutura da administração pública do Poder Executivo do Município.
Lei Complementar nº 595	2025	Controladoria Geral do Município	Dispõe sobre a Controladoria-Geral do Município de Criciúma, define seus princípios, organização e finalidades.
Plano Municipal de Educação	2015	Educação	Estabelece diretrizes para a educação no município, incluindo a promoção do uso de Tecnologias da Informação e Comunicação (TICs) nas escolas.
Lei Complementar nº 568	2024	Código Tributário Municipal	Altera dispositivos da Lei Complementar nº 287, de 27 de setembro de 2018, que institui o Código Tributário do Município de Criciúma.
Regimento Interno da Câmara Municipal	11/10/2023	Organização Legislativa	Dispõe sobre o Regimento Interno da Câmara Municipal de Criciúma, regulamentando seu funcionamento.
Decreto nº 969/23	17/04/2023	Regulamentação LGPD	Dispõe sobre a regulamentação e aplicação da Lei nº 13.709/2018

Fonte: Elaborado pelo autor (2025).

Em Criciúma, o levantamento das normativas municipais revela a existência de leis estruturantes com potencial para incorporação futura da agenda de cibersegurança, inclusive com apresentação de decreto sobre o uso da proteção de dados, segurança da informação em conformidade com a LGPD. O decreto nº 969/23 é o instrumento normativo que dispõe sobre

a regulamentação e aplicação da LGPD no município. A Lei Orgânica do Município (1990) define diretrizes gerais de organização administrativa e desenvolvimento, mas não contempla dispositivos específicos sobre governança digital ou proteção de dados. A Lei Complementar nº 511/2022, que organiza a estrutura do Poder Executivo, também não aborda cibersegurança, embora ofereça base para inserção futura de práticas de gestão de riscos e segurança informacional. O mesmo ocorre com a Lei Complementar nº 595/2025, que trata da Controladoria-Geral, cujas atividades de controle e auditoria poderiam integrar diretrizes de proteção de dados. No campo educacional, o Plano Municipal de Educação (2015) incentiva o uso de Tecnologias da Informação e Comunicação (TICs), mas não contempla medidas voltadas à segurança digital no ambiente escolar. Já a Lei Complementar nº 568/2024, de natureza tributária, e o Regimento Interno da Câmara Municipal (2023) tampouco incluem elementos relacionados à proteção da informação nos seus escopos. Assim, embora Criciúma disponha de marcos legais administrativos relevantes, não há internalização normativa da agenda da cibersegurança no município até o momento, o que evidencia uma lacuna institucional importante diante das exigências estabelecidas pelas políticas nacionais.

Quadro 10 – Leis municipais voltadas à segurança em Forquilhinha

Documento/Lei	Data	Tema da Lei	Assunto e relação com o tema
Lei Orgânica do Município	11/03/2020	Organização Administrativa / Poder Público	Define a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Projeto de Lei Executivo nº 46/2024	08/07/2024	Planejamento Urbano	Normas para regularização de obras fora do Plano Diretor Urbano e Código de Obras.
Projeto de Lei Executivo nº 7/2025	2025	Estrutura Administrativa	Altera e consolida a legislação sobre a organização administrativa do município.

Fonte: Elaborado pelo autor (2025).

No município de Forquilhinha, a análise das normativas municipais identificadas evidencia a ausência de dispositivos legais voltados à cibersegurança, proteção de dados ou governança digital. A Lei Orgânica do Município (2020), embora estabeleça diretrizes gerais sobre administração pública e desenvolvimento municipal, não contempla menções à segurança da informação ou à LGPD. O Projeto de Lei Executivo nº 46/2024, voltado à regularização de edificações fora do Plano Diretor Urbano, tampouco inclui diretrizes sobre segurança digital nos processos de licenciamento ou gestão urbana. Da mesma forma, o Projeto de Lei Executivo nº 7/2025, que trata da consolidação da estrutura administrativa do município, não apresenta dispositivos voltados à proteção de dados ou à gestão de riscos cibernéticos. Esse conjunto normativo revela que Forquilhinha ainda não internalizou institucionalmente a agenda da

cibersegurança, permanecendo distante das diretrizes estabelecidas pelas políticas nacionais, como a LGPD e a PNCiber. Contudo, os projetos legislativos em curso representam uma janela de oportunidade para a inclusão de políticas voltadas à maturidade digital, à proteção da informação e à estruturação de programas de segurança da informação no âmbito administrativo municipal.

Quadro 11 – Leis municipais voltadas à segurança em Içara

Documento/Lei	Data	Tema da Lei	Assunto e relação com o tema
Lei Orgânica do Município	11/03/2020	Organização Administrativa / Poder Público	Define a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Lei Complementar nº 232/2023	14/12/2023	Planejamento Urbano / Desenvolvimento Sustentável	Institui o Plano Diretor Participativo do Município de Içara, estabelecendo diretrizes para o desenvolvimento urbano e rural.
Lei Ordinária nº 3931/2016	14/12/2016	Estrutura Administrativa do Poder Executivo	Dispõe sobre a organização administrativa da Administração Direta e Indireta da Administração Municipal de Içara.
Lei Ordinária nº 3715/2015	15/06/2015	Educação / Plano Municipal de Educação	Aprova o Plano Municipal de Educação para o período de 2015 a 2024, estabelecendo metas e estratégias para a educação no município.

Fonte: Elaborado pelo autor (2025).

No município de Içara, a análise das normativas legislativas demonstra que ainda não há dispositivos legais que abordem diretamente a temática da cibersegurança, da proteção de dados ou da governança digital. A Lei Orgânica do Município (2020) trata da estrutura dos poderes municipais e de diretrizes gerais de gestão, mas não contempla mecanismos voltados à segurança da informação ou à conformidade com a LGPD. Da mesma forma, a Lei Complementar nº 232/2023, que institui o Plano Diretor Participativo, embora mencione o uso de tecnologias para gestão urbana, não apresenta diretrizes de proteção de dados ou maturidade digital. A Lei Ordinária nº 3931/2016, que organiza administrativamente o Executivo Municipal, também não trata de segurança informacional ou protocolos digitais, e o mesmo ocorre com a Lei Ordinária nº 3715/2015, que aprova o Plano Municipal de Educação até 2024 — apesar de estimular o uso de tecnologias, não contempla ações voltadas à proteção da informação no ambiente escolar. Este conjunto normativo revela que, embora existam estruturas administrativas e planos estratégicos relevantes em vigor, a cibersegurança permanece ausente da agenda legislativa local. Isso representa uma lacuna crítica frente às exigências das políticas nacionais e evidencia a oportunidade de integrar, de forma transversal, políticas de segurança digital em setores como planejamento urbano, gestão pública e educação.

Quadro 12 – Leis municipais voltadas à segurança em Lauro Muller

Documento/Lei	Data	Tema da Lei	Assunto e relação com o tema
Lei Orgânica do Município	11/03/2020	Organização Administrativa / Poder Público	Define a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Lei Ordinária nº 1549/2008	30/12/2008	Planejamento Urbano / Desenvolvimento Sustentável	Institui o Plano Diretor Participativo do Município de Lauro Müller, estabelecendo diretrizes para o desenvolvimento urbano e rural.
Lei Ordinária nº 1872/2015	16/12/2015	Educação / Plano Municipal de Educação	Aprova o Plano Municipal de Educação para o período de 2015 a 2025, estabelecendo metas e estratégias para a educação no município.

Fonte: Elaborado pelo autor (2025).

Em Lauro Müller, a análise das leis municipais revela que, embora existam normativas com potencial para integrar diretrizes de cibersegurança, nenhuma delas atualmente contempla de forma direta a proteção de dados pessoais, a segurança da informação ou a governança digital. A Lei Orgânica do Município (2020), ainda que trate da estrutura dos poderes municipais e dos direitos dos cidadãos, não inclui diretrizes sobre cibersegurança ou conformidade com a LGPD. A Lei Ordinária nº 1549/2008, que institui o Plano Diretor Participativo, menciona o uso de tecnologias para gestão urbana e desenvolvimento sustentável, mas não aborda medidas voltadas à proteção digital no licenciamento urbano ou em sistemas de gestão pública. Da mesma forma, a Lei Ordinária nº 1872/2015, que define o Plano Municipal de Educação até 2025, estimula o uso de tecnologias nas escolas, porém não prevê ações específicas de segurança digital ou de cultura de proteção de dados na educação pública. Assim, o município apresenta um vácuo normativo relevante em relação à agenda da cibersegurança, o que evidencia a necessidade de modernização legal para alinhar-se aos parâmetros estabelecidos nacionalmente e fortalecer sua capacidade institucional frente aos riscos digitais emergentes.

Quadro 13 – Leis municipais voltadas à segurança em Morro da Fumaça

Documento/Lei	Data	Tema da Lei	Assunto e relação com o tema
Lei Orgânica do Município	09/04/1990	Organização Administrativa / Poder Público	Define a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Lei Complementar nº 018/2014	09/05/2014	Planejamento Urbano / Desenvolvimento Sustentável	Institui o Plano Diretor Municipal, estabelecendo objetivos, diretrizes e instrumentos para as ações de planejamento no município.
Lei Ordinária nº 1701/2015	15/06/2015	Educação / Plano Municipal de Educação	Aprova o Plano Municipal de Educação para o período de 2015 a 2025, estabelecendo metas e estratégias para a educação no município.
Decreto nº 121/2019	09/09/2019	Regularização Fundiária / Planejamento Urbano	Disciplina o processo de regularização de edificações existentes no município antes

Documento/Lei	Data	Tema da Lei	Assunto e relação com o tema
			da entrada em vigor do Plano Diretor de 2014.

Fonte: Elaborado pelo autor (2025).

No município de Morro da Fumaça, a legislação vigente evidencia a ausência de dispositivos específicos sobre cibersegurança, proteção de dados pessoais ou governança digital. A Lei Orgânica do Município (1990), apesar de tratar da estrutura administrativa e dos direitos dos cidadãos, não contempla diretrizes sobre segurança da informação ou adequação à LGPD. A Lei Complementar nº 018/2014, que institui o Plano Diretor Municipal, menciona o uso de tecnologias para gestão urbana, mas não aborda medidas relativas à proteção de dados ou segurança digital nos processos de planejamento. O mesmo se aplica à Lei Ordinária nº 1701/2015, que estabelece o Plano Municipal de Educação: embora incentive o uso de TICs nas escolas, não propõe ações voltadas à segurança da informação no ambiente educacional. Já o Decreto nº 121/2019, voltado à regularização fundiária, também não apresenta qualquer previsão sobre segurança digital nos sistemas de licenciamento ou gestão urbana. O conjunto normativo demonstra que, até o momento, a cibersegurança permanece ausente da agenda legislativa local, mesmo diante da crescente digitalização de serviços e processos públicos. O município, contudo, apresenta oportunidades claras para a integração de diretrizes de proteção de dados e maturidade digital em setores como planejamento urbano, administração pública e educação.

Quadro 14 – Leis municipais voltadas à segurança em Nova Veneza

Documento/Lei	Data	Tema da Lei	Assunto e relação com o tema
Lei Orgânica do Município	25/04/1990	Organização Administrativa / Poder Público	Define a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Lei nº 1706/2004 - Plano Diretor Municipal	10/12/2004	Planejamento Urbano / Desenvolvimento Sustentável	Estabelece diretrizes para o desenvolvimento urbano e rural, dividindo o território municipal em zonas urbanas e rurais.
Lei Ordinária nº 2407/2015 - Plano Municipal de Educação	17/06/2015	Educação / Plano Municipal de Educação	Aprova o Plano Municipal de Educação para o período de 2015 a 2025, estabelecendo metas e estratégias para a educação no município.
Lei nº 2592/2017 - Plano Municipal de Cultura	23/10/2017	Cultura / Planejamento Cultural	Institui o Plano Municipal de Cultura, estabelecendo diretrizes para o desenvolvimento cultural do município.

Fonte: Elaborado pelo autor (2025).

Em Nova Veneza, a análise das legislações municipais evidencia a inexistência de marcos normativos voltados diretamente à cibersegurança, proteção de dados ou governança digital. A Lei Orgânica do Município (1990) trata da estrutura administrativa e dos direitos dos

cidadãos, mas não contempla dispositivos sobre segurança informacional ou adequação à LGPD. A Lei nº 1706/2004, que institui o Plano Diretor Municipal, menciona o uso de tecnologias para gestão urbana, porém não inclui diretrizes relacionadas à proteção de dados nos processos de planejamento e desenvolvimento urbano. O mesmo padrão se repete no setor educacional: a Lei Ordinária nº 2407/2015, que aprova o Plano Municipal de Educação, e a Lei nº 2592/2017, que define o Plano Municipal de Cultura, incentivam o uso de tecnologias em seus respectivos domínios, mas não incorporam ações voltadas à segurança digital, proteção de dados ou conscientização cibernética. Dessa forma, ainda que existam políticas voltadas à inovação em áreas como educação, cultura e urbanismo, a ausência de integração com a agenda da cibersegurança evidencia uma lacuna crítica no arcabouço legislativo local, que pode comprometer a proteção de dados sensíveis e a confiabilidade dos sistemas públicos digitais. A articulação de diretrizes de segurança digital nesses planos representa uma oportunidade concreta para alinhar Nova Veneza às exigências contemporâneas de governança da informação.

Quadro 15 – Leis municipais voltadas à segurança em Orleans

Documento/Lei	**Data**	**Tema da Lei**	**Assunto e relação com o tema**
Lei Orgânica do Município	25/04/1990	Organização Administrativa / Poder Público	Define a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Lei Complementar nº 3250/2024 - Plano Diretor Municipal	17/09/2024	Planejamento Urbano / Desenvolvimento Sustentável	Estabelece diretrizes para o desenvolvimento urbano e rural, dividindo o território municipal em zonas urbanas e rurais.
Plano Municipal de Educação	15/06/2015	Educação / Plano Municipal de Educação	Aprova o Plano Municipal de Educação para o período de 2015 a 2025, estabelecendo metas e estratégias para a educação no município.

Fonte: Elaborado pelo autor (2025).

Em Orleans, a análise do conjunto normativo evidencia que o município ainda não possui legislações específicas voltadas à cibersegurança, proteção de dados pessoais ou governança digital. A Lei Orgânica do Município (1990) define a estrutura dos poderes municipais e estabelece diretrizes gerais de administração e cidadania, mas não contempla elementos relacionados à segurança da informação ou à conformidade com a LGPD. A Lei Complementar nº 3250/2024, que institui o Plano Diretor Municipal, faz menção ao uso de tecnologias para fins de planejamento urbano, contudo não incorpora diretrizes relativas à proteção de dados ou maturidade digital nos sistemas de gestão territorial. O Plano Municipal de Educação (2015), por sua vez, incentiva o uso de tecnologias nas escolas, mas não propõe ações voltadas à segurança digital no ambiente educacional, permanecendo desconectado da

lógica de proteção da informação exigida pelas diretrizes federais. A ausência de uma política normativa articulada sobre cibersegurança revela uma fragilidade institucional relevante, mas ao mesmo tempo aponta para oportunidades concretas de inserção desse tema em documentos estratégicos já consolidados no município. A inclusão de políticas de proteção de dados nas áreas de administração, urbanismo e educação pode representar um avanço significativo na governança digital de Orleans.

Quadro 16 – Leis municipais voltadas à segurança em Siderópolis

Documento/Lei	**Data**	**Tema da Lei**	**Assunto e relação com o tema**
Lei Orgânica do Município	09/04/1990	Organização Administrativa / Poder Público	Define a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Lei Ordinária nº 2433/2021	29/06/2021	Planejamento Urbano / Parcelamento do Solo	Dispõe sobre o parcelamento do solo urbano e dá outras providências, estabelecendo diretrizes para o desenvolvimento urbano.
Plano Municipal de Educação	07/12/2016	Educação / Plano Municipal de Educação	Aprova o Plano Municipal de Educação, estabelecendo metas e estratégias para a educação no município.
Decreto nº 067/2024	26/04/2024	Educação / Tempo Integral	Dispõe sobre a política de educação em tempo integral da rede pública municipal de ensino de Siderópolis/SC.

Fonte: Elaborado pelo autor (2025).

Em Siderópolis, o conjunto de normas municipais analisado revela que, até o momento, não há legislação específica voltada à cibersegurança, proteção de dados pessoais ou governança digital. A Lei Orgânica do Município (1990), embora trate da organização administrativa e dos direitos dos cidadãos, não apresenta dispositivos voltados à segurança da informação ou à adequação à LGPD. A Lei Ordinária nº 2433/2021, que dispõe sobre o parcelamento do solo urbano, não aborda elementos de segurança digital nos processos de planejamento urbano, e o Plano Municipal de Educação (2016), apesar de incentivar o uso de tecnologias no ambiente escolar, não contempla medidas voltadas à proteção de dados educacionais. O mesmo ocorre com o Decreto nº 067/2024, que regulamenta a política de educação em tempo integral e menciona o uso de TICs, mas não inclui diretrizes de segurança digital nos ambientes educacionais estendidos. A ausência de políticas normativas específicas revela uma lacuna significativa frente aos marcos regulatórios nacionais e aos riscos crescentes relacionados à transformação digital. No entanto, os instrumentos legais já existentes podem ser estrategicamente atualizados para incorporar diretrizes de cibersegurança, sobretudo nos setores de educação, planejamento urbano e administração pública, de forma a alinhar Siderópolis às exigências contemporâneas da proteção digital no setor público.

Quadro 17 – Leis municipais voltadas à segurança em Treviso

Documento/Lei	Data	Tema da Lei	Assunto e relação com o tema
Lei Orgânica do Município	08/07/1995	Organização Administrativa / Poder Público	Define a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Lei Complementar nº 1056/2023 - Plano Diretor Municipal	2023	Planejamento Urbano / Desenvolvimento Sustentável	Estabelece diretrizes para o desenvolvimento urbano e rural, dividindo o território municipal em zonas urbanas e rurais.
Plano Municipal de Educação	2021	Educação / Plano Municipal de Educação	Aprova o Plano Municipal de Educação para o período de 10 anos, estabelecendo metas e estratégias para a educação no município.
Decreto nº 348/2023	13/07/2023	Educação / Monitoramento e Avaliação	Institui e designa a equipe técnica de monitoramento e avaliação do Plano Municipal de Educação (PME) de Treviso.

Fonte: Elaborado pelo autor (2025).

Em Treviso, a análise da legislação municipal revela a inexistência de normas específicas voltadas à cibersegurança, proteção de dados ou regulamentação da LGPD. A Lei Orgânica do Município (1995), embora estabeleça a estrutura dos poderes locais e diretrizes gerais de gestão, não contempla dispositivos sobre segurança da informação ou governança digital. A Lei Complementar nº 1056/2023, que define o Plano Diretor Municipal, faz referência ao uso de tecnologias no planejamento urbano, mas não inclui medidas de proteção de dados nos sistemas digitais de gestão territorial. No campo educacional, o Plano Municipal de Educação (2021) e o Decreto nº 348/2023, que regulamenta a equipe de monitoramento e avaliação do PME, incentivam o uso de tecnologias na educação, porém não apresentam diretrizes voltadas à segurança digital, à privacidade ou ao controle de dados educacionais. Esse conjunto normativo indica que o município ainda não incorporou institucionalmente a agenda da cibersegurança, mesmo em setores sensíveis como a educação e a gestão urbana. No entanto, os documentos analisados apresentam oportunidades relevantes para a inserção transversal de políticas de proteção digital, especialmente nos processos de monitoramento educacional e na governança urbana, o que poderia representar um importante avanço no alinhamento de Treviso às diretrizes nacionais de proteção de dados e maturidade digital no setor público.

Quadro 18 – Leis municipais voltadas à segurança em Urussanga

Documento/Lei	Data	Tema da Lei	Assunto e relação com o tema
Lei Orgânica do Município	1990	Organização Administrativa / Poder Público	Estabelece a estrutura dos poderes municipais, direitos dos cidadãos e diretrizes gerais de gestão.
Lei Complementar nº 29/2020 - Plano Diretor Municipal	17/09/2020	Planejamento Urbano / Desenvolvimento Sustentável	Estabelece diretrizes para o desenvolvimento urbano e rural, dividindo o território municipal em zonas urbanas e rurais.

Documento/Lei	Data	Tema da Lei	Assunto e relação com o tema
Lei Ordinária nº 2.722/2015 - Plano Municipal de Educação	17/07/2015	Educação / Plano Municipal de Educação	Aprova o Plano Municipal de Educação para o período de 2015 a 2024, estabelecendo metas e estratégias para a educação no município.
Lei Complementar nº 15/2016 - Estrutura Administrativa	27/09/2016	Organização Administrativa / Estrutura Organizacional	Estabelece a estrutura administrativa organizacional setorial da Prefeitura Municipal de Urussanga.
Lei Complementar nº 36/2022 - Criação da Diretoria do Meio Ambiente	14/03/2022	Meio Ambiente / Gestão Ambiental	Dispõe sobre a criação da Diretoria do Meio Ambiente, altera a Lei Complementar nº 15/2016 e dá outras providências.

Fonte: Elaborado pelo autor (2025).

Em Urussanga, o levantamento das normas municipais evidencia que ainda não foram incorporadas políticas específicas de cibersegurança, proteção de dados ou conformidade com a LGPD no arcabouço legislativo local. A Lei Orgânica do Município (1990) trata de aspectos gerais de organização administrativa e direitos dos cidadãos, mas não apresenta dispositivos voltados à segurança da informação. A Lei Complementar nº 29/2020, que institui o Plano Diretor Municipal, e a Lei Ordinária nº 2.722/2015, que aprova o Plano Municipal de Educação, fazem referência ao uso de tecnologias em suas áreas de atuação, mas não contemplam diretrizes sobre segurança digital ou proteção de dados. A Lei Complementar nº 15/2016, que estabelece a estrutura organizacional da prefeitura, e a Lei Complementar nº 36/2022, voltada à gestão ambiental, também não integram medidas de governança digital ou protocolos de segurança informacional em suas disposições. Esse cenário revela uma lacuna regulatória importante diante das exigências impostas pelas políticas nacionais de proteção de dados. No entanto, as normativas existentes fornecem base administrativa para a inclusão de diretrizes de segurança da informação nos processos urbanos, educacionais, ambientais e organizacionais, o que permitiria ao município avançar em maturidade institucional frente aos desafios da transformação digital.

A análise das legislações dos doze municípios que compõem a AMREC confirma um diagnóstico preocupante: mesmo diante da crescente digitalização da gestão pública e da obrigatoriedade imposta por marcos regulatórios federais como a LGPD, nenhum dos municípios apresenta um arcabouço normativo consolidado sobre cibersegurança, proteção de dados ou governança da informação. Embora algumas leis abordem, tangencialmente, o uso de tecnologias em setores como educação ou planejamento urbano, elas não incorporam diretrizes de segurança digital, protocolos de resposta a incidentes ou políticas estruturadas de capacitação e controle. A ausência de normatização é acompanhada por uma fragilidade institucional

crônica, expressa na inexistência de estruturas técnicas dedicadas, na dependência operacional de fornecedores privados e na ausência de políticas públicas voltadas ao fortalecimento da maturidade cibernética local.

Esse cenário revela um descompasso entre a velocidade da transformação digital dos serviços públicos e a capacidade institucional dos municípios para garantir segurança, legalidade e soberania informacional. A inexistência de políticas locais de cibersegurança não é apenas um problema técnico, mas um desafio de governança, com implicações diretas sobre os direitos fundamentais dos cidadãos, a integridade das informações públicas e a confiança nas instituições. Frente a esse panorama, a AMREC pode assumir papel estratégico ao induzir a construção de diretrizes regionais de proteção digital, promover capacitação técnica conjunta, apoiar a elaboração de normativas locais e articular soluções cooperadas que fortaleçam a resiliência cibernética dos municípios consorciados. O fortalecimento da cibersegurança no plano local requer, portanto, ações coordenadas, estruturação de capacidades e reconhecimento da segurança da informação como política pública essencial à gestão democrática, transparente e confiável dos territórios.

4.4.2 Diagnóstico dos municípios da AMREC sobre cibersegurança

Esta etapa qualitativa da pesquisa foi conduzida por meio da aplicação de um questionário estruturado com perguntas abertas, direcionado a representantes da área de tecnologia da informação, planejamento, administração, jurídica ou controladoria dos municípios da AMREC. O instrumento foi organizado em cinco blocos temáticos e um bloco de encerramento, com o objetivo de captar percepções institucionais e operacionais relacionadas à cibersegurança no contexto municipal. Cada bloco foi construído com base em referenciais teóricos consolidados, buscando explorar desde as capacidades organizacionais internas até os aspectos de governança, infraestrutura tecnológica, articulações intermunicipais e barreiras institucionais. O uso de perguntas abertas permitiu a identificação de práticas, desafios e interpretações locais, ampliando o entendimento sobre como a cibersegurança é percebida e implementada nas diferentes gestões.

O primeiro bloco investigou a capacidade institucional e organizacional dos municípios, com base em autores como Hall e Taylor (1996), Oliveira *et al.* (2020) e Dunn Cavelty (2019), enfatizando a profissionalização das equipes e os limites institucionais existentes. O segundo bloco abordou a governança digital e a normatização local, apoiando-se em Cravo (2023), Akdemir e Law (2021) e novamente Dunn Cavelty (2019), para analisar a

existência de políticas locais, sua implementação e articulação com legislações superiores. O terceiro bloco, por sua vez, explorou a infraestrutura tecnológica e as práticas operacionais dos municípios, dialogando com Stigler (1971), Posner (1974), Torres (2012), Zuboff (2019), Nissenbaum (2005) e Taddeo e Floridi (2018), a fim de compreender o grau de autonomia e as práticas de resiliência digital. O quarto bloco focalizou a cooperação intermunicipal e as redes colaborativas, com base em Shackelford, Russell e Kuehn (2020) e Calzada (2020), avaliando formas de colaboração regional. Por fim, o quinto bloco abordou as barreiras institucionais e as percepções políticas sobre a cibersegurança, com apoio teórico em Lipsky (2010), Martin (2021) e Dunn Cavelty (2019), revelando os conflitos entre segurança, transparência e inclusão. O bloco de encerramento buscou capturar avaliações finais e recomendações dos entrevistados, conectando diretamente a temática da cibersegurança com o desenvolvimento municipal.

Quadro 19 – Instrumento de pesquisa – objetivos de análise

Bloco temático	Objetivo
Capacidade Institucional e Organizacional	Investigar a estrutura administrativa e a qualificação das equipes responsáveis pela segurança digital no âmbito municipal, bem como as estratégias de capacitação e gestão interna.
Governança Digital e Normatização Local	Analisar a existência, implementação e alcance de normas e políticas públicas voltadas à cibersegurança nos municípios, incluindo a integração com legislações superiores.
Infraestrutura Tecnológica e Práticas Operacionais	Compreender os procedimentos técnicos adotados para proteção digital e verificar a autonomia ou dependência tecnológica das gestões locais.
Cooperação Intermunicipal e Redes Colaborativas	Identificar articulações regionais para a cibersegurança, trocas de experiências e iniciativas colaborativas entre municípios.
Barreiras Institucionais e Percepções	Captar percepções dos gestores sobre obstáculos enfrentados, prioridades políticas e valores subjacentes às decisões de cibersegurança.
Encerramento da Entrevista	Captar a avaliação dos entrevistados sobre a relação entre cibersegurança e desenvolvimento do município, além de reunir recomendações para fortalecer essa área nas gestões locais.

Fonte: Elaborado pelo autor (2025).

O Bloco 1 teve como objetivo investigar a estrutura administrativa e a qualificação das equipes responsáveis pela segurança digital nos municípios, bem como as estratégias de capacitação e gestão interna. As respostas evidenciam um quadro institucional heterogêneo e, em grande parte, fragilizado, em consonância com o que apontam Oliveira *et al.* (2020) sobre a fragilidade institucional nos municípios brasileiros. A ausência de equipes formalizadas é um padrão recorrente. Como afirmou um respondente: “Infelizmente, não temos uma equipe formada responsável, conforme prevê a LGPD.” Já outro apontou: “Não existe uma equipe de cibersegurança formalizada [...] Não é uma função reconhecida, e muito menos oficial.”

A comparação entre os relatos revela que a maior parte dos municípios opera com equipes reduzidas, frequentemente formadas por um ou dois profissionais, em que a segurança

digital é apenas uma das muitas atribuições. Um entrevistado relatou: “Somos hoje apenas dois profissionais originalmente de nível técnico [...] com ativo de mais de 200 dispositivos da gestão pública.” Outro reforça: “Atualmente contamos com três funcionários no setor de TI.” Tal realidade se distancia do modelo de profissionalização da burocracia proposto por Hall e Taylor (1996), o qual destaca a importância de estruturas institucionais estáveis e qualificadas para o bom funcionamento das políticas públicas.

