Campus Porto Velho Zona Norte
Coordenação do Curso Superior de Tecnologia em
Redes de Computadores

FRANCISCO DAS CHAGAS RAMOS DE ARAÚJO

HÁLISSON TORRES GOMES

RISCO CIBERNÉTICO NO SERVIÇO PÚBLICO

PORTO VELHO/RO

2025

FRANCISCO DAS CHAGAS RAMOS DE ARAÚJO

HÁLISSON TORRES GOMES

RISCO CIBERNÉTICO NO SERVIÇO PÚBLICO

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), *Campus* Porto Velho Zona Norte, como requisito parcial para obtenção do grau de tecnólogo, junto ao Curso Superior de Tecnologia em Redes de Computadores, sob a orientação do professor Ms. Silmar Antonio Buchner de Oliveira.

PORTO VELHO/RO

2025

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO.

Araújo, Francisco das Chagas Ramos de.
Risco cibernético no serviço público / Francisco das Chagas Ramos de Araújo, Hálisson Torres Gomes. - Porto Velho, 2025.
26 f.

Orientador(a): Prof. Ms. Silmar Antonio Buchner de Oliveira.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Redes de Computadores) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Porto Velho, 2025.

1. cibersegurança. 2. setor público. 3. governança digital . 4. resiliência institucional . I. Gomes, Hálisson Torres. II. Oliveira, Silmar Antonio Buchner de (orient.). III. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. IV. Título.

Bibliotecário(a) Responsável: Gizele de Melo Viana, CRB-11/914

FRANCISCO DAS CHAGAS RAMOS DE ARAÚJO

HÁLISSON TORRES GOMES

RISCO CIBERNÉTICO NO SERVIÇO PÚBLICO

Artigo entregue como Trabalho de Conclusão de Curso ao Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), *Campus* Porto Velho Zona Norte, como requisito parcial para obtenção do grau de tecnólogo, junto ao Curso Superior de Tecnologia em Redes de Computadores, sob a orientação do professor Ms. Silmar Antonio Buchner de Oliveira.

Aprovado em: 10/12/2025 pela banca examinadora:

Documento assinado digitalmente
gov.br
SILMAR ANTONIO BUCHNER DE OLIVEIRA
Data: 16/12/2025 01:10:24-0300
Verifique em https://validar.iti.gov.br

Prof. Ms. Silmar Antonio Buchner de Oliveira
Orientador

Documento assinado digitalmente
gov.br
MARIELA MIZOTA TAMADA
Data: 15/12/2025 16:35:06-0300
Verifique em https://validar.iti.gov.br

Prof.a Dr.a Mariela Mizota Tamada
Membro Avaliador

Documento assinado digitalmente
gov.br
DOUGLAS MORO PIFFER
Data: 11/07/2024 14:12:01-0300
Verifique em https://validar.iti.gov.br

Prof. Ms. Douglas Moro Piffer
Membro Avaliador

PORTO VELHO/RO
2025

RISCO CIBERNÉTICO NO SERVIÇO PÚBLICO

RESUMO: O presente estudo analisa a incidência de riscos cibernéticos no serviço público brasileiro, buscando compreender suas causas, impactos e estratégias de mitigação. A partir de uma revisão bibliográfica sistemática, fundamentada em estudos nacionais e internacionais publicados entre 2020 e 2025, a pesquisa identifica que o aumento da digitalização da administração pública ampliou significativamente a exposição das instituições a ataques cibernéticos. O setor público, marcado por sistemas obsoletos, políticas fragmentadas e escassez de profissionais especializados, apresenta baixos níveis de maturidade em segurança da informação. A análise evidencia que, embora existam políticas nacionais e instrumentos normativos, como a Política Nacional de Segurança Cibernética (PNSC), a ausência de integração entre os diferentes níveis de governo e a falta de métricas de desempenho comprometem a eficácia da governança digital. Além disso, destaca-se que a segurança cibernética deve ser tratada como um elemento estratégico de Estado, articulando dimensões tecnológicas, humanas e organizacionais. O estudo conclui que fortalecer a resiliência institucional requer investimentos contínuos em infraestrutura, capacitação e cultura de segurança, aliados à cooperação intergovernamental e ao compartilhamento de informações. Assim, o trabalho contribui para o aprimoramento da governança cibernética e oferece subsídios teóricos e práticos para a formulação de políticas públicas voltadas à proteção digital e à sustentabilidade dos serviços públicos na era da transformação digital.

Palavras-chave: cibersegurança; setor público; governança digital; resiliência institucional.

ABSTRACT: This study analyzes the incidence of cyber risks in the Brazilian public service, seeking to understand their causes, impacts, and mitigation strategies. Based on a systematic literature review, grounded in national and international studies published between 2020 and 2025, the research identifies that the increased digitalization of public administration has significantly amplified the exposure of institutions to cyberattacks. The public sector, marked by obsolete systems, fragmented policies, and a shortage of specialized professionals, presents low levels of maturity in information security. The analysis shows that, although national policies and normative instruments exist, such as the National Cybersecurity Policy (PNSC), the lack of integration between different levels of government and the lack of performance metrics compromise the effectiveness of digital governance. Furthermore, it highlights that cybersecurity should be treated as a strategic element of the State, articulating technological, human, and organizational dimensions. The study concludes that strengthening institutional resilience requires continuous investments in infrastructure, training, and a security culture, coupled with intergovernmental cooperation and information sharing. Thus, this work contributes to the improvement of cyber governance and offers theoretical and practical support for the formulation of public policies aimed at digital protection and the sustainability of public services in the era of digital transformation.

Keywords: cybersecurity; public sector; digital governance; institutional resilience.

1 INTRODUÇÃO

O avanço da transformação digital no setor público trouxe consigo novos riscos, especialmente em termos de segurança da informação e proteção de dados sensíveis. A maioria dos governos ao redor do mundo já implementou plataformas digitais para aumentar a eficiência administrativa, promover a transparência e a inclusão digital dos cidadãos. Porém, essa expansão do ciberespaço governamental tem sido acompanhada por um aumento significativo na incidência de ataques cibernéticos, criando um cenário em que o risco cibernético representa uma ameaça concreta à integridade das instituições públicas. No Brasil, órgãos em diferentes níveis têm sido alvo de incidentes relacionados a roubo de dados, vazamento de informações e interrupção de serviços essenciais, demonstrando fragilidades estruturais em políticas, infraestrutura e capacitação de pessoal (Santos; Filgueiras, 2022; Schneider, 2025).

