INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO
CAMPUS CERES
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

CARLOS HENRIQUE MOTA MARTINS

# DESAFIOS E ESTRATÉGIAS PARA A SEGURANÇA DA INFORMAÇÃO EM AMBIENTES DIGITAIS DO SERVIÇO PÚBLICO NAS PREFEITURAS DE PEQUENOS MUNICÍPIOS DO VALE DO SÃO PATRICIO

Ceres
2025

CARLOS HENRIQUE MOTA MARTINS

# DESAFIOS E ESTRATÉGIAS PARA A SEGURANÇA DA INFORMAÇÃO EM AMBIENTES DIGITAIS DO SERVIÇO PÚBLICO NAS PREFEITURAS DE PEQUENOS MUNICÍPIOS DO VALE DO SÃO PATRICIO

Trabalho de conclusão de curso de graduação apresentado para obtenção do grau de Bacharel em Sistemas de Informação ao Instituto Federal Goiano - Campus Ceres.

Orientador: Prof. MSc. Ramayane Bonacin Braga

Ceres

2025

**Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema Integrado de Bibliotecas do IF Goiano - SIBi**

Mota Martins, Carlos Henrique
M386d Desafios e estratégias para a segurança da informação em ambientes digitais do serviço público nas prefeituras de pequenos municípios do Vale do São Patricio / Carlos Henrique Mota Martins. Ceres 2025.

58f. il.

Orientadora: Profª. Ma. Ramayane Bonacin Braga.
Tcc (Bacharel) - Instituto Federal Goiano, curso de 0320203 - Bacharelado em Sistemas de Informação - Ceres (Campus

I. Título.

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

INSTITUTO FEDERAL
Goiano

**Repositório Institucional do IF Goiano - RIIF IF Goiano Sistema Integrado de Bibliotecas**

---

**TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO**

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano, a disponibilizar gratuitamente o documento no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

**Identificação da Produção Técnico-Científica**

| | |
|---|---|
| [ ] Tese | [ ] Artigo Científico |
| [ ] Dissertação | [ ] Capítulo de Livro |
| [ ] Monografia – Especialização | [ ] Livro |
| [ ] Artigo - Especialização | [ ] Trabalho Apresentado em Evento |
| [X] TCC - Graduação | [ ] Produção Técnica |

Nome Completo do Autor: Carlos Henrique Mota Martins
Matrícula: 2022103202030047
Título do Trabalho: DESAFIOS E ESTRATÉGIAS PARA A SEGURANÇA DA INFORMAÇÃO EM AMBIENTES DIGITAIS DO SERVIÇO PÚBLICO NAS PREFEITURAS DE PEQUENOS MUNICÍPIOS DO VALE DO SÃO PATRICIO

**Restrições de Acesso ao Documento**

Documento confidencial: [X] Não [ ] Sim, justifique: _____
Informe a data que poderá ser disponibilizado no RIIF Goiano:12/12/2025
O documento está sujeito a registro de patente? [ ] Sim [X] Não
O documento pode vir a ser publicado como livro? [ ] Sim [X] Não

**DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA**

O(a) referido(a) autor(a) declara que:

1. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;

2. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;

3. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Ceres, 10 de dezembro de 2025.

Carlos Henrique Mota Martins
*(Assinado Eletronicamente pelo o Autor e/ou Detentor dos Direitos Autorais)*

Ciente e de acordo:

Ramayane Bonacin Braga
*(Assinado Eletronicamente pela orientadora)*

Documento assinado eletronicamente por:

- **Ramayane Bonacin Braga**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 10/12/2025 19:10:51.
- **Carlos Henrique Mota Martins**, **2022103202030047 - Discente**, em 10/12/2025 19:12:17.

Este documento foi emitido pelo SUAP em 10/12/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

**Código Verificador:** 773361
**Código de Autenticação:** 88ec4d0cdd

INSTITUTO FEDERAL GOIANO
Campus Ceres
Rodovia GO-154, Km 03, SN, Zona Rural, CERES / GO, CEP 76300-000
(62) 3307-7100

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

**ATA DE DEFESA DE TRABALHO DE CURSO**

Aos 26 dias do mês de novembro do ano de dois mil e vinte e cinco, realizou-se a defesa de Trabalho de Curso do acadêmico Carlos Henrique Mota Martins, do Curso de Bacharelado em Sistemas de Informação, matrícula 2022103202030047, cujo título é "DESAFIOS E ESTRATÉGIAS PARA A SEGURANÇA DA INFORMAÇÃO EM AMBIENTES DIGITAIS DO SERVIÇO PÚBLICO NAS PREFEITURAS DE PEQUENOS MUNICÍPIOS DO VALE DO SÃO PATRICIO". A defesa iniciou-se às 21 horas e 03 minutos, finalizando-se às 21 horas e 26 minutos. A banca examinadora considerou o trabalho APROVADO com média 9,8 no trabalho escrito, média 9,8 no trabalho oral, apresentando assim média aritmética final de 9,8 pontos, estando o estudante APTO para fins de conclusão do Trabalho de Curso.

Após atender às considerações da banca e respeitando o prazo disposto em calendário acadêmico, o estudante deverá fazer a submissão da versão corrigida em formato digital (.pdf) no Repositório Institucional do IF Goiano – RIIF, acompanhado do Termo Ciência e Autorização Eletrônico (TCAE), devidamente assinado pelo autor e orientador.

Os integrantes da banca examinadora assinam a presente.

*(Assinado Eletronicamente)*
Ramayane Bonacin Braga

*(Assinado Eletronicamente)*
Lucas William de Lima Fortes Dourado

*(Assinado Eletronicamente)*
Vilson Soares de Siqueira

Documento assinado eletronicamente por:

- **Ramayane Bonacin Braga**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 26/11/2025 22:18:24.
- **Vilson Soares de Siqueira**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 26/11/2025 22:19:30.
- **Lucas Wiliam de Lima Fortes Dourado** , **700.032.791-03 - Usuário Externo**, em 10/12/2025 18:48:58.

Este documento foi emitido pelo SUAP em 26/11/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

**Código Verificador:** 767098
**Código de Autenticação:** 18d8ffed90

## RESUMO

A digitalização dos serviços públicos em pequenos municípios impõe desafios significativos de Segurança da Informação (SI), agravados pela escassez de recursos e pela necessidade de conformidade com a Lei Geral de Proteção de Dados (LGPD). Este trabalho objetivou investigar os desafios de SI em prefeituras de pequeno porte no Vale do São Patrício e, a partir de um diagnóstico, propor estratégias viáveis para mitigar os riscos. A pesquisa adotou uma abordagem mista (quali-quantitativa), de natureza exploratória-descritiva e aplicada, configurando-se como um estudo de caso múltiplo agregado em quatro municípios (23 respondentes). Os dados foram coletados por meio de questionários e análise documental. Os resultados revelaram vulnerabilidades críticas, caracterizando um "vácuo de governança" e instrucional. Diagnosticou-se que 95,7% dos servidores nunca receberam treinamento, 45,5% dos não treinados admitem compartilhar senhas, e 78,3% não possuem rotinas de backup. Identificou-se um "ponto cego"de conhecimento em ameaças, com o *Phishing* apresentando a menor média de conhecimento (1.87 em 5). Ademais, 47,8% dos servidores desconhecem a existência de uma equipe de SI, e a não obtenção de documentos (POSIC/PDTI) corrobora a percepção de informalidade nos processos. Conclui-se que a maior vulnerabilidade é humana e organizacional. Como produto, este trabalho propõe um conjunto de soluções adaptadas, consolidadas em um "Guia Prático de Segurança da Informação"(Apêndice C). O Guia foca nas lacunas diagnosticadas (*Phishing*, senhas, backup) como uma estratégia de baixo custo e alta aplicabilidade, alinhada à realidade de escassez dos municípios.



**Palavras-chave**: Segurança da Informação. Setor Público. Pequenos Municípios. Governança de TI. Vulnerabilidades.

## ABSTRACT

The digitization of public services in small municipalities imposes significant Information Security (IS) challenges, aggravated by resource scarcity and the need for compliance with the General Data Protection Law (LGPD). This study aimed to investigate IS challenges in small city halls in the Vale do São Patrício region and, based on a diagnosis, propose viable strategies to mitigate risks. The research adopted a mixed-methods (quali-quantitative) approach, with an exploratory-descriptive and applied nature, configured as an aggregated multiple case study across four municipalities (23 respondents). Data were collected through questionnaires and document analysis. The results revealed critical vulnerabilities, characterizing a "governance and instructional vacuum". It was diagnosed that 95.7% of employees have never received training, 45.5% of those untrained admit to sharing passwords, and 78.3% do not have backup routines. A knowledge "blind spot" regarding threats was identified, with Phishing showing the lowest average awareness (1.87 out of 5). Furthermore, 47.8% of employees are unaware of the existence of an IS team, and the failure to obtain documents (IS Policy/IT Master Plan) corroborates the perception of informal processes. It is concluded that the greatest vulnerability is human and organizational. As a product, this work proposes a set of adapted solutions, consolidated in a "Practical Information Security Guide" (Appendix C). The Guide focuses on the diagnosed gaps (Phishing, passwords, backup) as a low-cost, high-applicability strategy aligned with the municipalities' reality of scarcity.



**Keywords**: Information Security. Public Sector. Small Municipalities. IT Governance. Vulnerabilities.

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| LGPD | Lei Geral de Proteção de Dados Pessoais |
| ISO | Organização Internacional para Padronização |
| TCE-GO | Tribunal de Contas do Estado de Goiás |
| TI | Tecnologia da Informação |
| SI | Segurança da Informação |
| DBIR | Data Breach Investigations Report |
| GTI | Gestão de Tecnologia da Informação |
| TCE-PE | Tribunal de Contas do Estado de Pernambuco |
| IBGE | Instituto Brasileiro de Geografia e Estatística |
| POSIC | Política de Segurança da Informação e Comunicações |
| SGSI | Sistemas de Gestão de Segurança da Informação |
| NIST | National Institute of Standards and Technology |

**SUMÁRIO**

# 1 INTRODUÇÃO

Pequenos municípios lidam com desafios para garantir a segurança da informação, sobretudo devido à limitação de recursos financeiros, a falta de equipes especializadas e a carência de políticas de governança bem estruturadas. Essas vulnerabilidades tornam as infraestruturas tecnológicas do setor público suscetíveis a ataques cibernéticos, vazamentos de informações e falhas operacionais, comprometendo a entrega de serviços essenciais e a confiança dos cidadãos, Souza (2020).

Diante deste cenário, surge o seguinte questionamento: Como os pequenos municípios do Vale do São Patrício podem implementar estratégias eficazes de segurança da informação para proteger seus dados e sistemas, considerando suas limitações financeiras e técnicas?

Para responder a essa questão, a presente pesquisa foca no desenvolvimento de um "framework", ou guia prático de segurança da informação, adaptado às realidades de pequenos municípios, baseada nas normas ISO 27001 e ISO 27002, combinado à capacitação de servidores, que possui o potencial de reduzir os incidentes de segurança, como vazamentos de dados, ataques cibernéticos e falhas operacionais nas prefeituras que adotarem esta estratégia. Esta abordagem encontra respaldo no estudo de caso da Prefeitura de Mataraca, apresentado por Neto (2021), que demonstrou como a adoção de medidas básicas de segurança, incluindo a formalização de políticas de acesso, pode reduzir significativamente as vulnerabilidades em municípios de pequeno porte.

A proposta considera as restrições orçamentárias e técnicas típicas de municípios com menos de 50 mil habitantes, oferecendo um modelo viável e replicável para contextos similares. Um fator essencial é a utilização de ferramentas acessíveis e soluções de código aberto, que viabilizem medidas de segurança sem comprometer excessivamente os recursos financeiros do município. Segundo Neto (2021), a adoção de softwares de segurança gratuitos e bem configurados pode oferecer uma barreira eficiente contra ataques cibernéticos.

Complementarmente, a cooperação intermunicipal pode suprir a falta de recursos técnicos e financeiros, viabilizando a troca de conhecimento e o compartilhamento de soluções (Galante, 2014). Dessa forma, acredita-se que a adoção de um modelo estratégico, focado em medidas realistas e viáveis para a segurança da informação, pode ajudar a superar as limitações enfrentadas pelos pequenos municípios do Vale do São Patrício, tornando-os mais preparados para enfrentar as ameaças digitais e garantir a proteção dos dados e serviços públicos.

A urgência desta pesquisa se fundamenta em uma realidade incontornável: pequenos municípios brasileiros estão cada vez mais expostos a riscos digitais, enquanto dispõem de menos recursos para se proteger. O estudo de Neto (2021) em Mataraca revela o

custo humano por trás das estatísticas - servidores sobrecarregados, serviços essenciais vulneráveis e, principalmente, cidadãos com seus dados pessoais em risco. Quando um sistema municipal é comprometido, não são apenas bits que se perdem, mas a confiança da comunidade em suas instituições.

Optar por soluções adaptáveis não surge apenas por conveniência, mas sim, de uma necessidade ética. As prefeituras desses pequenos municípios não precisam reinventar algo que já existe, mas podem aprender umas com as outras. Os softwares de código aberto, longe de serem "últimas opções", são ferramentas de empoderamento digital, como comprovam os casos bem-sucedidos analisados por Neto (2021).

O presente trabalho se justifica pela junção de três fatores: (1) a obrigação legal imposta pela Lei Geral de Proteção de Dados Pessoais(LGPD), que não faz distinção por porte municipal; (2) o dever ético de proteger dados sensíveis da população; e (3) a oportunidade de construir modelos de segurança que realmente funcionem na escala e na realidade dos municípios pequenos.