Diante dessa limitação estrutural, os desafios operacionais sobressaem nas falas dos participantes. Em diversos casos, a sobrecarga de trabalho é citada como um dos principais entraves à qualificação e à gestão segura das informações. Como pontuado por um dos profissionais: “O principal desafio ainda é a questão dos próprios servidores no sentido de educação a respeito de segurança da informação [...] muitos profissionais acabam acostumando a trabalhar com senhas mais simples.” Esse relato ressoa com a crítica de Dunn Cavelty (2019) ao excesso de confiança em soluções tecnológicas desprovidas de políticas institucionais e capacitação.

No que se refere à capacitação continuada, as respostas são majoritariamente negativas. Muitos municípios declaram não possuir ações formais, como ilustra uma das falas: “Não tem, por não ser uma equipe interna.” ou ainda: “Infelizmente não temos [capacitação].” Apenas dois respondentes indicaram práticas de formação contínua, geralmente vinculadas a eventos externos ou iniciativas isoladas: “Realizamos ações de capacitação com treinamentos regulares focados no uso seguro dos sistemas.” e “Estamos sempre à procura de novos cursos [...] algumas que o município paga e outras a gente corre atrás pro nosso conhecimento pessoal.” Essas iniciativas, ainda que positivas, são insuficientes para garantir uma política de formação institucionalizada, como recomendam os autores mencionados.

A ausência de rotinas padronizadas ou avaliações formais relacionadas à segurança digital é outro ponto que se repete nos relatos. Um respondente afirma: “Não, não existe isso. E também não vai existir essa maturidade na maioria dos entes da gestão pública.” Outro pontua: “A gestão não realiza avaliação formal, mas será questão de pouco tempo [...] o TCE já está indicando cobranças num futuro próximo.” Esse padrão denota uma fragilidade normativa e operacional que dificulta o avanço da segurança digital como política pública consistente. A exceção está em poucos casos que relataram simulações de *phishing*, notificações formais e planos em elaboração, mas sem consolidação de uma rotina institucional.

No conjunto, as respostas indicam que a segurança digital nos municípios analisados ainda é tratada como responsabilidade técnica isolada, sem o devido reconhecimento organizacional ou prioridade política. Isso se alinha com a leitura de Dunn Cavelty (2019) sobre

os limites institucionais e os arranjos informais que predominam em muitas gestões públicas. A tentativa de superação dessas limitações aparece de forma incipiente em alguns municípios por meio de associações profissionais, planos de cargos e salários ou movimentos por formalização de cargos estratégicos, como apontado por um dos entrevistados: “Solicitei a volta do diretor de TI [...] precisamos de um profissional para dar segmento a essa demanda.”

Há entre os respondentes uma consciência crescente da necessidade de mudanças estruturais, embora ainda limitada pela precarização das estruturas institucionais. A fala de um participante resume bem essa tensão: “Estamos lutando para mudar esse cenário. Estamos tentando mudar isso da melhor forma possível.” Essa constatação reforça o diagnóstico de Oliveira *et al.* (2020) de que a transformação institucional nos municípios depende de reformas profundas e sustentadas, que vão além do esforço individual dos técnicos.

A definição dos níveis de maturidade institucional — muito baixa, baixa, média ou alta — atribuídos aos municípios no Quadro 19 e nos quadros subsequentes foi realizada com base na análise qualitativa das respostas obtidas nas entrevistas semiestruturadas. Essa classificação levou em consideração a presença ou ausência de políticas, estruturas e práticas relacionadas à cibersegurança, bem como a profundidade, regularidade e abrangência dessas ações. Municípios classificados com maturidade muito baixa demonstraram inexistência total de iniciativas estruturadas, desconhecimento sobre marcos legais e ausência de qualquer protocolo de segurança da informação. A maturidade baixa foi atribuída a municípios que apresentaram ações pontuais ou incipientes, geralmente reativas e sem respaldo normativo ou institucional claro. A classificação média correspondeu a contextos nos quais havia certo grau de institucionalização, como a presença de normas internas, servidores designados para a área ou iniciativas de capacitação, ainda que fragmentadas ou limitadas. Já a maturidade alta deveria ser atribuída a municípios que demonstrassem práticas consolidadas, alinhadas a diretrizes nacionais ou internacionais, com estruturas normativas ativas, equipes qualificadas e integração com políticas mais amplas de governança digital, porém esse nível não foi identificado em nenhum município. Essa tipologia não pretende esgotar a complexidade do fenômeno, mas oferecer uma referência interpretativa coerente com as evidências empíricas levantadas.

Quadro 20 – Matriz de Evidência – Bloco 1

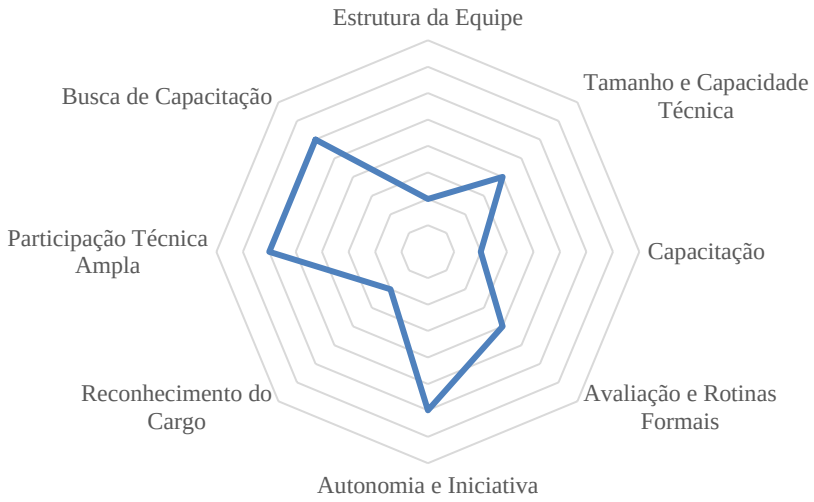
Categoria Temática	Falas Representativas (empíricas)	Análise/Observação	Status
Estrutura da Equipe	*“Não há exatamente equipe estruturada para segurança de informação, sendo responsabilidade dos diversos setores respeitar as normas básicas.”*	Atribuições descentralizadas e difusas, com ausência de estrutura formal. Reforça a informalidade institucional.	Muito Baixa

Categoria Temática	Falas Representativas (empíricas)	Análise/Observação	Status
Tamanho e Capacidade Técnica	*"Nós temos três na administração e cuidando de todas as secretarias, exceto da saúde."*	Indicativo de equipe pequena frente à demanda, com divisão improvisada de responsabilidades.	Baixa
Capacitação	*"Capacidade por parte da administração não existe para nosso setor [...] na administração é um setor que não fazem isso muito não."*	Reforça a negligência institucional com capacitação da área de TI, mesmo quando outras áreas são contempladas.	Muito Baixa
Avaliação e Rotinas Formais	*"Isso é uma falha, a gente não tem protocolado, a gente resolve a situação [...] só que não tem um protocolo padrão."*	A ausência de rotinas ou protocolos formais leva à atuação reativa, não preventiva — limita a gestão de riscos.	Baixa
Autonomia e Iniciativa	*"Eu explico pro Samai: houve uma mudança, tô te notificando [...] muitas vezes mando por e-mail para ter uma confirmação."*	Iniciativas individuais de controle e notificação substituem mecanismos institucionais. Demonstra esforço, mas revela carência organizacional.	Média
Reconhecimento do Cargo	*"Foi um cargo extinto pela gestão anterior, um grande revés. E este cargo não é ocupado há 10 anos."*	Reflexo de descontinuidade administrativa e negligência com cargos estratégicos, dificultando consolidação de políticas de cibersegurança.	Muito Baixa
Participação Técnica Ampla	*"A segurança da informação é coordenada pelas Secretarias e Fundações, com a participação da Procuradoria e do Órgão Central do Sistema de Controle Interno."*	Indica tentativa de estruturação em rede institucional, o que demonstra preocupação com governança interna, ainda que possivelmente fragilizada por ausência de recursos.	Média
Busca de Capacitação	*"Eu tô sempre à procura de novos cursos [...] tem algumas que o município paga e outras a gente corre atrás pro nosso conhecimento pessoal mesmo."*	Demonstra proatividade individual para suprir a ausência de política de formação institucionalizada.	Média

Fonte: Elaborado pelo autor (2025).

As evidências levantadas no Bloco 1 revelam que a maioria dos municípios ainda se encontra em estágios iniciais ou muito incipientes no que se refere à institucionalização da cibersegurança. A inexistência de equipes formalizadas, a carência de capacitação continuada e a ausência de rotinas padronizadas expõem limitações estruturais que comprometem a resiliência digital local. Embora algumas iniciativas individuais apontem para esforços relevantes, como a busca autônoma por capacitação e notificações informais de incidentes, elas não substituem políticas públicas robustas nem asseguram a continuidade administrativa, conforme sugerem Hall e Taylor (1996) e Dunn Cavelty (2019). A heterogeneidade das respostas reforça o diagnóstico de fragilidade institucional descrito por Oliveira *et al.* (2020), destacando que, sem reformas internas mais profundas, a segurança da informação continuará sendo uma função marginalizada nas gestões públicas municipais.

Figura 6 – Status de maturidade - Capacidade Institucional e Organizacional



Fonte: Elaborado pelo autor (2025).

O gráfico do bloco 1 – Capacidade Institucional e Organizacional revela um padrão de maturidade predominantemente baixa, com algumas exceções pontuais. Os pontos mais críticos estão na categoria “Reconhecimento do Cargo”, que apresenta o menor valor, indicando uma ausência de valorização institucional da função exercida pelos profissionais da área de tecnologia. Isso está em consonância com os relatos qualitativos, nos quais os entrevistados mencionaram a falta de cargos formais, planos de carreira e respaldo político para suas atividades. Tal invisibilidade institucional compromete diretamente a capacidade do setor de assumir um papel estratégico na administração pública, como argumentam Oliveira *et al.* (2020) e Hall & Taylor (1996).

Por outro lado, os indicadores “Autonomia e Iniciativa” e “Busca de Capacitação” aparecem com pontuações mais elevadas, sugerindo que, apesar da fragilidade estrutural, há movimentos individuais de aprimoramento e engajamento técnico. Essa assimetria revela uma dependência das ações voluntárias e do esforço pessoal dos profissionais, o que corrobora a ideia de que a maturidade organizacional em cibersegurança, nesse contexto, ainda não está institucionalizada, mas sustentada por indivíduos que atuam de forma proativa. Essa condição reflete o que Lipsky (2010) chamou de "trabalhadores de rua", agentes que compensam falhas estruturais com ações adaptativas no cotidiano institucional.

O eixo referente à “Participação Técnica Ampla” e à “Avaliação e Rotinas Formais” também mostra níveis intermediários, sugerindo a existência parcial de processos que incluem a área técnica na tomada de decisões ou que adotam algumas práticas sistematizadas de gestão. No entanto, os dados empíricos revelam que essa participação é pontual e frequentemente

reativa, o que limita a consolidação de rotinas de governança digital. Sem processos institucionalizados, qualquer avanço permanece vulnerável à descontinuidade administrativa.

Já as categorias “Estrutura da Equipe” e “Capacitação” mantêm níveis baixos, evidenciando a dificuldade dos municípios em compor equipes minimamente dimensionadas e qualificadas para lidar com a complexidade da segurança digital. Isso reforça o argumento de que a limitação técnica não decorre apenas da escassez de recursos, mas da ausência de prioridade institucional, como discutido na análise qualitativa do bloco.

O gráfico traduz visualmente uma realidade já evidenciada nos dados empíricos: a presença de iniciativas individuais e isoladas em um contexto institucional fragilizado, com pouca valorização da área de TI e ausência de estruturas permanentes. Essa configuração torna a maturidade institucional dependente de pessoas, e não de sistemas, o que compromete a continuidade e a efetividade das ações em cibersegurança no nível municipal.

Esses limites estruturais apontados no bloco 1 revelam um terreno institucional ainda frágil para a consolidação da cibersegurança como política pública. A ausência de valorização da área técnica impacta diretamente a capacidade normativa e jurídica dos municípios, tema que será aprofundado no bloco seguinte, ao se analisar a presença (ou ausência) de instrumentos formais de governança digital e adequação à LGPD.

O segundo bloco da entrevista buscou analisar a existência, implementação e alcance de normas e políticas públicas voltadas à cibersegurança nos municípios, bem como sua articulação com legislações superiores, como a LGPD. De forma geral, as respostas revelam um cenário marcado pela ausência de normativas específicas, pela baixa institucionalização da governança digital e pela fragilidade no alinhamento com marcos legais nacionais. Em grande parte dos municípios, a governança da segurança da informação ocorre sem base normativa consistente, o que reforça o diagnóstico de Dunn Cavelty (2019) sobre o descompasso entre a complexidade dos riscos digitais e a precariedade das estruturas normativas locais.

A primeira pergunta do bloco evidencia a lacuna regulatória: a maioria dos respondentes afirmou não possuir normativas próprias sobre segurança da informação ou cibersegurança. Quando há alguma menção normativa, trata-se de decretos antigos e genéricos. Um exemplo é a fala: “Tem um decreto ali que fala um pouco a respeito do uso dos equipamentos na prefeitura, mas é um decreto antigo [...] precisaria de um plano diretor de segurança da informação.” Essa constatação reforça o que aponta Cravo (2023): os municípios tendem a reproduzir normativas de outros entes públicos, sem ajustá-las ao seu contexto institucional e sem internalizar seus princípios.

A elaboração e a implementação prática das normas também se mostram frágeis. Há casos em que o decreto existente foi copiado de outro município, como relatou um entrevistado: “Foi uma cópia de uma outra prefeitura. Copiaram e lançaram.” Essa prática revela não apenas a limitação técnica para produção normativa, mas também uma ausência de participação e construção institucional, o que esvazia o conteúdo e enfraquece sua legitimidade. Akdemir e Law (2021) já advertiam que a governança digital precisa ser construída com base em processos participativos e adaptativos, algo ainda distante da realidade apresentada pelos municípios entrevistados.

Sobre a articulação com legislações superiores, como a LGPD, os relatos variam, mas apontam majoritariamente para um desconhecimento institucional ou ações muito incipientes. Um dos participantes afirmou: “Hoje nós do TI pelo menos não estamos sabendo disso. Se existe, não soubemos.” Já outro indicou o início de um processo normativo com base na LGPD, por meio de decreto: “O Decreto nº 285/2024 expressamente regulamenta a aplicação da LGPD [...] transformando seus preceitos gerais em normas operacionais específicas, ajustadas à realidade local.” Esta última resposta representa uma exceção no conjunto e reflete uma tentativa mais madura de construção normativa com respaldo legal.

A distribuição de responsabilidades também se apresenta como um ponto crítico. Em muitos casos, não há clareza institucional sobre quem é responsável por implementar, fiscalizar ou aplicar normas de segurança digital. Como exemplificado: “Não há distribuição ainda.” Ou ainda: “A gente vai se atualizando por conta, muita coisa a gente faz já fora das atribuições.” Isso evidencia um vazio de governança, reforçando o que Dunn Cavelty (2019) chama de "gestão por omissão", onde os riscos digitais não são devidamente distribuídos nem enfrentados como política pública integrada.

Em contraste, algumas respostas mostram ensaios de estruturação mais formalizada. Em um dos casos, há menção clara à atuação coordenada entre alta gestão, setores técnicos e fornecedores, com definição de papéis e responsabilidades no tratamento de dados pessoais, conforme o decreto local. Essa modelagem aproxima-se do que preconiza a literatura sobre governança multinível e corresponsabilização institucional. Contudo, trata-se de uma exceção, o que reforça a desigualdade institucional entre os municípios.

Portanto, a análise deste bloco confirma que a maturidade normativa e de governança digital nos municípios ainda é baixa. A ausência de normas específicas, a pouca articulação com legislações federais e a indefinição de atribuições institucionais limitam severamente a capacidade de implementação de políticas efetivas de segurança da informação. A maioria das práticas é informal, baseada em esforços individuais, ou ainda restrita a ações

paliativas, com raríssimos casos que demonstram um alinhamento mais estruturado e normativo.

Quadro 21 – Matriz de Evidência – Bloco 2

Categoria Temática	Falas Representativas (empíricas)	Análise/Observação	Status
Existência de Normativas	*"Não existe."* / *"Tem um decreto, mas é antigo e desatualizado."*	A ausência de normativas próprias ou a presença de decretos genéricos e defasados é predominante. Há dependência de modelos externos e falta de atualização.	Muito Baixa
Elaboração das Normas	*"Foi uma cópia de uma outra prefeitura."*	Normas muitas vezes são copiadas, sem elaboração participativa ou técnica local. Isso compromete a legitimidade e a efetividade das regulamentações.	Muito Baixa
Integração com a LGPD	*"Possui apenas o agente nomeado e está buscando informações para implantação."*	Indica início muito incipiente da articulação com a LGPD. Em geral, há desconhecimento sobre os preceitos legais e ausência de ações de adequação.	Baixa
Responsabilidade Institucional	*"O cargo da analista tem determinadas atribuições [...] já estão defasadas [...] a gente vai se atualizando por conta."*	Cargos técnicos acumulam responsabilidades sem atualização institucional. A gestão do risco digital é informal e desprovida de suporte normativo atualizado.	Baixa
Governança Estruturada	*"As responsabilidades pela aplicação da LGPD são distribuídas de forma coordenada entre a alta gestão, os setores técnicos e os fornecedores."*	Exemplo isolado de governança normatizada com atribuições definidas, demonstrando modelo potencialmente replicável para os demais entes.	Baixa
Percepção Institucional	*"A gente não tem isso ainda. Mas o TCE já está indicando cobranças num futuro próximo."*	Ainda que incipiente, essa percepção aponta para uma consciência emergente sobre a necessidade de avançar na formalização normativa da cibersegurança.	Média

Fonte: Elaborado pelo autor (2025).

A análise do Bloco 2 evidencia que a governança digital e a normatização da cibersegurança nos municípios ainda se encontram em um estágio predominantemente incipiente. A ausência de normativas específicas, a utilização de decretos genéricos e desatualizados, bem como a fragilidade na articulação com legislações superiores como a LGPD, apontam para uma lacuna crítica na capacidade regulatória local. Embora uma ou outra resposta demonstre esforços mais estruturados de conformidade legal e distribuição de responsabilidades, esses casos são claramente exceções. O que prevalece é uma gestão marcada por informalidade, reprodução normativa sem contextualização e indefinição de papéis institucionais, elementos que comprometem o avanço da segurança digital como política pública. A governança da cibersegurança ainda depende fortemente da iniciativa de indivíduos

ou setores isolados, carecendo de respaldo jurídico, planejamento estratégico e coordenação multissetorial, como defendem Cravo (2023), Akdemir e Law (2021) e Dunn Cavelty (2019).

Figura 7 – Status de maturidade - Governança Digital e Normatização Local

Fonte: Elaborado pelo autor (2025).

O gráfico do bloco 2 – Governança Digital e Normatização Local revela um padrão de maturidade institucional baixa e desigual, com destaque negativo para a "Existência de Normativas" e a "Elaboração das Normas", que aparecem com os menores valores. Esses resultados reforçam o achado da análise qualitativa, segundo o qual a maioria dos municípios ainda opera sem marcos normativos específicos voltados à cibersegurança ou à proteção de dados, limitando-se a decretos amplos ou desatualizados. A ausência dessas normativas compromete tanto a segurança jurídica das ações administrativas quanto a capacidade de resposta frente a incidentes, como discutido por Dunn Cavelty (2019).

A "Integração com a LGPD" e a "Responsabilidade Institucional" apresentam um nível um pouco mais elevado, mas ainda restrito, indicando que alguns municípios iniciaram tentativas de adequação à Lei Geral de Proteção de Dados, embora sem estruturação robusta ou clareza sobre os atores responsáveis. Esse quadro reflete o que Taddeo e Floridi (2018) classificam como um estágio de governança reativa, em que as ações são motivadas por pressões externas ou exigências legais, e não por uma política pública planejada e integrada.

A categoria "Governança Estruturada", por sua vez, aparece com baixa maturidade, sinalizando que mesmo onde há alguma percepção institucional sobre a importância da cibersegurança, ela ainda não se traduz em estruturas estáveis ou em planos de ação contínuos. Isso corrobora o diagnóstico apresentado por Stigler (1971) e Torres (2012), que apontam para a fragilidade dos arranjos normativos locais diante da assimetria técnica e da dependência de

fornecedores externos, o que, no contexto municipal, gera um ciclo de informalidade e vulnerabilidade institucional.

O ponto mais alto do gráfico é a “Percepção Institucional”, que revela que, apesar da baixa normatização, há um reconhecimento crescente da importância do tema por parte de alguns setores da gestão pública. No entanto, essa percepção ainda é incipiente e pouco operacionalizada, o que gera um descompasso entre intenção e prática. Isso se alinha ao que Martin (2021) descreve como um desafio ético e organizacional: reconhecer os riscos digitais, mas não dispor dos meios institucionais para enfrentá-los adequadamente.

Em síntese, o gráfico do bloco 2 revela um cenário em que a percepção da relevância da cibersegurança avança mais rápido que a estrutura normativa necessária para sustentá-la. O resultado é uma governança digital fragmentada, sem clareza de papéis e com baixa capacidade de institucionalização, o que reforça a vulnerabilidade das administrações municipais diante dos desafios crescentes da era digital. Esse descompasso compromete não apenas a eficácia técnica das ações, mas também a legitimidade e a *accountability* da gestão pública em ambientes digitais.

A fragilidade normativa identificada no bloco 2 compromete diretamente o planejamento e a execução de ações técnicas sustentáveis. Sem marcos legais claros, as práticas operacionais ficam sujeitas à informalidade e à improvisação. Esse desdobramento é explorado no bloco 3, que examina o grau de maturidade técnica e a autonomia dos municípios na gestão de sua infraestrutura digital.

O bloco 3 teve como objetivo compreender os procedimentos técnicos adotados para proteção digital nos municípios e verificar o grau de autonomia ou dependência tecnológica das gestões locais. As respostas revelam que, embora haja uso pontual de ferramentas técnicas, como firewall e backup em nuvem, a maioria das prefeituras não dispõe de práticas sistematizadas, tampouco de planos de contingência, resposta a incidentes ou rotinas de atualização bem definidas. A segurança digital é, na prática, reativa e fragmentada, o que contribui para uma postura de vulnerabilidade estrutural frente aos riscos cibernéticos, conforme alertam Taddeo e Floridi (2018).

Quanto às práticas técnicas declaradas, destaca-se o uso de ferramentas mínimas, como backup e firewall. Um entrevistado relatou: “Firewall (Ostec), Backup nuvem (Box Tecnologia).” Outro declarou: “Apenas backup e utilização de senhas básicas.” Embora esses elementos sejam relevantes, a ausência de autenticação multifator, criptografia de dados sensíveis ou segmentação de redes expõe os limites operacionais das prefeituras. Como discutem Zuboff (2019) e Nissenbaum (2005), a segurança da informação não se sustenta

apenas em ferramentas pontuais, mas requer um ecossistema de proteção, governado por princípios de privacidade contextual e responsabilidade institucional.

No que se refere à existência de procedimentos formais para resposta a incidentes, a resposta é quase unânime: não existem. Um dos participantes foi direto: “Não existe.” Outro respondeu: “Não temos ainda um plano de contingência. Estamos em processo de levantamento.” Essa carência de protocolos demonstra que a gestão da segurança é baseada na resolução pontual de falhas, sem mecanismos de prevenção, monitoramento ou mitigação de riscos. Esse modelo improvisado contraria os princípios de resiliência digital e de ética da informação, defendidos por Taddeo e Floridi (2018), que destacam a necessidade de preparar os sistemas públicos para a inevitabilidade dos incidentes, reduzindo impactos e restaurando rapidamente a operação.

A autonomia técnica dos municípios para gerir sua própria infraestrutura digital é limitada. Diversos respondentes afirmam depender quase integralmente de fornecedores externos para manutenção, atualização e operação dos sistemas. Uma das falas ilustra esse cenário: “Não, depende do fornecedor.” Em outro caso: “A atualização e testes de protocolos não são documentados, ocorrem de forma informal e dependem do suporte contratado.” Essa dependência tecnológica reforça o que Stigler (1971) e Posner (1974) apontam como risco de captura regulatória: quando o poder público perde a capacidade de fiscalizar ou direcionar os serviços prestados, ficando à mercê das decisões técnicas de fornecedores privados.

Ainda mais crítico é o fato de que, mesmo quando existe algum grau de autonomia operacional, os processos são informais ou inexistem. Um entrevistado relatou: “Não existe teste, não existe controle. É um risco grande que nós temos.” Isso revela a presença de vazios operacionais, que dificultam a rastreabilidade de incidentes, a recuperação de dados e a responsabilização em caso de falhas. Segundo Torres (2012), essa situação aprofunda a assimetria entre as instituições públicas e os atores do mercado digital, limitando a governança da tecnologia.

Por outro lado, alguns poucos municípios demonstraram certo grau de organização, ainda que incipiente. Um participante apontou: “Estamos estudando uma forma de ter o próprio domínio do município, com servidores internos.” Essa iniciativa aponta para uma preocupação com soberania digital, tema debatido por autores como Zuboff (2019) e Calzada (2020). Ainda assim, trata-se de exceção e não de regra entre os municípios entrevistados.

Esses relatos confirmam a existência de uma infraestrutura tecnológica vulnerável, sustentada por soluções mínimas, dependência de terceiros e ausência de protocolos formais. A governança operacional da cibersegurança municipal ainda não se consolidou como uma

política pública sistematizada, o que fragiliza a proteção de dados e impede o desenvolvimento de práticas éticas e resilientes no setor público.

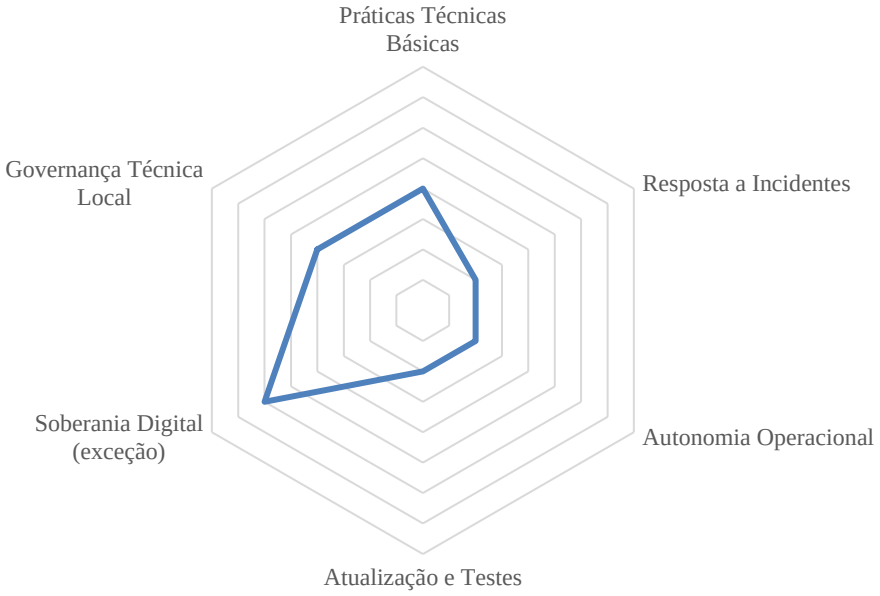
Quadro 22 – Matriz de Evidência – Bloco 3

Categoria Temática	Falas Representativas (empíricas)	Análise/Observação	Status
Práticas Técnicas Básicas	*"Utilizamos backup, antivírus, firewall e filtros de conteúdo."*	Adoção de ferramentas básicas, sem integração ou estrutura padronizada. Foco em soluções isoladas, sem abordagem de segurança por camadas.	Baixa
Resposta a Incidentes	*"Não temos nenhum plano de resposta. Se dá um problema, a gente resolve na hora com o suporte."*	Ausência de protocolo formal. Respostas são reativas e dependentes do fornecedor. Falta de capacidade de gestão de crise.	Muito Baixa
Autonomia Operacional	*"Toda infraestrutura digital do município é gerida por empresa terceirizada. Não temos servidores próprios nem equipe capacitada."*	Altíssimo grau de dependência tecnológica, com risco de perda de controle sobre dados públicos e serviços essenciais.	Muito Baixa
Atualização e Testes	*"A gente atualiza quando o sistema exige, mas não temos controle sobre isso."*	Falta de planejamento e de rotinas de atualização. Atualizações são feitas por demanda do fornecedor, sem governança local.	Muito Baixa
Soberania Digital (exceção)	*"Estamos estudando uma forma de ter o próprio domínio do município, com servidores internos."*	Indica preocupação com controle da infraestrutura. Iniciativa promissora, mas ainda em fase exploratória e isolada.	Média
Governança Técnica Local	*"Não existe teste, não existe controle. É um risco grande que nós temos."*	Falta de cultura organizacional de segurança. Gestores reconhecem os riscos, mas não possuem meios institucionais para enfrentá-los.	Baixa

Fonte: Elaborado pelo autor (2025).