Os riscos cibernéticos no serviço público representam mais do que simples perdas técnicas ou financeiras; eles afetam diretamente a confiança da sociedade nas instituições públicas. A falta de proteção estratégica da informação ameaça o princípio da soberania digital e pode impactar a governança pública tanto em nível macroeconômico quanto social. A literatura atual destaca que um dos setores mais expostos ao cibercrime é o setor público, devido à obsolescência dos sistemas, à fragmentação das políticas de segurança e à baixa maturidade da cibersegurança (Azambuja; Neto, 2020; Ferreira Neto, 2020; Souza Junior; Streit, 2017).

Por outro lado, a sistematização de experiências internacionais evidencia que governos locais e federais enfrentam desafios semelhantes, o que caracteriza uma tendência universal: a crescente exposição a ameaças digitais. Essas vulnerabilidades exigem o desenvolvimento de políticas públicas mais robustas e integradas para lidar com os riscos cibernéticos (Hossain, 2025; Cremer et al., 2022).

A pandemia da COVID-19 acelerou a digitalização dos serviços públicos e expôs ainda mais as vulnerabilidades de segurança existentes. Durante esse período, a necessidade de expandir o acesso remoto a plataformas institucionais incentivou a rápida implantação de sistemas digitais sem o devido planejamento de

segurança da informação, aumentando a superfície de ataque das infraestruturas governamentais. Além disso, pesquisas mostram que as instituições públicas ainda carecem de protocolos padronizados de resposta a incidentes, investimentos consistentes em cibersegurança e integração nos níveis federal, estadual e municipal (Gsi, 2023; Pena, 2024; Medeiros Et Al., 2020; Rodrigues, 2023). Esse contexto aumenta o interesse em compreender a ocorrência e as causas dos riscos cibernéticos para desenvolver políticas preventivas e estratégias de mitigação.

Considerando esse cenário, o problema central é: Como a literatura especializada caracteriza os tipos de riscos cibernéticos presentes no serviço público brasileiro, avalia as políticas, mecanismos de governança e o nível de maturidade em segurança cibernética, e descreve as estratégias de mitigação voltadas ao fortalecimento da resiliência institucional? Essa questão orienta o estudo, que examina não apenas a natureza das ameaças e seus efeitos, mas também as respostas institucionais estruturadas em três dimensões: a identificação dos tipos de riscos cibernéticos; a análise das políticas, governança e maturidade da segurança cibernética; e a avaliação das estratégias de mitigação e de fortalecimento da resiliência institucional. Ao compreender essas camadas analíticas e suas inter-relações, busca-se oferecer suporte teórico e prático para o aprimoramento da cibersegurança estatal.

Dessa forma, o objetivo geral da pesquisa é analisar os riscos cibernéticos no serviço público brasileiro, articulando sua compreensão às dimensões de identificação dos incidentes, avaliação da governança e definição de estratégias de mitigação. Os objetivos específicos são: (1) investigar os tipos de riscos cibernéticos no serviço público, mapeando os principais incidentes registrados e suas características; (2) analisar as políticas, mecanismos de governança e o nível de maturidade da segurança cibernética adotados por instituições governamentais; e (3) examinar as estratégias de mitigação e fortalecimento da resiliência institucional, formulando recomendações para aprimorar a proteção e a capacidade de resposta do Estado frente às ameaças digitais.

Este estudo torna-se relevante em um mundo onde as administrações públicas dependem cada vez mais de sistemas digitais interdependentes, o que deixa aberta a possibilidade de vulnerabilidades e ataques. Assim como muitos

outros países, o Brasil enfrenta o desafio de consolidar uma política nacional de cibersegurança eficaz e integrada, capaz de acompanhar o dinamismo das ameaças digitais. Além disso, a escassez de profissionais especializados e a fragilidade das políticas de defesa digital aumentam a vulnerabilidade das instituições estatais. Investigações apontam que muitos incidentes recentes ocorreram devido a erro humano, falta de planejamento estratégico e infraestrutura tecnológica precária (Pena et al., 2024; Petry; Hupffer, 2023).

Este trabalho, tanto do ponto de vista científico quanto social, contribui para o desenvolvimento da literatura sobre cibersegurança no setor público, fornecendo uma análise sistematizada da incidência de riscos e um modelo analítico para sua compreensão. Discute também abordagens nacionais e internacionais, aborda a necessidade de políticas públicas baseadas em evidências e integra eixos tecnológicos, humanos e organizacionais. Assim, além de preencher uma lacuna acadêmica identificada em pesquisas anteriores, este artigo visa subsidiar gestores públicos na formulação de estratégias adequadas de cibersegurança, fortalecendo a resiliência institucional diante dos desafios contemporâneos da era digital (Alves; Georg; Nunes, 2023; Hossain, 2025; Vianna; Fernandes, 2015).

2 METODOLOGIA

A presente pesquisa caracteriza-se como uma revisão bibliográfica sistemática de abordagem qualitativa, elaborada conforme as diretrizes do método PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), amplamente utilizado em estudos de revisão científica. Esse método busca garantir transparência, rastreabilidade e rigor metodológico em todas as etapas da revisão, desde a identificação e seleção dos estudos até a análise e síntese dos resultados (Gil, 2015).

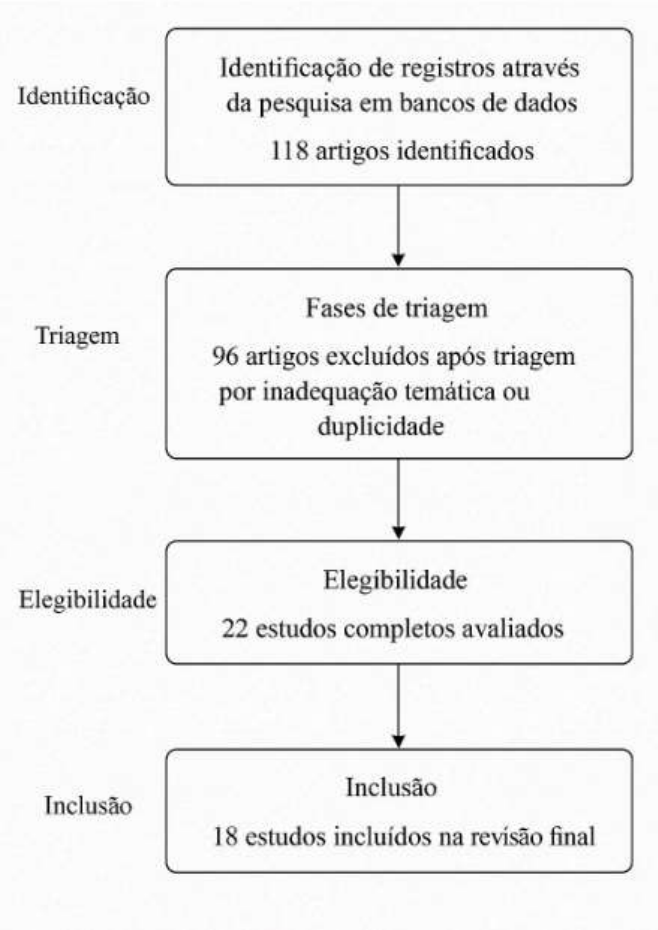
O processo iniciou-se com a formulação da questão norteadora: “Como a literatura especializada caracteriza os tipos de riscos cibernéticos presentes no serviço público brasileiro, avalia as políticas, mecanismos de governança e o nível de maturidade em segurança cibernética, e descreve as estratégias de mitigação voltadas ao fortalecimento da resiliência institucional?” A partir dessa questão, foram definidos critérios de inclusão e exclusão: incluíram-se artigos publicados entre 2020 e 2025, em português e inglês, que abordassem riscos cibernéticos no contexto da administração pública, governança digital, políticas de segurança da informação e ciberdefesa. Foram excluídos estudos duplicados, textos opinativos e publicações sem acesso ao conteúdo completo.