O objetivo não é a solução tecnicamente perfeita, mas a socialmente possível, aquela que considera tanto as limitações orçamentárias quanto o potencial transformador da capacitação. Como mostra a experiência de Neto (2021), muitas vezes, são as medidas mais simples, aplicadas com consistência, que geram os impactos mais duradouros na segurança institucional.

## 1.1 OBJETIVOS

### 1.1.1 OBJETIVOS GERAIS

Investigar os desafios relacionados à segurança da informação em pequenos municípios e propor estratégias viáveis para mitigar riscos e garantir a proteção dos dados e sistemas públicos.

### 1.1.2 OBJETIVOS ESPECÍFICOS

1. Diagnosticar o nível de maturidade atual e as práticas de segurança da informação adotadas nas prefeituras de pequenos municípios do Vale do São Patrício.

2. Identificar as principais vulnerabilidades em ambientes digitais nas prefeituras de pequenos municípios.

3. Analisar os impactos da falta de segurança da informação na prestação de serviços públicos.

4. Propor soluções adaptáveis às realidades locais, considerando limitações orçamentárias e técnicas.

# 2 REFERENCIAL TEÓRICO

A aceleração da transformação digital no setor público, intensificada pela necessidade de serviços 24/7 (TCE-GO, 2023), criou uma dependência crítica de sistemas informatizados. Conforme Souza (2020) 78% dos serviços municipais essenciais (saúde, educação, tributos) dependem de plataformas digitais, o que faz surgir um alarme acerca da segurança desses sistemas, principalmente do fator humano. Souza (2020) diz que, por maior que seja a eficiência dos controles de segurança em lidar com as ameaças da internet, o fator humano é de extrema importância para que a empresa alcance um nível de segurança desejável; porém, esse não é o único fator que pode influenciar na segurança de TI.

Este cenário demanda uma análise fundamentada em três pilares:

- **Segurança da informação**: Normas e práticas para proteção de ativos digitais (ISO 27001)
- **Contexto municipal**: Restrições orçamentárias e técnicas de pequenos municípios (Galante, 2014)
- **Conformidade legal**: Exigências da LGPD para órgãos públicos (Art. 46)

Este capítulo estrutura-se progressivamente, partindo dos conceitos gerais de segurança da informação, gestão e governança de TI, criando a base teórica para a análise dos dados coletados.

## 2.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação configura-se como um princípio atemporal, cujos fundamentos remontam às primeiras organizações sistemáticas de dados, mas que adquiriu nova dimensão na era da transformação digital (Neto, 2021). Essa permanência histórica revela-se particularmente relevante no âmbito municipal, onde a proteção dos ativos informacionais públicos demanda uma abordagem interdisciplinar que articula, por um lado, os controles técnicos vindos da Ciência da Computação - como sistemas de criptografia e autenticação - e, por outro, as práticas de gestão documental originárias da Ciência da Informação, incluindo classificação, preservação e controle de acessos (Freund; Karpinski; Macedo, 2022).

(Freund; Karpinski; Macedo, 2022) também traz que a implementação efetiva da segurança da informação é construída sobre princípios fundamentais. (Sêmola, 2003) estabelece a clássica tríade CIA (Confidencialidade, Integridade e Disponibilidade), que forma a base da proteção de dados. Esse conceito é ampliado por (Nakamura; Geus, 2007), que incorpora duas dimensões críticas para o contexto digital atual: Autenticidade (garantia

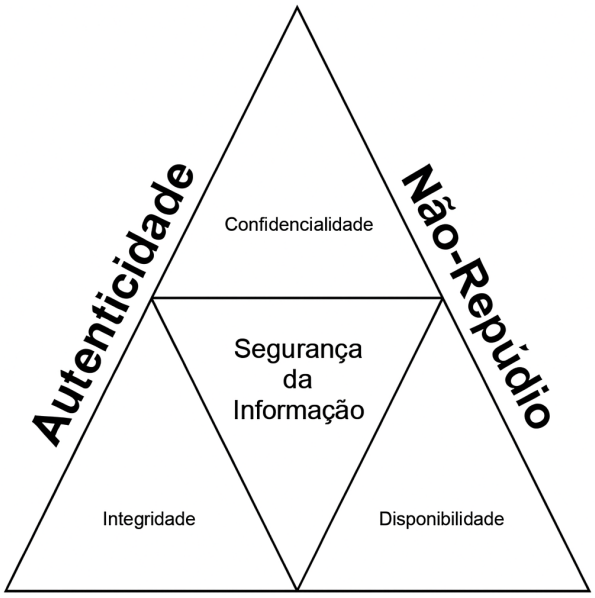


Figura 1 – Pilares de Segurança da Informação

Fonte: Elaboração Própria com base nos conceitos de Nakamura & Geus (2007).

da origem legítima da informação) e Não-repúdio (impossibilidade de negar a autoria de ações digitais).

Para entendermos melhor a importância da segurança da informação, precisamos entender como classificar a importância da informação e sua fundamentalidade para aquela organização. Lyra (2015) introduz que a definição da relevância das informações organizacionais requer uma cuidadosa avaliação dos impactos operacionais e estratégicos que sua perda ou exposição indevida poderiam causar. Esse diagnóstico crítico deve integrar o processo de planejamento estratégico institucional, garantindo que os ativos informacionais recebam níveis de proteção adequados à sua importância para os processos-chave da organização.

Lyra (2008 *apud* Mascarenhas Neto; Araújo, 2019, p. 11-12) também demonstra que a proteção efetiva dos dados organizacionais só se concretiza quando se adota um sistema integrado de medidas que abrange desde políticas e fluxos de trabalho até recursos tecnológicos. Essa abordagem multidimensional requer não apenas a aplicação inicial desses mecanismos, mas um ciclo contínuo de acompanhamento, avaliação e aprimoramento - garantindo assim que tanto as metas operacionais quanto as necessidades de proteção digital da instituição sejam plenamente atendidas.

O volume de ciberataques tem crescido de forma acentuada; o *Security Report* da Check Point Software (2025), por exemplo, reportou um aumento de 44% nos ciberataques globais ano a ano, impulsionado pela maturação de táticas como GenAI e *infostealers*. Paralelamente, o foco na identidade como vetor de ataque intensificou-se; o Microsoft (2024) observa que os seus sistemas enfrentam mais de 600 milhões de ataques de identidade diários, com 99% desses ataques a serem baseados em *passwords*. Em termos de com-

promissos de dados que resultam em violações, o Identity Theft Resource Center (2025) registou 3.158 compromissos nos EUA em 2024. Este número representa um aumento substancial em relação aos 754 compromissos registados em 2018, embora ligeiramente abaixo do recorde de 3.202 estabelecido em 2023. Numa escala global, o Verizon (2025) analisou 22.052 incidentes de segurança, que resultaram em 12.195 violações de dados confirmadas. Notavelmente, o relatório do ano anterior, o Verizon (2024), analisou um número maior de incidentes (30.458) mas menos violações (10.626), sugerindo um aumento significativo na taxa de sucesso (eficiência) dos ataques de um ano para o outro.

No cenário digital contemporâneo, a informação, reconhecida como um ativo de valor inestimável para as organizações, enfrenta um volume crescente de ameaças e ataques cibernéticos que evoluem constantemente em sofisticação e frequência. Essa realidade impõe um desafio contínuo às instituições, que precisam salvaguardar seus dados não apenas contra perdas acidentais ou falhas de sistema, mas também contra as investidas de agentes mal-intencionados. A facilidade com que os atacantes exploram vulnerabilidades, seja por meio de softwares maliciosos, técnicas de engenharia social ou intrusões diretas, sublinha a urgência de uma postura proativa e abrangente na proteção dos ativos informacionais (Nakamura; Geus, 2007).

## 2.2 DESAFIOS ESTRUTURAIS, HUMANOS E POLÍTICOS

Na administração pública contemporânea, a informação transcendeu seu papel tradicional de registro para se consolidar como um ativo estratégico fundamental. É a matéria-prima para o planejamento de políticas públicas, a otimização da prestação de serviços ao cidadão, a garantia da transparência democrática e a base para a transformação digital do Estado (Rezende, 2007). As prefeituras, como entes federativos mais próximos da população, estão no epicentro dessa transformação, gerenciando um volume crescente de dados pessoais e sensíveis, que vão desde prontuários de saúde e registros educacionais até informações tributárias e cadastros sociais (Xavier, 2021). Nesse contexto, a segurança da informação deixa de ser uma preocupação meramente técnica para se tornar um pilar da boa governança e da confiança pública.

### 2.2.1 ESCASSEZ DE RECURSOS ESSENCIAIS

A barreira mais citada e talvez a mais fundamental para a implementação de políticas de segurança robustas é a falta de recursos, tanto financeiros quanto humanos. Em um contexto de restrições orçamentárias crônicas, as administrações municipais frequentemente priorizam despesas mais visíveis e politicamente urgentes, como saúde, educação e infraestrutura urbana, relegando a segurança da informação a um segundo plano (Silva, 2022). Essa limitação financeira tem um impacto direto e paralisante: impede a aquisi-

ção de tecnologias de segurança modernas, a contratação de consultorias especializadas e, crucialmente, a formação e manutenção de equipes técnicas qualificadas.

A falta de pessoal qualificado é um desafio particularmente agudo. O mercado de cibersegurança enfrenta um déficit global de profissionais, e no Brasil, estima-se que a demanda por talentos em tecnologia superará a oferta em mais de 500 mil vagas até 2025 (BRASSCOM, 2021). Para os municípios, especialmente os de menor porte e com menor capacidade de arrecadação, competir por esses talentos com o setor privado, que oferece salários e pacotes de benefícios muito mais atrativos, é uma batalha perdida (Pereira, 2023). A consequência é a existência de equipes de TI subdimensionadas, sobrecarregadas e, muitas vezes, sem o conhecimento específico necessário para lidar com as complexidades da segurança cibernética moderna. Sem profissionais capacitados, a criação, implementação e gestão contínua de uma política de segurança tornam-se tarefas hercúleas, quando não impossíveis. A falta de recursos, portanto, não é apenas uma questão de não poder comprar o "melhor" software; é uma questão de não ter a capacidade humana para planejar, executar e sustentar uma estratégia de segurança coerente (Silva, 2022).

## 2.3 GOVERNANÇA E GESTÃO

Para compreender a dinâmica da TI e SI no setor público, é fundamental estabelecer uma base teórica sólida sobre os conceitos de governança e gestão, tanto em sua acepção mais ampla quanto em suas especificidades tecnológicas.

### 2.3.1 GOVERNANÇA DE TI (GTI)

A GTI constitui um campo especializado da governança corporativa. Sua função é estabelecer estruturas de tomada de decisão e mecanismos de responsabilização que orientem o uso da TI, garantindo que ela contribua efetivamente para o alcance dos objetivos organizacionais e para o atendimento das necessidades das partes interessadas (Figueiredo; Santos; Freitas, 2018). A ABNT NBR ISO/IEC 38500 define a GTI como o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado (Tribunal de Contas do Estado de Pernambuco, 2024).

No setor público brasileiro, a implementação da GTI é motivada por diversos fatores, incluindo os já mencionados altos gastos com TI e a necessidade imperativa de alinhar os projetos de TI com os objetivos estratégicos e os processos de negócio da organização (Figueiredo; Santos; Freitas, 2018). O TCU, em suas análises, tem reiterado que a GTI é crucial para que os investimentos em TI agreguem valor ao negócio e proporcionem benefícios tangíveis na prestação de serviços públicos (Tribunal de Contas do Estado de Pernambuco, 2024).

Os princípios e mecanismos importantes da GTI abrangem:

- **Alinhamento Estratégico:** Um dos pilares da GTI é assegurar que a TI não opere em silos, mas que esteja intrinsecamente alinhada à estratégia geral da organização, adicionando valor ao negócio (Figueiredo; Santos; Freitas, 2018).
- **Otimização de Recursos:** A GTI busca garantir o uso eficiente e eficaz dos recursos de TI, sejam eles financeiros, humanos ou tecnológicos (Figueiredo; Santos; Freitas, 2018).
- **Mitigação de Riscos:** Gerenciar e reduzir os riscos associados aos investimentos e à operação da TI é um objetivo central da GTI, protegendo a organização contra falhas, ataques e perdas (Figueiredo; Santos; Freitas, 2018).
- **Entrega de Valor:** A GTI visa assegurar que a TI não seja apenas um centro de custo, mas que efetivamente contribua para a realização dos objetivos organizacionais e para a entrega de valor aos stakeholders (Figueiredo; Santos; Freitas, 2018).
- **Mecanismos de Liderança e Suporte da Alta Administração:** A responsabilidade pela GTI reside na alta administração e nos executivos. Seu envolvimento direto é crucial para priorizar iniciativas, alocar recursos necessários e garantir a adesão às práticas de governança (Figueiredo; Santos; Freitas, 2018).
- **Comitês de TI e Gestão de Portfólio:** Estruturas formais como comitês de direção de TI são importantes para a tomada de decisões estratégicas sobre projetos, determinação de prioridades, análise de custo-benefício, gestão de riscos e monitoramento de níveis de serviço (Figueiredo; Santos; Freitas, 2018). A gestão de um portfólio de investimentos em TI também é um mecanismo reconhecido para auxiliar nas decisões e no monitoramento das ações de TI (Figueiredo; Santos; Freitas, 2018).