A análise do bloco 3 evidencia que os municípios enfrentam sérias limitações no que diz respeito à infraestrutura tecnológica e às práticas operacionais voltadas à cibersegurança. A predominância de soluções técnicas básicas, como backup e firewall, aliada à ausência de protocolos formais de resposta a incidentes e à dependência quase total de fornecedores externos, revela um cenário de vulnerabilidade estrutural. A autonomia técnica é reduzida e, na maioria dos casos, inexistente, o que compromete a capacidade de gestão dos próprios ativos digitais. Como alertam Stigler (1971), Posner (1974) e Torres (2012), essa dependência excessiva transfere o controle da operação pública para o setor privado, reduzindo a soberania informacional dos entes locais. Ainda que algumas poucas iniciativas apontem para tentativas de internalização da infraestrutura e busca por maior controle institucional, estas são pontuais e não representam um padrão. Assim, a segurança digital permanece dissociada de uma política pública sistematizada, sem planejamento, continuidade ou integração com os demais instrumentos de governança municipal.

Figura 8 – Status de maturidade - Infraestrutura Tecnológica e Práticas Operacionais



Fonte: Elaborado pelo autor (2025).

O gráfico do bloco 3 – Infraestrutura Tecnológica e Prática Operacional apresenta um perfil de maturidade técnica marcadamente baixa, mas com dois polos distintos de comportamento. Por um lado, a categoria “Práticas Técnicas Básicas” aparece com a maior pontuação entre os itens avaliados, sugerindo que os municípios mantêm, ainda que de forma não estratégica, ações operacionais elementares, como backups, antivírus e manutenção mínima da rede. Isso indica que a TI local consegue sustentar a continuidade dos serviços digitais no cotidiano, mesmo sem planejamento formalizado.

Por outro lado, as categorias “Atualização e Testes”, “Autonomia Operacional” e “Resposta a Incidentes” apresentam os menores níveis de maturidade. Isso confirma os achados qualitativos de que os municípios raramente testam seus sistemas ou realizam simulações de incidentes, e que a resposta a ataques cibernéticos tende a ser improvisada ou dependente de terceiros. Essa lacuna entre operação básica e resposta a crise reflete um ambiente altamente vulnerável, que Taddeo e Floridi (2018) descrevem como tecnicamente funcional, mas institucionalmente frágil em termos de resiliência.

A categoria “Governança Técnica Local” aparece com maturidade intermediária, apontando que há certo nível de organização técnica, geralmente concentrado em profissionais experientes, mas ainda sem autonomia decisória nem recursos suficientes. A baixa pontuação em “Autonomia Operacional” reforça esse ponto, pois evidencia que, mesmo havendo domínio técnico, as decisões estratégicas são tomadas externamente, seja por fornecedores terceirizados,

seja por instâncias administrativas alheias à área de TI — um cenário que remete à dependência tecnológica descrita por Zuboff (2019) e Torres (2012).

A “Soberania Digital (exceção)” é um caso isolado de maturidade mais elevada neste bloco, representando uma única experiência municipal que opera com maior controle sobre sua infraestrutura e dados. Essa exceção é reveladora porque mostra que, mesmo em contextos adversos, é possível desenvolver soluções locais mais autônomas e resilientes — o que se conecta à proposta de governança descentralizada de Calzada (2020). No entanto, o fato de esse caso ser isolado reforça o diagnóstico geral de dependência estrutural e falta de planejamento técnico na maior parte dos municípios.

O gráfico do bloco 3 evidencia um cenário no qual os municípios realizam o mínimo necessário para manter suas operações digitais em funcionamento, mas sem estratégias preventivas, testes de robustez ou governança técnica consolidada. A maturidade técnica é reativa e fragmentada, o que os torna altamente expostos a falhas e ataques — e revela, novamente, a urgência de transformar a cibersegurança em uma política pública estruturada, e não apenas uma função técnica operacional.

O padrão de dependência tecnológica e a carência de governança técnica observados no bloco 3 tornam ainda mais urgente a articulação de soluções cooperativas entre municípios. Diante de limitações compartilhadas, a formação de redes e consórcios se torna uma estratégia potencial para fortalecer capacidades locais. O próximo bloco analisa justamente essa dimensão colaborativa e sua atual configuração na região.

O objetivo do bloco 4 foi identificar a existência de articulações regionais voltadas à cibersegurança, por meio da participação dos municípios em redes, fóruns ou consórcios, bem como avaliar a troca de experiências e as iniciativas colaborativas no território. As respostas, de forma geral, revelam um cenário de isolamento institucional, com baixíssima integração regional para o tema da segurança digital. A maioria dos municípios afirma não participar de nenhuma rede estruturada, o que contraria as recomendações de autores como Shackelford *et al.* (2020), que apontam a cooperação regional como um eixo estratégico para o fortalecimento da resiliência cibernética em governos locais.

A primeira pergunta do bloco teve respostas marcadamente negativas. Vários participantes afirmaram de forma direta: “Não.” ou “Não participa de nenhuma rede ou consórcio.” A ausência de pertencimento a redes intermunicipais, fóruns técnicos ou consórcios dedicados à segurança da informação indica uma desconexão institucional que compromete a capacidade dos municípios de aprender coletivamente e compartilhar soluções.

Mesmo em contextos nos quais os municípios participam de associações regionais mais amplas, como associações de municípios, não há estruturação de espaços técnicos voltados especificamente à cibersegurança. Um entrevistado relata: “Participei de uma reunião no Colegiado da AMREC. Porém, não havia nada voltado à segurança digital.” Outro afirma: “Estamos em um grupo que está iniciando os trabalhos. A ideia é criar um fórum técnico regional.” Esses trechos mostram que, embora o tema esteja começando a surgir nas pautas institucionais coletivas, ainda não existe um ambiente colaborativo consolidado, tampouco ações práticas entre os municípios.

A ausência de cooperação também se reflete na falta de troca de experiências e na construção coletiva de soluções. Como afirmou um dos respondentes: “Tudo é feito de forma isolada. Quando há troca, é por contato pessoal.” Esse tipo de colaboração informal e espontânea não se configura como uma política pública de cooperação, mas sim como um recurso individualizado que depende da iniciativa de servidores específicos. Tal realidade confirma a advertência de Shackelford *et al.* (2020) sobre a dificuldade de municípios pequenos desenvolverem sozinhos sua estrutura de defesa digital, recomendando, portanto, consórcios de cibersegurança como alternativa viável.

No entanto, algumas falas revelam um interesse emergente na cooperação regional. Um participante compartilha: “Estamos tentando propor para a AMREC a criação de um grupo específico de TI para discutir essas demandas.” Outro menciona: “Existe uma conversa inicial para a criação de uma rede entre os municípios, mas nada formal ainda.” Essas manifestações indicam um potencial latente para a formação de redes colaborativas, embora ainda dependam de liderança institucional e vontade política para se efetivarem.

É importante destacar que a inexistência de redes regionais prejudica não apenas a eficiência da gestão da cibersegurança, mas também a capacidade dos municípios de negociar com fornecedores, compartilhar ferramentas, padronizar normativas e se preparar conjuntamente para riscos cibernéticos. Como reforça Calzada (2020), a fragmentação das soluções e o individualismo institucional são barreiras à constituição de territórios digitais resilientes.

Em resumo, o bloco 4 evidencia uma lacuna crítica na cooperação intermunicipal. A falta de redes técnicas e fóruns de discussão impede a construção de uma governança regional da segurança digital, isolando os municípios em práticas improvisadas e desiguais. Embora haja uma percepção crescente da necessidade de colaboração, essa intenção ainda não se traduziu em arranjos institucionais consolidados, o que limita o avanço da cibersegurança como estratégia territorial compartilhada.

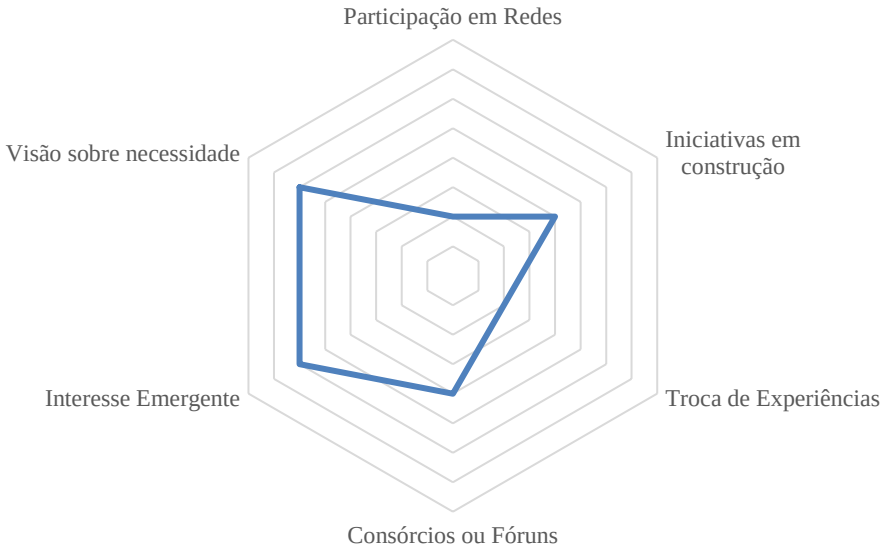
Quadro 23 – Matriz de Evidência – Bloco 4

Categoria Temática	Falas Representativas (empíricas)	Análise/Observação	Status
Participação em Redes	*"Não participa de nenhuma rede ou consórcio voltado à segurança digital."*	A ausência de redes colaborativas entre municípios demonstra isolamento institucional. Não há articulação regional consolidada.	Muito Baixa
Iniciativas em construção	*"Estamos tentando propor para a AMREC a criação de um grupo específico de TI para discutir essas demandas."*	Indica movimentação inicial de articulação. Ainda carece de formalização e estrutura, mas pode evoluir se houver vontade política e liderança institucional.	Baixa
Troca de Experiências	*"Quando há troca, é por contato pessoal ou rede de colegas da área, não institucionalizada."*	Colaborações pontuais e informais entre servidores. Não há processos coletivos nem registros sistematizados de boas práticas.	Muito Baixa
Consórcios ou Fóruns	*"Participei de uma reunião no CISAMREC. Porém, não havia nada voltado à segurança digital."*	Participação institucional ocorre em espaços amplos, mas o tema da segurança digital não está presente na pauta técnica dos consórcios.	Baixa
Interesse Emergente	*"Existe uma conversa inicial para a criação de uma rede entre os municípios, mas nada formal ainda."*	Há percepção sobre a importância da cooperação, mas os arranjos ainda são incipientes. Potencial futuro, mas sem estrutura atual.	Média
Visão sobre necessidade	*"Hoje se tivéssemos um fórum regional, poderíamos até comprar serviços em conjunto e montar protocolos padrão."*	Reconhecimento dos benefícios da articulação regional. Ausência dessa estrutura representa uma oportunidade perdida de ganho de escala e padronização.	Média

Fonte: Elaborado pelo autor (2025).

A análise do bloco 4 evidencia que a cooperação intermunicipal em cibersegurança ainda é praticamente inexistente entre os municípios analisados. A ausência de redes técnicas, fóruns regionais ou consórcios voltados ao tema revela um padrão de isolamento institucional que dificulta o compartilhamento de experiências, a padronização de procedimentos e o fortalecimento conjunto da resiliência digital. Embora alguns respondentes mencionem iniciativas embrionárias ou intenções de articulação, essas propostas ainda carecem de formalização e estrutura. Como alertam Shackelford *et al.* (2020), os municípios, sobretudo os de menor porte, enfrentam limitações que dificilmente serão superadas de forma isolada, tornando a cooperação um caminho estratégico necessário. A falta de uma governança regional integrada para a cibersegurança representa não apenas uma fragilidade técnica, mas também uma barreira ao desenvolvimento de políticas públicas digitais coordenadas, como propõe Calzada (2020) em sua visão de ecossistemas urbanos colaborativos.

Figura 9 – Status de maturidade - Cooperação Intermunicipal e Redes Colaborativas



Fonte: Elaborado pelo autor (2025).

O gráfico do bloco 4 – Cooperação Intermunicipal e Redes de Colaboração revela um quadro em que a percepção sobre a importância da cooperação começa a se formar, mas ainda não se traduz em estruturas concretas de ação conjunta. A categoria com maior pontuação é “Visão sobre necessidade”, indicando que os respondentes reconhecem a relevância de estratégias regionais, consórcios ou redes para tratar da cibersegurança. Esse reconhecimento, embora tardio, é um sinal positivo de conscientização coletiva, mesmo que não acompanhado de ações institucionalizadas — algo que Shackelford *et al.* (2020) colocam como passo inicial para formação de consórcios digitais.

Ainda nesse bloco, as categorias “Interesse Emergente” e “Iniciativas em Construção” aparecem com níveis intermediários, sugerindo que há movimentações pontuais, como a menção a tentativas de cooperação ou participação em eventos regionais. No entanto, essas iniciativas são geralmente desarticuladas, sem cronograma, orçamento ou governança comum, o que impede o fortalecimento de capacidades compartilhadas — elemento que Calzada (2020) considera essencial em contextos de cidades inteligentes e interdependentes.

Em contrapartida, categorias como “Participação em Redes”, “Troca de Experiências” e “Consórcios ou Fóruns” apresentam os menores níveis de maturidade. Esses dados indicam que, na prática, os municípios ainda operam de forma altamente isolada, sem mecanismos regulares de comunicação técnica entre si. A ausência de fóruns permanentes ou de instâncias formais de troca representa um gargalo crítico para municípios pequenos, que individualmente não conseguem sustentar soluções robustas de cibersegurança. Essa carência

fragiliza a construção de uma resiliência territorial integrada, defendida por autores como Taddeo e Floridi (2018).

Esse padrão reflete uma cultura de gestão que ainda vê a cibersegurança como atribuição exclusiva de cada ente, mesmo diante de desafios que extrapolam as fronteiras institucionais locais. Essa desconexão entre percepção e prática coopera para a fragmentação das respostas públicas frente aos riscos digitais e reduz a eficiência coletiva da região. A dificuldade em articular redes ou consórcios se alinha aos achados de Martin (2021), ao evidenciar que, sem incentivos estruturais e coordenação regional, a cooperação segue no campo da intenção.

Em síntese, o gráfico do bloco 4 evidencia que os municípios estão em um estágio embrionário de cooperação regional, marcado por baixa institucionalização e forte assimetria de maturidade. O reconhecimento da importância das redes já existe, mas ainda falta uma estrutura política e operacional para transformar essa percepção em arranjos colaborativos duradouros. Trata-se de um campo com grande potencial de desenvolvimento, mas que exige estímulo externo e mecanismos de coordenação intergovernamental mais claros.

A ausência de estruturas regionais de cooperação em cibersegurança, como revelado no bloco 4, não pode ser dissociada da forma como o tema é percebido e priorizado politicamente pelas gestões locais. O bloco 5 aprofunda essa discussão, focalizando valores, percepções e tensões políticas que influenciam diretamente a condução — ou a omissão — das políticas públicas de segurança digital no território analisado.

O bloco 5 teve como objetivo captar as percepções dos respondentes sobre os principais obstáculos enfrentados para a implementação de políticas de cibersegurança, as prioridades institucionais atribuídas ao tema e as tensões percebidas entre segurança, transparência e inclusão digital. As respostas evidenciam um contexto institucional marcado por limitações estruturais, baixa priorização política da segurança digital e dificuldades na conciliação entre proteção de dados e justiça informacional. Tais elementos remetem diretamente às análises de Lipsky (2010) sobre o comportamento dos implementadores de políticas públicas em contextos de escassez e ambiguidade, e de Martin (2021), que propõe a cibersegurança como um campo permeado por decisões morais e políticas, além de técnicas.

A maioria dos respondentes identifica falta de recursos financeiros, carência de pessoal qualificado e ausência de apoio político como os principais entraves à construção de uma política de cibersegurança efetiva. Uma das falas resume bem essa sobrecarga estrutural: “A TI sempre foi colocada de lado. Só se corre atrás quando há um problema sério.” Essa lógica reativa e fragmentada é coerente com o conceito de “burocracia de rua” de Lipsky (2010), em

que servidores operam sob pressões constantes e tomam decisões pragmáticas frente à falta de condições institucionais adequadas. A precariedade da TI municipal não é apenas técnica, mas política e simbólica: ela ocupa um lugar marginal dentro das prioridades da gestão pública local.

Outros participantes destacam a descontinuidade administrativa e a instabilidade política como barreiras significativas. Um deles afirmou: “A gestão passada acabou com o cargo de direção da TI. A atual está tentando reconstruir, mas há resistência.” Essa oscilação entre gestões reflete a ausência de uma visão estratégica de longo prazo para a área tecnológica, evidenciando como a cibersegurança, mesmo diante da LGPD e de riscos crescentes, ainda não foi incorporada como um tema transversal nas políticas públicas municipais. Como afirma Dunn Cavelty (2019), a segurança digital frequentemente não é tratada como uma questão de governança, mas sim como um problema técnico periférico.

Ao tratar da relação entre segurança e inclusão, as respostas revelam tensões latentes e contradições não resolvidas. Em alguns casos, a segurança é percebida como um impeditivo ao acesso digital mais amplo, como indica a fala: “Quanto mais segurança, mais restrição. E às vezes isso vai contra a inclusão.” Essa percepção ilustra o dilema apontado por Martin (2021), que argumenta que a cibersegurança, quando baseada apenas em controle e restrição, pode reproduzir desigualdades e comprometer o acesso democrático aos serviços públicos digitais. Em contraponto, outras falas mostram que parte dos gestores reconhece a importância de equilibrar os princípios: “A segurança é condição para garantir a transparência e a inclusão digital de forma responsável.” Essa visão ainda é minoritária, mas aponta para uma compreensão mais ampla do papel ético da segurança da informação.

A falta de compreensão técnica por parte das lideranças políticas também é apontada como uma barreira recorrente. Um dos entrevistados afirma: “A gente fala de LGPD e tem que explicar tudo do zero, porque ninguém entende nem o básico.” Esse distanciamento entre os setores técnicos e a alta gestão reforça o cenário em que a segurança digital é implementada de forma marginal, sem respaldo orçamentário, normativo ou estratégico. Como alertam os autores analisados, esse tipo de dissociação enfraquece a capacidade do setor público de responder aos desafios cibernéticos de maneira coordenada.

Em alguns relatos, nota-se que os servidores da área técnica operam em um ambiente de baixa valorização e reconhecimento institucional, o que contribui para o desgaste e a rotatividade. Um dos participantes comentou: “A gestão não enxerga o TI como área estratégica. Quando dá problema, aí lembram que existimos.” Essa percepção reforça o argumento de que a implementação de políticas públicas de cibersegurança esbarra em barreiras simbólicas e disputas internas por legitimidade e prioridade.

Em síntese, as respostas evidenciam que as barreiras institucionais enfrentadas pelos municípios não são apenas técnicas, mas profundamente políticas, culturais e estruturais. A ausência de visão estratégica, o distanciamento entre setores técnicos e decisores, e a tensão entre segurança, inclusão e transparência configuram um cenário adverso à consolidação da cibersegurança como política pública. Como destacam Lipsky (2010), Martin (2021) e Dunn Cavelty (2019), enfrentar esses obstáculos requer mais do que ferramentas tecnológicas: exige mudanças organizacionais, investimento político e sensibilidade ética diante dos múltiplos valores em jogo.

Quadro 24 – Matriz de Evidência – Bloco 5

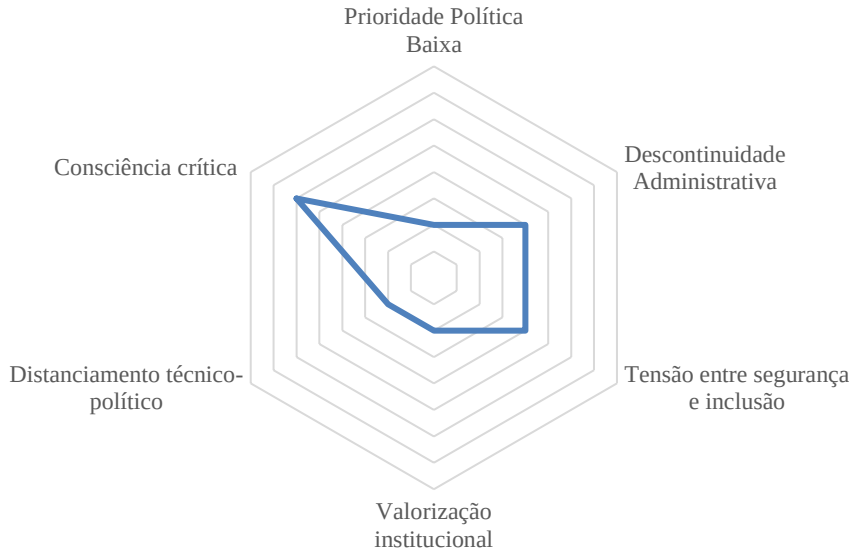
Categoria Temática	Falas Representativas (empíricas)	Análise/Observação	Status
Prioridade Política Baixa	*"A TI sempre foi colocada de lado. Só se corre atrás quando há um problema sério."*	A segurança digital não é tratada como prioridade estratégica na gestão pública, sendo acionada apenas em momentos de crise.	Muito Baixa
Descontinuidade Administrativa	*"A gestão passada acabou com o cargo de direção da TI. A atual está tentando reconstruir, mas há resistência."*	Oscilações entre gestões comprometem qualquer tentativa de institucionalização da segurança da informação.	Baixa
Tensão entre segurança e inclusão	*"Quanto mais segurança, mais restrição. E às vezes isso vai contra a inclusão."*	Percepção de que medidas de segurança digital podem comprometer o acesso da população aos serviços públicos digitais.	Baixa
Valorização institucional	*"A gestão não enxerga o TI como área estratégica. Quando dá problema, aí lembram que existimos."*	Falta de reconhecimento institucional da TI como pilar de governança pública.	Muito Baixa
Distanciamento técnico-político	*"A gente fala de LGPD e tem que explicar tudo do zero, porque ninguém entende nem o básico."*	Ruptura entre técnicos e gestores compromete a integração da cibersegurança nas estratégias institucionais.	Baixa
Consciência crítica (exceção)	*"A segurança é condição para garantir a transparência e a inclusão digital de forma responsável."*	Exceção em que a segurança é compreendida em articulação com valores democráticos e inclusão digital, sinalizando maturidade ética e política.	Média

Fonte: Elaborado pelo autor (2025).

A análise do bloco 5 demonstra que as barreiras à institucionalização da cibersegurança nos municípios vão muito além da escassez de recursos técnicos ou financeiros. Elas são estruturais, simbólicas e políticas. A segurança digital é, na maioria dos casos, tratada como uma demanda secundária, acionada apenas diante de crises e ausente das prioridades estratégicas da gestão pública. Soma-se a isso a descontinuidade administrativa, a falta de compreensão das lideranças políticas sobre o tema e o distanciamento entre técnicos e decisores. As percepções dos entrevistados revelam ainda uma tensão latente entre segurança, inclusão e transparência, com alguns enxergando essas dimensões como opostas, enquanto outros

apontam caminhos para sua integração. Como destacam Lipsky (2010), Martin (2021) e Dunn Cavelty (2019), enfrentar essas barreiras exige transformar a cibersegurança em política pública estruturada, transversal e ética — algo que, até o momento, aparece apenas de forma incipiente no conjunto das respostas analisadas.

Figura 10 – Status de maturidade - Barreiras Institucionais e Percepções



Fonte: Elaborado pelo autor (2025).

O gráfico do bloco 5 – Percepções Institucionais e Valores Políticos apresenta um padrão de maturidade fragmentado, com um eixo se destacando de forma expressiva: “Consciência crítica” aparece com o maior nível, indicando que alguns respondentes demonstraram reflexão aprofundada e sensível sobre as contradições e os desafios da cibersegurança no contexto público local. Essa percepção revela que há agentes dentro da estrutura pública que compreendem a importância da segurança digital, mas também reconhecem seus dilemas éticos, sociais e institucionais — algo discutido por Martin (2021) ao tratar da justiça cibernética e da necessidade de pensar a segurança digital como política pública inclusiva.

Por outro lado, categorias como “Valorização institucional” e “Distanciamento técnico-político” estão entre as mais baixas. Esse contraste reforça a ideia já explorada nos blocos anteriores: mesmo onde há reflexão e consciência crítica, falta respaldo institucional e conexão entre os agentes técnicos e os tomadores de decisão. A presença desse abismo compromete a transformação das percepções em políticas e ações concretas, corroborando as análises de Hall e Taylor (1996) sobre os limites da mudança institucional em ambientes de baixa capacidade estatal.

A “Tensão entre segurança e inclusão” e a “Descontinuidade administrativa” aparecem com valores intermediários. Esses indicadores revelam que os municípios vivenciam conflitos entre proteger os dados dos cidadãos e garantir acesso amplo à informação — um dilema recorrente na literatura, como discutido por Nissenbaum (2005) e Taddeo e Floridi (2018). Já a descontinuidade reforça o impacto das mudanças de gestão, onde políticas iniciadas em uma administração são desconsideradas na seguinte, dificultando qualquer planejamento de médio ou longo prazo na área de segurança digital.

A categoria “Prioridade política baixa” reforça esse diagnóstico: a cibersegurança ainda é vista como um tema secundário, geralmente reativo, e raramente incorporado às pautas estratégicas dos governos locais. Esse dado revela o quanto o tema ainda não se consolidou como uma prioridade institucional transversal, sendo tratado, muitas vezes, como uma função periférica da área técnica, o que contraria as recomendações de Dunn Cavelty (2019) e Zuboff (2019), que defendem o papel da cibersegurança como infraestrutura pública essencial.

Em resumo, o gráfico do bloco 5 mostra que há ilhas de consciência crítica e compreensão ética sobre os desafios da cibersegurança, mas essas percepções coexistem com um cenário de baixa valorização institucional, descontinuidade política e distanciamento entre áreas técnicas e decisórias. O resultado é um campo de atuação potencialmente fértil, mas ainda não cultivado pelas estruturas de poder local — reforçando a necessidade de políticas integradas que alinhem percepção, prioridade e institucionalização da segurança digital nos municípios.

A parte final da entrevista abordou de forma aberta a percepção dos respondentes sobre o tema. A primeira questão de encerramento solicitou aos entrevistados que apontassem quais os principais desafios para os próximos anos em relação à segurança digital. As respostas evidenciam uma percepção generalizada de que os riscos cibernéticos irão se intensificar, ao passo que os municípios ainda não estão preparados para enfrentá-los. Um dos participantes resumiu essa preocupação ao afirmar: “O desafio maior é conseguir acompanhar a velocidade das mudanças tecnológicas com uma estrutura mínima e poucos profissionais.” A fala destaca a assimetria entre a velocidade do avanço tecnológico e a lentidão das estruturas públicas para responder a essas transformações, como discutem Martin (2021) e Calzada (2020).

Outro aspecto recorrente nas respostas diz respeito à educação digital dos próprios servidores públicos, que continuam adotando práticas inseguras, como o uso de senhas fracas, compartilhamento de acessos e desconhecimento das ameaças. Um entrevistado mencionou: “Precisamos ensinar os servidores que o problema não é só do TI. Segurança depende de todos.” Essa fala evidencia a necessidade de construir uma cultura institucional de cibersegurança, ultrapassando a visão técnica e isolada do tema. A ausência dessa cultura reforça o que aponta

Dunn Cavelty (2019) sobre os riscos de tratar a segurança digital apenas como um campo especializado, quando, na verdade, ela demanda um envolvimento organizacional amplo e contínuo.

As falas também revelam que a falta de investimento e de vontade política continuam sendo reconhecidas como barreiras para o futuro. Um respondente afirmou: “Sem um plano de cargos, sem valorização e sem estrutura, não tem como avançar.” A percepção de estagnação e negligência institucional aparece como um entrave à inovação e à profissionalização da gestão pública digital. A esse respeito, Lipsky (2010) já alertava para os limites da ação de servidores públicos quando operam em condições adversas e sem respaldo político. Em outras palavras, os desafios do futuro são percebidos com clareza pelos profissionais, mas sua superação parece condicionada a mudanças que estão fora do alcance direto da área técnica.

A segunda questão de encerramento solicitou sugestões ou caminhos possíveis para a construção de políticas públicas mais robustas em segurança digital. As contribuições dos entrevistados, embora variadas, convergem em três eixos principais: (1) formação continuada, (2) estruturação institucional da área de TI e (3) criação de instâncias regionais de cooperação. Sobre o primeiro ponto, um participante propôs: “Capacitação constante, para todos os setores. TI e usuários precisam estar sempre atualizados.” A fala reflete a percepção de que a segurança da informação é um processo contínuo, que demanda educação permanente e transversal.