A coleta dos dados ocorreu entre setembro e novembro de 2025, nas seguintes bases: SciELO, Scopus, Dialnet, SpringerLink, Revista do Serviço Público, Revista IBSP e portal do GSI (Gabinete de Segurança Institucional). Foram inicialmente identificados 118 artigos, dos quais 25 foram excluídos após triagem por inadequação temática ou duplicidade. Dos 22 estudos restantes, 18 foram considerados elegíveis e incluídos na revisão final (figura 1).

A análise qualitativa dos artigos seguiu a abordagem de análise de conteúdo, estruturando-se diretamente nas três categorias de resultados do estudo: (a) tipos de riscos cibernéticos no serviço público, identificando vulnerabilidades e padrões de ataques; (b) políticas, governança e nível de maturidade da segurança cibernética, examinando normas, práticas institucionais e limitações estruturais; e (c) estratégias de mitigação e fortalecimento da resiliência institucional, mapeando ações, recomendações e respostas adotadas pelos órgãos públicos. A síntese dos achados

foi apresentada de forma descritiva e interpretativa, permitindo integrar evidências empíricas e normativas sobre o tema (Gil, 2015; GSI, 2023).

Figura 1: Diagrama PRISMA de busca de artigos



Fonte: elaborado pelos autores, 2025.

3 RESULTADOS E DISCUSSÃO

O avanço da digitalização dos serviços públicos consolidou o ciberespaço como um componente estratégico da administração contemporânea, mas, simultaneamente, ampliou a exposição das instituições governamentais a um conjunto crescente de vulnerabilidades técnicas e humanas. A transformação digital no setor público, embora impulsione a eficiência e a transparência, introduz uma complexa teia de riscos associados à segurança cibernética, à proteção de dados e à integridade das operações estatais. O conceito de risco cibernético, nesse contexto, ultrapassa a dimensão puramente tecnológica: trata-se de uma categoria multifacetada que envolve ameaças à soberania informacional, à continuidade de serviços essenciais e à confiança pública nas instituições democráticas.

Conforme argumentam Azambuja e Neto (2020), o Estado brasileiro enfrenta um déficit de maturidade cibernética, marcado pela ausência de padrões integrados de segurança e pela desarticulação entre políticas, estruturas e práticas institucionais. Esse cenário reforça a necessidade de compreender, de modo sistemático, a natureza e a incidência dos riscos cibernéticos no serviço público, analisando tanto a tipologia das ameaças quanto seus impactos estruturais e as respostas governamentais implementadas nos últimos anos.

3.1 TIPOS DOS RISCOS CIBERNÉTICOS NO SERVIÇO PÚBLICO

Quadro 1: Achados referentes aos tipos dos riscos cibernéticos no serviço público

Ataques Diretos a Sistemas	Sequestro de dados e paralisação total de sistemas institucionais.	Alves; Georg; Nunes (2023)
	Enganos direcionados para capturar credenciais e informações sensíveis.	Alves; Georg; Nunes (2023); Vianna; Fernandes (2015)
	Alteração de páginas oficiais e portais públicos.	Alves; Georg; Nunes (2023)
	Tornam portais governamentais indisponíveis por sobrecarga.	GSI (2023)
	Tentativas ou invasões bem-sucedidas a sistemas restritos.	
Riscos Humanos, Culturais, Financeiros, Administrativos e Sociais	Erros humanos propiciam invasões, vazamentos e golpes.	Vianna; Fernandes (2015)
	Segurança vista como tarefa apenas da TI, reduzindo proteção institucional.	Santos; Filgueiras (2022); Vianna; Fernandes (2015)
	Custos com recuperação, sistemas, multas, paralisações.	Alves; Georg; Nunes (2023)

	Ataques minam a confiança pública e a legitimidade democrática.	Santos; Filgueiras (2022);
	Exposição pública de vulnerabilidades aumenta críticas ao governo.	

Fonte: Elaborado pelos autores, 2025.

Os estudos sobre riscos cibernéticos na administração pública evidenciam que a incidência de ataques digitais em instituições estatais tem se intensificado de forma exponencial, especialmente após a aceleração da transformação digital provocada pela pandemia da COVID-19 (Medeiros et al., 2020). Esse aumento não decorre apenas do maior volume de dados processados pelos sistemas governamentais, mas também da ampliação das superfícies de ataque e da complexidade dos ecossistemas digitais interconectados.

As vulnerabilidades decorrem, sobretudo, da coexistência de sistemas legados, infraestrutura defasada e ausência de políticas robustas de governança da informação. Cremer et al. (2022) reforçam que o crescimento dos ataques está associado à insuficiência de dados consolidados sobre a postura de segurança dos órgãos públicos, o que impede a criação de estratégias baseadas em evidências e dificulta a avaliação da resiliência cibernética. Dessa forma, compreender os tipos de riscos predominantes é o primeiro passo para o delineamento de políticas públicas eficazes e para o fortalecimento da defesa digital estatal.

Entre os principais tipos de ataques reportados contra o setor público, destacam-se os incidentes de *ransomware, phishing, defacement* de portais institucionais e vazamentos de dados pessoais sensíveis. Segundo Alves, Georg e Nunes (2023), o Poder Judiciário brasileiro foi um dos alvos mais frequentes dessas ofensivas, evidenciando uma lacuna crítica na gestão de riscos de negócio e na proteção da confidencialidade das informações judiciais.

O caso dos tribunais demonstra que os ataques cibernéticos podem comprometer diretamente a credibilidade do sistema de justiça, além de causar prejuízos financeiros e administrativos significativos. Esses incidentes, em muitos casos, exploram vulnerabilidades humanas, como falhas de autenticação ou descuido na manipulação de credenciais, tanto quanto falhas técnicas. Tal constatação reforça a natureza sociotécnica do risco cibernético, onde a interação entre usuários, sistemas e processos determina a robustez da defesa (Vianna; Fernandes, 2015).