Um estudo empírico sobre o impacto da governança de TI no desempenho organizacional, embora focado em empresas brasileiras, revelou um "efeito de defasagem" significativo. Os benefícios da GTI, especialmente nas medidas de lucratividade como Retorno sobre Ativos (ROA), Retorno sobre o Patrimônio Líquido (ROE) e Margem Líquida, tendem a se intensificar ao longo do tempo, tornando-se mais expressivos à medida que a implementação dos mecanismos de governança amadurece (Lunardi; Becker; Maçada, 2012). Essa observação é crucial para o setor público, onde a complexidade e a burocracia podem até amplificar essa defasagem. A compreensão de que a governança de TI é um processo contínuo de amadurecimento, e não um evento único, é fundamental para evitar a frustração com resultados não imediatos e para sustentar o compromisso de longo prazo com a iniciativa.

### 2.3.2 GESTÃO DE TI

A Gestão de Tecnologia da Informação (Gestão de TI) concentra-se na execução das diretrizes de alto nível estabelecidas pela governança, buscando qualidade, eficácia e eficiência nas operações. A ABNT NBR ISO/IEC 38500 a descreve como o sistema de controles e processos necessários para alcançar os objetivos estratégicos definidos pela liderança da organização (Tribunal de Contas do Estado de Pernambuco, 2024). O papel da Gestão de TI envolve a coordenação de todos os processos relacionados à TI, desde a priorização de atividades e a execução do planejamento até o controle de resultados (Tribunal de Contas do Estado de Pernambuco, 2024). É importante notar que, diferentemente da governança, a gestão pode ser delegada ou terceirizada, desde que haja uma governança adequada para supervisioná-la e garantir a conformidade com as diretrizes estratégicas.

Um exemplo prático da Gestão de TI em ação é a percepção dos gestores do Tribunal Regional Eleitoral de Santa Catarina (TRE/SC). Após a implementação de práticas de governança de TI, os gestores operacionais notaram impactos positivos nos processos de trabalho, resultando em maior eficiência, agilidade e qualidade dos serviços prestados pela área de TI aos usuários (Klumb; Azevedo, 2014).

Apesar dos avanços observados, o caso do TRE/SC também ilustra uma tensão inerente entre a eficiência operacional e a visão estratégica na Gestão de TI. Embora a implementação da governança de TI tenha gerado melhorias tangíveis, os gestores operacionais ainda possuíam uma "visão limitada da governança de TI", muitas vezes restrita aos seus papéis operacionais. Isso indica uma dificuldade em transcender o foco na execução diária para uma compreensão sistêmica e estratégica da "Governança de TI". Foram identificadas "burocratização natural" e falhas de comunicação que, por vezes, afetavam a operação, mesmo com a intenção de melhoria. A eficácia da Gestão de TI no setor público, portanto, não depende apenas da adoção de melhores práticas e frameworks, mas também da capacidade de seus gestores de desenvolver uma mentalidade mais estratégica e de superar barreiras culturais e de comunicação que podem minar a integração entre os níveis tático e operacional e a visão de governança (Klumb; Azevedo, 2014).

### 2.3.3 GESTÃO DE SEGURANÇA DA INFORMAÇÃO (GSI)

A Gestão de Segurança da Informação (GSI) é um componente crítico da gestão de TI e da governança de dados, focada na proteção dos ativos de informação de uma organização contra ameaças internas e externas (Assis, 2011). Seu objetivo primordial é garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações. No setor público, a GSI é impulsionada por um arcabouço normativo robusto e pela necessidade de proteger dados sensíveis dos cidadãos e garantir a continuidade dos serviços públicos digitais (Belli et al., 2024).

A implementação da GSI no setor público é guiada por diversas normas e programas nacionais:

- **Política Nacional de Segurança da Informação (PNSI):** Estabelecida pelo Decreto nº 9.637/2018, visa "assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação em nível nacional" (Carvalho, 2020). Regulando atividades da administração pública federal que envolvem dados.

- **Estratégia Nacional de Cibersegurança (E-Ciber):** Conforme o Decreto nº 10.222/2020, estabelece ações para modificar o posicionamento institucional e individual em relação à cibersegurança, visando tornar o Brasil mais resiliente a ameaças cibernéticas (Carvalho, 2020).

- **Programa de Privacidade e Segurança da Informação (PPSI):** É apresentado por Belli et al. (2024) que a portaria SGD/MGI nº 852/2023 do PPSI, busca aumentar a maturidade e a resiliência em privacidade e segurança da informação nos órgãos da administração pública federal, estabelecendo um "Framework de Privacidade e Segurança da Informação" alinhado à LGPD, PNSI e regulamentações da ANPD.

- **Rede de Gestão de Incidentes Cibernéticos:** O Decreto nº 10.748/2021 regulamenta a obrigação de estabelecer uma equipe para prevenção, tratamento e resposta a incidentes cibernéticos, coordenando essas atividades entre os órgãos federais (Belli et al., 2024).

A GSI também se beneficia da adoção de frameworks internacionais como a família de normas ISO/IEC 27000, que fornece um referencial para Sistemas de Gestão de Segurança da Informação (SGSI) (Belli et al., 2024). A ISO/IEC 27001, em particular, é a norma para certificação de um SGSI e é essencial para a proteção de dados (Instituto Brasileiro de Geografia e Estatística, 2023). O IBGE, por exemplo, baseia sua POSIC em conceitos da ISO/IEC 27000, estabelecendo princípios como pontualidade, aplicabilidade, autenticidade, clareza, conhecimento, confidencialidade, disponibilidade, integridade e privacidade (Assis, 2011).

A Gestão de Segurança da Informação é um dos pilares para uma governança de dados sólida e para a transformação digital no setor público. Ela não se limita a aspectos técnicos, mas envolve a conscientização e o treinamento contínuo dos funcionários para promover comportamentos seguros no ambiente digital (Belli et al., 2024). Além disso Belli et al. (2024) também apresenta que a GSI deve garantir a auditabilidade das medidas de segurança e priorizar ferramentas de código aberto sempre que possível. A eficácia da GSI é crucial para proteger os ativos informacionais, garantir a continuidade dos serviços e manter a confiança dos cidadãos na administração pública.

# 3 MÉTODO

Este capítulo detalha a abordagem científica definida para investigar os desafios de segurança da informação em pequenos municípios do Vale do São Patrício, alinhando-se diretamente aos objetivos estabelecidos na seção de objetivos.

## 3.1 ABORDAGEM E TIPO DE PESQUISA

Como categorizado por Núcleo do Conhecimento (2020), este estudo adota uma abordagem **mista** (quali-quantitativa), combinando métodos qualitativos e quantitativos. Quanto aos seus fins, a pesquisa classifica-se como exploratória-descritiva e aplicada. O caráter exploratório se justifica pela investigação de um tema—desafios de SI em pequenos municípios—que carece de literatura específica adaptada a esse contexto, buscando "proporcionar maior familiaridade com o problema" (Gil, 2008). É descritiva ao mapear o estado atual da segurança, "observando, registrando e analisando" os fatos (Cervo; Bervian; Silva, 2007). Concomitantemente, é uma pesquisa aplicada, pois visa "gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos" (Gil, 2008), o que se materializa na proposta de intervenção.

Quanto aos meios, o delineamento da pesquisa é o estudo de caso múltiplo. Um estudo de caso é definido por Yin (2015) como uma "investigação empírica que investiga um fenômeno contemporâneo em profundidade e em seu contexto de mundo real". Esta abordagem é selecionada como a estratégia metodológica preferencial precisamente porque o fenômeno investigado (Sistemas de Informação) é indissociável de seu contexto (cultura organizacional e orçamento municipal). Esta condição alinha-se perfeitamente à justificativa central de Yin para o método, que é ideal.

Utiliza-se a abordagem de múltiplos casos, analisando quatro municípios. O objetivo desta abordagem não é a generalização estatística, nem a replicação teórica. O propósito é aumentar a robustez e a validade do diagnóstico regional. Ao coletar dados de quatro contextos distintos, em vez de apenas um, a análise agregada resultante torna-se mais confiável e representativa dos desafios comuns e sistêmicos enfrentados pelos pequenos municípios do Vale do São Patrício, diluindo possíveis idiossincrasias de um caso único.

## 3.2 COLETA DE DADOS

A coleta de dados desta pesquisa foi estruturada em múltiplas frentes para permitir a triangulação das informações, combinando dados primários e secundários. As etapas foram divididas em: (1) elaboração e aplicação de questionário; (2) análise documental e (3) levantamento de dados secundários.

### 3.2.1 ELABORAÇÃO E APLICAÇÃO DO QUESTIONÁRIO

O principal instrumento para a coleta de dados primários foi um questionário estruturado, aplicado a gestores e servidores públicos dos municípios participantes.

A elaboração deste instrumento partiu da adaptação de questões já validadas em pesquisas anteriores que abordam temas correlatos, como maturidade em SI, governança e percepção de riscos. Foram utilizados como base principal os construtos e questionários desenvolvidos por Souza (2020) e Rocha (2020).

O processo de desenvolvimento do questionário envolveu a análise dos dois instrumentos que foram anteriormente citados, da qual foram selecionadas apenas as questões mais pertinentes ao presente estudo e aos seus objetivos. Houve também a necessidade de alteração e correção de algumas questões e de suas respectivas opções de resposta. Tal adaptação foi realizada de forma criteriosa, assegurando que o objetivo original de cada questão não fosse comprometido, visando apenas otimizar a interpretação por parte dos respondentes. O questionário desenvolvido, é composto majoritariamente por questões objetivas (fechadas), contendo apenas uma questão discursiva (aberta) para coleta de texto.

Visando maximizar a participação e garantir o conforto dos respondentes, o questionário foi disponibilizado em duas modalidades: um formulário digital (via Google Forms) presente no Apêndice B, e uma versão impressa para aplicação presencial Apêndice A.

Adicionalmente, elaborou-se, em articulação com a Gestão do Instituto Federal Goiano - Campus Ceres, um ofício institucional visando formalizar a apresentação do estudo junto às prefeituras. Este documento teve por finalidade atestar a natureza acadêmica da investigação e solicitar oficialmente a colaboração dos entes municipais, conferindo, assim, maior credibilidade e respaldo institucional à abordagem em campo.

A seleção dos casos para este estudo consistiu em uma amostragem não-probabilística intencional. Os municípios do Vale do São Patrício foram submetidos a um primeiro critério de inclusão: o porte. Foram selecionados 4 (quatro) municípios cuja população fosse inferior a 50 mil habitantes, alinhando-se à estratificação de "pequeno município" adotada pelo IBGE.

Um segundo critério, de conveniência e acessibilidade, foi aplicado para a seleção final. Optou-se pelos municípios que demonstraram maior celeridade e facilidade de contato institucional. Tal decisão metodológica justifica-se pela natureza dos prazos acadêmicos e pela complexidade logística e temporal frequentemente associada à obtenção de autorizações em instituições públicas de maior porte.

Definidos os casos, a aplicação dos questionários foi direcionada aos servidores. A seleção dos participantes também seguiu um filtro intencional: foram convidados a participar apenas servidores cujo ofício dependesse diretamente do uso de computadores e sistemas de informação. A partir deste convite, a participação efetiva ocorreu por adesão

voluntária.

A coleta resultou em um total de 23 respostas válidas. Os dados dos questionários foram analisados de forma agregada, representando o diagnóstico consolidado dos quatro municípios investigados.

Cabe ressaltar que os instrumentos de coleta de dados primários (questionários), foram desenhados para garantir o anonimato total dos respondentes, não havendo, portanto, a identificação da prefeitura de lotação. Por conseguinte, a análise dos dados oriundos dos questionários será realizada de forma agregada. Esta abordagem, embora impeça uma análise comparativa direta entre as gestões municipais, fortalece o diagnóstico dos desafios comuns e sistêmicos enfrentados pelo conjunto de pequenos municípios do Vale do São Patrício, alinhando-se ao objetivo de propor soluções regionais e adaptáveis.

### 3.2.2 ANÁLISE DOCUMENTAL

A segunda frente de coleta de dados primários consistiu na análise documental, focada nos artefatos de gestão e governança de TI e SI. Foram solicitados aos municípios participantes documentos como: Políticas de Segurança da Informação (POSIC) (caso existentes), Planos Diretores de Tecnologia da Informação (PDTI) e outros relatórios ou normativas internas pertinentes ao objeto de estudo.

### 3.2.3 COLETA DE DADOS SECUNDÁRIOS

Por fim, realizou-se um levantamento de dados secundários para contextualizar e complementar os achados primários. Esta etapa centrou-se na coleta de relatórios e diagnósticos públicos do Tribunal de Contas do Estado de Goiás (TCE-GO) e do Instituto Brasileiro de Geografia e Estatística (IBGE), que versam sobre a maturidade em TI, governança e dados demográficos dos municípios do Vale do São Patrício.

## 3.3 ETAPAS DE ANÁLISE

O processamento e a análise dos dados coletados seguirão uma abordagem sistemática, alinhada à natureza exploratório-descritiva e à abordagem mista (quali-quantitativa) desta pesquisa. Conforme preconiza a literatura metodológica, a pesquisa descritiva tem como objetivo primário "observar, registrar, analisar e correlacionar fatos ou fenômenos (variáveis) sem manipulá-los" (Cervo; Bervian; Silva, 2007).

Neste estudo, a análise descritiva visa mapear o estado atual da segurança da informação, caracterizar as vulnerabilidades e compreender as percepções dos envolvidos. Para dar conta da natureza mista dos dados, os procedimentos foram divididos em duas frentes complementares, seguidas de uma síntese triangulada.