Quanto à estrutura institucional, vários respondentes enfatizaram a importância de criar cargos específicos, definir atribuições formais e garantir orçamento para a área de tecnologia. Um exemplo disso está na fala: “É preciso que os municípios reconheçam que TI é estratégico e merece estrutura, não improviso.” Essa recomendação vai ao encontro do que discutem os autores analisados ao longo da tese, sobretudo Hall e Taylor (1996) e Oliveira *et al.* (2020), que defendem a profissionalização e institucionalização da burocracia como condição essencial para a efetividade das políticas públicas. Logo, surgem com destaque sugestões ligadas à criação de redes regionais e fóruns técnicos, como expressa a fala: “Um grupo regional ajudaria muito a compartilhar soluções e criar padrões.” Essas sugestões reforçam a importância da cooperação intermunicipal como estratégia para superar a fragmentação atual e ampliar a capacidade dos municípios diante de desafios cada vez mais complexos e interdependentes.

De modo geral, a análise dos blocos temáticos e a sistematização dos dados empíricos evidenciaram padrões recorrentes de fragilidade institucional, informalidade normativa, dependência técnica e baixa articulação regional. Ao mesmo tempo, emergem sinais

pontuais de percepção crítica, esforços individuais e experiências isoladas que revelam potencial de avanço, especialmente quando alinhadas a políticas públicas estruturadas e apoio técnico-jurídico. Esses achados, embora contextualizados na realidade de municípios de pequeno e médio porte, dialogam com desafios mais amplos da governança digital em contextos de baixa capacidade estatal. A seção seguinte se propõe a discutir esses resultados de forma integrada, à luz dos marcos teóricos mobilizados nos Estudos I, II e III, com o objetivo de interpretar os níveis de maturidade observados e propor caminhos possíveis para o fortalecimento da cibersegurança como política pública local.

4.5 SÍNTESE ANALÍTICA DA MATURIDADE INSTITUCIONAL

A teoria institucionalista apresentada por Hall e Taylor (1996) parte da compreensão de que as instituições não apenas restringem comportamentos, mas moldam preferências e práticas administrativas. Isso se materializa em regras, rotinas e estruturas que sustentam a ação pública. Quando aplicado ao campo da cibersegurança, como se propôs no estudo, o modelo evidencia a necessidade de uma estrutura mínima institucional que sustente as práticas digitais. As entrevistas mostraram que essa institucionalidade ainda é extremamente frágil, com falas como: “Não temos um setor específico para isso, fazemos conforme a demanda”. A ausência de uma estrutura perene demonstra que as ações são desprovidas de rotinas consolidadas, sendo pautadas mais pela contingência do que por planejamento.

March e Olsen (1984), ao diferenciarem a lógica da adequação da lógica da consequência, ajudam a entender o comportamento dos agentes públicos frente à cibersegurança. A lógica da consequência, mais presente nas entrevistas, indica ações motivadas por urgência, riscos iminentes ou pressão externa, como no caso relatado por um respondente: “A LGPD nos pegou de surpresa, aí tivemos que correr atrás”. Isso contrasta com a lógica da adequação, que pressupõe ação guiada por normas internalizadas. A recorrência da atuação reativa nas falas evidencia que os municípios ainda não interiorizaram a cibersegurança como parte de uma prática institucional consolidada.

A abordagem de Lipsky (2010), que descreve os profissionais de linha de frente como mediadores entre as diretrizes institucionais e a realidade prática, também se mostra pertinente. Muitos dos entrevistados revelaram desempenhar múltiplas funções e tomar decisões sem respaldo institucional, agindo como “fazedores de política pública” em contextos de ausência normativa. Um exemplo disso está na fala: “A gente decide o que é prioridade,

porque não tem uma política definida". Esse deslocamento da responsabilidade institucional para o nível operacional reforça a fragilidade institucional e a personalização das decisões.

Outro autor importante no Estudo II é Dunn Cavelty (2019), que argumenta que a cibersegurança só se concretiza como política pública efetiva quando deixa de ser tratada como função técnica e passa a ser articulada transversalmente nas estruturas de governo. A realidade encontrada nas entrevistas é oposta: a cibersegurança ainda é vista como tarefa do "setor de informática", o que é explicitado por falas como: "Esse assunto não chega no gabinete, é a gente que cuida". Essa segmentação inviabiliza a construção de uma governança sistêmica da segurança digital e revela um déficit de transversalidade.

A discussão trazida por Martin (2021), sobre a tensão entre segurança e inclusão digital, também aparece de forma implícita nas entrevistas. Um dos entrevistados disse: "A gente tenta abrir o máximo possível os acessos, mas isso aumenta o risco de ataque". Esse dilema confirma a observação de Martin de que a segurança digital, quando não discutida de forma ética e participativa, pode gerar contradições entre controle e acesso. O mesmo se aplica à ausência de diretrizes claras sobre como tratar dados sensíveis da população.

Ao relacionar esses achados com as três correntes teóricas discutidas no Estudo I — técnico-operacional, institucionalista e sociotécnica — é possível perceber que os municípios analisados operam, majoritariamente, sob a lógica técnico-operacional. Há uma prevalência de práticas voltadas para o funcionamento básico dos sistemas, como backups e antivírus, mas sem planejamento estratégico ou integração com diretrizes normativas. A maturidade técnica existe, mas é limitada à capacidade de "manter funcionando", como atestado na fala: "Fazemos backup diário, mas não temos plano de recuperação".

A abordagem institucionalista, que exige a existência de marcos legais, estruturas organizacionais e processos formalizados, está em estágio inicial. Poucos municípios possuem normativas específicas sobre cibersegurança ou políticas formalizadas de proteção de dados. Isso se evidencia em frases como: "Estamos aguardando a orientação do Estado para ver o que precisa ser feito". A dependência de diretrizes externas é um sinal claro da baixa institucionalização da política.

Já a perspectiva sociotécnica, que propõe compreender a cibersegurança como fruto da interação entre tecnologia, pessoas e valores organizacionais, aparece de forma incipiente. Embora haja percepções críticas sobre os riscos, essas reflexões não se transformam em práticas institucionais. Um dos poucos indícios dessa abordagem aparece na fala: "A gente depende da confiança das pessoas que lidam com os sistemas, não temos como monitorar tudo". Essa

afirmação revela uma consciência sobre a dimensão humana da segurança digital, mas ainda desconectada de práticas estruturadas de formação, monitoramento ou cultura organizacional.

As categorias do instrumento de pesquisa, como “autonomia técnica”, “estrutura da equipe”, “normativas locais” e “resposta a incidentes”, foram diretamente extraídas dos referenciais teóricos. No entanto, as entrevistas mostraram que muitas dessas categorias estão ausentes da realidade dos municípios ou são interpretadas de forma limitada. Por exemplo, a “resposta a incidentes” foi descrita em termos reativos: “Quando tem problema, a gente vê o que pode fazer”, o que mostra ausência de protocolos preventivos, contrariamente ao que preconiza a literatura.

Outro ponto de tensão entre teoria e prática está na dimensão da “governança digital estruturada”. Enquanto os autores defendem a necessidade de um modelo de governança com papéis bem definidos, os entrevistados relatam improviso e sobreposição de funções. “Sou eu quem resolve tudo, desde trocar a senha até responder ao MP”, afirmou um dos respondentes. Essa personalização das funções vai de encontro à ideia de cibersegurança como política pública institucionalizada.

As falas também revelam descontinuidade administrativa, um problema apontado na literatura como um dos entraves para a maturidade em políticas digitais. Vários municípios relataram que as iniciativas anteriores foram abandonadas com a troca de gestão, como exemplificado na fala: “O sistema de segurança que existia foi desativado quando mudou o governo”. Isso mostra como a ausência de estruturas permanentes inviabiliza o acúmulo institucional.

A teoria também aponta que a maturidade institucional requer monitoramento, avaliação e adaptação contínua das práticas. Esse aspecto é quase inexistente nas respostas dos municípios. Nenhum dos entrevistados mencionou a existência de mecanismos de auditoria, indicadores de desempenho ou revisão de políticas. O que prevalece é a prática da tentativa e erro, como resume a fala: “A gente vai aprendendo com os erros”.

Apesar do predomínio de um modelo técnico-operacional, há indícios de transição para abordagens mais amplas. Alguns municípios demonstraram intenção de criar normativas, integrar setores e buscar capacitação, ainda que de forma incipiente. Isso sugere que o campo está em movimento e que a presença de agentes engajados pode impulsionar processos de mudança, mesmo diante da ausência de marcos formais.

Os achados reforçam a hipótese central do estudo: a maturidade institucional em cibersegurança nos municípios analisados ainda é baixa, marcada por iniciativas pontuais, dependência de indivíduos e ausência de estruturas consolidadas. A teoria oferece ferramentas

para compreender essas lacunas, e os dados empíricos as confirmam com nitidez. Essa articulação entre teoria e realidade é fundamental para pensar políticas públicas mais realistas e ajustadas ao contexto dos pequenos e médios municípios brasileiros.

4.6 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo compreender o grau de maturidade institucional em cibersegurança dos municípios da Região Carbonífera de Santa Catarina, utilizando como base entrevistas semiestruturadas realizadas com representantes técnicos e gestores públicos. A escolha da abordagem qualitativa e do uso de um roteiro de entrevista ancorado teoricamente permitiu acessar percepções, práticas e obstáculos enfrentados pelos municípios em relação à proteção de dados, governança digital e respostas a incidentes de segurança.

O instrumento de pesquisa foi construído a partir de cinco blocos temáticos — capacidade institucional, arcabouço jurídico, práticas técnicas, cooperação regional e valores/política — organizando os dados a partir das dimensões propostas pelos autores que embasaram o Estudo II, especialmente Hall e Taylor (1996), March e Olsen (1984), Dunn Cavelty (2019) e Martin (2021). A estrutura das entrevistas, alinhada ao modelo de análise institucional, possibilitou captar a distância entre as recomendações teóricas e a realidade concreta das práticas municipais.

Os resultados apontaram que a maioria dos municípios apresenta níveis iniciais de maturidade institucional, com forte presença de práticas improvisadas, dependência de poucos agentes técnicos e ausência de normatização. A atuação é marcada pela lógica da consequência — isto é, ações orientadas por urgência ou pressão externa — em detrimento da lógica da adequação institucional. A fala de um entrevistado — “Fazemos o que dá, quando dá” — é ilustrativa desse cenário, onde a informalidade é a regra, e a política de cibersegurança inexiste como campo estruturado.

No primeiro bloco, dedicado à capacidade institucional, observou-se a centralização das funções de TI em poucos profissionais, muitas vezes sem formação específica em segurança. O “chefe de informática” ou “analista de sistemas” é o principal responsável por todos os processos, desde o suporte cotidiano até o atendimento a notificações do Ministério Público. A ausência de equipes multidisciplinares, recursos financeiros e apoio das instâncias decisórias configura um cenário de baixa institucionalidade, onde o conhecimento técnico se sobrepõe à formulação de política pública.

O segundo bloco, referente ao arcabouço jurídico, revelou uma lacuna crítica. A maioria dos municípios não possui normativas locais voltadas à segurança da informação ou à aplicação da LGPD. Em muitos casos, os entrevistados relataram que o tema foi pautado apenas após notificações externas. A frase “Só começamos a pensar nisso depois que recebemos um ofício” é emblemática de uma cultura jurídica reativa e dependente de indução externa. A ausência de políticas formais impede a construção de rotinas de proteção, responsabilização e transparência.

O terceiro bloco tratou das práticas técnicas e operacionais. Embora muitos municípios realizem rotinas básicas como backups e controle de antivírus, não há planejamento estruturado, protocolos de resposta a incidentes, testes regulares ou monitoramento de vulnerabilidades. Em diversos relatos, ações mais elaboradas dependem de fornecedores terceirizados ou são postergadas por falta de pessoal. Um dos entrevistados afirmou: “A gente sabe que precisa fazer mais, mas não temos braço para isso”.

O quarto bloco abordou a cooperação intermunicipal e regional. O que se observou foi um cenário de isolamento técnico e ausência de redes estruturadas de apoio mútuo. Embora a maioria dos entrevistados reconheça a importância da cooperação, poucos municípios participam de fóruns, consórcios ou grupos de trabalho voltados à segurança digital. A inexistência de espaços institucionais de cooperação impede o compartilhamento de boas práticas, padronização de procedimentos e capacitação coletiva.

No quinto bloco, que examinou valores, percepções e política, emergiu a baixa priorização da cibersegurança nas agendas locais. Para muitos entrevistados, o tema ainda é “técnico demais” para entrar no radar da gestão executiva. A visão da segurança digital como um problema operacional, e não como um direito da população ou um elemento da infraestrutura pública, contribui para a sua marginalização. A fala “os secretários não se envolvem, acham que é problema do TI” sintetiza essa barreira simbólica.

A articulação dos achados com a teoria mostrou-se consistente. Hall e Taylor (1996) explicam que a maturidade institucional é alcançada quando práticas são estabilizadas por rotinas, normas e estruturas. March e Olsen (1984) defendem que a ação pública deve ser guiada pela lógica da adequação, não apenas por incentivos. Já Dunn Cavelty (2019) aponta que a cibersegurança deve ser política pública transversal. Em todos esses marcos teóricos, o que se observou nos municípios analisados foi o oposto: práticas instáveis, ausência normativa, baixa transversalidade e descontinuidade.

Além disso, a análise dialoga com as três correntes da cibersegurança discutidas no Estudo I. O modelo técnico-operacional predomina, com foco em soluções imediatas e

ferramentas básicas. A abordagem institucionalista é incipiente, visível apenas em tentativas isoladas de elaborar normativas ou comissões. A sociotécnica, por sua vez, aparece discretamente em algumas percepções críticas, mas não se traduz em políticas inclusivas, éticas ou participativas.

Os gráficos e matrizes de evidência reforçam essas observações, indicando que a maioria das categorias analisadas se encontra nos níveis de maturidade 1 e 2. Isso demonstra que a governança da cibersegurança nos municípios da região está em estágio inicial, ainda dependente de agentes individuais e sem articulação regional. A exceção está em municípios com profissionais mais experientes ou com alguma indução institucional externa, como projetos estaduais ou cobranças do judiciário.

Apesar das limitações, o Estudo III identificou indícios de mudança institucional. Alguns municípios demonstraram interesse em avançar, criar políticas, buscar capacitação e fortalecer equipes. Ainda que incipientes, essas movimentações indicam que o campo da cibersegurança pública está em processo de construção, com potencial para consolidar-se como política local estruturada.

Por fim, registra-se que a ausência de institucionalização da cibersegurança compromete não apenas a proteção de dados, mas também a confiança na gestão pública, a continuidade administrativa e a soberania digital dos municípios. O estudo oferece subsídios empíricos e teóricos para que gestores, legisladores e redes de apoio formulem estratégias mais eficazes, realistas e aderentes ao contexto dos pequenos e médios municípios brasileiros.

5 ESTUDO IV – PROPOSIÇÃO DE UM MARCO LEGAL MUNICIPAL EM CIBERSEGURANÇA: DIRETRIZES ESTRATÉGICAS PARA A REGIÃO DA AMREC A PARTIR DA ANÁLISE DE MATURIDADE INSTITUCIONAL

5.1 INTRODUÇÃO

A crescente digitalização das atividades públicas municipais tem ampliado a dependência dos entes locais em relação a sistemas informatizados, redes digitais e fluxos contínuos de dados. Em contrapartida, a ausência de mecanismos de proteção da informação, aliada à baixa institucionalização de práticas de segurança cibernética, tem tornado as administrações locais vulneráveis a ameaças digitais cada vez mais complexas e frequentes. Esse cenário exige que as políticas públicas municipais incorporem a cibersegurança como um vetor estratégico de governança, proteção institucional e desenvolvimento.

No contexto da Associação dos Municípios da Região Carbonífera (AMREC), essa dinâmica se manifesta de maneira significativa. Os municípios da região vêm adotando gradualmente ferramentas tecnológicas para modernizar serviços e ampliar a eficiência administrativa. No entanto, como evidenciado no Estudo III desta tese, essa modernização não tem sido acompanhada por uma institucionalização proporcional da cibersegurança. Falta um arcabouço normativo capaz de organizar, orientar e garantir a continuidade das ações de proteção digital no ambiente público municipal.

O Estudo III teve como objetivo principal caracterizar o estágio da maturidade institucional em cibersegurança nos municípios que compõem a AMREC, com ênfase nas práticas de regulação, gestão e proteção de ativos digitais em instituições públicas locais. Por meio de uma abordagem qualitativa, fundamentada na análise documental de legislações municipais, planos estratégicos, normativas internas e entrevista semiestruturada, foi possível identificar padrões e lacunas no tratamento da segurança cibernética. Os resultados revelaram uma atuação predominantemente reativa por parte dos municípios, com ausência de estruturas normativas robustas, baixo grau de institucionalização de políticas de cibersegurança e fragilidades na formação técnica dos servidores. Mesmo nas cidades com maior porte populacional e orçamentário, observou-se a carência de mecanismos formais de governança digital, o que evidencia a necessidade de ações coordenadas e políticas públicas regionais voltadas à segurança da informação.

A ausência de um marco legal local foi um dos pontos mais críticos observados. Nenhum dos municípios analisados dispunha, até o momento da pesquisa, de legislação própria voltada à cibersegurança. Tampouco foram identificados decretos, portarias ou instrumentos

normativos internos que tratassem de políticas de proteção da informação, gestão de incidentes ou segurança de sistemas. Essa lacuna normativa compromete diretamente a continuidade das ações, fragiliza a responsabilização institucional e expõe os municípios a riscos operacionais, legais e reputacionais.

Além da ausência normativa, o Estudo III revelou que há, nos municípios da AMREC, uma clara dependência de agentes externos — principalmente empresas terceirizadas — para lidar com questões de tecnologia da informação. Essa dependência, por não estar juridicamente regulada, gera vulnerabilidades tanto no campo técnico quanto no campo legal. A inexistência de cláusulas contratuais específicas, planos de resposta a incidentes ou níveis de serviço acordados compromete a *accountability* e a segurança dos dados tratados.

Paradoxalmente, a mesma pesquisa evidenciou uma disposição positiva para a cooperação intermunicipal. Muitos gestores manifestaram interesse em ações conjuntas, consórcios ou compartilhamento de recursos tecnológicos. Esse dado, embora não tenha sido o foco primário do Estudo III, reforça a ideia de que os municípios estão abertos a soluções articuladas, o que cria um terreno propício para a construção de uma proposta normativa regionalizada, que respeite a autonomia dos entes federados, mas ofereça diretrizes comuns mínimas.

Diante desse panorama, o Estudo IV tem como objetivo propor um modelo de legislação municipal em cibersegurança, com base nas evidências empíricas levantadas no Estudo III. Trata-se de uma proposta normativa construída a partir das necessidades reais observadas nos municípios da AMREC, com o intuito de oferecer um instrumento jurídico viável, adaptável e orientado para a elevação da maturidade cibernética institucional.

A questão de pesquisa que orienta este estudo é a seguinte: de que forma um marco legal municipal pode contribuir para o fortalecimento da maturidade institucional em cibersegurança nos municípios da AMREC? A partir dessa pergunta, o objetivo de análise é projetar os elementos estruturantes de uma minuta de lei municipal que responda às lacunas identificadas e promova a institucionalização da governança cibernética no ambiente público local.

A elaboração de uma proposta normativa ancorada em diagnóstico empírico encontra respaldo em abordagens de pesquisa aplicada com viés propositivo. Gil (2008) destaca que a pesquisa propositiva visa à elaboração de soluções para problemas concretos, por meio do desenvolvimento de modelos, normas ou produtos que possam ser aplicados em contextos reais. Nessa mesma direção, Demo (2009) defende que a pesquisa científica deve ir além da

crítica descritiva e avançar na proposição de alternativas viáveis, reflexivas e argumentadas, com base em fundamentos teóricos e dados empíricos consistentes.

A construção de uma legislação municipal em cibersegurança não se trata, portanto, de um exercício abstrato, mas de uma resposta estratégica às limitações institucionais diagnosticadas. A proposta legislativa que emerge deste estudo não busca replicar modelos genéricos de outros entes federados, mas sim adaptar as boas práticas à realidade institucional, técnica e financeira dos municípios da AMREC. Trata-se de um esforço de territorialização normativa, no qual as soluções são construídas a partir do reconhecimento das capacidades locais existentes.

Além disso, a proposição legislativa considera as diretrizes e princípios estabelecidos em normativas superiores, como a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014) e a Estratégia Nacional de Cibersegurança. A minuta de lei aqui apresentada busca dialogar com esses marcos legais, traduzindo-os para o nível municipal, de forma compatível com a competência constitucional dos entes locais e com os princípios da administração pública.

A escolha pela construção de um projeto de lei como produto final da tese reforça o compromisso deste trabalho com a transformação da realidade institucional dos municípios estudados. A produção acadêmica aqui desenvolvida pretende, assim, cumprir um duplo papel: contribuir para o avanço teórico no campo da governança cibernética e oferecer um instrumento prático que possa ser apropriado por gestores públicos comprometidos com a proteção digital de suas administrações e dos cidadãos que representam.

Nesse sentido, este Estudo IV se configura como uma extensão natural dos achados empíricos anteriores, articulando diagnóstico e ação. Enquanto os Estudos I, II e III se ocuparam da construção conceitual, da validação de modelos e da análise de campo, o Estudo IV propõe-se a devolver à sociedade um produto aplicável, juridicamente consistente e politicamente viável. É a materialização de um percurso científico que se iniciou no campo teórico e agora deságua na proposição normativa.

O presente estudo se estrutura em três partes principais: uma fundamentação teórica e legal que contextualiza o papel das normas municipais em segurança cibernética; a apresentação do modelo jurídico proposto, com destaque para os princípios, eixos e artigos que compõem a minuta de lei; e, por fim, a discussão das hipóteses estratégicas que emergem da implementação desse marco legal, orientando pesquisas futuras e processos de monitoramento e avaliação.

5.2 BASE TEÓRICA E NORMATIVA

A governança cibernética no contexto municipal tem ganhado contornos cada vez mais relevantes diante da crescente digitalização dos serviços públicos e da ampliação da dependência tecnológica por parte dos entes federativos. Com o avanço das infraestruturas de tecnologia da informação, tornou-se urgente compreender os mecanismos institucionais e legais disponíveis para que os municípios operem com segurança, resiliência e responsabilidade no ciberespaço.

A construção de um ambiente digital seguro exige mais do que soluções técnicas; envolve arcabouços normativos, capacidade institucional e políticas públicas estruturadas. Essa dimensão normativa-institucional da segurança digital foi, ao longo da última década, o foco de diversas produções acadêmicas que, de diferentes formas, buscaram compreender as lacunas e desafios da cibersegurança pública no Brasil.

Entre os marcos legais mais relevantes está o Marco Civil da Internet (Lei nº 12.965/2014), que estabeleceu os princípios da liberdade de expressão, privacidade, proteção de dados e neutralidade da rede. Embora seja um diploma fundante da regulação da internet no país, sua aplicabilidade concreta no âmbito dos municípios depende de iniciativas complementares de normatização e implementação local.

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) veio a consolidar, no Brasil, um regime específico de proteção de dados pessoais, com obrigações claras aos agentes públicos e privados. No contexto municipal, isso se traduz na necessidade de estruturação de políticas próprias de tratamento de dados, nomeação de encarregados (DPOs), adequação de contratos e revisão de práticas administrativas.

Essas exigências legais são especialmente desafiadoras para os municípios de pequeno e médio porte, que muitas vezes não dispõem de infraestrutura técnica nem pessoal capacitado para implementar as mudanças exigidas. A literatura aponta que essa lacuna de implementação pode gerar não apenas riscos operacionais, mas também responsabilidade civil por omissão estatal.

A esse cenário se acrescenta o recente Decreto nº 11.856/2023, que instituiu a Política Nacional de Cibersegurança (PNCiber). Essa política estabelece princípios como soberania digital, prevenção de ataques, proteção de dados pessoais, educação em cibersegurança e cooperação federativa. O decreto representa um avanço no sentido de articular estratégias nacionais com o envolvimento dos entes subnacionais.

A PNCiber define como um de seus objetivos o incremento da atuação coordenada entre União, Estados e Municípios no tratamento de incidentes cibernéticos. Esse ponto é especialmente relevante para os municípios, que passaram a ser reconhecidos como partícipes formais da política nacional de cibersegurança, ainda que suas atribuições específicas não estejam plenamente detalhadas.

O decreto também institui o Comitê Nacional de Cibersegurança (CNCiber), com representantes de ministérios, agências, setor privado, sociedade civil e instituições científicas. Trata-se de um modelo multissetorial de governança, que pode abrir espaço para o compartilhamento de boas práticas e para a formulação de diretrizes específicas para os governos locais.

Na literatura nacional, essa perspectiva institucional já vinha sendo apontada como necessária. Alves Júnior (2011) alertava para a fragmentação das ações em cibersegurança no Brasil e defendia uma política nacional que integrasse os entes federativos, de forma coordenada, com foco na proteção das infraestruturas públicas e na governança da informação.

Vianna (2019), por sua vez, propôs um modelo nacional de ciberproteção estruturado sobre três eixos: soberania, governança e capacitação. O autor argumenta que a ausência de uma estratégia nacional articulada prejudica diretamente os municípios, que, por falta de diretrizes e apoio técnico, tornam-se vulneráveis e expostos a riscos que poderiam ser mitigados.

O novo decreto PNCiber alinha-se parcialmente a essas recomendações ao propor uma estratégia nacional, um plano de ação e a criação de mecanismos de cooperação vertical. No entanto, ainda persiste a necessidade de regulamentações específicas que indiquem com clareza o papel dos municípios e os recursos disponíveis para sua adaptação.

No plano da responsabilidade institucional, os trabalhos de Nunes (2022) e Santos (2023) destacam que o cumprimento da LGPD pelos entes públicos não se limita à criação de normativas internas. Envolve a efetiva estruturação de núcleos de governança da informação, a formação contínua dos servidores e a integração entre as áreas jurídica, tecnológica e administrativa.

Para Nunes (2022), a responsabilização civil do Estado por danos decorrentes de incidentes cibernéticos pode ser direta ou por omissão, especialmente quando há ausência de políticas mínimas de segurança da informação. A autora propõe que a LGPD seja lida em diálogo com os princípios constitucionais da eficiência, moralidade e proteção da dignidade da pessoa humana.

Esse entendimento é reforçado por Cheliga (2023), que, ao estudar a proteção de dados em cidades inteligentes, defende que a ausência de estrutura institucional dedicada à privacidade digital coloca em risco não apenas os direitos dos cidadãos, mas a própria legitimidade das políticas de modernização urbana. Para o autor, a cibersegurança precisa ser transversal e planejada desde a concepção das políticas públicas digitais.

Outro ponto de destaque no decreto PNCiber é a ênfase na educação, pesquisa e desenvolvimento tecnológico em cibersegurança. Essa diretriz dialoga com os apontamentos de Vianna (2015), que identificou a ausência de cultura organizacional voltada à proteção digital como um dos principais entraves à gestão da segurança cibernética na administração pública federal e, por consequência, nas instâncias subnacionais.

O decreto também propõe o estímulo ao intercâmbio de informações entre entes federativos, o que pode fomentar redes colaborativas e integração de soluções. Essa abordagem é compatível com a proposta de governança em rede sugerida por autores como Gherardi (2006), referenciada em estudos anteriores, que defende a articulação entre diferentes níveis de governo e setores da sociedade para o enfrentamento de problemas complexos.

No tocante à responsabilização e ao papel da regulação, observa-se que a criação do CNCiber traz potencial de fortalecer a fiscalização e induzir a padronização de práticas. Contudo, sua efetividade dependerá do grau de participação dos entes locais e da capacidade do governo federal em articular apoio técnico e financeiro.

Como apontado por Nogueira (2024), experiências internacionais demonstram que políticas de cibersegurança bem-sucedidas envolvem coordenação intergovernamental, educação pública e investimento contínuo. O autor cita a Estônia como exemplo de país que construiu uma governança digital robusta e descentralizada, com forte engajamento das administrações locais.

Esse modelo estoniano ressoa com as propostas contidas na PNCiber, ainda que o decreto brasileiro careça de mecanismos claros de financiamento, cronogramas de implementação e indicadores de desempenho aplicáveis aos municípios. A ausência desses elementos pode limitar a efetividade das ações no nível local.

Ao considerar os autores analisados e o novo marco normativo, percebe-se que a concretização da cibersegurança no plano municipal requer mais do que normatização centralizada. Exige a criação de capacidades institucionais locais, alinhadas com os princípios constitucionais e com os valores democráticos previstos na LGPD e no Marco Civil da Internet.