Os levantamentos do Gabinete de Segurança Institucional (GSI, 2023) mostram que, entre 2020 e 2023, houve um aumento de mais de 300% no número de notificações de incidentes envolvendo órgãos públicos federais. Esses eventos variam desde tentativas de acesso não autorizado até ataques de negação de serviço (DDoS) contra portais governamentais. As áreas mais visadas são aquelas com grande concentração de dados sensíveis, como ministérios, tribunais, universidades federais e autarquias vinculadas à gestão de benefícios sociais.

Essa concentração de ataques indica que o vetor principal é a busca por informações estratégicas que possam ser exploradas economicamente ou politicamente, ampliando o escopo do risco para além do dano técnico. Segundo Ferreira Neto (2020), a cibernética deve ser considerada um setor estratégico da defesa nacional, já que os ataques a sistemas públicos não representam apenas crimes digitais, mas também ameaças à soberania e à infraestrutura crítica do Estado.

A literatura internacional corrobora essa tendência, destacando que governos locais e nacionais em diferentes países enfrentam desafios similares na proteção de seus sistemas digitais. Hossain et al. (2024) observaram que a vulnerabilidade de governos locais decorre da descentralização das políticas de segurança, da falta de integração entre plataformas e da limitação orçamentária para investimentos em infraestrutura de cibersegurança.

No contexto brasileiro, esses fatores são agravados pela ausência de um sistema nacional de indicadores que meça a postura de segurança das instituições públicas, o que cria uma percepção fragmentada da real dimensão dos riscos. A revisão conduzida por Hossain (2025) aponta que a vulnerabilidade institucional é tanto maior quanto menor for a maturidade de gestão e coordenação intergovernamental, evidenciando a necessidade de políticas uniformes e integradas.

Outra dimensão crítica é a disponibilidade dos dados e a confiabilidade das informações utilizadas para avaliar a incidência dos riscos. Cremer et al. (2022) identificam uma lacuna global na sistematização de dados de cibersegurança, especialmente no setor público, onde a subnotificação e a falta de transparência comprometem a mensuração precisa das ameaças. No Brasil, embora o GSI (2023) tenha avançado na elaboração de relatórios periódicos, ainda há carência de

padronização na coleta de dados, o que limita comparações entre diferentes órgãos e níveis de governo. Essa insuficiência informacional dificulta a priorização de recursos e a elaboração de políticas baseadas em evidências, reforçando o caráter emergencial da criação de um observatório nacional de incidentes cibernéticos na administração pública.

Os impactos dos ataques cibernéticos no setor público ultrapassam os danos técnicos e financeiros, alcançando dimensões sociais e políticas relevantes. Segundo Santos e Filgueiras (2022), a segurança cibernética é hoje um componente essencial da confiança institucional e da legitimidade democrática. Cada ataque bem-sucedido mina a percepção de eficiência e controle do Estado, alimentando a desconfiança cidadã e abrindo espaço para narrativas de vulnerabilidade governamental. Isso torna o risco cibernético uma ameaça à governança pública e não apenas à infraestrutura digital, demandando respostas estratégicas que envolvam tanto a segurança da informação quanto a comunicação institucional e a gestão de crises.

Casos emblemáticos analisados por Alves, Georg e Nunes (2023) e Petry e Hupffer (2023) demonstram como a fragilidade das práticas de segurança, associada à falta de cultura organizacional voltada à proteção de dados, cria terreno fértil para incidentes severos. A análise do ataque a sistemas judiciais brasileiros em 2022, por exemplo, revelou que a ausência de redundância e a dependência de sistemas centralizados potencializaram o impacto da invasão. Além disso, o estudo de Petry e Hupffer (2023) destaca a importância da Lei Geral de Proteção de Dados (LGPD) como instrumento regulatório que obriga o Estado a aprimorar sua governança da informação, mas cuja aplicação ainda é incipiente em muitos órgãos. A conformidade normativa, embora necessária, não é suficiente se não for acompanhada de práticas técnicas e organizacionais consistentes de segurança digital.

É importante destacar que a incidência crescente de riscos cibernéticos no setor público reflete, em grande medida, a defasagem histórica entre o ritmo de modernização tecnológica e a capacidade institucional de proteção. Souza Junior e Streit (2017) já alertavam que o Brasil carece de uma política cibernética integrada e contínua, capaz de alinhar defesa, inteligência e gestão pública. Passados mais de cinco anos, o diagnóstico permanece atual: as ações ainda são reativas, fragmentadas e dependentes de iniciativas isoladas. Esse descompasso entre

avanço tecnológico e preparo institucional é um dos principais fatores que explicam a vulnerabilidade sistêmica do Estado diante de ameaças digitais cada vez mais sofisticadas e persistentes.

Por fim, deve-se considerar que a incidência de riscos cibernéticos também se relaciona com a dimensão cultural e comportamental das instituições. Vianna e Fernandes (2015) ressaltam que o gestor da segurança da informação enfrenta desafios complexos, que exigem não apenas domínio técnico, mas também habilidades de liderança, comunicação e gestão de pessoas. Em muitas organizações públicas, a segurança ainda é tratada como responsabilidade exclusiva da área de TI, e não como um componente estratégico transversal à administração. Essa visão limitada reduz a eficácia das políticas implementadas e perpetua vulnerabilidades comportamentais, como o uso de senhas fracas, compartilhamento indevido de dados e ausência de capacitação contínua. A consolidação de uma cultura de segurança é, portanto, elemento indispensável para reverter o quadro de alta incidência de riscos no serviço público.

3.2 POLÍTICAS, GOVERNANÇA E MATURIDADE DA SEGURANÇA CIBERNÉTICA

Quadro 2: Achados referentes às políticas, governança e maturidade da segurança cibernética

Governança, Política e Diretrizes no Setor Público	Falta de coordenação, competências fragmentadas, ausência de modelo de maturidade e respostas reativas.	Azambuja; Neto (2020)
	Governança precisa operar de forma cooperativa e não isolada.	Hossain (2025)
	Ausência de protocolos de interoperabilidade, escassez de técnicos e recursos.	Ferreira Neto (2020)
	PNSC carece de mecanismos coercitivos e monitoramento das políticas.	Santos; Filgueiras (2022)
	Necessidade de integrar ações com o contexto internacional para combater crimes cibernéticos.	Pena et al. (2024)
	Governança digital só é eficaz quando segurança é tratada como prioridade estrutural.	Schneider (2025)
Maturidade da Segurança Cibernética	Ausência de indicadores padronizados e dados comparáveis impede avaliar nível de maturidade.	Azambuja & Neto (2020); Cremer et al. (2022)
	Falta de banco de dados unificado de incidentes cibernéticos no Brasil.	Cremer et al. (2022)
	Ausência de equipes estruturadas, falta de análise de risco nos processos decisórios.	Hossain et al. (2024)
	Maturidade depende da conscientização e treinamento de servidores.	Vianna; Fernandes (2015)

	Novas tecnologias geram novos vetores de ataque e exigem maturidade avançada.	Rodrigues (2023)

Fonte: Elaborado pelos autores, 2025.