1. Os dados primários coletados por meio dos questionários serão processados com base na estatística descritiva. Segundo Gil (2008), esta técnica permite ao pesquisador organizar e sumarizar os dados de modo a facilitar sua interpretação e a obtenção de respostas ao tema investigado. Nesta fase, serão empregadas análises de frequência e distribuição percentual para:

   - Quantificar o perfil dos respondentes;
   - Mapear a percepção agregada sobre riscos e maturidade em SI;
   - Identificar a incidência de práticas de segurança (ou a ausência delas);
   - Mensurar o nível de conhecimento declarado sobre normas e políticas.

   Para a visualização de dados e a elaboração dos gráficos que ilustram essas distribuições, será utilizada a plataforma Google Charts, permitindo uma apresentação clara e objetiva dos achados. O objetivo é gerar um panorama quantificado das percepções e práticas predominantes no conjunto dos municípios analisados.

2. Para os dados secundários e a análise documental (políticas, relatórios, dados do TCE-GO), será empregada a técnica de Análise de Conteúdo. Esta abordagem é definida como um "conjunto de técnicas de análise das comunicações" visando obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitam a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) de conhecimentos (Bardin, 2016).

3. Após o tratamento separado dos dados, as descobertas quantitativas e qualitativas serão trianguladas. A triangulação é uma estratégia metodológica central para o rigor da pesquisa. Originalmente proposta como uma técnica de validação (Denzin, 2009), que opera através do confronto de diferentes fontes de dados, investigadores, teorias ou métodos, a triangulação é igualmente valorizada na pesquisa qualitativa por permitir um aprofundamento da análise. No paradigma específico de pesquisas mistas, esta lógica é essencial, permitindo a complementaridade entre dados quantitativos e qualitativos "palavras e números" visando superar as limitações de uma abordagem metodológica única (Creswell; Clark, 2011).

   Esta síntese analítica culminará nas etapas finais de consolidação, que respondem diretamente aos objetivos da pesquisa.

# 4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Este capítulo dedica-se à apresentação e análise dos dados coletados por meio dos instrumentos descritos no Capítulo 3. Inicialmente, será caracterizado o universo pesquisado e o perfil agregado dos respondentes. Subsequentemente, serão analisados os dados primários (questionários) e secundários (documentais) à luz do referencial teórico, culminando na categorização das vulnerabilidades sistêmicas identificadas na região.

## 4.1 UNIVERSO DA PESQUISA

O campo de investigação deste trabalho está situado na região do Vale do São Patrício, localizada na porção centro-oeste do estado de Goiás. Dita região, embora sua delimitação seja de natureza empírica, isto é, não registrada em documentação oficial, mas consagrada pelo uso em meios de comunicação e pela sociedade local, compreende um universo total de 23 municípios. A amostra desta pesquisa é composta por 4 prefeituras de pequenos municípios pertencentes à referida região. A seleção destas unidades de análise foi intencional e não-probabilística, alinhando-se diretamente aos objetivos da pesquisa, com foco em administrações que se enquadram na definição de pequeno porte. Conforme dados do IBGE, adotou-se como critério de inclusão populações inferiores a 50 mil habitantes. Tal critério de seleção é metodologicamente crucial, visto que a análise das restrições orçamentárias e técnicas constitui um pilar central do estudo. Visando garantir a confidencialidade das informações e o sigilo das instituições participantes, bem como o rigor ético da pesquisa, o questionário aplicado não apresenta questões que possibilitem uma possível identificação do respondente, da mesma forma sua instituição.

### 4.1.1 PERFIL DE ESCOLARIDADE

O perfil da amostra revela um bom nível de instrução formal. Conforme ilustrado na Figura 2, há uma divisão equilibrada entre respondentes com Ensino Superior Completo (34,8%) e Ensino Médio Completo (34,8%).

Somados os que possuem Ensino Superior (completo ou incompleto), tem-se que 52,2% dos servidores da amostra possuem ou estão cursando o nível superior. Este dado é significativo, pois indica um público com alta capacidade de absorção de treinamentos técnicos e de compreensão de políticas normativas.

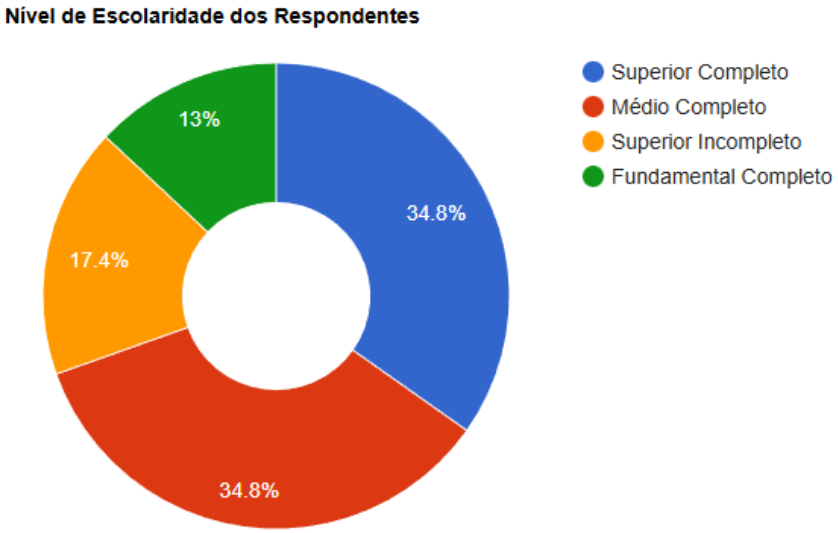


Figura 2 – Nível de Escolaridade dos Respondentes

Fonte: Elaboração Própria.

O perfil sociodemográfico da amostra é composto majoritariamente por respondentes do sexo Feminino (60,9%), contra 39,1% do sexo Masculino. A idade média dos participantes é de 39,0 anos, com o respondente mais jovem tendo 21 anos e o mais experiente 63 anos, indicando que a amostra contempla um vasto espectro de gerações de servidores. A Figura 3 ilustra a distribuição da amostra por faixas etárias.

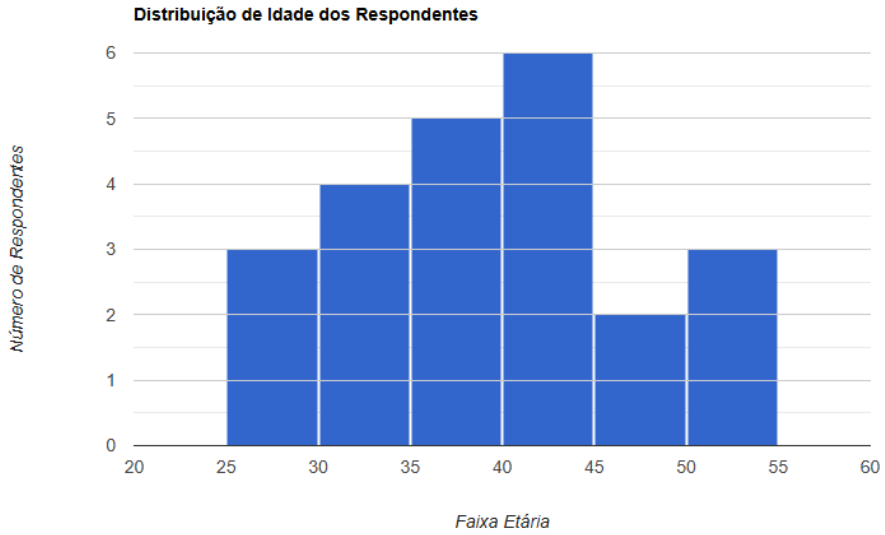


Figura 3 – Distribuição de idade dos Respondentes

Fonte: Elaboração Própria.

A análise da lotação dos respondentes (Figura 4) revela um dado crucial para a validação deste estudo. A maioria da amostra, 52,2% (12), está alocada em setores de Administração e Finanças (incluindo Contabilidade, RH e Coletoria).

Este achado é de alta relevância, pois estes setores manipulam os dados mais críticos e sensíveis da administração municipal (dados tributários, folhas de pagamento, dados de fornecedores). Em seguida, 21,7% (5) compõem um grupo diverso de "Outras Secretarias"(como Educação e Obras), 17,% (4) atuam na Assistência Social (que também lida com dados sensíveis de cidadãos em vulnerabilidade) e 8,7% (2) estão no Controle Interno.

A forte representatividade do núcleo administrativo e financeiro confere um peso significativo às vulnerabilidades que serão identificadas, pois elas partem da percepção dos servidores que operam o "coração" financeiro e de dados dos municípios.

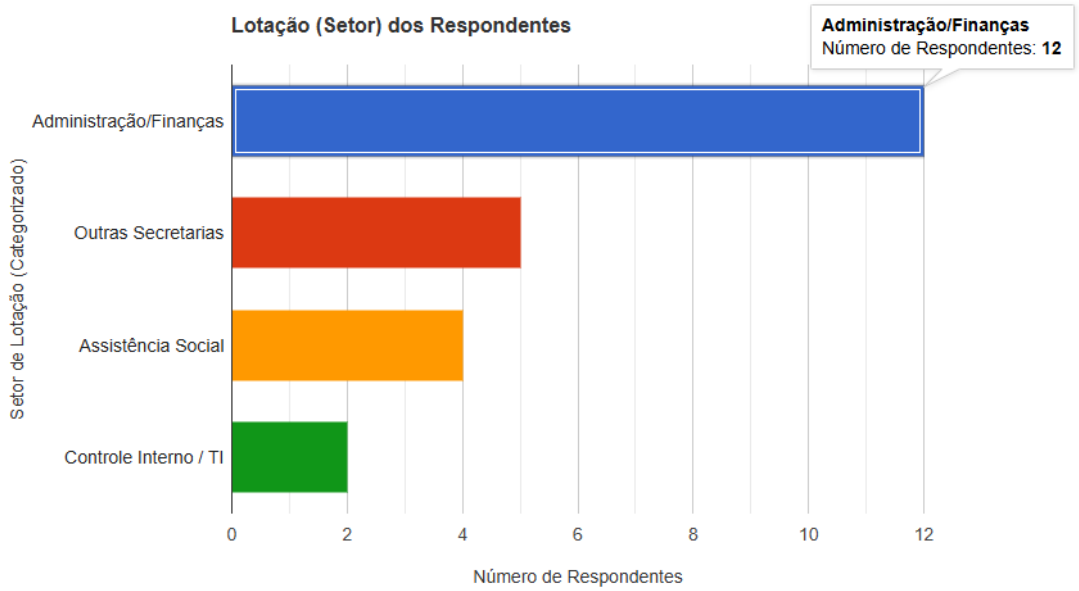


Figura 4 – Distribuição dos Respondentes por Setor

Fonte: Elaboração Própria.

## 4.2 DIAGNÓSTICO DE RISCOS

Iniciando a análise das vulnerabilidades, a primeira etapa consistiu em mapear o nível de conhecimento autodeclarado dos servidores (23) sobre ameaças cibernéticas comuns. Os participantes avaliaram seu conhecimento em uma escala de 1 ("Desconheço totalmente") a 5 ("Conheço totalmente").

Os resultados, apresentados na Figura 5, expõem uma lacuna de conhecimento crítica. A ameaça mais "conhecida" é o *Spam*, com uma nota média de 3.00 (regular). Contudo, ameaças tecnicamente mais perigosas e que exigem maior discernimento do usuário apresentam médias significativamente inferiores, como *Malware* (2.74) e *Trojan* (2.35).

O achado mais alarmante é o desconhecimento sobre *Phishing*, que registrou a menor média de conhecimento: 1.87. Este valor indica que, na média, os servidores "desconhecem totalmente" ou "quase totalmente" a principal forma de ataque de engenharia social, responsável pela vasta maioria dos incidentes de roubo de credenciais e infecções por *ransomware*.

Este dado diagnostica o "ponto cego"central da amostra: os servidores estão minimamente familiarizados com ameaças "passivas" (*Spam*), mas altamente vulneráveis a ameaças "ativas" (*Phishing*) que exigem sua interação. Isso direciona a proposta de intervenção (o Guia Prático) a focar prioritariamente na capacitação para identificação de engenharia social.

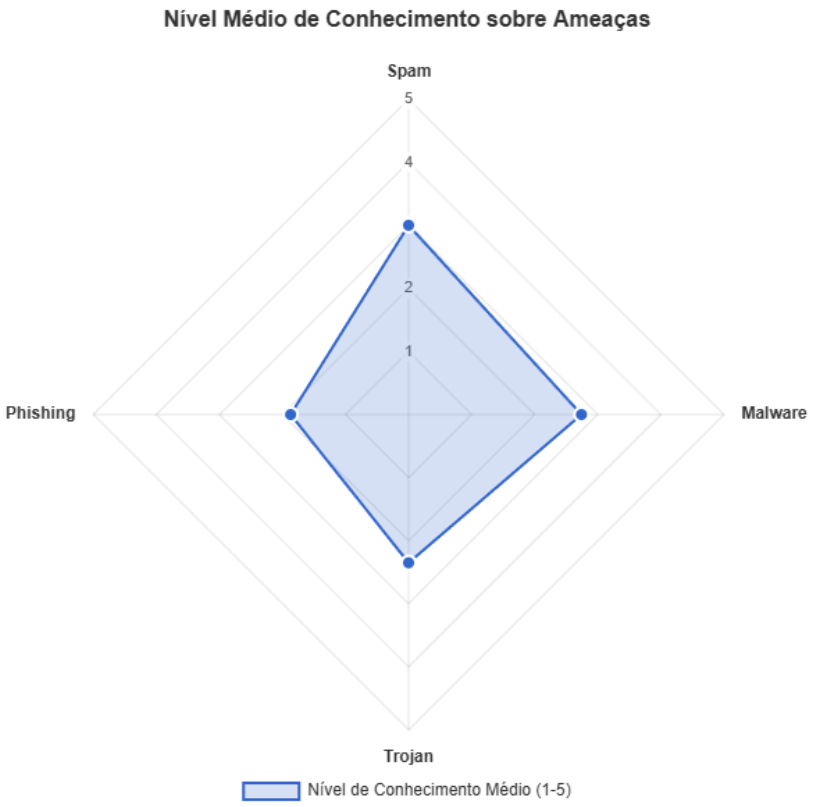


Figura 5 – Conhecimento sobre Ameaças Cibernéticas

Fonte: Elaboração Própria.