Essa realidade reforça a importância do desenvolvimento de indicadores de maturidade institucional em cibersegurança, capazes de orientar os gestores públicos na

elaboração de diagnósticos, planos de ação e avaliação de desempenho. No entanto, essa estrutura só produzirá resultados concretos se for acompanhada de investimento, capacitação e comprometimento institucional por parte dos municípios.

5.2.1 Convergências teóricas e normativas sobre governança cibernética

A literatura acadêmica nacional e internacional já vinha destacando, antes da formulação da Política Nacional de Cibersegurança (PNCiber), a importância de se consolidar um modelo de governança digital no setor público que vá além das soluções técnicas e passe a integrar elementos institucionais, normativos e culturais. Essa visão ampliada de cibersegurança está presente em diversos estudos que contribuíram para o amadurecimento do campo no Brasil.

Alves Júnior (2011) foi um dos primeiros autores a apontar a fragmentação da atuação estatal no campo da segurança cibernética e a ausência de uma política nacional coordenada. Ele defendia, ainda em 2011, que a proteção dos ativos digitais exigia a atuação conjunta de União, Estados e Municípios, sendo necessário um modelo federativo de segurança cibernética. Essa proposta dialoga diretamente com os objetivos mais recentes do Decreto nº 11.856/2023, que reconhece os entes subnacionais como parte da estratégia nacional.

Essa proposta de articulação federativa foi posteriormente reforçada por Vianna (2019), que propôs um modelo de ciberproteção baseado em soberania, governança e capacitação. O autor sustentou que a ausência de diretrizes nacionais claras repercute negativamente nos municípios, que permanecem sem parâmetros para desenvolver políticas locais de cibersegurança. O Decreto nº 11.856, ao instituir o Comitê Nacional de Cibersegurança e propor a elaboração de planos de ação, parece tentar responder a essa lacuna apontada anteriormente.

No campo da proteção de dados, a literatura jurídica identificou precocemente a dificuldade de implementação da LGPD no âmbito municipal. Nunes (2022) argumenta que a conformidade legal depende da existência de uma estrutura institucional mínima, com fluxos bem definidos de tratamento de dados e políticas de segurança da informação integradas ao planejamento da administração pública. Essa leitura converge com os princípios estabelecidos pela LGPD e com as exigências indiretas impostas pela PNCiber.

Santos (2023) contribui com a interpretação constitucional do direito à proteção de dados, destacando a responsabilidade objetiva do Estado em situações de falha de segurança. O autor alerta para o fato de que a inexistência de políticas públicas e a ausência de planejamento

institucional caracterizam omissão estatal. Essa responsabilidade é ainda mais evidente em contextos onde os municípios coletam dados sensíveis de populações vulneráveis, como nos serviços de saúde, assistência social e educação.

A interface entre cidades inteligentes e proteção de dados foi tratada por Cheliga (2023), que destacou os riscos de um processo de digitalização urbana dissociado de uma política clara de governança da informação. O autor argumenta que os dados coletados por sensores urbanos, câmeras e sistemas integrados devem estar submetidos a regras rígidas de proteção e uso. A ausência de normativas específicas nesse campo revela uma vulnerabilidade institucional que o decreto de 2023 busca, ainda que timidamente, mitigar.

Vianna (2015), em sua análise sobre o comportamento informacional na administração pública federal, já apontava que a ausência de cultura institucional voltada à proteção de dados é um dos principais entraves à efetividade das políticas de segurança digital. Esse elemento — o cultural — também é tratado no Decreto nº 11.856, que coloca a educação em cibersegurança como uma diretriz estratégica. A convergência entre os achados empíricos anteriores e os princípios normativos atuais revela o amadurecimento da agenda pública de segurança digital.

Outra convergência está no papel da legislação como vetor de indução de mudanças institucionais. O Marco Civil da Internet, a LGPD e agora o Decreto nº 11.856 formam um conjunto normativo que aponta para a necessidade de políticas transversais, intersetoriais e multiescalares. Autores como Nunes (2022) e Cheliga (2023) defendem que a atuação estatal nessa área precisa articular a dimensão jurídica com a administrativa e a tecnológica, criando núcleos de governança internos nas organizações públicas.

As pesquisas anteriores também apontaram que a adoção de medidas de segurança digital é frequentemente reativa, ocorrendo após incidentes ou pressões externas, e não como parte de um planejamento estratégico. Essa constatação aparece nos trabalhos de Vianna (2019) e é confirmada pelo diagnóstico realizado no presente estudo em municípios da AMREC, que revelou a ausência de políticas preventivas de segurança da informação, apesar da crescente digitalização dos serviços públicos.

No plano da responsabilização, as contribuições de Nunes (2022) são especialmente relevantes. A autora propõe a leitura da LGPD em conjunto com a jurisprudência sobre omissão do Estado, indicando que a não criação de estruturas mínimas de proteção de dados pode ser considerada negligência administrativa. O Decreto nº 11.856, ao prever planos de ação e metas, oferece um instrumento para que os entes públicos possam demonstrar diligência, ainda que não elimine o risco jurídico de responsabilização por inação.

A análise dos estudos anteriores revela, portanto, que as principais lacunas identificadas em nível local — ausência de políticas, de profissionais qualificados, de mecanismos de controle e de cultura institucional — já vinham sendo objeto de atenção por parte da academia. O que o Decreto nº 11.856 oferece é uma oportunidade normativa de alinhamento entre essas demandas e uma estratégia nacional integrada.

Ainda assim, a literatura aponta que decretos, por si só, não são suficientes. É necessário que eles se desdobrem em ações concretas, com financiamento, apoio técnico e monitoramento de resultados. Vianna (2019) e Cheliga (2023) são enfáticos ao afirmar que a governança digital eficaz depende da construção de capacidades estatais locais, o que exige planejamento, tempo e compromisso político.

Ao associar os princípios legais às evidências empíricas, torna-se possível propor um modelo de maturidade institucional que sirva de referência para a formulação de políticas públicas de cibersegurança nos municípios. Isso aponta que há uma forte coerência entre os diagnósticos teóricos desenvolvidos ao longo dos últimos anos e as recentes inovações legais. O desafio agora está na capacidade dos entes locais de internalizarem essas diretrizes e operacionalizá-las em contextos marcados por escassez de recursos, descontinuidade administrativa e baixa priorização política do tema.

5.3 PROCEDIMENTOS METODOLÓGICOS

O Estudo IV caracteriza-se metodologicamente como uma pesquisa propositiva, voltada à formulação de um marco legal municipal em cibersegurança fundamentado em evidências empíricas e referenciais teóricos previamente discutidos. Segundo Gil (2008), a pesquisa propositiva se distingue pela elaboração de soluções aplicáveis a problemas concretos, utilizando-se de conhecimento acumulado e sistematizado. Neste caso, a proposta normativa foi desenvolvida a partir da análise integrada dos estudos anteriores e da revisão de literatura, assumindo caráter instrumental e aplicável ao contexto das cidades.

A escolha desse enquadramento metodológico encontra respaldo na concepção de Marconi e Lakatos (2010), que destacam o papel da pesquisa aplicada em transformar conhecimento teórico em práticas concretas. A formulação do marco legal, portanto, não se restringiu à descrição de fenômenos, mas buscou intervir de forma estruturada, oferecendo um instrumento normativo que responde às demandas identificadas na realidade municipal.

O procedimento de construção da proposta envolveu três etapas centrais. Na primeira, consolidaram-se os resultados obtidos nos estudos anteriores, destacando lacunas

normativas e desafios operacionais enfrentados pelas administrações municipais na área de cibersegurança. Na segunda, definiram-se os eixos estruturantes do marco legal, baseados nas categorias do Quadro 23 e nas diretrizes estratégicas formuladas na seção 5.4.1. Já na terceira etapa, estruturou-se o texto normativo segundo modelos legislativos existentes, adaptando-os ao contexto e às necessidades locais.

A metodologia adotada também se caracteriza como qualitativa e exploratória, uma vez que buscou compreender em profundidade as dimensões sociotécnicas e jurídicas envolvidas na cibersegurança municipal. Conforme Flick (2009), a pesquisa qualitativa permite captar nuances, interações e significados que não seriam plenamente apreendidos por métodos puramente quantitativos, sendo essencial para fundamentar propostas normativas contextualizadas.

No desenvolvimento da proposta, foram utilizadas estratégias de análise documental, examinando legislações nacionais e internacionais correlatas, bem como normativas setoriais que influenciam a gestão da segurança digital. Essa abordagem comparativa, conforme Bardin (2011), possibilita identificar padrões, boas práticas e elementos transferíveis para o contexto-alvo, garantindo maior consistência e aplicabilidade do resultado.

A elaboração do marco legal também foi orientada por princípios da pesquisa-ação em sua vertente propositiva, na medida em que manteve foco na aplicabilidade prática e na potencial implementação pelos agentes públicos. Segundo Thiollent (2011), a pesquisa-ação se caracteriza por envolver diretamente o pesquisador no processo de transformação da realidade estudada, produzindo conhecimento e intervenção de forma simultânea.

A escolha metodológica reforça o compromisso da tese com a produção de conhecimento útil e socialmente relevante. Ao propor um instrumento legal concreto, o estudo não apenas descreve um problema ou avalia alternativas, mas apresenta uma solução estruturada, juridicamente fundamentada e alinhada às demandas contemporâneas de proteção digital no contexto urbano.

5.4 PROPOSIÇÃO DO MARCO LEGAL

A crescente digitalização dos serviços públicos municipais, somada à fragilidade institucional observada em diversas administrações locais, evidencia a urgência de proposições normativas que contribuam para estruturar uma governança cibernética efetiva. A proposição de um marco legal municipal de cibersegurança surge, assim, como resposta à ausência de

normativas específicas, estruturas administrativas organizadas e políticas de prevenção digital nas esferas subnacionais do poder público.

A estrutura aqui proposta parte da constatação empírica de que, nos municípios analisados da região da AMREC, há uma significativa carência de políticas voltadas à segurança da informação e à proteção de dados, mesmo após a promulgação de legislações como a Lei Geral de Proteção de Dados (LGPD) e a consolidação do Marco Civil da Internet. Essa ausência de normatização reflete não apenas um descompasso entre a legislação federal e a realidade municipal, mas também a urgência de instrumentos legais que ajudem os municípios a internalizar as diretrizes nacionais com base em sua realidade institucional.

A proposição está ancorada em três fundamentos essenciais: o legal-normativo, o institucional-operacional e o epistemológico. O primeiro, de caráter jurídico, refere-se à necessidade de conformidade com os marcos regulatórios já estabelecidos em nível federal. O Marco Civil da Internet (Lei nº 12.965/2014), a LGPD (Lei nº 13.709/2018) e, mais recentemente, o Decreto nº 11.856/2023, que institui a Política Nacional de Cibersegurança (PNCiber), são dispositivos que, embora abrangentes, demandam regulamentações locais para garantir sua efetiva aplicação.

O fundamento normativo exige que o marco municipal esteja alinhado com os direitos fundamentais previstos na Constituição, com o regime da responsabilização civil do Estado, e com os princípios da administração pública. A LGPD, ao estabelecer o tratamento adequado de dados pessoais, atribui ao Poder Público a responsabilidade pela integridade, confidencialidade e segurança das informações sob sua guarda. Já o Marco Civil assegura os princípios da privacidade, liberdade de expressão e proteção da neutralidade da rede, criando obrigações também para os entes subnacionais. A PNCiber, por sua vez, explicita a necessidade de atuação coordenada entre os entes federativos, reconhecendo o papel dos municípios na proteção do espaço digital público.

O segundo fundamento, institucional-operacional, remete à necessidade de criação de estruturas administrativas, normativas e organizacionais dentro das prefeituras. O estudo aplicado na AMREC evidencia que a ausência de órgãos, cargos ou comissões com atribuições específicas em segurança da informação impede a adoção de medidas mínimas de prevenção e resposta a incidentes cibernéticos. Assim, um marco legal eficaz deve prever a constituição de uma governança interna formalizada, capaz de implementar, fiscalizar e revisar continuamente as ações em cibersegurança.

Esse fundamento está em consonância com os aportes teóricos da literatura identificada no Estudo I da tese, especialmente nas abordagens de natureza institucional, onde

se reconhece que a cibersegurança não pode ser tratada como um conjunto de medidas tecnológicas isoladas, mas como uma política pública que requer liderança, recursos, coordenação intersetorial e integração normativa. A ausência de políticas internas, como planos de contingência ou manuais de boas práticas, reforça a necessidade de um modelo normativo orientador.

O terceiro fundamento é epistemológico e refere-se à base conceitual que sustenta a proposição normativa. Como descrito no Estudo I, três grandes abordagens estruturam o campo da cibersegurança pública: a técnico-operacional, a institucional e a sociotécnica. A corrente técnico-operacional trata da necessidade de protocolos, ferramentas e práticas específicas, como backup, criptografia, controle de acessos e gestão de riscos. A institucional destaca a importância de marcos legais, definição de competências e estrutura de governança. Por sua vez, a abordagem sociotécnica, apoiada por autores como Dunn Cavelty e Nye, trata a cibersegurança como um campo complexo, onde interagem tecnologia, valores sociais, direitos fundamentais e processos políticos.

Ao se considerar essas três abordagens em conjunto, torna-se evidente que uma política de segurança digital eficaz em nível municipal deve ser holística e integrada. A legislação proposta deve contemplar os aspectos operacionais e tecnológicos, mas também prever instrumentos de planejamento, controle e responsabilização, além de incorporar mecanismos de participação, educação digital e proteção cidadã.

Com base nesses fundamentos, propõe-se uma estrutura composta por cinco grandes categorias que devem compor o conteúdo de um marco legal de cibersegurança em nível municipal. Essas categorias derivam tanto da análise legal quanto da revisão teórica e dos dados coletados no campo empírico. São elas: (i) fundamentos e objetivos da política de cibersegurança; (ii) estrutura institucional de governança cibernética; (iii) normatização interna e gestão de riscos; (iv) capacitação e cultura organizacional; e (v) mecanismos de transparência e controle social.

A primeira categoria, de fundamentos e objetivos, deve consolidar os princípios que orientam a política pública municipal, alinhando-a com os direitos previstos na LGPD e no Marco Civil da Internet. Isso inclui a proteção da privacidade, a autodeterminação informativa, a soberania digital e a promoção da cidadania digital. Além disso, o marco deve declarar expressamente o compromisso com a prevenção de riscos cibernéticos e com a institucionalização da segurança da informação como valor público.

A segunda categoria refere-se à estrutura institucional, e contempla a formalização de órgãos, cargos e instâncias internas responsáveis pela coordenação da política de

cibersegurança. Deve prever a nomeação de um Encarregado de Dados Pessoais (DPO), a criação de um núcleo técnico de segurança da informação e, quando possível, a instituição de um Comitê Municipal de Cibersegurança com representação multissetorial. Essa estrutura deve garantir articulação entre áreas jurídicas, administrativas, de tecnologia e comunicação.

A terceira categoria está ligada à normatização interna e à gestão de riscos, e envolve a elaboração de documentos normativos como a Política de Segurança da Informação (PSI), o plano de contingência, o plano de resposta a incidentes e o protocolo de classificação da informação. Tais documentos devem estabelecer fluxos, responsabilidades, sanções e procedimentos em caso de eventos adversos, bem como requisitos mínimos de segurança em contratações públicas de tecnologia.

A quarta categoria compreende as ações voltadas à capacitação e à cultura organizacional. O marco legal deve prever programas contínuos de formação e conscientização, tanto para servidores quanto para gestores, além de estratégias educativas voltadas à população. A literatura demonstra que a formação técnica sem cultura organizacional é insuficiente, sendo necessário que os princípios da proteção de dados e da segurança digital sejam incorporados ao cotidiano institucional.

A quinta e última categoria se refere aos mecanismos de transparência, participação e controle social. O marco deve instituir obrigações de publicidade dos relatórios de conformidade com a LGPD, dos registros de incidentes e das auditorias internas. Também deve prever a participação cidadã na formulação de políticas digitais, por meio de conselhos, ouvidorias e canais digitais de escuta ativa. A prestação de contas nesse campo é essencial para fortalecer a confiança da população e a legitimidade das ações públicas.

A síntese das cinco categorias está representada no Quadro 25, ao final desta seção. O quadro não substitui a legislação, mas organiza visualmente os elementos centrais da proposta e suas respectivas referências normativas e teóricas, servindo como base para a redação futura de um projeto de lei ou decreto municipal.

Do ponto de vista empírico, os dados colhidos na região da AMREC evidenciam de maneira contundente a ausência desses elementos nas administrações locais. A pesquisa revelou que nenhum dos municípios investigados possui política de segurança da informação institucionalizada, tampouco plano de resposta a incidentes ou estrutura técnica dedicada à proteção de dados. Em grande parte das administrações, não há sequer conhecimento sobre as obrigações trazidas pela LGPD, e a figura do encarregado de dados (DPO) é desconhecida ou inexistente.

Outro achado preocupante refere-se à ausência de ações de capacitação. Servidores das áreas de TI relataram não ter recebido treinamento específico sobre proteção de dados ou gestão de riscos digitais. As atividades de formação, quando ocorrem, concentram-se em aspectos técnicos básicos e não alcançam os servidores de áreas administrativas, jurídicas ou de atendimento ao público, que frequentemente lidam com dados sensíveis da população.

Os portais de transparência municipais, por sua vez, não apresentam informações sobre a gestão de dados, a proteção da informação ou a adoção de medidas de segurança cibernética. Isso aponta para uma completa invisibilidade do tema na esfera pública, dificultando o controle social e a responsabilização institucional em casos de falha.

Considerando esse cenário, a proposição de um marco legal estruturado pode representar um divisor de águas na construção da cibersegurança pública local. Ao integrar fundamentos legais, categorias institucionais e evidências empíricas, a estrutura proposta visa ser adaptável às realidades dos municípios brasileiros, respeitando as diferentes capacidades institucionais, mas garantindo o cumprimento mínimo dos direitos fundamentais à privacidade, à informação e à proteção digital.

Quadro 25 – Estrutura Propositiva do Marco Legal Municipal de Cibersegurança

Categoria	Elementos-Chave
Fundamentos e Objetivos da Política de Cibersegurança	*- Princípios alinhados à LGPD e ao Marco Civil da Internet* *- Proteção da privacidade e autodeterminação informativa* *- Soberania digital e cidadania digital* *- Compromisso com prevenção de riscos* *- Institucionalização da segurança da informação como valor público*
Estrutura Institucional de Governança Cibernética	*- Nomeação de Encarregado de Dados Pessoais (DPO)* *- Criação de núcleo técnico de segurança da informação* *- Comitê Municipal de Cibersegurança com representação multissetorial* *- Articulação entre áreas jurídicas, administrativas, de TI e comunicação*
Normatização Interna e Gestão de Riscos	*- Política de Segurança da Informação (PSI)* *- Plano de contingência e de resposta a incidentes* *- Protocolo de classificação da informação* *- Definição de fluxos, responsabilidades e sanções* *- Requisitos mínimos de segurança em contratações públicas de TI*
Capacitação e Cultura Organizacional	*- Programas contínuos de formação e conscientização para servidores e gestores* *- Estratégias educativas voltadas à população* *- Integração dos princípios de proteção de dados e segurança digital no cotidiano institucional*

Categoria	Elementos-Chave
Mecanismos de Transparência, Participação e Controle Social	*- Publicidade de relatórios de conformidade com a LGPD* *- Divulgação de registros de incidentes e auditorias internas* *- Participação cidadã via conselhos, ouvidorias e canais digitais de escuta ativa*

Fonte: Elaborado pelo autor (2025).

A consolidação da estrutura propositiva do Marco Legal Municipal de Cibersegurança representa um avanço significativo na organização de mecanismos institucionais voltados à proteção do espaço digital local. Ao reunir fundamentos normativos, diagnósticos de maturidade e parâmetros técnicos, o modelo aqui proposto oferece não apenas um arcabouço jurídico, mas também um guia estratégico para orientar a tomada de decisões e a alocação de recursos. Essa abordagem integrada busca garantir que a política de cibersegurança municipal seja capaz de responder de forma eficiente a ameaças emergentes, promovendo simultaneamente a resiliência institucional e o fortalecimento do desenvolvimento socioeconômico regional. Nesse sentido, a etapa seguinte deste estudo consiste em apresentar um conjunto de diretrizes estratégicas que, ancoradas no marco legal proposto, possam orientar de forma estruturada e sustentável a implementação das políticas de cibersegurança na região da AMREC.

5.4.1 Diretrizes estratégicas para o Marco Legal em Cibersegurança

A consolidação de um marco legal municipal em cibersegurança exige que sua implementação seja guiada por diretrizes estratégicas capazes de orientar tanto a formulação quanto a execução de políticas públicas. Essas diretrizes, fundamentadas nas evidências empíricas obtidas no diagnóstico de maturidade institucional da região da AMREC e nos referenciais teóricos discutidos nos Estudos I, II e III, representam um conjunto de orientações normativas que visam garantir coerência, continuidade e efetividade nas ações voltadas à proteção do ambiente digital. Conforme destacam Mishra *et al.* (2022), a capacidade regulatória e a eficácia das políticas dependem diretamente da articulação entre dimensões técnicas, institucionais e sociopolíticas, sendo imprescindível que as diretrizes aqui propostas estejam alinhadas a essa visão integrada.

O primeiro eixo estratégico se refere ao fortalecimento da governança e da coordenação institucional. A fragmentação das responsabilidades e a ausência de estruturas formais de gestão da segurança cibernética nos municípios da AMREC evidenciam a

necessidade de criar instâncias permanentes de coordenação, como comitês municipais ou regionais de cibersegurança, com representação multissetorial. Essa medida vai ao encontro da perspectiva institucionalista descrita por Mishra *et al.* (2022), que destaca a importância de arranjos de governança que articulem atores públicos e privados. A criação desses comitês deve ser acompanhada da definição clara de competências, fluxos de decisão e mecanismos de supervisão, garantindo que as políticas formuladas sejam implementadas com transparência e *accountability*, conforme defendem Nissenbaum (2005) e Schubert e Barrett (2024).

Além disso, é fundamental que os municípios estabeleçam marcos de governança que transcendam ciclos políticos e assegurem a continuidade administrativa. Conforme observa Schmidt (2008), a descontinuidade de diretrizes vigentes acarreta desperdício de recursos e enfraquece a capacidade de resposta institucional. Assim, a formalização de planos plurianuais de cibersegurança, com metas e indicadores, torna-se um instrumento jurídico e administrativo essencial para assegurar previsibilidade e consistência nas ações.

A coordenação institucional deve ainda promover a integração com políticas públicas já existentes, especialmente aquelas voltadas à modernização administrativa, inclusão digital e proteção de dados. Essa integração evita sobreposição de esforços e amplia a sinergia entre iniciativas, permitindo que a cibersegurança seja tratada como um pilar transversal da gestão pública, como sugerem Margetts e Dorobantu (2019) ao analisar o impacto das escolhas tecnológicas sobre a equidade e a eficiência das políticas públicas.

A governança deve incorporar canais permanentes de participação social, garantindo que a formulação de políticas de cibersegurança seja sensível às demandas e percepções da população. Como destacam Tura e Ojanen (2022), a inclusão de múltiplas vozes na definição das estratégias de segurança digital não apenas aumenta a legitimidade das decisões, mas também contribui para o fortalecimento da cidadania digital.

O segundo eixo estratégico diz respeito à proteção de infraestruturas e serviços críticos. Os resultados do Estudo III evidenciaram que a maioria dos municípios da AMREC carece de planos de contingência e de protocolos estruturados para a proteção de sistemas essenciais, o que aumenta a vulnerabilidade frente a incidentes cibernéticos. De acordo com Srivastava *et al.* (2023), a proteção de infraestruturas críticas é condição indispensável para a estabilidade social e econômica, uma vez que sua interrupção impacta diretamente serviços de saúde, energia, transporte e administração pública.

Para enfrentar essa lacuna, as diretrizes propõem a adoção obrigatória de práticas de *security by design* e *privacy by design* em todos os sistemas e serviços digitais públicos. Essa abordagem, defendida por Nissenbaum (2005) e reforçada por Zuboff (2019), garante que a

segurança e a proteção de dados sejam incorporadas desde a concepção dos sistemas, prevenindo riscos e minimizando vulnerabilidades. Além disso, recomenda-se que os municípios realizem periodicamente auditorias técnicas e testes de invasão (*pen tests*), de modo a identificar e corrigir fragilidades antes que possam ser exploradas.

Outro aspecto fundamental é a formalização de planos de continuidade de negócios e recuperação de desastres, que definam protocolos claros para a manutenção ou rápida restauração dos serviços críticos em caso de incidentes. Como observam Parmentola *et al.* (2022), a resiliência digital está diretamente ligada à capacidade de absorver e se recuperar de impactos, o que exige não apenas tecnologia, mas processos bem estruturados e testados regularmente.

A proteção de infraestruturas críticas deve ser tratada como responsabilidade compartilhada entre diferentes esferas de governo e entre os setores público e privado. A cooperação interinstitucional e a definição de padrões mínimos de segurança para fornecedores e prestadores de serviços são elementos indispensáveis para reduzir a superfície de ataque e aumentar a robustez do ecossistema digital municipal.

O terceiro eixo estratégico aborda a capacitação e a cultura de segurança, elementos essenciais para a efetividade de qualquer política de cibersegurança. Os estudos de Tura e Ojanen (2022) mostram que a inclusão digital e a justiça informacional dependem de investimentos contínuos em formação e conscientização, tanto para servidores públicos quanto para a população em geral. No contexto da AMREC, onde o diagnóstico revelou a baixa especialização técnica em diversas prefeituras, a criação de programas de capacitação estruturados é uma prioridade.

Esses programas devem contemplar desde treinamentos técnicos avançados para equipes de TI até oficinas básicas de segurança digital para servidores de todas as áreas. Como argumenta Choo (2011), a segurança cibernética é tão forte quanto seu elo mais fraco, e este, muitas vezes, reside no comportamento humano. Assim, campanhas de sensibilização sobre *phishing*, engenharia social e boas práticas de uso de sistemas devem ser permanentes e adaptadas ao perfil dos usuários.

A capacitação também deve estar integrada a processos de certificação e avaliação periódica de competências, de forma a garantir a atualização contínua frente à evolução das ameaças. Nesse sentido, a criação de parcerias com universidades, institutos de pesquisa e entidades do terceiro setor pode ampliar o alcance e a qualidade das ações formativas, além de estimular a produção de conhecimento aplicado à realidade local.

Logo, fomentar uma cultura organizacional voltada à segurança implica inserir a cibersegurança como valor institucional, presente em todos os níveis da administração pública. Como observa Parmentola *et al.* (2022), a resiliência digital é resultado não apenas de ferramentas e processos, mas de uma mentalidade coletiva que reconhece a segurança como parte integrante da prestação de serviços públicos de qualidade.

O quarto eixo estratégico centra-se na gestão de dados e na privacidade, reconhecendo que a proteção das informações pessoais e institucionais é elemento estruturante de qualquer marco legal de cibersegurança. Conforme Nissenbaum (2005) e Schubert e Barrett (2024) defendem, a governança de dados deve ser entendida como processo técnico-político, no qual as decisões sobre coleta, uso e compartilhamento de informações precisam ser transparentes, participativas e alinhadas a princípios democráticos.

Nesse sentido, os municípios devem instituir políticas formais de governança de dados, definindo responsabilidades, procedimentos e padrões para todo o ciclo de vida das informações. Essas políticas devem incluir critérios claros para classificação da informação, regras de acesso e mecanismos de auditoria independentes, a fim de garantir o cumprimento da LGPD e de outros marcos normativos aplicáveis.

A privacidade deve ser tratada como direito fundamental, incorporando princípios de minimização de dados, anonimização e consentimento informado. Como alerta Zuboff (2019), a captura indiscriminada e o uso opaco de dados alimentam práticas de vigilância incompatíveis com a democracia e com a autonomia dos cidadãos. Portanto, o marco legal deve conter salvaguardas robustas contra usos abusivos ou indevidos de informações pessoais, inclusive no contexto de contratos com fornecedores de tecnologia.

Além disso, é imprescindível a criação de instâncias internas de supervisão e controle, como encarregados de proteção de dados (DPOs) e comissões de ética digital, capazes de monitorar a conformidade e de responder rapidamente a incidentes de violação. Essas instâncias devem atuar com independência e ter acesso direto às lideranças municipais, garantindo que a gestão de dados não seja subordinada a interesses político-partidários.

O quinto e último eixo estratégico diz respeito à cooperação e à integração regional. A natureza transfronteiriça das ameaças cibernéticas, associada à heterogeneidade das capacidades técnicas entre os municípios da AMREC, exige mecanismos de colaboração contínua e estruturada. Como defendem Visvizi e Del Hoyo (2021), modelos de governança multiescalar, que integrem ações locais, nacionais e internacionais, são fundamentais para aumentar a resiliência coletiva.