A governança da segurança cibernética no setor público brasileiro é marcada por assimetrias institucionais e lacunas de coordenação que comprometem a maturidade das políticas e a eficácia das respostas às ameaças digitais. O estudo de Azambuja e Neto (2020) destaca que a ausência de um modelo de maturidade uniforme e a fragmentação das competências entre órgãos resultam em uma postura reativa frente aos incidentes, em vez de uma abordagem preventiva e estratégica. A estrutura pública ainda carece de padrões consolidados para mensurar o nível de preparo das instituições em termos de governança da informação, controle de riscos e proteção de ativos digitais. Tal imaturidade é perceptível tanto nos níveis técnico e normativo quanto na esfera cultural das organizações, refletindo uma visão ainda limitada da cibersegurança como elemento essencial à continuidade administrativa e à soberania nacional. A inexistência de indicadores padronizados e de mecanismos de avaliação comparativa impede que os gestores identifiquem gargalos e priorizem investimentos, perpetuando um ciclo de vulnerabilidade e improvisação institucional (Azambuja; Neto, 2020).

O Gabinete de Segurança Institucional (GSI, 2023) reconhece que, embora o Brasil tenha avançado na formulação de diretrizes estratégicas, como a Política Nacional de Segurança Cibernética (PNSC) e o Comitê de Governança Digital, esses instrumentos ainda não alcançaram plena efetividade. A principal limitação reside na falta de integração entre as esferas federais, estaduais e municipais, o que dificulta a coordenação de ações conjuntas e o compartilhamento de informações sobre ameaças e vulnerabilidades.

A governança cibernética, para ser eficaz, deve operar como uma rede cooperativa e não como um conjunto de iniciativas isoladas. Essa perspectiva é reforçada por Hossain (2025), que, ao analisar o panorama de governos locais em diferentes países, observou que o sucesso das políticas de cibersegurança depende diretamente da capacidade de coordenação intergovernamental e do grau de autonomia das administrações subnacionais. No caso brasileiro, a centralização excessiva das decisões e a falta de canais estruturados de cooperação enfraquecem a resposta coletiva às ameaças digitais.

Ferreira Neto (2020) argumenta que o campo da cibernética deve ser encarado como uma extensão da política de defesa nacional, o que implica em reposicionar a cibersegurança não apenas como uma questão tecnológica, mas como uma dimensão estratégica da soberania estatal. Sob essa ótica, a governança da segurança digital deve articular-se às políticas de inteligência, defesa e desenvolvimento econômico, compondo um eixo transversal de proteção do Estado moderno.

Entretanto, o estudo revela que o Brasil ainda não consolidou uma cultura de segurança ancorada em valores estratégicos e de longo prazo, permanecendo preso a uma lógica operacional fragmentada. Isso se traduz em vulnerabilidades estruturais, como a insuficiência de quadros técnicos especializados, a ausência de protocolos de interoperabilidade entre órgãos e a escassez de recursos para atualização contínua de sistemas. Em contraste, países que incorporaram a ciberdefesa em sua agenda nacional, como Estados Unidos e Reino Unido, alcançaram níveis superiores de maturidade e capacidade de resposta (Ferreira Neto, 2020).

O relatório de Cremer et al. (2022) amplia essa análise ao demonstrar que a maturidade da cibersegurança institucional está diretamente relacionada à disponibilidade de dados, à padronização de processos e à integração de indicadores de desempenho. Na ausência de informações consolidadas e comparáveis, torna-se impossível estabelecer políticas baseadas em evidências e avaliar o impacto das iniciativas já implementadas. No contexto brasileiro, a falta de uma base de dados unificada sobre incidentes cibernéticos impede que os gestores compreendam a magnitude e as tendências das ameaças, o que reduz a eficiência dos planos de contingência e das estratégias preventivas. Essa lacuna metodológica é agravada pela dificuldade em integrar dados de diferentes órgãos e níveis administrativos, o que reforça a necessidade de um sistema nacional de métricas de segurança cibernética voltado à administração pública.

Segundo Santos e Filgueiras (2022), a PNSC constitui um marco importante na tentativa de institucionalizar a governança da segurança cibernética no país, mas enfrenta desafios na sua implementação prática. As principais barreiras identificadas pelos autores incluem a ausência de mecanismos de monitoramento, a indefinição de responsabilidades e a baixa aderência das instituições públicas às diretrizes

nacionais. Embora a política proponha um arcabouço normativo consistente, ela carece de instrumentos coercitivos que obriguem os órgãos públicos a adotarem padrões mínimos de segurança. Essa deficiência normativa é um reflexo da estrutura federativa brasileira, que confere autonomia administrativa a estados e municípios, dificultando a imposição de práticas uniformes. A superação desse obstáculo exige o fortalecimento de mecanismos de coordenação, auditoria e capacitação, de modo que a governança cibernética se torne efetivamente transversal e sustentável.

Hossain et al. (2024) reforçam que a maturidade da segurança digital está intrinsecamente vinculada à capacidade de aprendizado institucional e à existência de mecanismos de governança adaptativa. Em governos locais e regionais, essa capacidade depende da institucionalização de rotinas de auditoria, da criação de equipes de resposta a incidentes e da incorporação da análise de risco nos processos decisórios.

No Brasil, apesar de iniciativas pontuais como o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), as ações permanecem restritas a esferas técnicas, sem o devido envolvimento das lideranças políticas e administrativas. Essa ausência de compromisso estratégico fragiliza a cultura organizacional de segurança e compromete a capacidade de resposta em situações de crise. Além disso, a maturidade institucional depende do desenvolvimento de competências humanas, uma vez que a segurança cibernética é tão forte quanto o nível de conscientização e treinamento dos servidores públicos (Vianna; Fernandes, 2015).

O estudo de Pena et al. (2024) analisa as estratégias de políticas públicas no combate aos crimes cibernéticos e evidencia a necessidade de alinhar as ações governamentais com o contexto internacional, especialmente no que se refere à cooperação entre órgãos de investigação, defesa e regulação. A análise mostra que o Brasil ainda carece de uma estrutura coordenada que integre o sistema de justiça, as forças armadas e os órgãos civis na prevenção e mitigação de ataques.