### 4.2.1 TREINAMENTO E RISCO COMPORTAMENTAL

A segunda etapa da análise foca em um dos pilares da Segurança da Informação: a capacitação dos usuários. Ao investigar se os servidores já receberam algum tipo de treinamento de conscientização (Questão 13), a pesquisa revela um cenário de vácuo instrucional.

Conforme a Figura 6, dos 23 respondentes, 95,7% (22) afirmaram "não" ter recebido qualquer tipo de treinamento. Apenas 1 (um) respondente (4,3%) afirmou "sim".

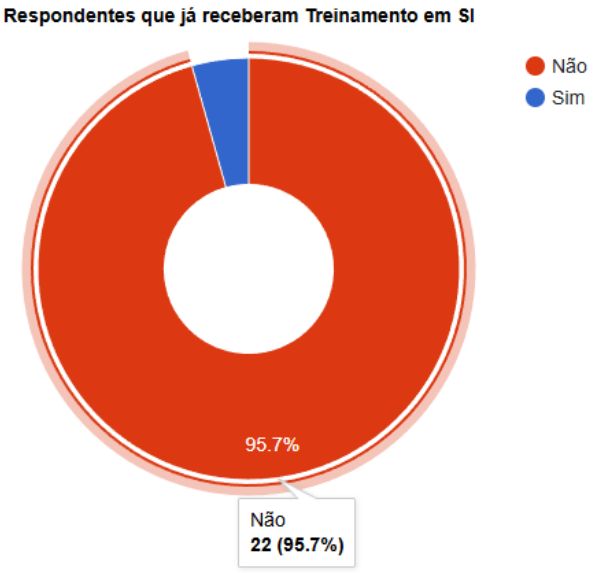


Figura 6 – Quantidade de Servidores que Receberam Treinamento em SI

Fonte: Elaboração Própria.

Esta descoberta é central, pois permite analisar o comportamento de risco (Questão 11: Compartilhamento de Senha) do grupo majoritário (22) que nunca foi treinado. Os resultados (Figura 7) são alarmantes:

- Apenas 54,5% (12 servidores) deste grupo adota a prática segura de "nunca" compartilhar sua senha.
- Os demais 45,5% (10 servidores) admitem compartilhar suas senhas em diferentes frequências: 22,7% "raramente", 13,6% "sempre" e 9,1% "às vezes".

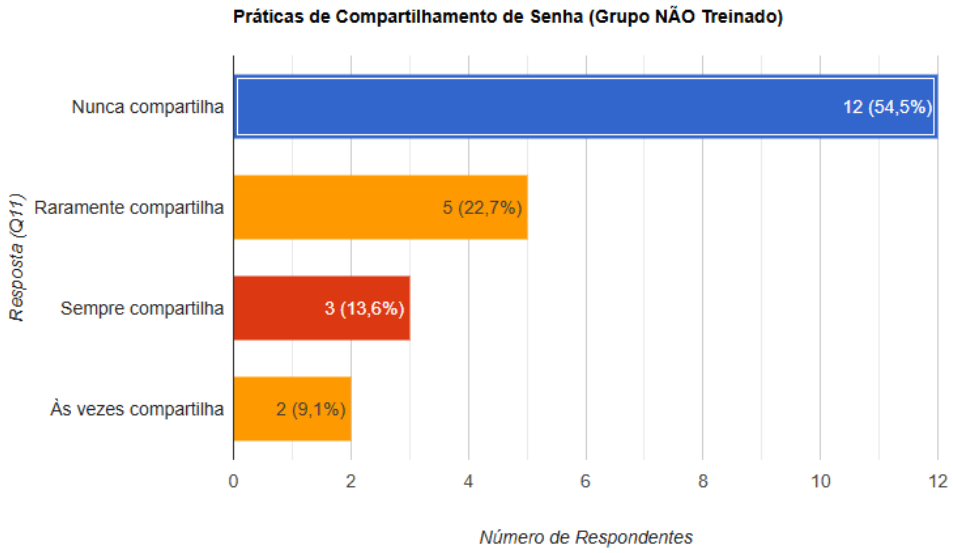


Figura 7 – Práticas de Compartilhamento de Senhas

Fonte: Elaboração Própria.

A análise demonstra uma vulnerabilidade humana e processual crítica: a ausência quase total de treinamento está diretamente associada a um índice elevado (45,5%) de práticas de risco que comprometem a confidencialidade e a autenticidade dos sistemas. O fato de quase metade dos servidores sem treinamento admitir o compartilhamento de senhas, uma violação primária de segurança, expõe as instituições a riscos significativos de acesso não autorizado, fundamentando a urgência da proposta de intervenção deste trabalho.

### 4.2.2 POLÍTICAS E EXPOSIÇÃO AO RISCO

A análise aprofunda-se na relação entre a governança (existência e conhecimento de políticas formais) e o risco técnico (conhecimento de ameaças). Os servidores foram questionados sobre seu nível de conhecimento das políticas de SI existentes na instituição (Questão 14).

Os resultados expõem uma lacuna de governança fundamental: 100% dos respondentes (23) avaliaram seu conhecimento como "médio" (Nota 3) ou "baixo" (Notas 1-2). Nenhum servidor indicou ter "alto" conhecimento (Notas 4-5) das normativas.

A grande maioria, 87% (20), se enquadra no grupo de "Baixo Conhecimento" (Notas 1-2). Apenas 13% (3) avaliaram seu conhecimento como "Médio" (Nota 3). Este dado, por si só, já indica que as políticas de segurança, caso existam, são "documentos de gaveta" e falham em atingir os servidores.

A análise torna-se mais crítica ao cruzar este dado com o conhecimento sobre *Phishing* (Questão 22), a ameaça mais perigosa diagnosticada na seção anterior (Figura 5). O grupo majoritário (20), que admite "Baixo Conhecimento" das políticas, possui uma nota média

de conhecimento em *Phishing* de apenas 1.75. O pequeno grupo (3) com "Conhecimento Médio" das políticas apresenta uma nota média ligeiramente superior (2.67), mas ainda muito baixa.

Conclui-se, portanto, que o desconhecimento generalizado das políticas de SI pode ser diretamente correlacionado a um possível desconhecimento igualmente perigoso da principal ameaça cibernética (*Phishing*). A ausência de uma governança de SI efetiva, que promova ativamente suas normativas, deixa os servidores expostos e sem referencial para identificar ataques, reforçando a vulnerabilidade humana da amostra.

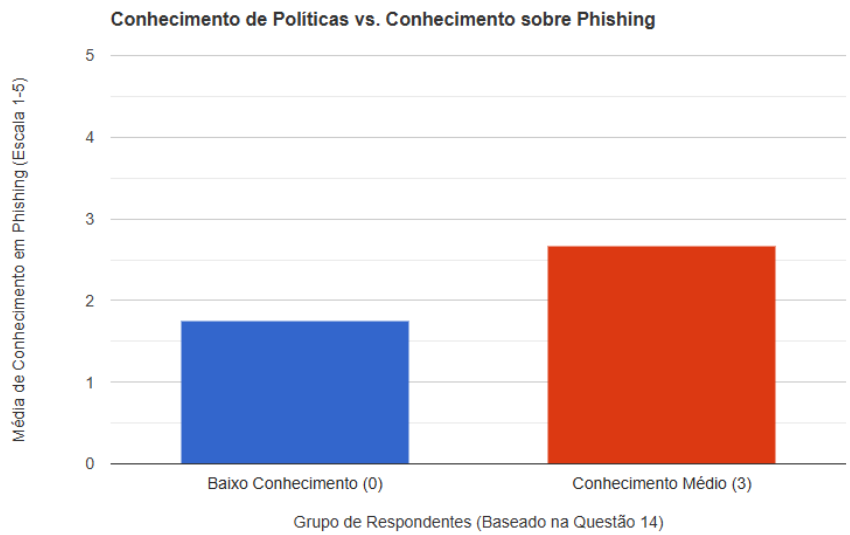


Figura 8 – Conhecimento das Políticas X Conhecimento sobre *Phishing*

Fonte: Elaboração Própria.

### 4.2.3 VÁCUO DE GOVERNANÇA

A análise final das vulnerabilidades investiga a percepção da governança de SI (Questão 15: "Existe Equipe?"), seu controle de continuidade mais crítico (Questão 17: "Existe *Backup*?") e a percepção de impacto (Questão 18: "Qual o prejuízo?"). Os resultados revelam um vácuo de comunicação e uma perigosa desconexão entre a estrutura e a realidade.

O primeiro achado (Figura 9) expõe um vácuo de governança: 47,8% (11) dos servidores afirmaram "não sei" se existe uma equipe formal de SI. Os demais dividem-se igualmente entre "sim" (26,1%) e "não" (26,1%). O fato de quase metade da amostra incluindo servidores de setores críticos como Administração e Finanças, não conseguir identificar se há responsáveis pela SI é, por si só, uma falha grave de gestão.

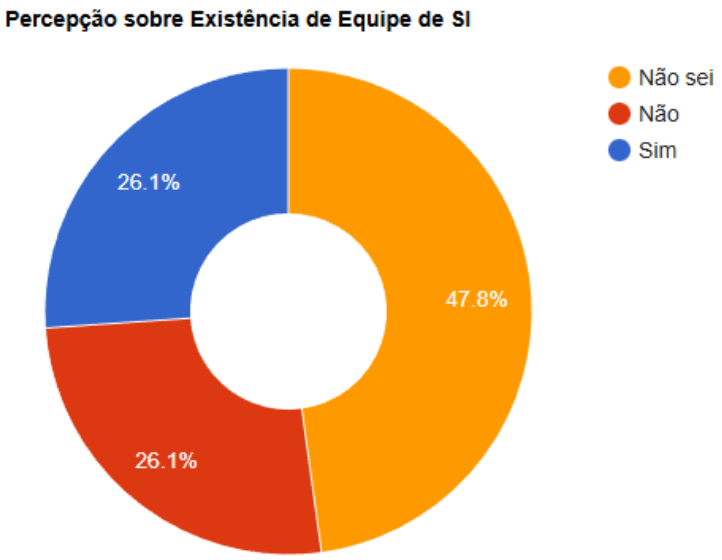


Figura 9 – Percepção da Existência de Equipe de SI

Fonte: Elaboração Própria.

A gravidade deste "vácuo" é confirmada ao analisar o controle de *backup* (Questão 17). A amostra total já demonstra um cenário alarmante: 78,3% (18) afirmaram "não" realizar *backups* setoriais.

O cruzamento (Figura 10) revela o "pior cenário" para um desastre (como um *ransomware*):

1. Grupo "sim" (6): (Servidores que dizem ter uma equipe). Mesmo neste grupo, apenas 50% (3 servidores) afirmam ter *backup*. Os outros 50% dizem "não" ou "não sei".

2. Grupo "não sei" (11): (Servidores "perdidos"). Este grupo é o mais vulnerável. 90,9% deles (10 servidores) afirmam "não" ter *backup*, enquanto 9,1% (1 servidor) dizem "sim".

3. Grupo "não" (6): (Servidores que dizem não ter equipe). Como esperado, 100% deste grupo também afirma "não" ter *backup*.

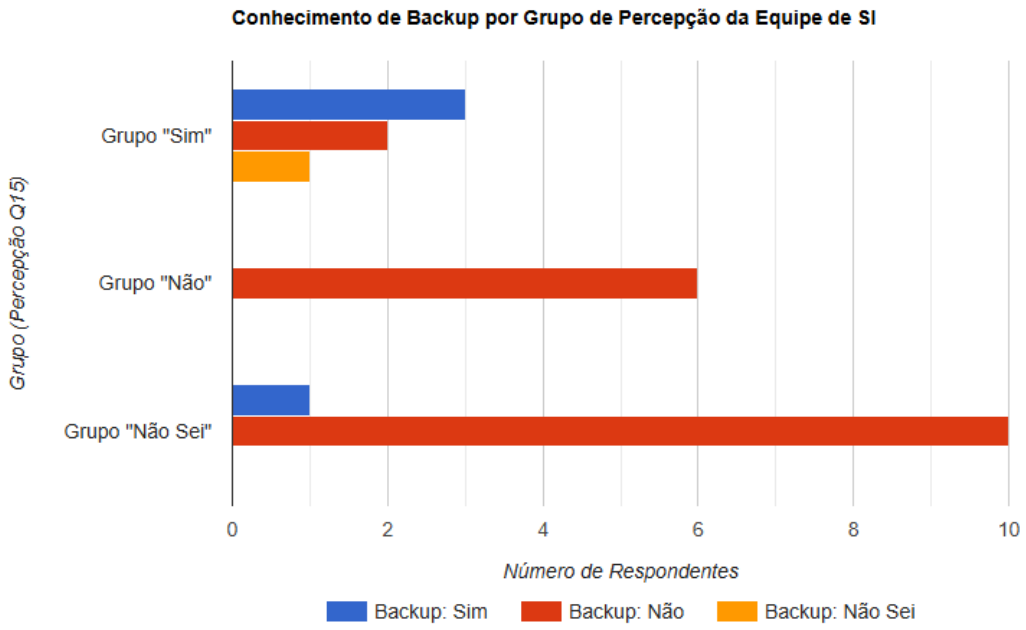


Figura 10 – Conhecimento do *Backup* por Percepção de Existência de Equipe de SI

Fonte: Elaboração Própria.