Nesse sentido, recomenda-se a criação de uma rede regional de cibersegurança, composta por representantes técnicos e políticos de cada município, com o objetivo de compartilhar informações sobre ameaças, vulnerabilidades e boas práticas. Essa rede deve operar com protocolos claros de comunicação e resposta a incidentes, permitindo que a detecção em um município possa gerar ações preventivas nos demais.

A cooperação também deve incluir acordos formais de apoio técnico e jurídico, possibilitando que municípios com maior capacidade ofereçam suporte a aqueles com estrutura mais limitada. Essa lógica de solidariedade institucional fortalece a coesão regional e potencializa o uso eficiente de recursos, evitando duplicação de esforços.

A integração regional deve ser articulada com órgãos estaduais e federais, bem como com iniciativas internacionais, a fim de alinhar padrões, acessar recursos estratégicos e ampliar a capacidade de dissuasão contra ameaças. Como apontam Chander *et al.* (2021), a fragmentação regulatória compromete a eficácia da proteção digital, e a harmonização normativa é passo indispensável para consolidar um ecossistema digital seguro e inclusivo.

A consolidação dessas cinco diretrizes estratégicas confere ao marco legal proposto um caráter abrangente e coerente com as necessidades identificadas no diagnóstico da AMREC. Ao articular governança, proteção de infraestruturas críticas, capacitação, gestão de dados e cooperação regional, o conjunto proposto não se limita a responder a vulnerabilidades imediatas, mas estrutura um modelo de governança cibernética sustentável, capaz de se adaptar às transformações tecnológicas e sociais.

Esse alinhamento entre teoria e prática, sustentado por referências como Mishra *et al*. (2022), Nissenbaum (2005), Zuboff (2019) e Schubert e Barrett (2024), demonstra que a efetividade da cibersegurança não é resultado apenas de investimentos tecnológicos, mas de um arranjo institucional sólido, ancorado em princípios democráticos e na participação social. Assim, as diretrizes aqui apresentadas se configuram como base normativa e operacional para que os municípios da região avancem de forma coordenada e equitativa, superando a fragmentação atualmente observada.

Ao mesmo tempo, essas diretrizes reconhecem que a cibersegurança é um bem público e que sua proteção requer compromisso político de longo prazo, evitando soluções episódicas ou dependentes de ciclos eleitorais. Conforme argumentam Parmentola *et al.* (2022), a resiliência digital depende da integração entre capacidades técnicas e cultura organizacional, e o marco legal proposto busca institucionalizar essa integração no âmbito municipal e regional.

Dessa forma, a proposição deste marco legal, acompanhada das diretrizes estratégicas aqui delineadas, oferece não apenas um instrumento jurídico, mas um plano de ação

estruturado para promover a segurança digital como vetor de desenvolvimento socioeconômico. As considerações finais a seguir retomam as principais contribuições deste estudo e indicam caminhos para a implementação e monitoramento contínuo dessas medidas, consolidando a cibersegurança como pilar central da governança pública na AMREC.

Quadro 26 – Relação entre elementos-chave, diretrizes estratégicas e o Marco Legal

Diretriz Estratégica	Elementos-Chave	Marco Legal
Governança e Coordenação Institucional; Gestão de Dados e Privacidade	- Princípios alinhados à LGPD e ao Marco Civil da Internet	Art. 7º, I e II; Art. 8º, I
Gestão de Dados e Privacidade	- Proteção da privacidade e autodeterminação informativa	Art. 7º, I; Art. 8º, I
Governança e Coordenação Institucional	- Soberania digital e cidadania digital	Art. 2º, VI
Proteção de Infraestruturas e Serviços Críticos	- Compromisso com prevenção de riscos	Art. 5º, III; Art. 7º, V e VI
Governança e Coordenação Institucional	- Institucionalização da segurança da informação como valor público	Art. 2º, II e III; Art. 9º; Art. 13
Gestão de Dados e Privacidade	- Nomeação de Encarregado de Dados Pessoais (DPO)	Art. 3º, VII
Governança e Coordenação Institucional	- Criação de núcleo técnico de segurança da informação	Art. 5º
Governança e Coordenação Institucional	- Comitê Municipal de Cibersegurança com representação multissetorial	Art. 4º
Governança e Coordenação Institucional	- Articulação entre áreas jurídicas, administrativas, de TI e comunicação	Art. 4º, §2º, I a IV
Governança e Coordenação Institucional; Gestão de Dados e Privacidade	- Política de Segurança da Informação (PSI)	Art. 4º, §2º, I; Art. 7º, II
Proteção de Infraestruturas e Serviços Críticos	- Plano de contingência e de resposta a incidentes	Art. 5º, III; Art. 7º, V
Gestão de Dados e Privacidade	- Protocolo de classificação da informação	Art. 7º, IV
Governança e Coordenação Institucional	- Definição de fluxos, responsabilidades e sanções	Art. 4º, §2º; Art. 15 e 16
Proteção de Infraestruturas e Serviços Críticos; Gestão de Dados e Privacidade	- Requisitos mínimos de segurança em contratações públicas de TI	Art. 8º
Capacitação e Cultura de Segurança	- Programas contínuos de formação e conscientização para servidores e gestores	Art. 9º
Capacitação e Cultura de Segurança; Cooperação e Integração Regional	- Estratégias educativas voltadas à população	Art. 10
Governança e Coordenação Institucional; Gestão de Dados e Privacidade	- Integração dos princípios de proteção de dados e segurança digital no cotidiano institucional	Art. 7º, I e II; Art. 9º e 10
Transparência e Participação Social	- Publicidade de relatórios de conformidade com a LGPD	Art. 11º, I
Transparência e Participação Social	- Divulgação de registros de incidentes e auditorias internas	Art. 11º, II e III
Cooperação e Integração Regional; Transparência e Participação Social	- Participação cidadã via conselhos, ouvidorias e canais digitais de escuta ativa	Art. 4º, §2º, IV; Art. 12

Fonte: Elaborado pelo autor (2025).
Obs.: O texto integral do marco legal proposto encontra-se disponível no apêndice desta tese.

A formulação das diretrizes estratégicas para o marco legal em cibersegurança representa a consolidação de um conjunto de princípios e ações capazes de sustentar políticas públicas eficientes e alinhadas às necessidades do contexto municipal. Ao estabelecer parâmetros claros para governança, proteção de infraestruturas, gestão de dados, capacitação e integração regional, estas diretrizes fornecem bases sólidas para a construção de um ambiente digital seguro e resiliente.

A coerência interna entre os eixos propostos, aliada à sua aderência a marcos regulatórios nacionais e boas práticas consolidadas, reforça a viabilidade de sua aplicação. Trata-se de um arcabouço que, além de atender a requisitos técnicos e jurídicos, incorpora uma dimensão sociopolítica, valorizando a participação social, a transparência e a preservação dos direitos fundamentais no espaço digital.

5.5 CONSIDERAÇÕES FINAIS

O Estudo IV representa a integração entre teoria, diagnóstico e proposição, consolidando-se como a etapa em que o conhecimento produzido ao longo da pesquisa se traduz em um instrumento normativo. A elaboração do marco legal municipal em cibersegurança permitiu operacionalizar conceitos e diretrizes discutidos nos capítulos anteriores, conferindo tangibilidade ao objetivo central desta tese.

A proposta normativa evidencia a possibilidade de alinhar referenciais jurídicos consolidados, como a LGPD e o Marco Civil da Internet, a uma abordagem local e setorial, adaptada às realidades e capacidades dos municípios. Esse alinhamento é essencial para garantir que as cidades tenham condições de implementar medidas efetivas de proteção digital sem desconsiderar os princípios de soberania, cidadania e participação social.

O processo de construção do marco legal reforçou a importância de tratar a cibersegurança como valor público, integrando-a à agenda estratégica das administrações municipais. Ao estabelecer diretrizes para governança, proteção de infraestruturas, gestão de dados, capacitação e cooperação regional, o estudo propõe uma arquitetura normativa que transcende a perspectiva técnica, incorporando dimensões políticas e sociais.

Além disso, o estudo destaca a contribuição da governança multissetorial, contemplada na criação do Comitê Municipal de Cibersegurança e no envolvimento de representantes da sociedade civil, setor privado e academia. Essa abordagem inclusiva amplia a legitimidade do marco legal e favorece a construção de soluções mais robustas e sustentáveis.

O Estudo IV também reafirma que a proteção das infraestruturas críticas digitais é condição indispensável para a continuidade dos serviços públicos essenciais. Ao prever protocolos de contingência, classificação da informação e requisitos mínimos para contratações de TI, a proposta normativa busca mitigar riscos e aumentar a resiliência institucional.

Outro aspecto relevante é o investimento na cultura de segurança, tanto no âmbito interno da administração pública quanto na sensibilização da população. Programas contínuos de capacitação, aliados a campanhas de conscientização, fortalecem a postura preventiva e reduzem a vulnerabilidade diante de ameaças cibernéticas.

A transparência, prevista na obrigatoriedade de divulgação de relatórios e incidentes, contribui para o controle social e para a melhoria contínua das práticas de segurança. Essa abertura de informações, quando realizada de forma responsável e equilibrada, fortalece a confiança da sociedade nas instituições públicas.

Do ponto de vista metodológico, o estudo demonstrou a eficácia de uma abordagem propositiva sustentada por diagnóstico prévio e fundamentação teórica sólida. Essa combinação favoreceu a elaboração de um documento normativo tecnicamente consistente e juridicamente aplicável.

Ainda que se trate de uma proposta inicial, sujeita a adaptações conforme as especificidades de cada realidade municipal, o marco legal apresentado oferece uma base estruturada sobre a qual é possível desenvolver e aprofundar políticas locais de cibersegurança. A flexibilidade e a adaptabilidade do texto legal são características que aumentam sua utilidade prática.

A análise realizada neste estudo reforça que a cibersegurança não é apenas uma questão técnica, mas também um desafio de governança, política pública e desenvolvimento socioeconômico. A integração dessas dimensões na proposta normativa é um dos pontos mais relevantes do trabalho. A contribuição prática do marco legal proposto complementa o aporte teórico da tese, demonstrando que é possível transformar conhecimento científico em instrumentos efetivos de política pública.

6 CONSIDERAÇÕES FINAIS DA TESE

Esta tese investigou a cibersegurança como elemento estratégico para o desenvolvimento socioeconômico de cidades, articulando conceitos, evidências e práticas capazes de sustentar a transformação digital urbana de forma segura, inclusiva e resiliente. Partindo da compreensão de que a proteção de infraestruturas críticas, dados e serviços digitais é condição necessária para a continuidade de funções essenciais e para a atração de investimentos, o estudo explorou como políticas, tecnologias e governança podem convergir para ampliar a competitividade urbana. A pesquisa abordou tanto dimensões técnicas quanto institucionais, evidenciando que a cibersegurança deve ser tratada como um ativo de desenvolvimento e não apenas como uma função operacional restrita a mitigar riscos.

O Estudo I consistiu em uma revisão bibliométrica e sistemática da literatura com o objetivo de mapear e compreender as abordagens acadêmicas sobre governança cibernética e segurança da informação no contexto governamental, identificando as principais tendências, construtos teóricos e lacunas de pesquisa. Já o Estudo II buscou aprofundar a compreensão das inter-relações entre cibersegurança e desenvolvimento, estruturando o campo conceitual em *clusters* temáticos identificados na literatura. Por meio dessa organização, buscou-se evidenciar constructos-chave e conexões conceituais que sustentam a formulação de políticas e estratégias, oferecendo uma base teórica para subsidiar análises e proposições nos estudos subsequentes.

O Estudo III aprofundou a análise ao realizar entrevistas com representantes municipais, mensurando o nível de maturidade em governança cibernética e identificando lacunas institucionais e capacidades locais, de modo a revelar fragilidades e potencialidades para o fortalecimento de políticas públicas na área. Por fim, o Estudo IV teve caráter propositivo, desenvolvendo um marco legal municipal de cibersegurança com base nas evidências empíricas dos estudos anteriores, apresentando diretrizes normativas, organizacionais e operacionais voltadas ao fortalecimento da governança digital e à promoção de uma infraestrutura segura e resiliente nos municípios analisados.

A articulação desses quatro estudos permitiu demonstrar que a cibersegurança, quando integrada a estratégias de desenvolvimento socioeconômico, potencializa inovação, confiança e sustentabilidade. As evidências apontam que investir em segurança digital não é apenas proteger contra ameaças, mas também criar condições para o florescimento de novos modelos de negócios, para a ampliação do capital social e para o fortalecimento da competitividade global das cidades. Assim, este trabalho contribui para o avanço do conhecimento científico e oferece subsídios práticos para a formulação de políticas públicas e

estratégias corporativas, reforçando a visão de que a cibersegurança é parte integrante e indissociável do futuro das cidades inteligentes.

6.1 RELAÇÃO ENTRE OS ESTUDOS DA TESE

O presente trabalho foi estruturado a partir de quatro estudos complementares que, embora possuam métodos, escopos e focos analíticos distintos, articulam-se de forma progressiva e integrada para responder à questão central da tese: compreender a cibersegurança como fator estratégico para o desenvolvimento social e econômico de municípios, especialmente no contexto da Região da AMREC. Cada estudo cumpre uma função específica dentro do encadeamento lógico da pesquisa, contribuindo para a construção de um arcabouço teórico-prático que sustente propostas concretas, garantindo coerência metodológica e aplicabilidade no contexto estudado.

O Estudo I estabeleceu a base conceitual e analítica da tese ao realizar uma análise bibliométrica e uma revisão sistemática da literatura científica recente sobre cibersegurança, regulação e desenvolvimento. O mapeamento de tendências, limitações e lacunas permitiu identificar que, apesar do crescimento da produção científica, predomina uma abordagem técnico-normativa e fragmentada, com escassa articulação com as realidades institucionais locais e com a dimensão socioeconômica. Essa constatação orientou o desenvolvimento dos estudos subsequentes, ao evidenciar a necessidade de contextualizar as discussões globais em marcos regulatórios e realidades regionais específicas.

O Estudo II aprofundou o trabalho iniciado no Estudo I, avançando na identificação de constructos emergentes que conectam cibersegurança e desenvolvimento. Utilizando técnicas de análise de *clusters* temáticos, o estudo revelou a existência de núcleos conceituais interdependentes que extrapolam a dimensão puramente técnica e incorporam categorias como governança de dados, soberania informacional, resiliência digital e inclusão tecnológica. Essa etapa foi fundamental para traduzir as tendências globais identificadas na literatura em categorias analíticas operacionais, capazes de dialogar com a realidade das instituições públicas municipais.

A transição do Estudo II para o Estudo III marca a passagem da análise predominantemente teórica e conceitual para a investigação empírica de campo. Com foco na Associação dos Municípios da Região Carbonífera (AMREC), o Estudo III aplicou as categorias e indicadores elaborados nas etapas anteriores para diagnosticar a maturidade institucional das prefeituras em relação à cibersegurança. O levantamento documental, a análise

de marcos normativos locais e a identificação de práticas vigentes permitiram avaliar a capacidade de resposta, a estrutura regulatória e o nível de integração da segurança digital às políticas públicas municipais.

Os resultados do Estudo III confirmaram, no plano empírico, várias hipóteses levantadas nos estudos iniciais: a fragmentação normativa, a dependência de soluções proprietárias e a baixa integração da cibersegurança ao planejamento de desenvolvimento socioeconômico. Ao mesmo tempo, revelaram experiências pontuais e boas práticas que indicam caminhos para fortalecer a governança digital municipal. Esses achados, ao conectarem a teoria com a prática, forneceram subsídios diretos para a formulação de diretrizes estratégicas no Estudo IV.

O Estudo IV encerra o ciclo de investigação ao propor um marco legal municipal em cibersegurança para a região da AMREC. A proposta foi construída com base no diagnóstico institucional realizado no Estudo III, nas categorias teóricas consolidadas no Estudo II e nas tendências e boas práticas identificadas no Estudo I. Trata-se, portanto, de um estudo propositivo que converte evidências científicas em instrumentos normativos, articulando parâmetros técnicos, institucionais e sociopolíticos.

A relação entre os estudos é, assim, cumulativa e mutuamente reforçada. O Estudo I, ao identificar lacunas e potenciais da literatura, orientou a seleção de categorias no Estudo II. Este, por sua vez, refinou os conceitos e forneceu um quadro interpretativo para a análise empírica do Estudo III. Os resultados deste último, ao revelarem o estado real das capacidades institucionais locais, fundamentaram as propostas do Estudo IV. Esse encadeamento garante que as proposições normativas finais não sejam abstrações deslocadas, mas respostas diretamente ancoradas na realidade regional.

Do ponto de vista metodológico, a sequência dos estudos representa uma triangulação progressiva entre métodos quantitativos, qualitativos e propositivos. O Estudo I predominou na abordagem quantitativa (bibliometria) com suporte qualitativo (revisão sistemática). O Estudo II consolidou a análise qualitativa conceitual, enquanto o Estudo III adotou métodos qualitativos de diagnóstico documental e normativo, complementados por elementos de análise comparativa. O Estudo IV, por sua vez, integrou os achados anteriores num exercício normativo-propositivo, buscando aplicabilidade prática.

Essa articulação também se manifesta na conexão entre escalas de análise. O Estudo I operou na escala global, examinando tendências e padrões internacionais. O Estudo II aproximou essa escala para uma perspectiva nacional e conceitual, destacando categorias adaptáveis ao contexto brasileiro. O Estudo III concentrou-se na escala local, diagnosticando a

realidade municipal da AMREC. Finalmente, o Estudo IV retornou a uma perspectiva regional, propondo um marco que integra princípios universais, requisitos nacionais e especificidades locais.

No plano conceitual, todos os estudos compartilham um eixo comum: a compreensão da cibersegurança como bem público e como vetor de desenvolvimento socioeconômico. Esse eixo orienta tanto as análises críticas do Estudo I quanto a construção de constructos no Estudo II, o diagnóstico de maturidade no Estudo III e a formulação normativa no Estudo IV. A coerência conceitual garante que, apesar das diferenças metodológicas, os quatro estudos dialoguem entre si de forma consistente.

Outro ponto de convergência é a incorporação de uma abordagem multissetorial e multiator. Desde o Estudo I, a literatura aponta a necessidade de articulação entre governos, setor privado e sociedade civil. O Estudo II traduziu essa exigência em categorias analíticas como governança de dados e resiliência digital. O Estudo III verificou empiricamente como essa articulação se apresenta — ou se ausenta — nas administrações municipais. O Estudo IV, por sua vez, propõe mecanismos normativos para institucionalizar essa cooperação.

Além disso, a progressão dos estudos reforça a importância de integrar dimensões técnicas e éticas da cibersegurança. O Estudo I evidenciou o predomínio de abordagens técnicas na literatura. O Estudo II incorporou a perspectiva sociotécnica e de justiça informacional. O Estudo III identificou que a ausência dessa integração compromete a efetividade das políticas locais. O Estudo IV formaliza diretrizes que equilibram requisitos técnicos com princípios democráticos, transparência e participação.

A interdependência entre os estudos também se observa no modo como cada um amplia o escopo do anterior. O Estudo I fornece a visão macro; o Estudo II refina o olhar para conceitos-chave; o Estudo III desce ao nível micro da gestão municipal; e o Estudo IV propõe um instrumento que conecta esses níveis, viabilizando a implementação prática. Assim, cada estudo é, ao mesmo tempo, resultado do anterior e insumo para o seguinte.

O conjunto dos quatro estudos representa uma jornada que vai da compreensão global à intervenção local, passando pela sistematização conceitual e pela verificação empírica. Essa trajetória assegura que a tese não apenas contribua para o avanço teórico no campo da cibersegurança, mas também ofereça um produto normativo aplicável, capaz de influenciar políticas públicas e fortalecer a capacidade institucional dos municípios.

6.2 CONTRIBUIÇÇOES TEÓRICAS DA TESE

A formulação das hipóteses desta tese resulta de um processo cumulativo e integrado que combina o arcabouço teórico desenvolvido nos Estudos I e II com as evidências empíricas observadas nos Estudos III e IV. A estratégia adotada buscou não apenas descrever ou diagnosticar fenômenos, mas construir proposições fundamentadas que expressem, de forma clara, as relações prováveis entre variáveis e conceitos identificados ao longo da investigação. Dessa forma, as hipóteses aqui apresentadas refletem tanto a compreensão teórica do fenômeno da cibersegurança no contexto do desenvolvimento socioeconômico quanto a constatação prática de suas manifestações na realidade dos municípios da Região da AMREC.

O processo de elaboração das hipóteses foi conduzido em duas etapas principais. Na primeira, derivaram-se hipóteses a partir da literatura científica e dos constructos emergentes identificados nas análises bibliométricas e conceituais (Estudos I e II). Esse exercício teórico permitiu identificar padrões, relações e lacunas no conhecimento, resultando em proposições que buscam testar ou validar conexões sugeridas pela teoria. Na segunda etapa, as hipóteses foram elaboradas a partir das observações e resultados empíricos, obtidos por meio de diagnóstico institucional, análise documental e avaliação normativa (Estudos III e IV). Esse procedimento possibilitou criar proposições alinhadas à realidade concreta e capazes de dialogar com problemas práticos de implementação de políticas públicas.

6.2.1 Hipóteses derivadas da teoria

Os Estudos I e II constituíram a base para a formulação das hipóteses teóricas. O Estudo I revelou que a literatura sobre cibersegurança, embora crescente, ainda apresenta forte fragmentação conceitual e predomínio de abordagens técnico-normativas. Identificou-se que, apesar de haver discussões sobre governança, regulação e desenvolvimento, poucas pesquisas exploram a cibersegurança em escalas subnacionais ou articulam esses conceitos de forma integrada. Essa constatação sugere que as dimensões técnica, institucional e sociotécnica precisam ser combinadas para compreender plenamente a relação entre segurança digital e desenvolvimento socioeconômico.

O Estudo II avançou ao organizar os constructos emergentes em *clusters* temáticos, revelando categorias como governança de dados, soberania informacional, resiliência digital e inclusão tecnológica. Essas categorias ampliam a compreensão da cibersegurança para além da simples proteção técnica, incorporando aspectos de justiça informacional, participação social e

articulação multiescalar. Ao conectar essas categorias com marcos regulatórios e práticas internacionais, o Estudo II reforçou a hipótese de que a maturidade institucional e a integração normativa são elementos centrais para fortalecer a segurança digital e, por consequência, promover o desenvolvimento.

A lógica de derivação das hipóteses teóricas, portanto, parte da premissa de que municípios não operam isoladamente no ecossistema da cibersegurança. Eles estão inseridos em redes complexas de regulação, dependências tecnológicas e fluxos de informação que atravessam escalas locais, nacionais e globais. Se a literatura indica que a integração de dimensões técnicas e sociotécnicas é um fator de sucesso para políticas nacionais, é razoável supor que a mesma lógica se aplique — com adaptações — ao nível municipal.

Hipóteses teóricas:

H1 – A maturidade institucional em cibersegurança, quando associada a estruturas robustas de governança de dados e soberania informacional, exerce influência positiva no desenvolvimento socioeconômico local, ampliando a capacidade de atração de investimentos, a competitividade e a inovação.

H2 – Marcos regulatórios municipais alinhados a princípios internacionais de proteção de dados e a práticas de *security by design* apresentam maior potencial de assegurar estabilidade institucional e reduzir vulnerabilidades sistêmicas, mesmo em contextos de limitações técnicas e orçamentárias.

H3 – A integração entre abordagens técnico-operacionais e sociotécnicas na formulação de políticas públicas de cibersegurança aumenta a efetividade da proteção digital, na medida em que combina salvaguardas tecnológicas com princípios de justiça informacional e participação social.

H4 – Municípios que incorporam a cibersegurança como elemento transversal em seus planos de desenvolvimento urbano tendem a apresentar maior resiliência digital, capacidade de resposta a incidentes e continuidade de serviços essenciais.

Nesse sentido, as hipóteses derivadas da teoria buscam testar se a incorporação de princípios amplamente discutidos na literatura (como *security by design*, governança participativa e marcos normativos robustos) realmente se traduz em benefícios para o desenvolvimento socioeconômico local. Além disso, essas hipóteses pretendem avaliar se as práticas regulatórias e institucionais identificadas em contextos globais e nacionais encontram ressonância ou barreiras no contexto subnacional brasileiro.

6.3 CONTRIBUIÇÕES EMPÍRICAS DA TESE

Os Estudos III e IV ofereceram a base para a formulação das hipóteses empíricas. O Estudo III, por meio de diagnóstico da maturidade institucional dos municípios da AMREC, demonstrou que, na maioria dos casos, a cibersegurança ainda não está plenamente integrada às estratégias de desenvolvimento socioeconômico local. Foram identificadas lacunas normativas, ausência de equipes técnicas especializadas, baixa interoperabilidade de sistemas e dependência de fornecedores externos, especialmente em soluções proprietárias. Esses fatores indicam que a capacidade de resposta a incidentes e a resiliência digital são desiguais e frequentemente insuficientes.

Já o Estudo IV propôs um marco legal municipal em cibersegurança, estruturado para responder a essas deficiências, estabelecendo diretrizes estratégicas, mecanismos de cooperação intermunicipal e parâmetros técnicos mínimos. Essa proposta foi construída a partir da constatação de que, sem normativas claras e estruturas institucionais estáveis, as ações de segurança digital tendem a ser reativas e fragmentadas. Assim, o Estudo IV evidenciou que a institucionalização da cibersegurança por meio de legislação específica pode gerar ganhos significativos de maturidade e resiliência, sobretudo quando acompanhada de mecanismos de capacitação e monitoramento.

6.3.1 Hipóteses derivadas dos achados empíricos

A lógica de construção das hipóteses empíricas baseia-se no confronto entre diagnóstico e solução proposta. Partindo das fragilidades constatadas no Estudo III e das diretrizes normativas do Estudo IV, buscou-se formular proposições que permitam verificar se a adoção de marcos regulatórios locais, mecanismos de cooperação e práticas de contratação mais estratégicas podem efetivamente alterar o nível de maturidade institucional e reduzir vulnerabilidades.

A análise das entrevistas revelou que os municípios da AMREC apresentam cenários institucionais bastante heterogêneos, variando desde estruturas mais organizadas e com certa familiaridade com práticas de proteção digital, até administrações com ausência completa de setores especializados ou políticas formais de segurança da informação. Essa

disparidade impõe o desafio de pensar a implantação do marco legal de forma escalonada e adaptativa, respeitando os diferentes níveis de maturidade institucional.

Para viabilizar a implementação da norma proposta, recomenda-se uma estratégia em três frentes complementares: (i) capacitação técnica das equipes municipais por meio de formações continuadas e parcerias com universidades ou entidades especializadas; (ii) criação de consórcios ou redes intermunicipais de cooperação, permitindo que municípios com menor capacidade técnica compartilhem recursos e soluções com aqueles mais avançados; e (iii) apoio técnico-normativo de instâncias estaduais ou federais, inclusive com editais de fomento, modelos-padrão de normatização e linhas de financiamento específicas para segurança cibernética. Essa abordagem modular e cooperativa pode assegurar maior aderência local e sustentabilidade da política proposta.

Além disso, as hipóteses empíricas têm caráter aplicado: não se limitam a explorar relações abstratas entre variáveis, mas propõem caminhos de intervenção que podem ser testados e monitorados ao longo do tempo. Ao fazê-lo, mantêm o vínculo direto com as necessidades práticas dos municípios e reforçam a relevância social e política desta pesquisa.

Hipóteses empíricas:

H5 – Municípios que possuem normativas próprias e estruturas administrativas específicas para a gestão da cibersegurança apresentam níveis superiores de maturidade institucional e menor vulnerabilidade digital em comparação àqueles sem regulamentação local.

H6 – A criação de mecanismos regionais de cooperação e compartilhamento de recursos técnicos em cibersegurança entre municípios eleva a eficiência na prevenção, detecção e resposta a incidentes, mesmo em localidades com baixa capacidade técnica individual.

H7 – A inclusão de cláusulas contratuais que priorizem soluções tecnológicas interoperáveis e auditáveis em contratos públicos de tecnologia contribui para a redução da dependência tecnológica e o fortalecimento da soberania digital municipal.

H8 – A efetividade das políticas municipais de cibersegurança está diretamente associada à presença de equipes técnicas capacitadas e à continuidade de programas de formação, sendo tais fatores determinantes para a implementação bem-sucedida de um marco legal local.

Assim, as hipóteses aqui apresentadas sintetizam a trajetória intelectual e investigativa desta tese, articulando o diálogo entre teoria e prática, entre tendências globais e realidades locais. Elas constituem não apenas um guia para a interpretação integrada dos resultados obtidos, mas também um conjunto de proposições passíveis de aplicação e

monitoramento no contexto da gestão pública municipal. Ao derivar hipóteses tanto de fundamentos conceituais consolidados quanto de evidências empíricas, busca-se garantir que as recomendações decorrentes desta pesquisa estejam simultaneamente ancoradas na base científica e orientadas para a solução de problemas reais, reforçando o papel da cibersegurança como vetor estratégico de desenvolvimento socioeconômico sustentável.