A fragmentação de competências e a sobreposição de atribuições geram ineficiências que enfraquecem o arcabouço normativo e dificultam a resposta a incidentes complexos, como ataques de *ransomware* contra infraestruturas críticas. Ademais, Pena (2024) enfatiza que a formulação de políticas públicas deve ser acompanhada de investimentos contínuos em tecnologia, pesquisa aplicada e

formação de especialistas, sob pena de as estratégias permanecerem apenas no nível discursivo.

Por outro lado, estudos como o de Rodrigues (2023) introduzem uma dimensão inovadora ao relacionar a adoção de tecnologias emergentes, como blockchain, à melhoria da governança digital. A implementação de artefatos descentralizados pode reduzir riscos de integridade e autenticação, ampliando a confiabilidade das transações governamentais. No entanto, o autor ressalta que a adoção dessas tecnologias deve ser acompanhada de políticas de segurança consistentes, pois novas soluções também trazem novos vetores de vulnerabilidade. A governança digital, portanto, precisa equilibrar inovação e segurança, garantindo que o avanço tecnológico não amplie o espectro de riscos. Essa visão reforça o argumento de Schneider (2025), segundo o qual a segurança cibernética é o alicerce da transformação digital do governo, e não um componente acessório. A maturidade institucional só se consolida quando a segurança é tratada como princípio estruturante da administração pública.

A maturidade da segurança cibernética no serviço público brasileiro permanece em um estágio intermediário, caracterizado por avanços pontuais e desafios estruturais persistentes. A governança ainda carece de integração entre esferas administrativas, de métricas padronizadas e de uma cultura organizacional voltada à prevenção e resiliência. Como indicam Azambuja e Neto (2020) e o GSI (2023), a consolidação de um modelo de maturidade exige não apenas normas e políticas, mas também capacidade técnica, recursos humanos qualificados e uma visão estratégica de longo prazo. A próxima seção, portanto, abordará as estratégias de mitigação e fortalecimento da resiliência institucional, discutindo caminhos possíveis para elevar o patamar de proteção e confiança do setor público brasileiro diante das ameaças digitais contemporâneas.

3.3 ESTRATÉGIAS DE MITIGAÇÃO E FORTALECIMENTO DA RESILIÊNCIA INSTITUCIONAL

Quadro 3: Achados referentes às estratégias de mitigação e fortalecimento da resiliência institucional

Estratégias de Mitigação / Fortalecimento	Reconhecer que segurança cibernética é problema de gestão pública, não apenas técnico.	Alves; Georg; Nunes (2023)
	Conformidade com a LGPD como instrumento de confiança pública.	Petry; Hupffer (2023)

	Criação de um ecossistema nacional de resiliência cibernética.	GSI (2023)
	Cooperação internacional e aprendizado com modelos estrangeiros.	GSI (2023); Souza Junior; Streit (2017)
	Treinamentos, campanhas educativas e desenvolvimento da cultura de prevenção.	Hossain (2025)
	Aprendizado contínuo baseado em incidentes reais ("aprender com o ataque")	Hossain et al. (2024)
	Modernização e interoperabilidade de sistemas digitais.	Ribeiro et al. (2023)
	Implementação de políticas de gestão segura de dados pessoais.	Petry; Hupffer (2023)
	Tratar segurança digital como parte da defesa nacional.	Ferreira Neto (2020)
	Investimentos em pesquisa, inovação e capacidade técnica.	
	Inserção de segurança cibernética nos planos estratégicos e de contingência.	Medeiros et al. (2020)
	Comunicação institucional clara em crises cibernéticas.	

Fonte: Elaborado pelos autores, 2025.

O fortalecimento da resiliência cibernética nas instituições públicas demanda um conjunto de estratégias que integrem dimensões tecnológicas, organizacionais e políticas. Como afirmam Alves, Georg e Nunes (2023), os ataques direcionados ao Poder Judiciário brasileiro evidenciam que a simples adoção de mecanismos técnicos de defesa é insuficiente para conter ameaças cada vez mais sofisticadas e persistentes. Os autores destacam que as invasões e tentativas de comprometimento de sistemas judiciais, especialmente em tribunais estaduais, resultam não apenas de vulnerabilidades técnicas, mas também de deficiências na governança, na gestão de riscos e na cultura de segurança dos servidores. Assim, o primeiro passo para a mitigação efetiva é o reconhecimento de que a cibersegurança é um problema de gestão pública e não apenas de tecnologia, exigindo políticas de prevenção, treinamento e coordenação interinstitucional. Essa abordagem holística deve envolver tanto a alta administração quanto os níveis operacionais, assegurando que a segurança da informação seja compreendida como um valor institucional e não como um conjunto de procedimentos isolados (Alves; Georg; Nunes, 2023).

O relatório do Gabinete de Segurança Institucional (GSI, 2023) indica que a criação de um ecossistema nacional de resiliência cibernética é uma das metas

prioritárias do Estado brasileiro. Tal ecossistema deve articular órgãos públicos, instituições de pesquisa e o setor privado em uma rede cooperativa de monitoramento, resposta e aprendizado contínuo. Essa rede, segundo o documento, deve ser capaz de identificar vulnerabilidades de forma antecipada, compartilhar indicadores de ameaças e desenvolver planos coordenados de mitigação. A experiência internacional demonstra que países com sistemas maduros de resposta a incidentes — como os Estados Unidos, a Estônia e Israel — baseiam sua eficácia na capacidade de troca de informações e no fortalecimento das capacidades locais. No caso do Brasil, o desafio é estruturar mecanismos de cooperação federativa que respeitem as autonomias institucionais sem comprometer a unidade estratégica da defesa cibernética nacional. Assim, a resiliência não se constrói apenas pela soma de esforços isolados, mas pela integração sistêmica das políticas e práticas de segurança digital (GSI, 2023).

Petry e Hupffer (2023) abordam a importância de alinhar as estratégias de resiliência às disposições da Lei Geral de Proteção de Dados (LGPD), destacando o princípio da segurança como eixo fundamental da governança de dados. A proteção das informações pessoais e sensíveis é componente indispensável da segurança cibernética institucional, e sua violação pode acarretar danos jurídicos, reputacionais e sociais. Para os autores, o cumprimento da LGPD deve ser compreendido como instrumento de fortalecimento da confiança pública e de legitimação das ações governamentais no ambiente digital. A mitigação dos riscos passa, portanto, pela implementação de políticas de gestão de dados seguras, pela criação de comitês de governança e pela auditoria contínua de fluxos informacionais. Ademais, a interseção entre privacidade e segurança exige um equilíbrio delicado entre transparência administrativa e proteção de dados, reforçando o papel estratégico das unidades de proteção de dados dentro das estruturas de governo (Petry; Hupffer, 2023).