A análise mostra que mesmo a percepção positiva da existência de uma equipe de SI (Grupo "sim") não garante o conhecimento ou a existência do controle de *backup*.

Finalmente, a análise explora como esse vácuo de governança impacta a percepção de risco (Questão 18). Em um achado surpreendente (Figura 11), o grupo que "não sei" se existe equipe (11) é o que se mostrou menos propenso a classificar o vazamento de dados como "muito prejudicial" (apenas 27,3%). Este grupo demonstrou uma percepção de risco diluída, tendendo a classificar o prejuízo majoritariamente como apenas "prejudicial" (72,7%).

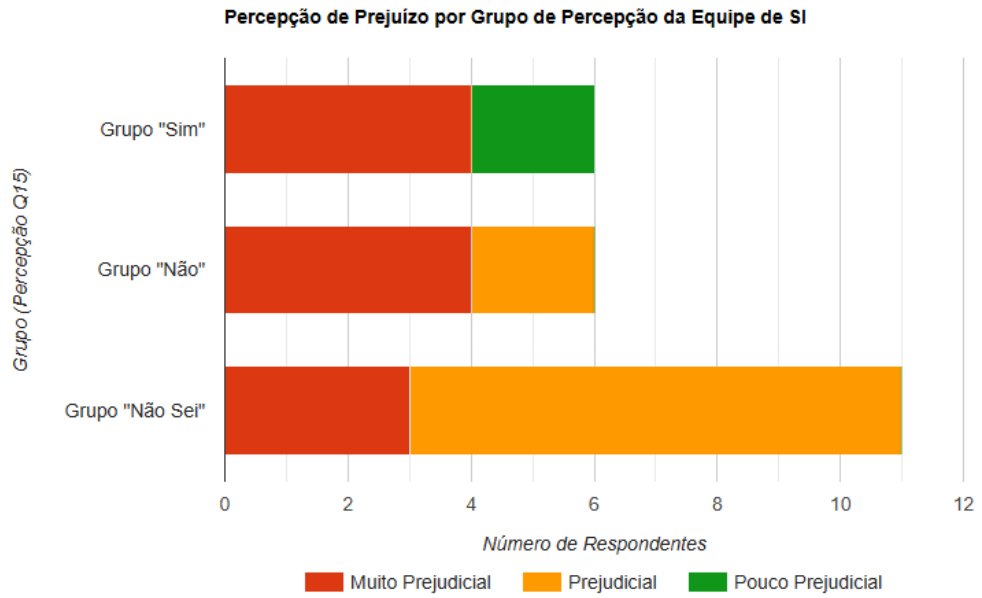


Figura 11 – Percepção de Prejuízo por Percepção de Existência de Equipe de SI

Fonte: Elaboração Própria.

Em contrapartida, os grupos "sim" e "não" (que possuem uma certeza sobre a estrutura, seja ela qual for) foram mais enfáticos, com 66,7% de ambos classificando o risco como "muito prejudicial".

O vácuo de governança (não saber se há equipe) cria uma "falsa sensação de segurança" ou uma diluição da responsabilidade. Servidores que não identificam os responsáveis pela SI são também os que (1) majoritariamente não possuem *backups* e (2) menosprezam o impacto real de um vazamento de dados, criando um ambiente organizacional de alto risco.

## 4.3 ANÁLISE DOCUMENTAL

Conforme delineado na metodologia (Seção 3.2.2), esta etapa da pesquisa buscou realizar a análise documental dos artefatos de governança e gestão, especificamente a POSIC e o Plano Diretor de Tecnologia da Informação (PDTI) dos quatro municípios da amostra.

Contudo, durante o período de coleta de dados, não foi possível obter acesso a estes documentos formais junto às administrações. A dificuldade em localizar e analisar estes artefatos é, em si, um achado relevante da pesquisa, pois corrobora e triangula os dados quantitativos obtidos nos questionários, que já indicavam uma baixa percepção sobre a formalização da governança de SI.

Como visto nas seções anteriores, os dados dos questionários demonstram que:

1. Desconhecimento de Políticas (Questão 14): 100% da amostra indicou ter nível "médio" ou "baixo" de conhecimento sobre as políticas formais (Seção 4.2.2).

2. Ausência de Comunicação (Questão 16): 95,7% dos respondentes afirmaram "não" (43,5%) ou "não sei" (52,2%) sobre a existência de campanhas ou cartilhas de orientação.

Dessa forma, a dificuldade em obter os documentos de POSIC e PDTI para análise alinha-se diretamente à percepção dos servidores. O achado empírico não é que os documentos não existem, mas sim que eles não são instrumentos de conhecimento público ou de fácil acesso dentro da organização.

Conclui-se, portanto, que os instrumentos formais de gestão e controle, mesmo que existam em algum nível burocrático, não estão disseminados na cultura organizacional e falham em atingir o usuário final, o que reforça o diagnóstico de uma governança de SI ainda incipiente nos casos estudados.

# 5 PROPOSTA DE DIRETRIZES: O GUIA PRÁTICO PARA A SI MUNICIPAL

Este capítulo apresenta a etapa final desta pesquisa aplicada: uma proposta de intervenção materializada em um "Guia Prático de Segurança da Informação para Servidores de Pequenos Municípios". A elaboração desta proposta de intervenção atende diretamente ao objetivo específico 4 deste trabalho e justifica-se pela necessidade de fornecer uma solução tangível, de baixo custo e alta aplicabilidade, desenhada especificamente para mitigar as vulnerabilidades críticas diagnosticadas no Capítulo 4.

## 5.1 APRESENTAÇÃO DA PROPOSTA

O Guia Prático proposto é um artefato de Gestão de Segurança da Informação (GSI), concebido para atuar diretamente no elo mais vulnerável identificado na análise: o fator humano.

A análise de dados (Capítulo 4) revelou um cenário de alto risco, caracterizado por:

1. Um vácuo instrucional, onde 95,7% dos servidores jamais receberam treinamento (Seção 4.2.1);

2. Um desconhecimento crítico de ameaças, com a média de conhecimento em *Phishing* atingindo apenas 1.87 (em um total de 5);

3. Um vácuo de governança, onde 95,7% desconhecem cartilhas (Questão 16) e 100% não se sentem confiantes sobre as políticas formais (Questão 14);

4. E uma falha processual grave, onde 78,3% afirmaram não possuir rotinas de *backup* (Questão 17).

   A proposta encontra respaldo no referencial teórico (Capítulo 2), que define a GSI não apenas como um conjunto de controles técnicos, mas como um processo que "envolve a conscientização e o treinamento contínuo dos funcionários para promover comportamentos seguros"(Belli et al., 2024).

   Adicionalmente, a proposta considera a "Escassez Crônica de Recursos Essenciais"(Seção 2.2.1) como premissa de design. O Guia foca em ações de baixo custo, mudanças comportamentais e no uso de ferramentas acessíveis (como soluções de código aberto), alinhando-se aos estudos que defendem a viabilidade de modelos adaptados à realidade de pequenos municípios (Silva, 2022).

   Dessa forma, o Guia atua como a "solução socialmente possível"e tecnicamente viável que este trabalho se propôs a investigar, servindo como o primeiro passo para

a estruturação de uma cultura de segurança da informação no contexto do Vale do São Patrício.

## 5.2 PÚBLICO-ALVO E APLICAÇÃO

O Guia Prático destina-se a todos os servidores que utilizam os recursos de TI da prefeitura, conforme o filtro de seleção desta pesquisa. O foco prioritário de aplicação, contudo, deve ser nos setores que manipulam dados críticos e sensíveis, como os de Administração/Finanças e Assistência Social, que representaram a maioria da amostra (Seção 4.1.1).

A aplicação do Guia não deve se limitar à sua simples distribuição. Para ser efetivo e combater o "vácuo instrucional" (Seção 4.2.1), o artefato deve ser utilizado como ferramenta central em Programas de Conscientização (*Security Awareness Programs*). A literatura em GSI aponta que a eficácia de tais programas depende da repetição e do reforço contínuo (Sêmola, 2003). Sugere-se, portanto, sua adoção formal em:

- Treinamentos de integração de novos servidores;
- Campanhas anuais de reciclagem sobre SI e LGPD;
- Material de consulta rápida disponibilizado na intranet ou pela equipe de TI.

## 5.3 ESTRUTURA DO GUIA PRÁTICO

O Guia foi estruturado em módulos para responder diretamente às vulnerabilidades diagnosticadas no Capítulo 4. Seu conteúdo foca menos na teoria técnica e mais na ação comportamental esperada do servidor. A estrutura básica compreende:

- Módulo 1: Proteção de Acesso (Senhas e Credenciais): Aborda o risco do compartilhamento de senhas e por que usa-las (identificado em 45,5% da amostra não treinada).
- Módulo 2: O Principal Risco (Engenharia Social e *Phishing*): Foco intensivo no "ponto cego" da amostra (média de 1.87), ensinando a identificar e-mails e mensagens fraudulentas.
- Módulo 3: Continuidade (*backups* e *Ransomware*): Responde ao achado de que 78,3% não realizam *backups*, explicando a responsabilidade do usuário e o risco de sequestro de dados.
- Módulo 4: Quem Contatar: Define o canal oficial para reportar incidentes, combatendo o "vácuo de governança" (identificado em 47,8% da amostra).

## 5.4 RESULTADOS ESPERADOS

A adoção e aplicação deste Guia Prático pelas administrações municipais proporciona benefícios diretos e mensuráveis, alinhados às boas práticas de governança de TI:

- Mitigação de Risco Humano: Eleva o nível de conscientização sobre ameaças (*Phishing*) e práticas de risco (compartilhamento de senhas).
- Resiliência Operacional: Fomenta a cultura de *backup*, reduzindo o impacto de desastres, como ataques de *ransomware*.
- Auxílio à Conformidade Legal: Serve como evidência de esforço de capacitação e conscientização, um dos requisitos fundamentais da LGPD.
- Otimização de Recursos: Representa uma solução de baixo custo e alta capilaridade para iniciar uma cultura de segurança, mesmo em cenários de restrição orçamentária.

## 5.5 REFERÊNCIA AO GUIA COMPLETO

O protótipo textual do Guia Prático, contendo o conteúdo integral da intervenção, encontra-se integralmente disponível no Apêndice C deste trabalho.

# 6 CONCLUSÃO E TRABALHOS FUTUROS

O presente Trabalho de Conclusão de Curso propôs-se a investigar os desafios da segurança da informação em pequenos municípios do Vale do São Patrício e, a partir de um diagnóstico empírico, propor estratégias viáveis para mitigar os riscos identificados, considerando as limitações de recursos inerentes a essas administrações.

Pode-se afirmar que o objetivo geral foi plenamente alcançado. Os objetivos específicos 1, 2 e 3 foram satisfeitos através do diagnóstico apresentado no Capítulo 4. A análise (23) revelou um cenário de alta vulnerabilidade, não apenas técnica, mas humana e organizacional. O diagnóstico identificou um "vácuo instrucional" (95,7% dos servidores sem treinamento), um "ponto cego" crítico (média de 1.87 de 5 em conhecimento de *Phishing*) e uma grave falha processual (78,3% sem rotinas de *backup*). Mais criticamente, a pesquisa expôs um "vácuo de governança" onde 47,8% dos servidores desconhecem a existência de uma equipe de SI, e este mesmo grupo demonstrou uma percepção de risco diluída, subestimando o impacto real de um vazamento de dados.

Em resposta direta a este diagnóstico, o objetivo específico 4 foi cumprido através da elaboração do Capítulo 5. Este trabalho não se limitou a diagnosticar, mas propôs um conjunto de soluções de baixo custo, consolidadas no "Protótipo para Elaboração do Guia Prático" (Apêndice C). Estas soluções focadas em comportamento (senhas), identificação de ameaças (*Phishing*), processos (*backup*) e comunicação (governança) representam a "solução socialmente possível" e tecnicamente viável para a realidade investigada.

Reconhece-se, contudo, as limitações deste estudo. A amostra (23), embora significativa para um estudo de caso múltiplo, é não-probabilística e não permite generalização estatística. A análise agregada, necessária pelo anonimato da coleta, impediu uma análise comparativa entre as gestões. Além disso, a análise baseou-se na percepção dos servidores, não em uma auditoria técnica de sistemas. A não obtenção dos documentos (PDTI/POSIC), embora um achado em si, também é uma limitação.

Para trabalhos futuros, sugere-se a elaboração e aplicação prática utilizando o protótipo em um município-piloto e a medição quantitativa de seu impacto na redução de incidentes. Recomenda-se também a replicação deste diagnóstico em outras microrregiões, bem como a realização de estudos que comparem a percepção dos servidores (aqui diagnosticada) com auditorias técnicas formais.