6.4 LIMITAÇÕES DA TESE

A cibersegurança configura-se como uma temática em franca expansão, caracterizada por constante evolução tecnológica e pela emergência de novos desafios normativos, institucionais e operacionais. Esse dinamismo, embora seja fonte de inovação e de oportunidades para aprofundamento científico, também impõe limites à pesquisa acadêmica, uma vez que o conhecimento produzido tende a se desatualizar rapidamente. No cenário científico internacional, a amplitude e a diversidade de linhas de investigação sobre cibersegurança dificultam a delimitação de um escopo que seja, ao mesmo tempo, abrangente o suficiente para captar tendências globais e específico para dialogar com a realidade regional estudada. Tal característica exigiu escolhas metodológicas que, inevitavelmente, deixaram de contemplar certas dimensões do fenômeno.

Apesar da robustez teórica e da aderência empírica da proposta normativa elaborada no Estudo IV, é importante reconhecer que a efetivação de um marco legal municipal de cibersegurança enfrenta barreiras significativas nos municípios, especialmente aqueles com menor capacidade técnica e orçamentária. A escassez de profissionais especializados, a ausência de cultura organizacional voltada à segurança digital e a limitação de recursos financeiros são fatores que dificultam a implantação efetiva das diretrizes propostas.

Além disso, a alta rotatividade de equipes técnicas e a descontinuidade administrativa — comum em contextos municipais — podem comprometer a sustentabilidade das ações, exigindo mecanismos de capacitação contínua e institucionalização das políticas. Há também o desafio de promover articulação entre os entes federativos, evitando sobreposições normativas e garantindo suporte técnico adequado. Essas barreiras não invalidam a proposta apresentada, mas indicam a necessidade de estratégias complementares de implementação, como redes intermunicipais de cooperação, apoio estadual/federal e incentivos à profissionalização da gestão digital local.

Outro aspecto relevante refere-se à fragmentação e, por vezes, à incongruência entre normas e diretrizes nacionais voltadas à segurança digital. No contexto brasileiro, instrumentos

como a Lei Geral de Proteção de Dados (LGPD), a Estratégia Nacional de Segurança Cibernética (E-Ciber) e regulamentos setoriais nem sempre apresentam plena coerência ou integração prática, dificultando sua aplicação uniforme no nível municipal. Essa falta de convergência normativa compromete a construção de uma governança de cibersegurança consistente, tanto na esfera pública quanto na privada, e limita a capacidade de os municípios desenvolverem políticas locais plenamente alinhadas a padrões nacionais e internacionais.

Do ponto de vista empírico, a pesquisa enfrentou obstáculos operacionais significativos durante a fase de coleta de dados, particularmente nas entrevistas com representantes das administrações municipais. A dificuldade de contato e a falta de retorno por parte de algumas prefeituras resultaram na exclusão de três municípios da amostra originalmente planejada — Forquilhinha, Balneário Rincão e Nova Veneza. Essa limitação reduziu a cobertura do diagnóstico e, consequentemente, restringiu a possibilidade de generalização dos resultados para o conjunto total da Região da AMREC, embora o número de casos estudados ainda tenha garantido a consistência das análises.

Constatou-se que a temática da cibersegurança ainda é pouco valorizada nas prefeituras, o que impactou diretamente a qualidade e a profundidade das informações obtidas. Em poucas ocasiões, os interlocutores designados para participar da pesquisa não possuíam qualificação técnica específica ou domínio aprofundado sobre as práticas e políticas de segurança digital em suas instituições. Essa realidade reflete não apenas a carência de recursos humanos especializados no setor público local, mas também a necessidade de maior conscientização sobre a relevância estratégica da cibersegurança como elemento estruturante do desenvolvimento socioeconômico municipal.

6.5 RECOMENDAÇÕES PARA ESTUDOS FUTUROS

A presente tese contribuiu para a compreensão da cibersegurança como vetor estratégico para o desenvolvimento socioeconômico de municípios, mas também evidenciou a amplitude e complexidade do tema, abrindo espaço para novas investigações. Uma primeira linha de aprofundamento consiste em expandir a análise para outras regiões do Brasil, permitindo comparações inter-regionais e identificando padrões ou singularidades nas estratégias locais de cibersegurança. Estudos comparativos poderiam explorar como diferentes contextos socioeconômicos, capacidades institucionais e arranjos normativos impactam a maturidade digital e a resiliência cibernética, enriquecendo a base de evidências disponível para formulação de políticas públicas.

Outra sugestão é ampliar a abordagem metodológica, incorporando estudos longitudinais que acompanhem a evolução da maturidade institucional em cibersegurança ao longo do tempo. Essa perspectiva permitiria avaliar o impacto de políticas, investimentos e capacitações em ciclos plurianuais, verificando se as diretrizes propostas — como as contidas no marco legal sugerido nesta tese — resultam efetivamente em melhoria na resiliência digital e na integração da cibersegurança ao planejamento estratégico municipal. Além disso, estudos longitudinais poderiam captar mudanças decorrentes de novos marcos regulatórios nacionais e internacionais, especialmente em um campo tão dinâmico quanto este.

Uma terceira vertente relevante para pesquisas futuras envolve a análise aprofundada da interação entre cibersegurança e inclusão digital. Embora esta tese tenha identificado a importância de políticas de acesso e capacitação, investigações específicas poderiam examinar como a proteção digital pode ser integrada a estratégias de inclusão, garantindo que populações vulneráveis tenham não apenas acesso à internet e aos serviços digitais, mas também condições de fazê-lo de forma segura.

Recomenda-se, investigar de forma mais detalhada a perspectiva organizacional e de gestão de pessoas nas prefeituras. Pesquisas voltadas à análise de competências, modelos de capacitação e estruturas organizacionais para a cibersegurança poderiam oferecer insumos práticos para a construção de equipes técnicas mais qualificadas e resilientes. Isso inclui compreender as barreiras à contratação e retenção de especialistas, as possibilidades de cooperação intermunicipal para compartilhamento de recursos humanos e técnicos, e os mecanismos de governança capazes de institucionalizar a cibersegurança como prioridade transversal na administração pública municipal.

6.6 CONTRIBUIÇÕES FINAIS DA TESE

A presente tese buscou compreender a cibersegurança como fator estratégico para o desenvolvimento socioeconômico de municípios, articulando tendências globais, constructos teóricos emergentes, diagnóstico institucional e proposição normativa aplicada à realidade da Região da AMREC. A partir de quatro estudos complementares, construiu-se um percurso investigativo que transita da análise da literatura científica internacional até a formulação de diretrizes jurídicas concretas, passando pela sistematização conceitual e pela observação empírica da realidade local. Esse encadeamento permitiu não apenas consolidar um arcabouço teórico-prático robusto, mas também oferecer subsídios aplicáveis à gestão pública municipal.

O trabalho evidenciou que a cibersegurança, embora frequentemente percebida como uma questão meramente técnica, constitui um campo multidimensional, que envolve governança, regulação, soberania informacional, resiliência digital e justiça informacional. Ao integrar essas dimensões, foi possível demonstrar que a proteção de dados e sistemas críticos transcende a defesa contra-ataques, tornando-se um pilar para a atração de investimentos, a inovação e a manutenção da confiança institucional. Nesse sentido, a tese reforça a ideia de que a cibersegurança deve ser tratada como política pública transversal e indutora de desenvolvimento, especialmente em contextos urbanos.

Os achados também revelaram que a ausência de integração entre normas nacionais, a falta de recursos técnicos especializados e a baixa valorização do tema no nível municipal limitam a maturidade institucional e aumentam as vulnerabilidades digitais. O marco legal proposto nesta pesquisa representa uma tentativa de enfrentar essas lacunas, oferecendo um instrumento adaptado às especificidades regionais e capaz de servir como modelo replicável em outros contextos. Ao fazê-lo, o estudo reafirma a importância de alinhar padrões internacionais e exigências nacionais à capacidade real de implementação das administrações locais.

Por fim, esta tese contribui para a construção de um campo de estudo que, apesar de recente no Brasil, apresenta potencial crescente de impacto social, econômico e político. Ao combinar rigor científico com aplicabilidade prática, o trabalho abre caminho para futuras pesquisas que aprofundem, ampliem e atualizem suas análises, considerando o caráter dinâmico da cibersegurança e as transformações contínuas das tecnologias digitais. Assim, espera-se que os resultados e proposições aqui apresentados sirvam de base não apenas para o avanço acadêmico, mas também para a formulação de políticas públicas mais eficazes, inclusivas e sustentáveis, fortalecendo a resiliência das cidades na era digital.

REFERÊNCIAS

ABBAS, Hafiz Syed Mohsin; QAISAR, Zahid Hussain; ALI, Ghulam; ALTURISE, Fahad; ALKHALIFAH, Tamim. Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. *PLOS ONE*, v. 17, n. 11, e0274550, 15 nov. 2022. DOI: https://doi.org/10.1371/journal.pone.0274550.

ABDULLAH, Ahmed; WHITE, Gareth R. T.; ALLEN, Robert A.; SAMUEL, Anthony; THOMAS, Robert J. Antecedents of cybersecurity implementation: a study of the cyber-preparedness of U.K. social enterprises. *IEEE Transactions on Engineering Management*, v. 69, n. 6, p. 3826–3837, jun. 2020. DOI: https://doi.org/10.1109/TEM.2020.2994981.

AHMAD, Ijaz; KUMAR, Ajitesh; SINGH, Akhilesh Kumar; SINGH, Pradeep Kumar; ANUSHREE; VERMA, Pawan Kumar; ALISSA, Khalid A.; BAJAJ, Mohit; REHMAN, Ateeq Ur; TAG-ELDIN, Elsayed. **A Novel Decentralized Blockchain Architecture for the Preservation of Privacy and Data Security against Cyberattacks in Healthcare.** *Sensors*, Basel, v. 22, n. 15, art. 5921, ago. 2022. DOI: https://doi.org/10.3390/s22155921.

AHMAD, Istiak; ALQURASHI, Fahad. **A data-driven multi-perspective approach to cybersecurity knowledge discovery through topic modelling**. *Alexandria Engineering Journal*, v. 107, p. 374–389, jul. 2024. DOI: https://doi.org/10.1016/j.aej.2024.07.044.

AHMED, Saif; ALAM, Md Shafiul; DHALI, Mohsin; ALAM, Syed Shah. Citizens' engagement with cybersecurity measures in Bangladesh: a cross-sectional study. *International Journal of Information Security*, v. 24, art. 4, 30 out. 2024. DOI: https://doi.org/10.1007/s10207-024-00918-9.

AKDEMIR, A.; LAW, J. Cybersecurity governance in smart cities: Policy, privacy, and surveillance. *Government Information Quarterly*, v. 38, n. 4, p. 101620, 2021.

AL-BESHER, Abdulaziz; KUMAR, Kailash. Use of artificial intelligence to enhance e-government services. *Measurement: Sensors*, v. 24, n. 7, p. 100484, out. 2022. DOI: https://doi.org/10.1016/j.measen.2022.100484.

ALVES JÚNIOR, Sérgio Antônio Garcia. *Políticas nacionais de segurança cibernética: elementos para uma proposta brasileira*. Brasília: Senado Federal, 2011.

ALLAM, Zaheer. *Smart governance for cities*. Cham: Springer, 2021.

ALZOUBI, Yehia Ibrahim; MISHRA, Alok; ANWAR, Mohammed J.; GILL, Asif Qumer. Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, v. 120, art. 102820, 30 jun. 2022. DOI: https://doi.org/10.1016/j.cose.2022.102820.

ALZOUBI, Yehia Ibrahim; MISHRA, Alok; TOPCU, Ahmet Ercan. Research trends in deep learning and machine learning for cloud computing security. *Artificial Intelligence Review*, v. 57, art. 132, maio 2024. DOI: https://doi.org/10.1007/s10462-024-10776-5.

ANATEL. **Resolução nº 740, de 25 de novembro de 2020**. Aprova o Regulamento de Segurança Cibernética Aplicado ao Setor de Telecomunicações. Brasília: ANATEL, 2020.

ANDERSON, Ross Joh. *Security engineering: a guide to building dependable distributed systems*. New York: Wiley, 2001.

ARIA, Massimo; CUCCURULLO, Corrado**. bibliometrix: An R-tool for comprehensive science mapping analysis**. Journal of informetrics, v. 11, n. 4, p. 959-975, 2017.

ARMELLIN, Alessandro; CAVIGLIA, Roberto; GAGGERO, Giovanni Battista; MARCHESE, Mario. A framework for the deployment of cybersecurity monitoring tools in the industrial environment. *IT Professional*, v. 26, n. 4, p. 62–70, jul./ago. 2024. DOI: https://doi.org/10.1109/MITP.2024.3396356.

ASIF, Muhammad. Evaluating digital governance maturity in local governments. *Technology in Society*, v. 69, p. 102945, 2024.

ASSOCIAÇÃO BRASILEIRA DAS ENTIDADES DOS MERCADOS FINANCEIRO E DE CAPITAIS – ANBIMA. **Guia de Cibersegurança ANBIMA**. 3. ed. Rio de Janeiro: ANBIMA, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2006**. Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27014:2013**. Tecnologia da informação – Técnicas de segurança – Governança de segurança da informação. Rio de Janeiro: ABNT, 2013.

AZAMBUJA, Antonio João Gonçalves de; NETO, João Souza. **Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal**. *Revista do Serviço Público*, Brasília, v. 71, n. 3, p. 660–712, jul./set. 2020. DOI: https://doi.org/10.21874/rsp.v71i3.3210.

BADA, Maria; NURSE, Jason R. C. The social and psychological impact of cyberattacks. *Cybersecurity*, v. 2, n. 1, p. 1-12, 2019. DOI: https://doi.org/10.1186/s42400-019-0030-3.

BADAL, Faisal R.; NAYEM, Zannatun; SARKER, Subrata K.; DATTA, Dristi; RAHMAN FAHIM, Shahriar; MUYEEN, S. M.; ISLAM SHEIKH, Md. Rafiqul; DAS, Sajal K. A Novel Intrusion Mitigation Unit for Interconnected Power Systems in Frequency Regulation to Enhance Cybersecurity. *Energies*, v. 14, n. 5, art. 1401, 04 mar. 2021. DOI: https://doi.org/10.3390/en14051401.

BADAL, Faisal R.; SARKER, Subrata K.; NAYEM, Zannatun; MOYEEN, Sumaya I.; DAS, Sajal K. Microgrid to smart grid's evolution: technical challenges, current solutions, and future scopes. *Energy Science & Engineering*, v. 11, n. 2, p. 874, out. 2022. DOI: https://doi.org/10.1002/ese3.1319.

BANCO CENTRAL DO BRASIL. **Instrução Normativa BCB nº 85, de 25 de março de 2021**. Dispõe sobre os procedimentos para a implementação da Resolução nº 4.893. Brasília: BCB, 2021.

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 4.893, de 26 de fevereiro de 2021**. Dispõe sobre a política de segurança cibernética e os requisitos para contratação de serviços de processamento e armazenamento de dados. Brasília: BCB, 2021.

BANCO INTERAMERICANO DE DESENVOLVIMENTO; ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Relatório de Cibersegurança 2020: risco, avanços e o caminho a seguir na América Latina e Caribe**. Washington, DC: BID; OEA, 2020. 204 p. Disponível em: https://publications.iadb.org/pt/publications/portuguese/viewer/Relatorio-de-Ciberseguranca-2020-riscos-avancos-e-o-caminho-a-seguir-na-America-Latina-e-Caribe.pdf. Acesso em: 18 jun 2025.

BANDA, Osiris A. Valdez; CHAAL, Meriam; REN, Xin; BAHOOTOROODY, Ahmad; BASNET, Sunil; BOLBOT, Victor; GELDER, Pieter Van. Research on risk, safety, and reliability of autonomous ships: a bibliometric review. *Safety Science*, v. 167, art. 106256, 2023. DOI: https://doi.org/10.1016/j.ssci.2023.106256.

BANDA, Osiris Valdez. BOLBOT, Victor; XIANG, La; BRUNOU, Päivi; KIVIHARJU, Mikko; DING, Yu. Cybersecurity risk assessment of a marine Dual-Fuel engine on inland waterways ship. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment*, v. 239, n. 1, p. 67–91, fev. 2025. DOI: https://doi.org/10.1177/14750902241265173.

BARDIN, Laurence. *Análise de conteúdo*. Lisboa: Edições 70, 2011.

BELLI, Luca *et al.* **Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano**. Rio de Janeiro: FGV Direito Rio, 2023. Disponível em: https://direitorio.fgv.br/publicacoes. Acesso em: 25 maio 2025.

BOLBOT, Victor; CHAAL, Meriam; REN, Xin; BAHOOTOROODY, Ahmad; BASNET, Sunil; VALDEZ BANDA, Osiris A.; VAN GELDER, Pieter. Research on risk, safety, and reliability of autonomous ships: a bibliometric review. *Safety Science*, v. 167, art. 106256, 2023. DOI: https://doi.org/10.1016/j.ssci.2023.106256.

BOLBOT, Victor; XIANG, La; BRUNOU, Päivi; KIVIHARJU, Mikko; DING, Yu; VALDEZ BANDA, Osiris; VAN GELDER, Pieter. Cybersecurity risk assessment of a marine Dual-Fuel engine on inland waterways ship. *Proceedings of the Institution of Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment*, v. 239, n. 1, p. 67-91, 2025. DOI: https://doi.org/10.1177/14750902241265173.

BRASIL. **Agência Nacional de Telecomunicações (Anatel).** Resolução nº 740, de 21 de dezembro de 2020. Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. *Publicada em* 24 dez. 2020. *Atualizada em* 17 fev. 2025.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação. *Diário Oficial da União*, Brasília, DF, 2018.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética – E-Ciber. *Diário Oficial da União*, Brasília, DF, 2020.

BRASIL. **Decreto nº 11.856, de 27 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança – CNCiber. *Diário Oficial da União*, Brasília, DF, 2023.

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, p. 1, 5 ago. 2025.

BRASIL. **Estratégia Nacional de Segurança Cibernética – E-Ciber**. Brasília: Presidência da República, 2020. Disponível em: https://www.gov.br/mj/pt-br/assuntos/seus-direitos/seguranca-cibernetica/e-ciber. Acesso em: 10 ago. 2025.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos. *Diário Oficial da União*, Brasília, DF, 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. *Diário Oficial da União*, Brasília, DF, 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais – LGPD. *Diário Oficial da União*, Brasília, DF, 2018.

BSI. ISO/IEC 27001 – **Gestão de Segurança da Informação**. Disponível em: https://www.bsigroup.com/pt-BR/ISO-IEC-27001-Seguranca-da-Informacao/. Acesso em: 18 maio 2025.

BYGRAVE, Lee A. Security by Design: Aspirations and Realities in a Regulatory Context. *Oslo Law Review*, v. 8, n. 3, p. 126–177, jun. 2022. DOI: https://doi.org/10.18261/olr.8.3.2.

BYGRAVE, Lee A. The emergence of EU cybersecurity law: a tale of lemons, angst, turf, surf and grey boxes. *Computer Law & Security Review*, v. 56, art. 106071, 2025. DOI: https://doi.org/10.1016/j.clsr.2024.106071.

CALZADA, Igor. *Smart city citizenship: Integrating information and communication technologies and citizen engagement*. London: Elsevier, 2020.

CAMILLIERI, Mark Anthony. Artificial Intelligence Governance: Ethical Considerations and Implications for Social Responsibility. *Expert Systems*, v. 41, e13406, 2023. DOI: https://doi.org/10.1111/exsy.13406.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999.

CHANDER, Anupam et al. *Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation*. Policy Research Working Paper 9594, World Bank, Washington, D.C., 2021. Disponível em: https://scholarship.law.georgetown.edu/facpub/2374. Acesso em: 18 maio 2025.

CHANDER, Anupam; ABRAHAM, Meaza; CHANDY, Sandeep; FANG, Yuan; PARK, Dayoung; YU, Isabel. *Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation*. World Bank, Policy Research Working Paper No. 9594, 2021.

Disponível em: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/933281618588644214. Acesso em: 18 maio 2025.

CHELIGA, Vinicius. *Cidades inteligentes: implementação, responsabilidade e proteção de dados pessoais*. Dissertação (Mestrado em Direito), Universidade Federal de Santa Catarina, 2023.

CHEN, Yulin; YANG, Shaohua; LAO, Keng-Weng; HUI, Hongxun. Secure distributed control for demand response in power systems against deception cyber-attacks with arbitrary patterns. *IEEE Transactions on Power Systems*, 25 mar. 2024. DOI: https://doi.org/10.1109/TPWRS.2024.3381231.

CHEN, Yi-Chou; HU, Jin-Li; YANG, Ya-Po. The Development and Issues of Energy-ICT: A Review of Literature with Economic and Managerial Viewpoints. *Energies*, v. 15, n. 2, art. 594, jan. 2022. DOI: https://doi.org/10.3390/en15020594.

CHEN, Yunpeng; ZHAO, Xin; LI, Shaolong; ZHAO, Ying; FU, Shuowen; ZHOU, Fangfang; HUANG, Xin; LI, Yuwei; CHEN, Zhuo. An Open Dataset of Cyber Asset Graphs for Cybercrime Research. *IEEE Transactions on Big Data*, v. 11, n. 2, p. 438–446, abr. 2025. DOI: https://doi.org/10.1109/TBDATA.2024.3403371.

CHOO, Kim-Kwang Raymond. **The cyber threat landscape: Challenges and future research directions.** Computers & Security, v. 30, n. 8, p. 719–731, nov. 2011. https://doi.org/10.1016/j.cose.2011.08.004.

COMISSÃO EUROPEIA. **Artificial Intelligence Act: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act).** Bruxelas: Comissão Europeia, 2023. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206. Acesso em: 16 jun. 2025.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime (Convenção de Budapeste)**. Budapeste, 23 nov. 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185. Acesso em: 16 jun. 2025.

CONVERGÊNCIA DIGITAL. Brasil registra custo médio de R$ 7,19 milhões por violação de dados em 2025. **Abranet / Convergência Digital**, 30 jul. 2025. Disponível em: https://www.abranet.org.br/publicacoes/noticias/5702. Acesso em: 10 ago. 2025.

CNN BRASIL. Brasil é o 4º país da América Latina com mais ameaças digitais no 1º semestre de 2024, diz pesquisa. **CNN Brasil**, São Paulo, 4 jul. 2024. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/brasil-e-o-4o-pais-da-america-latina-com-mais-ameacas-digitais-no-primeiro-semestre-de-2024-diz-pesquisa/. Acesso em: 10 ago. 2025.

CNN BRASIL. Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo. 2024. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo/. Acesso em: 18 maio 2025.

CRAIGEN, Daniel; DIETEREN, Neil; PURSE, D'Arcy. Defining cybersecurity. *Technology Innovation Management Review*, v. 4, n. 10, p. 13-21, 2014. DOI: https://doi.org/10.22215/timreview/835.

CRAVO, Thiago Vieira. Governança e Fragmentação Normativa na Segurança da Informação Municipal. *Revista Brasileira de Políticas Públicas*, v. 13, n. 2, p. 255–276, 2023.

CRESWELL, John W. **Projeto de pesquisa métodos qualitativo, quantitativo e misto**. 5. Porto Alegre Penso 2021 1 recurso online (Métodos de pesquisa). ISBN 9786581334192.

CRESWELL, John W. *Designing and Conducting Mixed Methods Research*. 3. ed. Thousand Oaks: SAGE Publications, 2021.

CSIRT eSentire. *Cybersecurity Ventures Report on Cybercrime*. eSentire, [S. l.], s.d. Disponível em: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime. Acesso em: 10 ago. 2025.

DE BRUIJN, Hans; JANSSEN, Marijn. Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, v. 34, n. 1, p. 1-7, 2017. DOI: https://doi.org/10.1016/j.giq.2017.02.007.

DEMO, Pedro. **Metodologia do conhecimento científico**. São Paulo: Atlas, 2009.

DHIRANI, L. Institutional *frameworks* for digital resilience: A comparative study. *Information Policy Journal*, v. 28, n. 4, p. 445–468, 2023.

DONTHU, Naveen; KUMAR, Satish; PANDEY, Nitesh; LIM, Wei Choon. *How to conduct a bibliometric analysis: An overview and guidelines*. Journal of Business Research, v. 133, p. 285–296, 2021.

DONTHU, Naveen; KUMAR, Satish; PANDEY, Neeraj; LIM, Wi-Liam. A retrospective and prospective overview of cybersecurity research: Data-driven analysis using topic modeling. *Computers & Security*, v. 105, 2021.

DUNN CAVELTY, Myriam. *Cyber-security and the politics of risk: The shaping of a new technology*. London: Routledge, 2019.

DUNN CAVELTY, Myriam. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. 1. ed. London: Routledge, 2007. Disponível em: https://doi.org/10.4324/9780203937419. Acesso em: 10 ago. 2025.

ENISA – European Union Agency for Cybersecurity. *ENISA Threat Landscape 2023*. Atenas: ENISA, 2023. Disponível em: https://www.enisa.europa.eu. Acesso em: 9 ago. 2025.

EL-SAYEGH, Sameh; ROMDHANE, Lotfi; MANJIKIAN, Solair. A critical review of 3D printing in construction: benefits, challenges, and risks. *Archives of Civil and Mechanical Engineering*, v. 20, art. 34, 10 mar. 2020. DOI: https://doi.org/10.1007/s43452-020-00038-w.

EL PAÍS. Brasil sofre uma epidemia de roubo de celulares e ciberfraudes. 2024. Disponível em: https://elpais.com/america/2024-08-19/brasil-sufre-una-epidemia-de-robo-de-celulares-y-ciberfraudes.html. Acesso em: 18 maio 2025.

FLICK, Uwe. *Introdução à pesquisa qualitativa*. Porto Alegre: Artmed, 2009.

FORTINET. Emerging ransomware tactics and trends – 2H 2023. Fortinet, Sunnyvale, 2024. Disponível em: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-emerging-ransomware-trends.pdf. Acesso em: 10 ago. 2025.

FRANCO, Muriel Figueredo et al. *CyberTEA: a technical and economic approach for cybersecurity planning and investment*. In: IEEE/IFIP Network Operations and Management Symposium (NOMS), 2023. DOI: https://doi.org/10.23919/NOMS56928.2023.10154480.

FRANCO, Muriel Figueredo; GRANVILLE, Lisandro Zambenedetti; STILLER, Burkhard. *CyberTEA: a technical and economic approach for cybersecurity planning and investment*. In: IEEE/IFIP Network Operations and Management Symposium (NOMS), 2023. DOI: https://doi.org/10.1109/NOMS56928.2023.10154307.

GHERARDI, Silvia. **Organizational knowledge: The texture of workplace learning.** Malden, MA: Blackwell Publishing, 2006.

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

GOMES, Alexandra Manuela. 2000, 266f, **Níveis de desenvolvimento na União Europeia - Uma análise comparativa Inter-regional, Coimbra**, Ed. INE-Direcção Regional do Centro, Disponível: http://www.ine.pt/estudos. Acesso em: 16 ago 2022.

GORDON, Lawrence A.; LOEB, Martin P.; LUCYSHYN, William. **Sharing information on computer systems security: An economic analysis.** Journal of Accounting and Public Policy, v. 22, n. 6, p. 461–485, 2003. https://doi.org/10.1016/j.jaccpubpol.2003.09.001.

GORDON, Lawrence A.; LOEB, Martin P.; ZHOU, Lei. *Information segmentation and investing in cybersecurity*. Journal of Information Security, v. 12, p. 115–136, 2021. DOI: https://doi.org/10.4236/jis.2021.121006.

FORMOSA, Paul; WILSON, Michael; RICHARDS, Deborah. *A principlist framework for cybersecurity ethics*. **Computers and Security**, v. 109, p. 1–15, out. 2021. DOI: 10.1016/j.cose.2021.102382**.**

FORTINET. *2024 Global Ransomware Report*. 2024. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2024/global-ransomware-report-2024. Acesso em: 17 abr. 2025.

HALL, Peter A.; TAYLOR, Rosemary C. R. **Political Science and the Three New Institutionalisms.** *Political Studies*, v. 44, n. 5, p. 936-957, dez. 1996. DOI: https://doi.org/10.1111/j.1467-9248.1996.tb00343.x.

HANSEN, Lene; NISSENBAUM, Helen. **Digital Disaster, Cyber Security, and the Copenhagen School.** International Studies Quarterly, v. 53, n. 4, p. 1155–1175, dez. 2009. https://doi.org/10.1111/j.1468-2478.2009.00572.x.

HOSSEN, Md. Digital inclusion and municipal cybersecurity in the Global South. *Urban Governance*, v. 5, p. 33–47, 2025.