Hossain (2025) defende que as estratégias de mitigação em governos locais devem priorizar a educação cibernética e o fortalecimento das capacidades humanas. O autor demonstra que muitas vulnerabilidades decorrem não de falhas tecnológicas, mas de comportamentos inadequados, falta de conscientização e ausência de protocolos básicos de segurança entre os servidores. Assim, programas de treinamento, campanhas de sensibilização e a criação de uma cultura

organizacional orientada à prevenção são componentes fundamentais para a construção de um ambiente digital resiliente. Além disso, Hossain et al. (2024) reforçam que a resiliência é resultado de processos contínuos de aprendizado e adaptação. As instituições precisam incorporar mecanismos de retroalimentação que permitam revisar políticas e corrigir falhas a partir de incidentes reais, transformando cada crise em oportunidade de aprimoramento. Esse ciclo virtuoso de aprender com o ataque é o que diferencia organizações vulneráveis de organizações resilientes.

No contexto da administração pública brasileira, Medeiros et al. (2020) destacam que a pandemia da COVID-19 acelerou o uso do ciberespaço e escancarou as fragilidades das infraestruturas digitais governamentais. A rápida migração de serviços presenciais para plataformas digitais ocorreu sem o devido planejamento de segurança, ampliando significativamente a superfície de ataque. Essa experiência revelou a necessidade de políticas estruturadas de governança digital resiliente, baseadas em princípios de continuidade operacional e proteção de dados. A resposta a emergências digitais deve estar prevista nos planos estratégicos das instituições, com protocolos claros para atuação em caso de comprometimento de sistemas. A mitigação de riscos, portanto, passa pela incorporação da cibersegurança nos planos de gestão de crises e pela criação de unidades especializadas capazes de coordenar ações de resposta, recuperação e comunicação institucional (Medeiros et al., 2020).

Ferreira Neto (2020) argumenta que a construção da resiliência cibernética no Brasil também exige o reconhecimento da cibernética como setor estratégico de defesa nacional. Isso implica uma mudança de paradigma: a segurança digital deve ser tratada como componente da segurança nacional, com investimentos contínuos em pesquisa, inovação e capacitação técnica. As Forças Armadas e o setor de inteligência desempenham papel essencial nesse processo, não apenas como agentes de proteção, mas como promotores do desenvolvimento tecnológico e da integração entre os setores público e privado. O fortalecimento da resiliência depende de uma visão geoestratégica capaz de antecipar tendências e compreender a guerra cibernética como um campo de disputa global. Dessa forma, as estratégias de mitigação não podem limitar-se à defesa passiva, devendo incluir capacidades ofensivas e dissuasórias, alinhadas a padrões internacionais de ciberdefesa (Ferreira Neto, 2020).

Ribeiro et al. (2023) complementam esse debate ao apresentar um panorama global da postura de segurança dos serviços públicos online, demonstrando que a eficácia das estratégias de mitigação depende da maturidade das infraestruturas digitais e do grau de automação dos processos de segurança. Países com estruturas mais integradas e automatizadas são capazes de detectar e responder a incidentes em tempo real, reduzindo significativamente os impactos sobre a continuidade dos serviços. No Brasil, a ausência de uma arquitetura digital unificada e a fragmentação de sistemas dificultam a detecção precoce de anomalias e a coordenação das respostas. Portanto, a modernização tecnológica, a interoperabilidade de sistemas e a adoção de ferramentas de inteligência artificial para análise de ameaças são componentes indispensáveis para a mitigação de riscos e fortalecimento da resiliência (Ribeiro et al., 2023).

Por fim, Souza Junior e Streit (2017) afirmam que a experiência internacional demonstra que o sucesso das políticas de segurança cibernética depende de uma combinação entre regulação, cooperação e cultura institucional. A regulação cria os parâmetros normativos e de responsabilidade; a cooperação viabiliza a troca de informações e recursos; e a cultura institucional sustenta a adesão dos agentes públicos aos valores de segurança e ética digital. Essa tríade deve orientar as estratégias brasileiras de mitigação e resiliência, assegurando que as políticas não se limitem ao discurso, mas se traduzam em práticas concretas e sustentáveis. Nesse sentido, Pena (2024) e Springer (2024) destacam que a excessiva burocratização da regulação cibernética pode gerar riscos ocultos, enfraquecendo a agilidade das respostas e desestimulando a inovação. Assim, a regulação deve buscar equilíbrio entre controle e flexibilidade, permitindo que as instituições públicas adaptem suas políticas sem comprometer a conformidade legal e a segurança nacional.

Em síntese, as estratégias de mitigação e fortalecimento da resiliência institucional na administração pública brasileira devem ser compreendidas como um processo contínuo, transversal e multidimensional. A construção da resiliência exige a integração de políticas de defesa, governança digital, proteção de dados e educação cibernética, ancoradas em princípios de cooperação e aprendizado permanente. Somente por meio dessa abordagem sistêmica o Estado brasileiro poderá enfrentar com eficácia os riscos crescentes do ciberespaço e garantir a

segurança de seus ativos informacionais e da própria soberania digital. As experiências e estudos analisados demonstram que o caminho para a maturidade cibernética está na convergência entre estratégia, tecnologia e cultura organizacional, pilares fundamentais para a consolidação de um governo digital seguro, confiável e resiliente.

4 CONSIDERAÇÕES FINAIS

A análise realizada ao longo deste estudo demonstra que a incidência de riscos cibernéticos no serviço público brasileiro reflete uma realidade estrutural e multifacetada, onde fragilidades tecnológicas, organizacionais e humanas se entrelaçam em um cenário de vulnerabilidade crescente. Os resultados revelam que a digitalização acelerada das funções estatais, embora tenha ampliado a eficiência administrativa e a transparência, também expôs o Estado a ameaças sofisticadas e dinâmicas. A ausência de uma cultura institucional sólida de segurança, a defasagem dos sistemas e a carência de investimentos contínuos em infraestrutura cibernética agravam o problema e tornam as instituições públicas mais suscetíveis a ataques e interrupções. Compreender a natureza e a incidência desses riscos é, portanto, essencial para garantir a soberania informacional e a continuidade dos serviços públicos digitais.

Verificou-se que, apesar dos avanços na formulação de políticas nacionais de segurança cibernética e na consolidação de estruturas normativas, o Brasil ainda enfrenta desafios expressivos na implementação prática e na articulação entre os diferentes níveis de governo. A falta de integração entre órgãos federais, estaduais e municipais, aliada à escassez de profissionais especializados e à fragmentação das políticas, compromete a eficácia das ações preventivas e corretivas. O fortalecimento da governança digital exige, assim, uma abordagem sistêmica, baseada na cooperação interinstitucional, na padronização de protocolos e na disseminação de uma cultura de segurança orientada à prevenção. A maturidade cibernética não se limita à capacidade técnica de defesa, mas envolve a institucionalização de valores, processos e responsabilidades compartilhadas.