Este trabalho contribui para o campo ao fornecer um raro diagnóstico da realidade da SI em pequenos municípios e ao entregar um artefato prático e instrucional. Este guia pode servir como o primeiro passo para a construção de uma cultura de segurança resiliente e de baixo custo no setor público.

# REFERÊNCIAS


ASSIS, C. B. *Governança e Gestão da Tecnologia da Informação: diferenças na aplicação em empresas brasileiras*. Dissertação (Dissertação (Mestrado em Engenharia de Produção)) — Escola Politécnica, Universidade de São Paulo, São Paulo, 2011. Orientador: Prof. Dr. Fernando José Barbin Laurindo.

BARDIN, L. *Análise de Conteúdo*. São Paulo: Edições 70, 2016.

BELLI, L. et al. *Governança de Dados no Setor Público*: Dados abertos, proteção de dados pessoais e segurança da informação para uma transformação digital sustentável. Rio de Janeiro: Editora Lumen Juris, 2024. ISBN 978-85-519-2992-6.

BRASSCOM. *Demanda de Talentos em TIC e Estratégia TCEM*. São Paulo, 2021. Disponível em: https://files.cercomp.ufg.br/weby/up/1159/o/Brasscom_Estudo_Demanda_de_Talentos_em_TIC_e_Estrat%C3%A9gia_TCEM_2021-2025.pdf.

CARVALHO, L. E. *Governança de TIC no contexto da transformação digital*. Brasília, DF, 2020. (Governança de TIC no Setor Público, Módulo 2). Curso produzido em 2020. Desenvolvimento do curso realizado no âmbito do acordo de Cooperação Técnica FUB/CDT/Laboratório Latitude e Enap.

CERVO, A. L.; BERVIAN, P. A.; SILVA, R. d. *Metodologia científica*. [S.l.]: Pearson Prentice Hall, 2007. 61 p.

Check Point Software. *Check Point Software's 2025 Security Report finds alarming 44% increase in cyber-attacks amid maturing cyber threat ecosystem*. [S.l.], 2025. Disponível em: https://www.globenewswire.com/news-release/2025/01/14/3009378/0/en/Check-Point-Software-s-2025-Security-Report-Finds-Alarming-44-Increase-in-Cyber-Attacks-Amid-Ma html.

CRESWELL, J.; CLARK, V. *Designing and Conducting Mixed Methods Research*. SAGE Publications, 2011. ISBN 9781412975179. Disponível em: https://books.google.com.br/books?id=YcdlPWPJRBcC.

DENZIN, N. *The Research Act: A Theoretical Introduction to Sociological Methods*. AldineTransaction, 2009. (Methodological perspectives). ISBN 9780202362489. Disponível em: https://books.google.com.br/books?id=nWsDswEACAAJ.

FIGUEIREDO, R. M. d. C.; SANTOS, R. R. d.; FREITAS, S. A. A. d. (Ed.). *Governança em Tecnologia de Informação e Comunicação para o Setor Público [recurso eletrônico]*. Brasília, DF: Tribunal de Contas da União, 2018. Publicação resultante das obras produzidas pelos participantes do Curso de Especialização em Governança em Tecnologia de Informação e Comunicação para o Setor Público resultante de uma parceria entre a Universidade de Brasília (UnB) e o Tribunal de Contas da União (TCU). ISBN 978-85-60365-27-2. Disponível em: http://portal.tcu.gov.br/biblioteca-digital/.

FREUND, G. P.; KARPINSKI, C.; MACEDO, D. D. J. d. O contexto histÓrico da produÇÃo cientÍfica sobre seguranÇa da informaÇÃo. *Inf. Inf., Londrina*, v. 27, n. 4, p. 280–302, out./dez. 2022.

GALANTE, T. F. A. *Segurança da Informação e Qualidade dos Sistemas na Prefeitura de Luiziânia-SP: Um Estudo de Caso*. 2014. Trabalho Monográfico - FATEC Americana. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/601/1/20141S_GALANTETalesFranciscoAntonio%20_CD1819.pdf.

GIL, A. *Métodos e técnicas de pesquisa social*. Atlas, 2008. ISBN 9788522451425. Disponível em: https://books.google.com.br/books?id=T3BwPgAACAAJ.

Identity Theft Resource Center. *2024 Data Breach Report*. [S.l.], 2025. Disponível em: https://www.idtheftcenter.org/publication/2024-data-breach-report/.

Instituto Brasileiro de Geografia e Estatística. *Política de Segurança da Informação e Comunicações do IBGE (POSIC)*. Rio de Janeiro, 2023. Aprovada pela Resolução CD/IBGE Nº 33, de 08 de novembro de 2023. Elaborada pelo Comitê de Segurança da Informação e Comunicações (CSI) do IBGE.

KLUMB, R.; AZEVEDO, B. M. d. A percepção dos gestores operacionais sobre os impactos gerados nos processos de trabalho após a implementação das melhores práticas de governança de TI no TRE/SC. *Revista de Administração Pública*, Rio de Janeiro, v. 48, n. 4, p. 961–982, jul./ago. 2014.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G. Um estudo empírico do impacto da governança de TI no desempenho organizacional. *Produção*, v. 22, n. 3, p. 612–624, maio/ago. 2012.

LYRA, M. R. *Segurança e auditoria em sistemas de informação*. Rio de Janeiro: Ciência Moderna, 2008.

LYRA, M. R. (Ed.). *Governança da Segurança da Informação*. 1ª. ed. Brasília: Mauricio Rocha Lyra, 2015. ISBN 978-85-920264-1-7.

Microsoft. *Relatório de defesa digital da Microsoft 2024*. [S.l.], 2024. Disponível em: https://www.microsoft.com/pt-pt/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024.

NAKAMURA, E.; GEUS, P. de. *Segurança de Redes em Ambientes Cooperativos*. Novatec, 2007. ISBN 9788575221365. Disponível em: https://books.google.com.br/books?id=AamSIJuLc34C.

NETO, I. M. R. A importância da segurança da informação em prefeituras. *Universidade Federal da Paraíba*, 2021. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/32336/1/IldefonsoMarcelinoRodriguesNeto_ARTIGO.pdf.

NETO, P. T. M.; ARAúJO, W. J. *Segurança da informação: Uma visão sistêmica para implantação em organizações*. João Pessoa: Editora da UFPB, 2019. 160 p. Recurso digital (14,4MB) formato: ePDF. ISBN 978-85-237-1473-4.

Núcleo do Conhecimento. Tipos de pesquisas científicas. *Revista Científica Multidisciplinar Núcleo do Conhecimento*, v. 5, n. 11, p. 05–15, 11 2020. ISSN: 2448-0959. Disponível em: https://www.nucleodoconhecimento.com.br/wp-content/uploads/2020/11/tipos-de-pesquisas.pdf.

PEREIRA, A. *Cibersegurança no setor público: por que o Brasil está ficando para trás*. 2023. Publicado em: Mundo Conectado. Disponível em: https://mundoconectado.com.br/artigos/ciberseguranca-no-setor-publico-por-que-o-brasil-esta-ficando-para-tras.

REZENDE, D. A. Planejamento de informações públicas municipais: sistemas de informação e de conhecimento, informática e governo eletrônico integrados aos planejamentos das prefeituras e municípios. *Revista de Administração Pública*, v. 41, n. 3, p. 505–536, may 2007. Disponível em: https://doi.org/10.1590/S0034-76122007000300007.

ROCHA, R. M. d. S. *SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO SERVIÇO PÚBLICO MUNICIPAL*. [S.l.], 2020. Orientador: Prof. MSc. José Ivo Fernandes de Oliveira. Defendido em 24 de novembro de 2020. Disponível em: https://gestaopublica.bag.ifmt.edu.br/media/filer_public/75/46/7546e45a-992c-48be-b3cf-f5de01f01526/seguranca_da_informacao_no_ambito_do_servico_publico_municipal.pdf.

SILVA, J. C. d. *Governança de Tecnologia da Informação em Municípios de Pequeno Porte: uma análise dos desafios à transformação digital*. 145 p. Dissertação (Dissertação (Mestrado em Administração Pública)) — Escola Nacional de Administração Pública, Brasília, 2022.

SOUZA, D. C. R. d. *Análise da Segurança da Informação no Setor Público*. Dissertação (Mestrado) — Universidade Federal da Paraíba, 2020. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/20370/1/DiegoChavesReinaldoDeSouza_Dissert.pdf.

SêMOLA, M. *Gestão da segurança da informação: uma visão executiva*. 2. ed. [S.l.]: Elsevier, 2003.

Tribunal de Contas do Estado de Pernambuco. *A diferença entre governança e gestão de TI*. 2024. O ano de publicação (2024) foi inferido a partir da data de copyright/atualização mais recente no rodapé do site, pois uma data específica para este conteúdo não foi encontrada. Disponível em: https://www.tcepe.tc.br/internet/index.php/downloads/430-igovti/igovti-governanca/7123-a-diferenca-entre-governanca-e-gestao-de-ti.

Verizon. *2024 Data Breach Investigations Report*. [S.l.], 2024. Disponível em: https://verizon.com/dbir.

Verizon. *2025 Data Breach Investigations Report*. [S.l.], 2025. Disponível em: https://www.verizon.com/business/resources/Td52/reports/2025-dbir-data-breach-investigations-report.pdf.

XAVIER, F. C. *Recomendações de medidas técnicas e administrativas de segurança da informação para municípios de pequeno porte na jornada de adequação à LGPD*. 2021. ARTIGO, Coordenadoria de Comunicação Social (CCS), Tribunal de Contas do Estado de São Paulo (TCESP). Jornalista responsável: Laércio Bispo MTB 33.444.

YIN, R. *Estudo de Caso - 5.Ed.: Planejamento e Métodos*. Bookman Editora, 2015. ISBN 9788582602324. Disponível em: https://books.google.com.br/books?id=EtOyBQAAQBAJ.

# APÊNDICES

# **APÊNDICE A** – QUESTIONÁRIO FÍSICO

**Questionário**

Convidamos você a participar desta pesquisa acadêmica, desenvolvida como parte do Trabalho de Conclusão de Curso (TCC) de Bacharelado em Sistemas de Informação.

O estudo é intitulado: “Desafios e Estratégias para a Segurança da Informação em Ambientes Digitais do Serviço Público nas Prefeituras de Pequenos Municípios do Vale do São Patrício”. A pesquisa é conduzida pelo discente Carlos Henrique Mota Martins, sob orientação da Profª. MSc. Ramayane Bonacin Braga.

Este instrumento é um questionário breve, composto por 22 questões objetivas relacionadas à área de segurança da informação.

Asseguramos que este formulário não solicita informações privilegiadas da instituição.

Todos os dados coletados serão analisados exclusivamente de forma agregada (em conjunto), impossibilitando qualquer tipo de identificação individual dos participantes ou de suas respectivas instituições.

| Item | Pergunta | Resposta |
|---|---|---|
| 1) | Sexo: | [ ] Masculino<br>[ ] Feminino<br>[ ] Prefiro não dizer |
| 2) | Idade: | _____ |
| 3) | Nível de Escolaridade: | [ ] Analfabeto<br>[ ] Fund. Incompleto<br>[ ] Fund. Completo<br>[ ] Médio Incompleto<br>[ ] Médio Completo<br>[ ] Superior Incompleto<br>[ ] Superior Completo |

| | | |
|---|---|---|
| 4) | Setor/secretaria pertencente: | _____ |
| 5) | Com que frequência você discute assuntos relacionados à segurança da informação? | [ ] Nunca<br>[ ] Às vezes<br>[ ] Sempre<br>[ ] Não tem relevância |
| 6) | Seu computador possui proteção antivírus? | [ ] Sim<br>[ ] Não<br>[ ] Não sei informar |
| 7) | Você executa o antivírus antes de executar algum arquivo presente em alguma mídia removível (pendrives, HD, DVD, CD-ROM)? | [ ] Sim<br>[ ] Não<br>[ ] Às vezes<br>[ ] Não sei informar |
| 8) | O acesso a sites da internet é monitorado/controlado por alguma aplicação/firewall ou setor de TI da organização? | [ ] Sim<br>[ ] Não<br>[ ] Não sei informar |
| 9) | A alteração da senha do computador de trabalho é realizada com frequência ou somente quando o sistema operacional solicita? | [ ] Mudo com frequência por conta própria<br>[ ] Mudo apenas quando o sistema me obriga<br>[ ] Raramente ou nunca mudo minha senha<br>[ ] Não utilizo senha |

| | | |
|---|---|---|
| 10) | A escolha das suas senhas segue alguma política de segurança? | [ ] Sim<br>[ ] Não |
| 11) | Você compartilha sua senha de acesso com terceiros? | [ ] Sempre<br>[ ] Às vezes<br>[ ] Raramente<br>[ ] Nunca |
| 12) | Já ouviu falar sobre sequestro digital de computadores ou de sequestro de dados? | [ ] Sim<br>[ ] Não |
| 13) | Você já recebeu algum tipo de treinamento de conscientização sobre segurança da informação na instituição? | [ ] Sim<br>[ ] Não |
| 14) | **Em uma escala de 1 a 5**, como você conhece as políticas de segurança da informação existentes na instituição? (**Desconheço totalmente** 1 2 3 4 5 **Conheço totalmente**) | _____ |
| 15) | Existe uma área, departamento, unidade ou equipe formal, seja ela, terceirizada ou não, responsável pela segurança da informação na instituição? | [ ] Sim<br>[ ] Não<br>[ ] Não sei |
| 16) | Existe algum tipo de campanha institucional, cartilha ou recomendações sobre segurança da informação na instituição? | [ ] Sim<br>[ ] Não<br>[ ] Não sei |
| 17) | É realizado algum procedimento de backup dos dados pertencentes ao setor? | [ ] Sim<br>[ ] Não<br>[ ] Não Sei |
| 18) | Como você classifica ser prejudicial a perda ou vazamento das informações para sua instituição? | [ ] Não causa prejuízo<br>[ ] Prejudicial<br>[ ] Pouco prejudicial<br>[ ] Muito prejudicial |

| | | |
|---|---|---|
| 19) | **Em uma escala de 1 a 5,** quanto você tem conhecimento do que se trata um **Spam** ?<br>(**Desconheço totalmente** 1 2 3 4 5 **Conheço totalmente**) | _____ |
| 20) | **Em uma escala de 1 a 5,** quanto você tem conhecimento do que se trata um **Trojan** ?<br>(**Desconheço totalmente** 1 2 3 4 5 **Conheço totalmente**) | _____ |
| 21) | **Em uma escala de 1 a 5,** quanto você tem conhecimento do que se trata um **Malware**?<br>(**Desconheço totalmente** 1 2 3 4 5 **Conheço totalmente**) | _____ |
| 22) | **Em uma escala de 1 a 5,** quanto você tem conhecimento do que se trata **Phishing**?<br>(**Desconheço totalmente** 1 2 3 4 5 **Conheço totalmente**) | _____ |