HOSSEN, Md. Deluar; ABEDIN, Md. Zainal; CHOWDHURY, Tahsina Meher; ISLAM, Zahidul; KABIR, Md. Rishad. Unveiling the Impact of E-Governance on the Transformation from Digital to Smart Bangladesh. *Pakistan Journal of Life and Social Sciences*, v. 23, n. 1, p. 85–108, 2025. DOI: https://doi.org/10.57239/PJLSS-2025-23.1.009.

HUI, Haoyu. Data sovereignty in municipal contexts: Concepts and case studies. *International Journal of Information Management*, v. 50, p. 55–64, 2020.

IBM. *Cost of a Data Breach Report 2023*. 2023. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 17 abr. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27032:2023**. Cybersecurity – Guidelines for Internet security. 2. ed. Geneva: ISO, 2023.

IT FÓRUM. Custo de violação de dados no Brasil cresce 6,5% e atinge R$ 7,19 mi. IT Fórum, 30 jul. 2025. Disponível em: https://itforum.com.br/noticias/custo-violacao-dados-brasil-atinge-r-719-mi/. Acesso em: 10 ago. 2025.

KASPERSKY. *Cybercrime Statistics 2023*. 2023. Disponível em: https://www.kaspersky.com.br/resource-center/threats/cybercrime-statistics. Acesso em: 17 abr. 2025.

KHAIRI, Amar; PETLACH, Martin. NEED FOR DIGITALISATION TO PROVIDE SECURITY? A comparative study on the member states of the European Union. *Obrana a Strategie*, v. 23, n. 1, p. 24–48, jun. 2023. DOI: https://doi.org/10.3849/1802-7199.23.2023.01.024-048.

KHATOUN, Rida; ZEADALLY, Sherali. Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, v. 55, n. 3, p. 51–59, mar. 2017. DOI: 10.1109/MCOM.2017.1600297CM.

KOSTOPOULOS, G.; LIANOS, I.; VOGIATZAKIS, E. The institutional foundations of cybersecurity governance: A multi-level analysis. *Journal of Cyber Policy*, v. 5, n. 3, p. 411-432, 2020.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. *Fundamentos de metodologia científica*. 7. ed. São Paulo: Atlas, 2010.

LIPSKY, Michael. *Street-Level Bureaucracy: Dilemmas of the Individual in Public Services*. 30. ed. New York: Russell Sage Foundation, 2010.

LUZ NETO, Luiz Guedes da. *Agências reguladoras e o fenômeno da captura: um estudo à luz da teoria da regulação econômica*. 2016. Dissertação (Mestrado em Direito Econômico) – Faculdade de Direito, Universidade Federal da Paraíba, João Pessoa, 2016.

MANN, S.; SUTCLIFFE, J.; WASSERMAN, H. Urban surveillance, pandemic politics and digital inequality. *Urban Studies*, [S. l.], v. 59, n. 13, p. 2631–2650, 2022.

MARCH, James G.; OLSEN, Johan P. **The New Institutionalism: Organizational Factors in Political Life.** *American Political Science Review*, v. 78, n. 3, p. 734–749, set. 1984

MARGETTS, H.; DOROBANTU, C. Rethink government with AI. *Nature*, [s.l.], v. 568, p. 163–165, 2019.

MARGETTS, Helen; DOROBANTU, Catalina. Rethinking Public Policy in the Era of Artificial Intelligence. *Journal of European Public Policy*, v. 26, n. 10, p. 1415–1433, 2019.

MARTIN, A. Justice in cybersecurity: A *framework* for ethical governance. *Ethics and Information Technology*, v. 23, n. 1, p. 19-31, 2021.

MARTIN, Kirsten. Ethics of AI and Big Data: Implementing Responsible Data Governance. *Journal of Business Ethics*, v. 168, n. 4, p. 603–618, 2021.

MARTINHO, Ana Paula. Normative gaps in local cybersecurity policy: Insights from Lusophone countries. *Revista de Administração Pública*, v. 55, n. 3, p. 497–519, 2021.

MISHRA, A. Regulating cybersecurity in the Global South: The case of fragmented institutions. *Policy and Internet*, [S. l.], v. 14, n. 2, p. 226–245, 2022.

MISHRA, Alok; ALZOUBI, Yehia Ibrahim; ANWAR, Memoona Javeria; GILL, Asif Qumer. Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security*, v. 120, p. 102820, 2022.

MISHRA, A.; PANDEY, R.; SINGH, S.; et al. *Attributes impacting cybersecurity policy development: Evidence from seven nations*. Computers & Security, v. 120, p. 102820, 2022. DOI: https://doi.org/10.1016/j.cose.2022.102820. Acesso em: 18 maio 2025.

MORELATO, André Luis; CARRARA, Emanuela; SOUZA, Carlos Henrique Medeiros de. A bibliometric analysis of the scientific production on cybersecurity in Brazil. *Revista Tecnologia e Sociedade*, Curitiba, v. 17, n. 46, p. 1-18, 2021. Disponível em: https://periodicos.utfpr.edu.br/rts/article/view/12246. Acesso em: 9 ago. 2025.

MOZELLI, Rodrigo. *Brasil: dobram ataques aos sistemas do governo no primeiro semestre de 2024*. Olhar Digital, 25 jul. 2024. Disponível em: https://olhardigital.com.br/2024/07/25/seguranca/brasil-dobram-ataques-aos-sistemas-do-governo-no-primeiro-semestre-de-2024/. Acesso em: 18 maio 2025.

MUSTAFA, Rashid; SARKAR, Nurul I.; MOHAGHEGH, Mahsa; PERVEZ, Shahbaz. A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey. *Sensors*, v. 24, n. 22, art. 7209, 11 nov. 2024. DOI: https://doi.org/10.3390/s24227209.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Framework for Improving Critical Infrastructure Cybersecurity.** Version 1.1. Gaithersburg, MD: NIST, Apr. 2018. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Acesso em: 16 jun. 2025.

NEVES, Paulo Sérgio Ccosta. Direitos humanos e cidadania simbólica no Brasil. *In*: Lyra, R. P. (org.). **Direitos humanos**: os desafios do século XXI. Uma abordagem interdisciplinar. Brasília: Brasília Jurídica, 2010.

NISHANT, Richa. AI and the public sector: Balancing innovation and accountability. *Government Information Quarterly*, v. 37, n. 3, 2020.

NISSENBAUM, H. Privacy as contextual integrity. Washington Law Review, v. 79, n. 1, p. 119–158, 2005.

NISSENBAUM, Helen. **Where Computer Security Meets National Security1**. Ethics Inf Technol 7, 61–73 (2005). https://doi.org/10.1007/s10676-005-4582-3.

NOGUEIRA, Michel Gomes. *Cibersegurança: uma análise dos principais conflitos cibernéticos globais e seus impactos no Brasil*. Tese (Doutorado em Relações Internacionais), Universidade de Brasília, 2024.

NUNES, Ana Luísa Tarter. *Regime dual de responsabilidade civil na proteção de dados pessoais no ordenamento jurídico brasileiro*. Tese (Doutorado em Direito), Universidade Federal do Paraná, 2022.

NYE, Joseph S. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010.

OBLOCK. Os 10 ataques cibernéticos mais marcantes de 2024. 2024. Disponível em: https://www.oblock.com.br/ataques-ciberneticos-2024/. Acesso em: 18 maio 2025.

OCDE (Organização para a Cooperação e Desenvolvimento Econômico). *Digital Government Index: 2019 Results*. Paris: OECD Publishing, 2020.

OCDE (Organização para a Cooperação e Desenvolvimento Econômico). **Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document.** Paris: OECD Publishing, 2015. DOI: 10.1787/9789264245471-en

OLIVEIRA, A.; FIGUEIREDO, N.; NASCIMENTO, M. Cybersecurity and public policy: A framework for analysis in urban contexts. *Revista de Administração Pública*, v. 54, n. 3, p. 565-584, 2020.

ONU (Assembleia Geral). **Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security**. Relatório A/76/135, Nova Iorque: Assembleias Gerais, 14 jul. 2021.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – OEA; UNIVERSIDADE DE OXFORD. *Cybersecurity Capacity Review: Federative Republic of Brazil*. Oxford: University

of Oxford; Washington, D.C.: OEA, 2020. Disponível em: https://www.oas.org/en/sms/cicte/cybersecurity.asp. Acesso em: 21 maio 2025.

PARMENTOLA, A.; PETRUZZELLI, A. M.; PERRONE, G.; VERGANTI, R. When Blockchain meets smart cities: A review, synthesis and research agenda. *Technological Forecasting and Social Change*, [S. l.], v. 176, 2022.

PELTZMAN, Sam. Toward a More General Theory of Regulation. *Journal of Law and Economics*, v. 19, n. 2, p. 211–240, 1976.

POSNER, Richard A. Theories of economic regulation. *The Bell Journal of Economics and Management Science*, v. 5, n. 2, p. 335–358, 1974.

RAMADHAN, Iqbal; SUMADINATA, R. Widya Setiabudi; DJUMALA, Darmansjah; DARMAWAN, Wawan Budi. **Interpreting the role of state, non-state, and international organization to form cybersecurity governance in Southeast Asia.** *Geopolitics Quarterly*, v. 20, n. 2, p. 255–278, 2024. DOI: https://doi.org/10.22034/igq.2024.198274.

RIBEIRO, Ana Beatriz Nunes. **Avaliação da maturidade em cibersegurança do tecido industrial português**. 2023. Dissertação (Mestrado em Cibersegurança e Informática Forense) – Instituto Politécnico de Leiria, Leiria, 2023.

ROBERTS, Andrew; MARKSTEINER, Stefan; SOYTURK, Mujdat; YAMAN, Berkay; YANG, Yi. **A Global Survey of Standardization and Industry Practices of Automotive Cybersecurity Validation and Verification Testing Processes and Tools.** *SAE International Journal of Connected and Automated Vehicles*, v. 7, n. 2, p. 199–213, 2024. DOI: https://doi.org/10.4271/12-07-02-0013.

SAID, Dhaou. **A survey on information communication technologies in modern demand-side management for smart grids: challenges, solutions, and opportunities.** *IEEE Engineering Management Review*, Piscataway, NJ, 2022. DOI: https://doi.org/10.1109/EMR.2022.3186154.

SANTOS, Jamerson Lima dos. *A garantia do direito à proteção de dados no âmbito da ordem jurídico-constitucional brasileiro*. Tese (Doutorado em Direito), Universidade Federal da Bahia, 2023.

SCHMIDT, João Pedro. **Para entender as políticas públicas: aspectos conceituais e metodológicos**. In: REIS, Jorge Reis; LEAL, Rogério Gesta (Orgs.). *Direitos sociais e políticas públicas*: desafios contemporâneos, Santa Cruz do Sul: Edunisc, 2008, v. 8, p. 2307- 2333.

SCHUBERT, Karl D.; BARRETT, David. Data Governance, Privacy, and Ethics. In: LACITY, Mary C.; COON, Laura (org.). *Human Privacy in Virtual and Physical Worlds: Technology, Work and Globalization*. Cham: Springer, 2024. cap. 5, p. 97–123. DOI: 10.1007/978-3-031-51063-2_5.

SEN, Amartya, citado por DINIZ, Eli. **O Contexto Internacional e a Retomada do Debate sobre Desenvolvimento no Brasil Contemporâneo** (2000/2010). Revista de Ciências Sociais, Rio de Janeiro, v. 54, n. 4, 2011, p. 493 a 531.

SENADO FEDERAL. Golpes digitais atingem 24% da população brasileira, revela DataSenado. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado. Acesso em: 18 maio 2025.

SHACKELFORD, S. J.; RUSSELL, S.; KUEHN, A. Cyber peace: Promoting cybersecurity norms and governance through international collaboration. *Georgetown Journal of International Affairs*, v. 21, p. 22-31, 2020.

SHARIFI, Ayyoob. Smart city governance: A review of challenges and future research agenda. *Cities*, v. 129, p. 103926, 2024.

SHARIFI, A.; BIBRI, S. E.; ALLAM, Z. The pursuit of smart and sustainable cities through the lens of urban resilience: A review. *Cities*, [S. l.], v. 144, 2024.

SRIVASTAVA, Ajay. Institutional trust and public digital infrastructure: Lessons from Indian municipalities. *Policy & Internet*, v. 17, n. 2, p. 210–229, 2025.

SRIVASTAVA, A. K.; MISHRA, S. K.; PANDEY, P. Cybersecurity threats to critical infrastructure: Challenges and response strategies. *Urban Computing*, [S. l.], v. 9, 2023.

STIGLER, George J. The theory of economic regulation. *The Bell Journal of Economics and Management Science*, v. 2, n. 1, p. 3–21, 1971.

TADDEO, M.; FLORIDI, L. How AI can be a force for good. *Science*, v. 361, n. 6404, p. 751-752, 2018.

TETTEY, Francis. Regional cooperation and cybersecurity in Africa. *African Journal of Information Systems*, v. 16, n. 1, p. 113–129, 2024.

THIOLLENT, Michel. *Metodologia da pesquisa-ação*. 18. ed. São Paulo: Cortez, 2011.

TORRES, Caroline de Fátima da Silva. *A regulação e sua captura: estudo sobre os limites do modelo brasileiro de regulação estatal à luz da teoria econômica da regulação*. 2012. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2012.

TREVISO (Mun.). Decreto nº 285, de 2024. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), no âmbito da administração direta e indireta do Município de Treviso.

TURA, N.; OJANEN, V. Addressing digital exclusion and cybersecurity challenges in peripheral regions. *Sustainable Futures*, [S. l.], v. 4, 2022.

União Europeia (Parlamento Europeu e Conselho). **Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).** *Official Journal of the European Union*, L 277:1–102, 27 out. 2022.

UNITED STATES OF AMERICA. **National Cyber Strategy of the United States of America.** Washington, D.C.: The White House, Sept. 2018. Disponível em: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso em: 10 ago. 2025.

VIANNA, Eduardo Wallier. *Análise do comportamento informacional na gestão da segurança cibernética da Administração Pública Federal*. Dissertação (Mestrado em Ciência da Informação), Universidade de Brasília, 2015.

VIANNA, Eduardo Wallier. *Segurança da informação digital: proposta de modelo para a ciberproteção nacional*. Tese (Doutorado em Ciência da Informação), Universidade de Brasília, 2019.

VISVIZI, A.; DEL HOYO, M. Smart cities and governance: Towards a multidimensional and multilevel framework. *Journal of Urban Technology*, [S. l.], v. 28, n. 1-2, p. 35–52, 2021.

WEF – WORLD ECONOMIC FORUM. *Cybersecurity Outlook 2022*. 2022. Disponível em: https://www.weforum.org/reports/global-cybersecurity-outlook-2022. Acesso em: 17 abr. 2025.

WU, Jiajing; LIN, Kaixin; LIN, Dan; ZHENG, Ziye; HUANG, Huawei; ZHENG, Zibin. **Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities.** *IEEE Open Journal of the Computer Society*, v. 4, p. 37–49, 2023. DOI: https://doi.org/10.1109/OJCS.2023.3245801.

WU, Mingzhi; LUO, Feng; ZHANG, Xuan; YANG, Zhenyu; JIANG, Yifan; WANG, Jiajia; FENG, Wanqiang. **Cybersecurity testing for automotive domain: a survey.** *Sensors*, Basel, v. 22, n. 23, art. 9211, nov. 2022. DOI: https://doi.org/10.3390/s22239211.

XIA, L.; SEMIRUMI, D. T.; REZAEI, R. A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, v. 98, p. 104771, 2023. DOI: 10.1016/j.scs.2023.104771.

XU, Feng *et al. Do strategy and timing in IT security investments matter? An empirical investigation of the alignment effect*. Information Systems Frontiers, v. 21, p. 1069–1083, 2019. DOI: https://doi.org/10.1007/s10796-017-9807-6.

YANG, Shaohua; LAO, Keng-Weng; HUI, Hongxun; CHEN, Yulin. **Secure distributed control for demand response in power systems against deception cyber-attacks with arbitrary patterns**. *IEEE Transactions on Power Systems*, v. 39, n. 6, p. 7277–7290, nov. 2024. DOI: https://doi.org/10.1109/TPWRS.2024.3381231.

YU, Xiaoxi; ZHAO, Liurong; ZHOU, Xinyu. **The impact of regulatory mechanisms on vulnerability disclosure behavior during crowdsourcing cybersecurity testing**. *Mathematical Biosciences and Engineering*, v. 20, n. 11, p. 19012–19039, out. 2023. DOI: https://doi.org/10.3934/mbe.2023841.

ZHOU, Tianyu. Machine learning-based security models in municipal digital infrastructures. *IEEE Transactions on Cybernetics*, v. 53, n. 2, p. 1560–1574, 2023.

ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

APÊNDICES

APÊNDICE A – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Pró-Reitoria de Pesquisa, Pós-Graduação, Inovação e Extensão – PROPIEX
Diretoria de Pesquisa e Pós-Graduação
Programa de Pós-Graduação em Desenvolvimento Socioeconômico - PPGDS

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Título da Pesquisa: Cibersegurança e Desenvolvimento Socioeconômico das cidades: maturidade institucional e regulação nos municípios da região da Amrec
Doutorando: Luan Philippi Machado
Orientador: Prof. Dr. Silvio Parodi Oliveira Camilo

Você está sendo convidado(a) a participar da pesquisa de doutorado que tem como objetivo analisar as capacidades institucionais, estratégias locais e práticas relacionadas à cibersegurança nos municípios da AMREC, considerando seus impactos para o desenvolvimento socioeconômico local. A sua participação será por meio de entrevista individual, com base em um roteiro estruturado com perguntas abertas. As respostas serão registradas de forma confidencial e utilizadas exclusivamente para fins acadêmicos.
Esta pesquisa não envolve riscos diretos aos participantes. Espera-se que seus resultados possam contribuir com o aprimoramento das políticas públicas e da governança digital nos municípios. O participante não terá custos nem receberá remuneração. Todas as informações fornecidas serão tratadas com confidencialidade. Os dados poderão ser apresentados em relatórios, artigos e na tese de doutorado, sem identificação nominal dos participantes, exceto se o participante autorizar expressamente o uso de sua identificação institucional.
A sua participação é voluntária. Você pode se recusar a participar ou retirar seu consentimento a qualquer momento, sem que isso acarrete qualquer prejuízo ou penalidade. Declaro que fui adequadamente informado(a) sobre os objetivos e procedimentos desta pesquisa. Compreendi que minha participação é voluntária e autorizo a utilização das informações fornecidas para fins acadêmicos e científicos.
(X) Autorizo a menção do instituição/município que represento nos resultados da pesquisa.

Cidade/SC, de de 2025.

Nome do Participante:
Cargo/Função:
Município:

_____
Assinatura do participante

APÊNDICE B - INSTRUMENTO DE PESQUISA – ESTUDO III: CIBERSEGURANÇA NA AMREC

Instrumento de Pesquisa – Estudo III: Cibersegurança na AMREC

Bloco 1 – Capacidade Institucional e Organizacional

Objetivo: Investigar a estrutura administrativa e a qualificação das equipes responsáveis pela segurança digital no âmbito municipal, bem como as estratégias de capacitação e gestão interna.

Perguntas:

1. Como está estruturada a equipe responsável por segurança da informação ou cibersegurança no município?
2. Quais são os principais desafios enfrentados por essa equipe?
3. Existem ações de capacitação contínua? Em que áreas?
4. A gestão realiza algum tipo de avaliação formal ou rotinas padronizadas relacionadas à segurança digital?

Bloco 2 – Governança Digital e Normatização Local

Objetivo: Analisar a existência, implementação e alcance de normas e políticas públicas voltadas à cibersegurança nos municípios, incluindo a integração com legislações superiores.

Perguntas:

1. O município possui normativas específicas relacionadas à segurança da informação ou cibersegurança? Quais?
2. Como se deu a elaboração dessas normas e sua implementação prática?
3. Como se articula a política local com legislações estaduais e federais, como a LGPD?
4. Como são distribuídas as responsabilidades entre os atores envolvidos (gestão, fornecedores, setores técnicos)?

Bloco 3 – Infraestrutura Tecnológica e Práticas Operacionais

Objetivo: Compreender os procedimentos técnicos adotados para proteção digital e verificar a autonomia ou dependência tecnológica das gestões locais.

Perguntas:

1. Quais práticas técnicas de segurança digital são adotadas no município (backup, criptografia, autenticação, etc.)?
2. Existem procedimentos formais para resposta a incidentes ou falhas de segurança?
3. O município possui autonomia técnica para gerenciar sua infraestrutura digital ou depende de fornecedores?

4. Como ocorrem atualizações e testes de protocolos? Quem participa dessas decisões?

Bloco 4 – Cooperação Intermunicipal e Redes Colaborativas

Objetivo: Identificar articulações regionais para a cibersegurança, trocas de experiências e iniciativas colaborativas entre municípios.

Perguntas:

1. O município participa de redes, fóruns ou consórcios voltados à segurança digital?
2. Quais são os benefícios e limitações dessas parcerias? Poderia exemplificar?
3. Como ocorre a cooperação com outros municípios nessa temática? Existem práticas consolidadas?

Bloco 5 – Barreiras Institucionais e Percepções

Objetivo: Captar percepções dos gestores sobre obstáculos enfrentados, prioridades políticas e valores subjacentes às decisões de cibersegurança.

Perguntas:

1. Quais são as principais barreiras institucionais para implementar ações de cibersegurança?
2. O tema é tratado como prioridade política? Por quê?
3. Existe preocupação com privacidade, justiça digital e inclusão? Como isso é refletido na prática?
4. Já houve conflito entre a exigência de segurança e a necessidade de transparência ou inclusão digital? Como foi tratado?

Encerramento da Entrevista

Perguntas:

1. Como você avalia a relação entre a cibersegurança e o desenvolvimento do município?
2. Que recomendações daria para fortalecer essa área nas gestões locais?

APÊNDICE C - ESBOÇO DE MARCO LEGAL MUNICIPAL EM CIBERSEGURANÇA

Marco Legal Municipal em Cibersegurança

LEI Nº ___, DE __ DE _____ DE 2025

Estabelece normas, procedimentos e diretrizes para a governança, proteção, capacitação, gestão de dados e cooperação regional em cibersegurança no município de _____.

O PREFEITO DO MUNICÍPIO DE _____, Faço saber a todos os habitantes deste Município que a Câmara Municipal aprovou e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei institui o Marco Legal Municipal em Cibersegurança, dispondo sobre a governança, a proteção de infraestruturas e serviços críticos digitais, a capacitação e a cultura de segurança, a gestão de dados e privacidade e a cooperação regional em matéria de segurança cibernética no âmbito do Município de _____, conforme os princípios, diretrizes e objetivos estabelecidos nesta Lei.

Art. 2º São objetivos desta Lei:

I – proteger a integridade, a confidencialidade e a disponibilidade das informações e sistemas digitais municipais;

II – garantir a continuidade e a resiliência dos serviços públicos frente a ameaças cibernéticas;

III – fomentar a cultura de segurança digital e a capacitação técnica;

IV – assegurar a proteção dos dados pessoais e sensíveis tratados pela administração pública municipal;

V – promover a integração regional e a cooperação interinstitucional em cibersegurança;

VI – assegurar a soberania digital e a cidadania digital no âmbito municipal.

Art. 3º Para fins desta Lei, consideram-se:

I – Cibersegurança: conjunto de medidas técnicas, administrativas e jurídicas destinadas a prevenir, detectar, responder e recuperar-se de incidentes de segurança digital;

II – Infraestrutura crítica digital municipal: ativos tecnológicos e sistemas cuja falha, comprometimento ou destruição possa impactar significativamente a prestação de serviços essenciais;

III – Serviços críticos digitais: sistemas que suportam funções vitais para o funcionamento da cidade, como saúde, educação, arrecadação, segurança pública e administração;

IV – Governança em cibersegurança: processo de tomada de decisão estratégica e coordenação institucional voltado à proteção do ecossistema digital municipal;

V – Plano Municipal de Cibersegurança (PMC): instrumento de planejamento de médio e longo prazo contendo metas, indicadores e ações para a segurança cibernética;

VI – Autoridade Municipal de Cibersegurança (AMC): órgão ou unidade administrativa responsável por coordenar a execução desta Lei;

VII – Encarregado de Proteção de Dados (DPO): pessoa física ou jurídica designada para atuar como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), nos termos da LGPD.

CAPÍTULO II
GOVERNANÇA E ESTRUTURA ORGANIZACIONAL

Art. 4º Fica instituído o Comitê Municipal de Cibersegurança, com caráter consultivo e deliberativo, composto por representantes:
I – da administração direta e indireta;
II – da sociedade civil organizada;
III – do setor empresarial e acadêmico;
IV – de órgãos de controle interno e externo.
§1º O Comitê será presidido pelo titular da AMC e terá reuniões trimestrais ou sempre que convocado em caráter extraordinário.
§2º Compete ao Comitê:
I – propor atualizações na Política de Segurança da Informação (PSI) municipal;
II – acompanhar a execução do PMC;
III – avaliar incidentes relevantes e propor medidas corretivas;
IV – promover a participação cidadã por meio de consultas e audiências públicas.
Art. 5º Fica criado o Núcleo Técnico de Segurança da Informação, vinculado à AMC, com a função de executar ações técnicas, administrativas e educativas em conformidade com esta Lei.

CAPÍTULO III
LIMITAÇÕES À APLICAÇÃO DESTA LEI

Art. 6º As disposições desta Lei não se aplicam:
I – a sistemas e redes sob competência exclusiva da União ou do Estado, regulados por legislação específica;
II – a operações de segurança pública ou defesa nacional cujo sigilo seja imprescindível à sua eficácia;
III – a contratos e serviços cuja regulamentação federal já estabeleça requisitos técnicos superiores aos desta Lei.

CAPÍTULO IV
CRITÉRIOS E REQUISITOS MÍNIMOS DE SEGURANÇA

Art. 7º A implantação de novas soluções tecnológicas no âmbito municipal deverá observar os seguintes critérios:
I – adoção de princípios de *security by design* e *privacy by design*;
II – conformidade com os padrões mínimos de segurança definidos no PMC e na PSI;
III – implementação de controles de acesso, criptografia e autenticação multifator;
IV – protocolo de classificação da informação, definindo níveis de sigilo e regras de acesso;
V – previsão de plano de contingência e recuperação de desastres;
VI – realização periódica de testes de segurança, incluindo testes de invasão (pen tests).
Art. 8º Todos os contratos para aquisição de sistemas e serviços digitais deverão conter cláusulas obrigatórias de:
I – conformidade com a LGPD e o Marco Civil da Internet;
II – auditoria de segurança por entidade independente, quando aplicável;
III – comunicação de incidentes no prazo máximo de 24 horas após a detecção.

CAPÍTULO V
CAPACITAÇÃO E CULTURA DE SEGURANÇA

Art. 9º O Município implementará programas contínuos de capacitação em cibersegurança para servidores e gestores, abrangendo:
I – boas práticas de segurança digital;
II – protocolos de resposta a incidentes;
III – atualização tecnológica constante.

Art. 10 O Município promoverá campanhas e ações educativas voltadas à população, com foco em:
I – conscientização sobre proteção de dados pessoais;
II – prevenção a golpes e fraudes digitais;
III – incentivo à cidadania digital responsável.

CAPÍTULO VI
TRANSPARÊNCIA E PARTICIPAÇÃO SOCIAL

Art. 11 A AMC deverá publicar anualmente:
I – relatórios de conformidade com a LGPD;
II – registros de incidentes e suas respectivas ações de resposta;
III – resultados de auditorias internas e externas.
Art. 12 A participação cidadã será garantida por:
I – conselhos municipais temáticos;
II – ouvidorias;
III – canais digitais de escuta ativa e sugestões.

CAPÍTULO VII
PROCESSO DE CERTIFICAÇÃO E FISCALIZAÇÃO

Art. 13 Fica instituído o Certificado Municipal de Conformidade em Cibersegurança, emitido pela AMC, com validade de 12 meses, renovável mediante nova avaliação.
Art. 14 A fiscalização do cumprimento desta Lei será exercida pela AMC, podendo contar com apoio de órgãos estaduais, federais ou de cooperação regional.

CAPÍTULO VIII
PENALIDADES E CANCELAMENTO

Art. 15 Constituem infrações administrativas:
I – deixar de implementar medidas de segurança exigidas;
II – operar sistemas com vulnerabilidades críticas não corrigidas;
III – descumprir protocolos de resposta a incidentes;
IV – compartilhar dados de forma irregular.
Art. 16 As penalidades aplicáveis incluem:
I – advertência;
II – multa administrativa;
III – suspensão ou cancelamento do Certificado Municipal de Conformidade.
Art. 17 O cancelamento do Certificado poderá ocorrer por reincidência em infrações graves ou decisão administrativa fundamentada.

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 18 O Poder Executivo regulamentará esta Lei no prazo de 180 dias, estabelecendo procedimentos e critérios técnicos.
Art. 19 Esta Lei entra em vigor na data de sua publicação.