Por fim, as estratégias de mitigação e resiliência precisam transcender o aspecto técnico e consolidar-se como um projeto de Estado, sustentado por políticas públicas consistentes, regulação equilibrada e mecanismos permanentes de aprendizado organizacional. A construção de uma administração pública digital segura e resiliente depende da integração entre tecnologia, gestão e educação cibernética, assegurando que servidores e gestores compreendam seu papel na proteção de ativos informacionais estratégicos. A resiliência institucional será o principal indicador da capacidade do Estado brasileiro de enfrentar as ameaças

digitais futuras, garantindo a continuidade dos serviços, a proteção dos cidadãos e a preservação da confiança pública na era da transformação digital.

REFERÊNCIAS

ALVES, Renato Solimar; GEORG, Marcus Aurélio Carvalho; NUNES, Rafael Rabelo. Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E56, p. 344-357, 2023. Disponível em: https://dialnet.unirioja.es/descarga/articulo/5173596.pdf. Acesso em 20 de nov. de 2025.

AZAMBUJA, Antônio João G.; 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, 2020. Disponível em: https://revista.enap.gov.br/index.php/RSP/article/view/3210. Acesso em: 20 nov. 2025. Revista do Serviço Público

CREMER, F. et al. Cyber risk and cybersecurity: a systematic review of data availability. **European Journal of Risk Regulation**, 2022. Disponível em: https://pmc.ncbi.nlm.nih.gov/articles/PMC8853293/. Acesso em: 20 nov. 2025.

FERREIRA NETO, Walfredo Bento. Cibernética como setor estratégico no Brasil e seus reflexos para a estrutura da Defesa. **Análise Estratégica — Centro de Estudos Estratégicos do Exército**, v. 17, n. 3, p. 45-64, 2020. Disponível em: https://ebrevistas.eb.mil.br/CEEExAE/article/view/6409. Acesso em: 20 nov. 2025. EB Revistas

GIL, A. C. **Como elaborar projetos de pesquisa**. 16. ed. São Paulo: Atlas, 2015. 176 p.

GSI, Gabinete de Segurança Institucional da Presidência Da República. **Revisão da Capacidade de Segurança Cibernética do Brasil**. Brasília: GSI, 2023. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/eventos/CMMreportBrazil2023_final_PT.pdf. Acesso em: 20 nov. 2025.

HOSSAIN, S. T. Cybersecurity in local governments: A systematic review. **Journal of Cybersecurity and Privacy**, 2025. Disponível em: https://www.sciencedirect.com/science/article/pii/S2664328624000792. Acesso em: 20 nov. 2025.

HOSSAIN, S. T. et al. Local Government Cybersecurity Landscape: A Systematic Review. **Applied Sciences**, v. 14, n. 13, p. 5501, 2024. Disponível em: https://www.mdpi.com/2076-3417/14/13/5501. Acesso em: 20 nov. 2025.

MEDEIROS, B. P.; et al. O uso do ciberespaço pela administração pública na pandemia da COVID-19: desafios para a governança digital. **Revista Administração Pública (RAP)**, v. 54, n. 4, p. 889-908, 2020. Disponível em: https://www.scielo.br/j/rap/a/x3VKDBRYpkvNb8dmXN4rNyR/. Acesso em: 20 nov. 2025.

PENA, S. A. Estratégias de políticas públicas no combate aos crimes cibernéticos. **Revista IBSP de Segurança Pública**, 2024. Disponível em: https://revista.ibsp.org.br/index.php/RIBSP/article/view/244. Acesso em: 20 nov. 2025.

PENA, Stanley Araújo; FILHO, Cid Gonçalves; GALIZA, João Pedro Lima de Medeiros; MARQUES, Júnio Souto. Estratégias de políticas públicas no combate aos crimes cibernéticos: uma análise crítica. **Revista do Instituto Brasileiro de Segurança Pública (RIBSP)**, 2024. Disponível em: https://revista.ibsp.org.br/index.php/RIBSP/article/view/244. Acesso em: 20 nov. 2025. revista.ibsp.org.br

PETRY, Gabriel Cemin; HUPFFER, Haide Maria. O princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD. **Revista CNJ**, Brasília, v. 7, n. 1, p. 85-98, 2023. Disponível em: https://www.cnj.jus.br/ojs/revista-cnj/article/view/445. Acesso em: 20 nov. 2025. Conselho Nacional de Justiça+1

RIBEIRO, D.; SILVA, J. M.; RAMOS, L. F.; FONTE, V. A worldwide overview on the information security posture of online public services. **arXiv preprint**, 2023. Disponível em: https://arxiv.org/abs/2310.01200. Acesso em: 20 nov. 2025.

RODRIGUES, Dênis. Fatores sociotécnicos na adoção de artefatos baseados em blockchain para governo. **Revista do Serviço Público**, Brasília, v. 74, n. 3, p. 570-590, 2023. Disponível em: https://revista.enap.gov.br/index.php/RSP/article/view/7933. Acesso em: 20 nov. 2025.

SANTOS, C. S. A.; FILGUEIRAS, F. Proposta de avaliação da Política Nacional de Segurança Cibernética: riscos, desafios e caminhos. **Política & Sociedade (PCI)**, 2022. Disponível em: https://www.scielo.br/j/pci/a/ks9gSpJbgRNJP9vZxbfHJqL/. Acesso em: 20 nov. 2025.

SCHNEIDER, G. B. C. The Importance of Cybersecurity in Digital Government. **Revista Cognitionis**, v. 6, n. 2, 2025. Disponível em: https://revista.cognitioniss.org/index.php/cogn/article/view/585. Acesso em: 20 nov. 2025.

SOUZA JUNIOR, Alcyon Ferreira de; STREIT, Rosalvo Ermes. Segurança cibernética: política brasileira e a experiência internacional. **Revista do Serviço Público**, Brasília, v. 68, n. 1, p. 107-130, 2017. Disponível em: https://revista.enap.gov.br/index.php/RSP/article/view/864. Acesso em: 20 nov. 2025. Revista do Serviço Público+1

SPRINGER. More than malware: unmasking the hidden risk of cybersecurity regulations. **International Cybersecurity Law Review**, 2024. Disponível em: https://link.springer.com/article/10.1365/s43439-024-00111-7. Acesso em: 20 nov. 2025.

VIANNA, Eduardo Wallier; FERNANDES, Jorge Henrique Cabral. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos. **Brazilian Journal of Information Science**, v. 9, n. 1, p. 4, 2015. Disponível em: https://dialnet.unirioja.es/descarga/articulo/5173596.pdf. Acesso em 20 de nov. de 2025.