**SEGURANÇA DA INFORMAÇÃO NO ÂMBITO DO SERVIÇO PÚBLICO MUNICIPAL**

Robson Moreira da Silva Rocha [1]

Orientador: Prof. MSc, José Ivo Fernandes de Oliveira

e

**SEGURANÇA DA INFORMAÇÃO: UMA METODOLOGIA PARA IMPLANTAÇÃO DE UM SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO**

DIEGO CHAVES REINALDO DE SOUZA [1]

Orientador: Prof. Dr. Mariano Castro Neto

# **APÊNDICE B** – QUESTIONÁRIO NA VERSÃO ONLINE (FORMULÁRIOS GOOGLE)

# Questionário

Prezado(a) Colaborador(a),

Convidamos você a participar desta pesquisa acadêmica, desenvolvida como parte do Trabalho de Conclusão de Curso (TCC) de Bacharelado em Sistemas de Informação.

O estudo é intitulado: “Desafios e Estratégias para a Segurança da Informação em Ambientes Digitais do Serviço Público nas Prefeituras de Pequenos Municípios do Vale do São Patrício”. A pesquisa é conduzida pelo discente Carlos Henrique Mota Martins, sob orientação da Profª. MSc. Ramayane Bonacin Braga.

**Garantia de Anonimato e Confidencialidade**

Este instrumento é um questionário breve, composto por 22 questões objetivas relacionadas à área de segurança da informação.

Asseguramos que este formulário **não solicita** informações privilegiadas da instituição.

**Todos os dados coletados serão analisados exclusivamente de forma agregada (em conjunto)**, impossibilitando qualquer tipo de identificação individual dos participantes ou de suas respectivas instituições.

**Objetivo e Importância**

Sua resposta é de suma importância para diagnosticar os desafios atuais e contribuir para o aprimoramento da segurança digital dos servidores, da sua instituição e, consequentemente, dos cidadãos.

Agradecemos desde já sua valiosa colaboração.
Contato para retirada das dúvidas:
carlos.mota1@estudante.ifgoiano.edu.br



* Indica uma pergunta obrigatória

1. Sexo: *

   *Marcar apenas uma oval.*

   - ◯ Masculino
   - ◯ Feminino
   - ◯ Prefiro não dizer

2. Idade *

   _____

3. Nível de Escolaridade? *

   *Marcar apenas uma oval.*

   - ◯ Analfabeto
   - ◯ Fund. Incompleto
   - ◯ Fund. Completo
   - ◯ Médio Incompleto
   - ◯ Médio Completo
   - ◯ Superior Incompleto
   - ◯ Superior Completo

4. Setor/Secretaria pertencente? *

   _____

5. Com que frequência você discute assuntos relacionados à segurança da informação? *

*Marcar apenas uma oval.*

- ◯ Nunca
- ◯ Às vezes
- ◯ Sempre
- ◯ Não tem relevância

6. Seu computador possui proteção antivírus? *

*Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Não sei informar

7. Você executa o antivírus antes de executar algum arquivo presente em alguma mídia removível (pendrives, HD, DVD, CD-ROM)? *

*Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Às vezes
- ◯ Não sei informar

8. O acesso a sites da internet é monitorado/controlado por alguma aplicação/firewall ou setor de TI da organização? *

*Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Não sei informar

9. A alteração da senha do computador de trabalho é realizada com frequência ou somente quando o sistema operacional solicita? *

*Marcar apenas uma oval.*

- ◯ Mudo com frequência por conta própria
- ◯ Mudo apenas quando o sistema me obriga
- ◯ Raramente ou nunca mudo minha senha
- ◯ Não utilizo senha

10. A escolha das suas senhas segue alguma política de segurança? *

*Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não

11. Você compartilha sua senha de acesso com terceiros? *

*Marcar apenas uma oval.*

- ◯ Sempre
- ◯ Às vezes
- ◯ Raramente
- ◯ Nunca

12. Já ouviu falar sobre sequestro digital de computadores ou de sequestro de dados? *

*Marcar apenas uma oval.*

- Sim
- Não

13. Você já recebeu algum tipo de treinamento de conscientização sobre segurança da informação na instituição? *

*Marcar apenas uma oval.*

- Sim
- Não

14. **Em uma escala de 1 a 5**, como você conhece as políticas de segurança da informação existentes na instituição? *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Des | ◯ | ◯ | ◯ | ◯ | ◯ | Conheço totalmente |

15. Existe uma área, departamento, unidade ou equipe formal, seja ela, terceirizada ou não, responsável pela segurança da informação na instituição? *

*Marcar apenas uma oval.*

- Sim
- Não
- Não sei

16. Existe algum tipo de campanha institucional, cartilha ou recomendações sobre segurança da informação na instituição? *

*Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Não sei

17. É realizado algum procedimento de backup dos dados pertencentes ao setor? *

*Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não
- ◯ Não sei

18. Como você classifica ser prejudicial a perda ou vazamento das informações para sua instituição? *

*Marcar apenas uma oval.*

- ◯ Não causa prejuízo
- ◯ Prejudicial
- ◯ Pouco prejudicial
- ◯ Muito prejudicial

Sobre ataques cibernéticos:

Assinale em uma escala de 1 a 5 o quanto você conhece os ataques abaixo.

19. **Em uma escala de 1 a 5**, quanto você tem conhecimento do que se trata um **Spam ?** *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Des | ◯ | ◯ | ◯ | ◯ | ◯ | Conheço totalmente |

20. **Em uma escala de 1 a 5**, quanto você tem conhecimento do que se trata um **Trojan ?** *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Des | ◯ | ◯ | ◯ | ◯ | ◯ | Conheço totalmente |

21. **Em uma escala de 1 a 5**, quanto você tem conhecimento do que se trata um **Malware ?** *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Des | ◯ | ◯ | ◯ | ◯ | ◯ | Conheço totalmente |

22. **Em uma escala de 1 a 5**, quanto você tem conhecimento do que se trata **Phishing** *

*Marcar apenas uma oval.*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Des | ◯ | ◯ | ◯ | ◯ | ◯ | Conheço totalmente |

# APÊNDICE C – PROTÓTIPO PARA ELABORAÇÃO DO GUIA PRÁTICO

MÓDULO 1: PROTEÇÃO DE ACESSO

**Título: Sua Senha é a Porta de Entrada da Prefeitura**

A Importância da Senha de Login: O login do seu computador (Windows + L) é a "porta da frente" digital da Prefeitura. Sem uma senha, qualquer pessoa que entre na sua sala (um visitante, um colega mal-intencionado) pode aceder a todos os dados do seu computador, ler e-mails e aceder aos sistemas financeiros ou de cadastro em seu nome.

**O Risco Real: O Tempo de um Ataque**

Uma senha fraca é um convite ao hacker.

- Uma senha como **prefeitura** ou **123456** é descoberta por um hacker em menos de 1 segundo.
- Uma senha como **Prefeitura@2025** (8 caracteres com maiúscula e símbolos) é forte, mas pode ser descoberta em **poucas horas** ou **dias**.
- Uma frase-senha como **MeuCachorroBobAdoraPassear!24** pode levar **milhares de anos** para ser quebrada.

**O QUE FAZER (Checklist):**

1. **NUNCA** compartilhe sua senha.
2. **BLOQUEIE** seu computador sempre que se levantar da mesa (Pressione Windows + L).
3. **CRIE** frases-senha longas com letras, números e caracteres especiais, em vez de senhas curtas e complexas.

   **NÃO CONSIGO LEMBRAR DE TUDO!**

   Se você tem dificuldade em memorizar muitas senhas fortes, não as anote em papéis (post-its). Utilize um **Gerenciador de Senhas**. Ferramentas como o **BitWarden** são gratuitas, de código aberto e funcionam como um "cofre digital" seguro para todas as suas senhas.

MÓDULO 2: O RISCO Nº 1 (ENGENHARIA SOCIAL)

**Título: Não morda a isca! O Perigo da Manipulação**

O que é Engenharia Social? É a arte de manipular pessoas para obter informações confidenciais. O criminoso não ataca o computador, ele ataca o funcionário, explorando a confiança ou o medo.

Este ataque pode vir de três formas:

1. *Phishing* (E-mail): É a "pescaria" digital. O golpista envia um e-mail falso (a "isca") fingindo ser uma autoridade (banco, governo, Receita Federal) para enganá-lo e fazer com que você clique no link ou baixe o anexo. O objetivo é roubar sua senha ou instalar um vírus.

2. *Vishing* (Voz): O golpe vem por uma ligação telefônica. O golpista finge ser do banco, do suporte de TI ou de um tribunal, pedindo que você "confirme" sua senha ou dados pessoais. Desligue imediatamente. Nenhuma instituição legítima pede sua senha por telefone.

3. *Smishing* (SMS/WhatsApp): O golpe vem por mensagem de texto. ("Parabéns, você ganhou um prêmio, clique aqui!" ou "Seu CPF foi negativado, regularize agora: [link malicioso]"). Não clique.

**COMO IDENTIFICAR UM E-MAIL FALSO:**

**O Remetente é Estranho?** Cuidado com e-mails "oficiais" vindos de domínios públicos (Ex: ReceitaFederal@gmail.com).

**O Tom é de Urgência?** Frases como "Sua conta será bloqueada em 24h" ou "Você recebeu uma intimação" são táticas para fazer você clicar sem pensar.

**O Link é Suspeito?** Passe o mouse em cima do link **(NÃO CLIQUE!)**. Olhe no canto inferior da tela. O endereço que aparece é estranho? (Ex: O texto diz www.banco.com.br, mas o link mostra www.cliqueseguro.xyz).

MÓDULO 3: SEUS ARQUIVOS (BACKUP E *RANSOMWARE*)

**Título: E se tudo sumir? A Defesa contra Sequestro de Dados**

O que é Ransomware? *Ransomware* (de "Ransom" = Resgate) é um vírus que "sequestra" seus arquivos. Ele entra no seu computador (geralmente por um *Phishing*) e criptografa (tranca) tudo: planilhas, documentos do Word, PDFs. Os criminosos então

exigem um resgate (geralmente em criptomoeda) para lhe dar a "chave". A única defesa 100% eficaz contra isso é o Backup.

**RESPONSABILIDADE DO SERVIDOR: ONDE SALVAR?**

- **ERRADO:** Salvar arquivos importantes apenas na sua "Área de Trabalho (Desktop)" ou na pasta "Meus Documentos".
- **CERTO:** Salvar **SEMPRE** todos os arquivos de trabalho no **SERVIDOR DE REDE** (a pasta G:, Z: ou S:, etc.).

**Por quê?** A equipe de TI só consegue fazer o backup automático dos arquivos que estão no SERVIDOR. Se seus arquivos estiverem apenas na "Área de Trabalho", eles serão perdidos em um ataque de ransomware ou se o computador quebrar.

**Sugestões de Baixo Custo para Backups (Direcionado à Gestão/TI):**

Para mitigar o risco de ausência de backup, a Gestão de TI pode:

- **Implementar a Regra 3-2-1:** Tenha 3 cópias dos dados, em 2 mídias diferentes, com 1 cópia fora do local (offline ou em nuvem).
- **Usar a Nuvem:** Plataformas em nuvem (Google Drive, OneDrive, etc.) garantem que os dados estarão seguros mesmo em caso de desastre físico (incêndio, inundação) na sede da prefeitura.
- **Usar Ferramentas Open Source:** Soluções como **Bacula** ou **rsync** podem ser usadas para automatizar backups de servidores sem custo de licença.

MÓDULO 4: QUEM CONTATAR

**Título: Viu algo estranho? Chame ajuda!**

A sua melhor defesa é a desconfiança. Se você receber um e-mail estranho ou seu computador apresentar um comportamento esquisito, não tente resolver sozinho e não o ignore.

**NA DÚVIDA, PARE!**

- **NÃO** delete o e-mail suspeito (a TI pode precisar analisá-lo).
- **NÃO** encaminhe o e-mail para seus colegas (você pode estar espalhando o vírus).
- **NÃO** tenha vergonha de perguntar. É melhor perguntar sobre um e-mail legítimo do que clicar em um vírus.